

Management Software

AT-S63

Web Browser Interface User's Guide

AT-9400 Series Layer 2+ Gigabit Ethernet Switches

Version 1.1.0

Copyright © 2005 Allied Telesyn, Inc.

All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesyn, Inc. 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 Telesyn, 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 Telesyn, 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 Telesyn, Inc. has been advised of, known, or should have known, the possibility of such damages.

Contents

Preface	17
Where to Find Web-based Guides	18
Contacting Allied Telesyn	19
Online Support	19
Email and Telephone Support.....	19
Returning Products	19
Sales or Corporate Information	19
Management Software Updates.....	19
Chapter 1: Overview	21
Management Overview.....	22
Local Connection.....	24
Remote Connection.....	25
Using an SNMP Network Management Application.....	25
Management Access Levels.....	27
Online Help.....	28
Section I: Basic Operations	29
Chapter 2: Starting a Web Browser Management Session	31
Establishing a Remote Connection to Use the Web Browser Interface	32
Web Browser Tools	36
Saving Your Parameter Changes.....	37
Quitting a Web Browser Management Session.....	38
Chapter 3: Basic Switch Parameters	39
Configuring an IP Address and Switch Name	40
Activating the BOOTP and DHCP Client Software.....	43
Displaying System Information.....	44
Configuring the Manager and Operator Passwords	46
Rebooting a Switch.....	48
Pinging a Remote System.....	49
Returning the AT-S63 Management Software to the Factory Default Values	51
Chapter 4: SNMPv1 and SNMPv2c	53
Enabling or Disabling SNMP Management	54
Creating a New SNMPv1 and SNMPv2c Community	56
Modifying an SNMPv1 and SNMPv2c Community.....	59
Deleting an SNMPv1 and SNMPv2c Community	62
Displaying the SNMPv1 and SNMPv2c Communities.....	63
Chapter 5: Enhanced Stacking	67
Setting a Switch's Enhanced Stacking Status	68
Selecting a Switch in an Enhanced Stack	71
Returning to the Master Switch	74
Displaying the Enhanced Stacking Status.....	75

Chapter 6: Port Parameters	77
Configuring Port Parameters	78
Displaying Port Status.....	85
Displaying Port Statistics	89
Resetting a Port to the Default Settings	92
Chapter 7: Port Trunking	93
Creating a Port Trunk.....	94
Modifying a Port Trunk.....	97
Deleting a Port Trunk	99
Displaying the Port Trunks	100
Chapter 8: Port Mirroring	103
Creating a Port Mirror	104
Modifying a Port Mirror.....	107
Disabling a Port Mirror	108
Deleting a Port Mirror	109
Displaying the Port Mirror	110
Section II: Advanced Operations	113
Chapter 9: File System	115
Listing the Files in Flash Memory	116
Listing Files on the Compact Flash Card	118
Chapter 10: File Downloads and Uploads	121
Downloading a File	122
Uploading a File	125
Chapter 11: Event Log	127
Working with the Event Log	128
Enabling or Disabling the Event Log	128
Displaying Events	130
Disabling the Event Log.....	136
Clearing the Event Log	136
Saving the Event Log to a File.....	136
Working with Log Outputs	138
Configuring a Log Output Definition	138
Viewing a Log Output Definition	140
Modifying a Log Output Definition	142
Deleting a Log Output Definition.....	144
Chapter 12: Classifiers	145
Configuring a Classifier.....	146
Modifying a Classifier	149
Deleting a Classifier	151
Displaying the Classifiers.....	152
Chapter 13: Access Control Lists	155
Configuring an Access Control List.....	156
Modifying an Access Control List.....	158
Displaying the Access Control Lists	160
Chapter 14: Denial of Service Defense	163
Configuring Denial of Service Defense	164
Displaying the DoS Settings	167
Chapter 15: Quality of Service	169

Managing Flow Groups	170
Configuring Flow Groups	170
Modifying a Flow Group	172
Deleting a Flow Group	173
Displaying Flow Groups	173
Managing Traffic Classes	176
Configuring Traffic Classes	176
Modifying a Traffic Class	178
Deleting a Traffic Class	180
Displaying the Traffic Classes	180
Managing Policies	184
Configuring a Policy	184
Modifying a Policy	186
Deleting a Policy	188
Displaying Policies	188
Chapter 16: Class of Service	191
Configuring CoS	192
Mapping CoS Priorities to Egress Queues	195
Configuring Egress Scheduling	198
Displaying the CoS Settings	200
Displaying the QoS Schedule	202
Chapter 17: IGMP Snooping	203
Configuring IGMP Snooping	204
Displaying a List of Host Nodes	207
Displaying a List of Multicast Routers	210
Section III: SNMPv3	213
Chapter 18: SNMPv3	215
Configuring the SNMPv3 Protocol	216
Enabling or Disabling SNMP Management	217
Configuring the SNMPv3 User Table	220
Creating a User Table Entry	220
Deleting a User Table Entry	223
Modifying a User Table Entry	224
Configuring the SNMPv3 View Table	228
Creating a View Table Entry	228
Deleting a View Table Entry	231
Modifying a View Table Entry	231
Configuring the SNMPv3 Access Table	234
Creating an Access Table	234
Deleting an Access Table Entry	237
Modifying an Access Table Entry	238
Configuring the SNMPv3 SecurityToGroup Table	241
Creating a SecurityToGroup Table Entry	241
Deleting a SecurityToGroup Table Entry	244
Modifying a SecurityToGroup Table Entry	244
Configuring the SNMPv3 Notify Table	247
Creating a Notify Table Entry	247
Deleting a Notify Table Entry	249
Modifying a Notify Table Entry	250
Configuring the SNMPv3 Target Address Table	252
Creating a Target Address Table Entry	252
Deleting a Target Address Table Entry	255

Modifying Target Address Table Entry	256
Configuring the SNMPv3 Target Parameters Table.....	259
Creating a Target Parameters Table Entry.....	259
Deleting a Target Parameters Table Entry	262
Modifying a Target Parameters Table Entry	263
Configuring the SNMPv3 Community Table	266
Creating an SNMPv3 Community Table Entry	266
Deleting an SNMPv3 Community Table Entry.....	269
Modifying an SNMPv3 Community Table Entry	269
Displaying SNMPv3 Tables	272
Displaying User Table Entries	272
Displaying View Table Entries	274
Displaying Access Table Entries	275
Displaying SecurityToGroup Table Entries.....	276
Displaying Notify Table Entries.....	277
Displaying Target Address Table Entries	278
Displaying Target Parameters Table Entries	279
Displaying SNMPv3 Community Table Entries	280

Section IV: Spanning Tree Protocols 283

Chapter 19: STP and RSTP	285
Enabling or Disabling a Spanning Tree Protocol	286
Configuring STP.....	288
Displaying the STP Settings	292
Resetting STP to the Default Settings	295
Configuring RSTP	296
Resetting RSTP to the Default Settings	300
Displaying RSTP Settings	300
Chapter 20: MSTP	303
Enabling MSTP	304
Configuring MSTP.....	306
Configuring MSTP Parameters.....	306
Configuring the CIST Priority.....	309
Creating, Deleting, or Modifying MSTI IDs.....	310
Creating an MSTI ID	310
Deleting an MSTI ID	311
Modifying an MSTI ID	311
Adding, Removing, or Modifying VLAN Associations to MSTIs	314
Adding a VLAN Association.....	314
Removing a VLAN Association.....	314
Modifying a VLAN Association	315
Configuring MSTP Port Parameters	317
Displaying the MSTP Port Configuration	319
Displaying the MSTP Port Status.....	322
Resetting MSTP to the Default Settings	324

Section V: Virtual LANs 325

Chapter 21: Virtual LANs	327
Creating a New Port-Based or Tagged VLAN	328
Modifying a VLAN	332
Deleting a VLAN	334
Selecting a VLAN Mode.....	335

Displaying VLANs	337
Specifying a Management VLAN.....	339
Chapter 22: Protected Ports VLANs	341
Creating a New Protected Ports VLAN.....	342
Modifying a Protected Ports VLAN	347
Deleting a Protected Ports VLAN	351
Displaying a Protected Ports VLAN.....	352
Chapter 23: GARP VLAN Registration Protocol (GVRP)	355
Configuring GVRP	356
Enabling or Disabling GVRP on a Port.....	358
Displaying the GVRP Configuration	359
Displaying the GVRP Port Configuration.....	361
Displaying the GVRP Database	362
Displaying the GVRP State Machine.....	363
Displaying the GVRP Counters	366
Displaying the GIP Connected Ports Ring.....	369
Section VI: Port Security	371
Chapter 23: Port Security	373
Configuring Port Security.....	374
Displaying the Port Security Level.....	376
Chapter 24: 802.1x Port-based Network Access Control	379
Setting Port Roles.....	380
Enabling or Disabling 802.1x Port-based Network Access Control.....	382
Configuring Authenticator Port Parameters.....	383
Configuring Supplicant Port Parameters	386
Displaying the Port-based Network Access Control Parameters	388
Displaying the Port Status.....	388
Displaying the Port Settings.....	389
RADIUS Accounting	393
Configuring RADIUS Accounting	393
Displaying the RADIUS Accounting Settings	394
Chapter 25: MAC Address Table	397
Adding Static Unicast and Multicast MAC Addresses	398
Deleting Unicast and Multicast MAC Addresses	400
Deleting All Dynamic MAC Addresses	401
Displaying the MAC Address Tables	402
Changing the Aging Time	405
Section VII: Management Security	407
Chapter 26: Encryption Keys, PKI, and SSL	409
Displaying the Encryption Keys.....	410
Displaying the PKI Settings and Certificates	412
Displaying the SSL Settings	415
Chapter 27: Secure Shell (SSH)	417
Configuring SSH.....	418
Displaying the SSH Settings.....	420
Chapter 28: TACACS+ and RADIUS	423
Enabling or Disabling TACACS+ or RADIUS	424

Configuring TACACS+	425
Displaying the TACACS+ Settings	427
Configuring RADIUS	429
Displaying the RADIUS Settings	431
Chapter 29: Management Access Control Lists	433
Configuring a Management ACL	434
Deleting a Management ACL	436
Displaying the Management Access Control Lists	437
Appendix A: AT-S63 Default Settings	439
Basic Switch Default Settings	440
Boot Configuration File Default Setting	440
Management Access Default Settings	440
Management Interface Default Settings	440
RJ-45 Serial Terminal Port Default Settings	441
SNTP Default Settings	441
Switch Administration Default Settings	442
System Software Default Settings	442
Enhanced Stacking Default Setting	443
SNMP Default Settings	444
Port Configuration Default Settings	445
Event Log Default Settings	446
Quality of Service	447
IGMP Snooping Default Settings	448
Denial of Service Prevention Default Settings	449
STP, RSTP, and MSTP Default Settings	450
Spanning Tree Switch Settings	450
STP Default Settings	450
RSTP Default Settings	450
MSTP Default Settings	451
VLAN Default Settings	452
GVRP Default Settings	453
Port Security Default Settings	454
802.1x Port-Based Network Access Control Default Settings	455
Web Server Default Settings	456
SSL Default Settings	457
PKI Default Settings	458
SSH Default Settings	459
Server-Based Authentication Default Settings	460
Server-Based Authentication Default Settings	460
RADIUS Default Settings	460
TACACS+ Client Default Settings	460
Management Access Control List Default Setting	461
Index	463

Figures

Figure 1. Entering a Switch's IP Address in the URL Field.....	32
Figure 2. AT-S63 Login Page	33
Figure 3. Home page	34
Figure 4. Save Option in the Configuration Menu.....	37
Figure 5. General Tab (Configuration).....	40
Figure 6. General Tab (Monitoring)	44
Figure 7. File System Tab (Monitoring)	49
Figure 8. Ping Client Tab (Monitoring).....	50
Figure 9. System Utilities Tab (Configuration).....	52
Figure 10. Server-based Authentication Tab (Configuration)	54
Figure 11. SNMP Tab (Configuration).....	55
Figure 12. SNMPv1 & SNMPv2c Communities Tab.....	56
Figure 13. Add New SNMPv1 & SNMPv2c Community Page.....	57
Figure 14. Modify SNMPv1 & SNMPv2c Community Page.....	60
Figure 15. Server-based Authentication Tab (Configuration).....	63
Figure 16. SNMP Tab (Monitoring).....	64
Figure 17. SNMPv1 & SNMPv2c Communities Tab (Monitoring).....	65
Figure 18. Server-based Authentication Tab (Configuration)	69
Figure 19. Enhanced Stacking Tab (Configuration).....	69
Figure 20. Stacking Switches Page.....	72
Figure 21. Server-based Authentication Tab (Monitoring).....	75
Figure 22. Enhanced Stacking Tab (Monitoring)	76
Figure 23. Port Settings Tab (Configuration).....	78
Figure 24. Port Configuration Page	79
Figure 25. Port Settings Tab (Monitoring).....	85
Figure 26. Port Status Page	86
Figure 27. Port Statistics Page	89
Figure 28. Port Trunking Tab (Configuration).....	95
Figure 29. Add New Trunk Page	95
Figure 30. Modify Trunk Page	98
Figure 31. Port Trunking Tab (Monitoring).....	100
Figure 32. Port Mirroring Tab (Configuration).....	104
Figure 33. Modify Mirror Page	105
Figure 34. Example of a Modify Mirror Page	106
Figure 35. Port Mirroring Tab (Monitoring)	110
Figure 36. File System Tab (Configuration).....	116
Figure 37. List Files Page.....	117
Figure 38. File System Tab (Configuration) with Compact Flash	118
Figure 39. List Files Menu for a Compact Flash Card	119
Figure 40. Event Log Tab (Configuration)	129
Figure 41. Event Log Tab (Monitoring).....	130
Figure 42. Event Log Example Displayed in Normal Mode	134
Figure 43. Event Log Example Displayed in Full Mode	135
Figure 44. Create Event Log Output Page	138
Figure 45. View Event Log Output Page	141
Figure 46. Configure Log Outputs Section	142
Figure 47. Modify Event Log Output Page	142
Figure 48. Port Security Tab (Configuration).....	146
Figure 49. Classifier Tab (Configuration).....	147
Figure 50. Create Classifier Page.....	147

Figure 51. Modify Classifier Page	149
Figure 52. CoS Tab (Monitoring)	152
Figure 53. Classifier Tab (Monitoring).....	153
Figure 54. View Classifier Page.....	154
Figure 55. ACL Tab (Configuration).....	156
Figure 56. Create ACLs Page.....	157
Figure 57. Modify ACLs Page	158
Figure 58. Port Security Tab (Monitoring).....	160
Figure 59. ACL Tab (Monitoring)	161
Figure 60. View ACLs Page.....	162
Figure 61. DoS Tab (Configuration).....	164
Figure 62. DoS Configuration for Ports Page	165
Figure 63. DoS Tab (Monitoring)	167
Figure 64. DoS Monitor for Ports Page.....	168
Figure 65. CoS Tab (Configuration).....	170
Figure 66. Flow Group Tab (Configuration)	171
Figure 67. Create Flow Group Page.....	171
Figure 68. Modify Flow Group Page	172
Figure 69. Flow Group Tab (Monitoring).....	174
Figure 70. View Flow Group Page.....	175
Figure 71. Traffic Class Tab.....	176
Figure 72. Create Traffic Class Page.....	177
Figure 73. Modify Traffic Class Page.....	179
Figure 74. Traffic Class Tab (Monitoring)	181
Figure 75. View Traffic Class Page.....	182
Figure 76. Policies Tab (Configuration)	184
Figure 77. Create Policy Page	185
Figure 78. Modify Policy Page	187
Figure 79. Policies Tab (Monitoring).....	189
Figure 80. View Policy Page	190
Figure 81. CoS Tab (Configuration).....	192
Figure 82. CoS Setting for Port Page	193
Figure 83. Queuing & Scheduling Tab (Configuration).....	196
Figure 84. CoS Tab (Monitoring)	200
Figure 85. CoS Setting for Port Page	201
Figure 86. QoS Scheduling Tab (Monitoring)	202
Figure 87. IGMP Tab (Configuration).....	204
Figure 88. IGMP Tab (Monitoring)	207
Figure 89. View Multicast Hosts List Page.....	208
Figure 90. View Multicast Routers List Page	210
Figure 91. View (Static) Multicast Routers List Page.....	211
Figure 92. SNMP Tab (Configuration)	218
Figure 93. SNMPv3 User Table Tab (Configuration).....	221
Figure 94. Add New SNMPv3 User Page.....	221
Figure 95. Modify SNMPv3 User Page.....	225
Figure 96. SNMPv3 View Table Tab (Configuration).....	229
Figure 97. Add New SNMPv3 View Page.....	229
Figure 98. Modify SNMPv3 View Page.....	232
Figure 99. SNMPv3 Access Table Tab (Configuration).....	234
Figure 100. Add New SNMPv3 Access Page.....	235
Figure 101. Modify SNMPv3 Access Page.....	239
Figure 102. SNMPv3 SecurityToGroup Table Tab (Configuration)	242
Figure 103. Add New SNMPv3 SecurityToGroup Page	242
Figure 104. Modify SNMPv3 SecurityToGroup Page	245
Figure 105. SNMPv3 Notify Table Tab (Configuration)	248
Figure 106. Add New SNMPv3 Notify Page	248
Figure 107. Modify SNMPv3 Notify Page	250
Figure 108. SNMPv3 Target Address Table Tab (Configuration).....	253
Figure 109. Add New SNMPv3 Target Address Page.....	253
Figure 110. Modify SNMPv3 Target Address Page.....	256

Figure 111. SNMPv3 Target Parameters Table Tab (Configuration)	259
Figure 112. Add New SNMPv3 Target Parameters Page	260
Figure 113. Modify SNMPv3 Target Parameter Page	263
Figure 114. SNMPv3 Community Table Tab (Configuration)	267
Figure 115. Add New SNMPv3 Community Page	267
Figure 116. Modify SNMPv3 Community Page	270
Figure 117. SNMP Tab (Monitoring).....	273
Figure 118. SNMPv3 User Table Tab (Monitoring)	274
Figure 119. SNMPv3 View Table Tab (Monitoring)	275
Figure 120. SNMPv3 Access Table Tab (Monitoring)	276
Figure 121. SNMPv3 SecurityToGroup Table Tab (Monitoring).....	277
Figure 122. SNMPv3 Notify Table Tab (Monitoring).....	278
Figure 123. SNMPv3 Target Address Table Tab (Monitoring)	279
Figure 124. SNMPv3 Target Parameters Table Tab (Monitoring).....	280
Figure 125. SNMPv3 Community Table Tab (Monitoring).....	281
Figure 126. MAC Address Tab (Configuration)	286
Figure 127. Spanning Tree Tab (Configuration).....	287
Figure 128. Configure STP Parameters Tab (Configuration)	289
Figure 129. STP Settings - Port(s) Page	291
Figure 130. MAC Address Tab (Monitoring).....	293
Figure 131. Spanning Tree Tab (Monitoring).....	293
Figure 132. Monitor STP Parameters Tab (Monitoring).....	294
Figure 133. STP Settings Page	294
Figure 134. Configure RSTP Parameters Tab (Configuration).....	297
Figure 135. RSTP Settings - Port(s) Page.....	299
Figure 136. Monitor RSTP Parameters Tab (Monitoring).....	301
Figure 137. RSTP Settings Page	301
Figure 138. Spanning Tree Tab (Configuration).....	304
Figure 139. Configure MSTP Parameters Tab (Configuration)	307
Figure 140. Add New MSTI Page	310
Figure 141. Modify MSTI Page	312
Figure 142. MSTP Settings - Port(s) Page	317
Figure 143. Monitor MSTP Parameters Tab (Monitoring).....	320
Figure 144. MSTP Settings - Port(s) Page	320
Figure 145. MSTP Port Status - Port(s) Page	322
Figure 146. VLAN Tab (Configuration)	328
Figure 147. Add New VLAN Page	329
Figure 148. VLAN Tab (Monitoring).....	337
Figure 149. Add New VLAN Page	343
Figure 150. Add New Protected VLAN Page	345
Figure 151. Modify Protected VLAN Page.....	349
Figure 152. View Protected VLAN Page.....	352
Figure 153. GVRP Tab (Configuration)	356
Figure 154. GVRP Port Configuration Page	358
Figure 155. GVRP Tab (Monitoring).....	359
Figure 156. GVRP Port Configuration Page	361
Figure 157. GVRP Database Page	362
Figure 158. GVRP State Machine for VLAN Page	363
Figure 159. GVRP Counters Page	366
Figure 160. GIP Connected Ports Ring Page.....	369
Figure 161. Port Security Tab (Configuration).....	374
Figure 162. Security for Ports Page (Configuration).....	375
Figure 163. Port Security Tab (Monitoring).....	376
Figure 164. Security for Port(s) Page	377
Figure 165. 802.1x Port Access Tab (Configuration).....	380
Figure 166. Port Role Configuration Page.....	381
Figure 167. Authenticator Parameters Page	383
Figure 168. Supplicant Parameters Page.....	386
Figure 169. 802.1x Port Access Tab (Monitoring)	389
Figure 170. Port Access Port Status Page	389

Figures

Figure 171. Authenticator Port Parameters Page390
Figure 172. Supplicant Port Parameters Page391
Figure 173. 802.1x Port Access Tab (Monitoring)395
Figure 174. MAC Address Tab (Configuration).....398
Figure 175. Add MAC Address Page.....399
Figure 176. MAC Address Tab (Monitoring)402
Figure 177. View MAC Addresses Page.....404
Figure 178. Mgmt. Security Tab (Monitoring)410
Figure 179. Keys Tab (Monitoring)411
Figure 180. PKI Tab (Monitoring).....412
Figure 181. X509 Certificate Details Page.....413
Figure 182. SSL Tab (Monitoring).....415
Figure 183. Secure Shell Tab (Configuration)418
Figure 184. Secure Shell Tab (Monitoring).....420
Figure 185. TACACS+ Client Configuration Page425
Figure 186. Server-Based Authentication Tab (Monitoring).....427
Figure 187. TACACS+ Client Configuration Page428
Figure 188. RADIUS Client Configuration Page429
Figure 189. RADIUS Client Configuration Page431
Figure 190. Mgmt. ACL Tab (Configuration).....434
Figure 191. Mgmt. ACL Tab (Monitoring)437

Tables

Table 1. AT-S63 Software Modules	132
Table 2. Event Severity Levels	134
Table 3. Default Syslog Facilities	140
Table 4. Default Mappings of IEEE 802.1p Priority Levels to Priority Queues	193
Table 5. Example of Weighted Round Robin Priority	198
Table 6. Bridge Priority Value Increments	290
Table 7. Port Priority Value Increments	291
Table 8. GVRP State Machine Parameters	363
Table 9. GVRP Counters	367

Preface

This guide contains instructions on how to configure and maintain an AT-LX3800U Multi-Service Transport System using the AT-S65 management software and contains the following sections:

- “Where to Find Web-based Guides” on page 18
- “Contacting Allied Telesyn” on page 19

Where to Find Web-based Guides

The installation and user guides for all Allied Telesyn products are available in portable document format (PDF) on our web site at **www.alliedtelesyn.com**. You can view the documents online or download them onto a local workstation or server.

Contacting Allied Telesyn

This section provides Allied Telesyn contact information for technical support as well as sales and corporate information.

Online Support

You can request technical support online by accessing the Allied Telesyn Knowledge Base: <http://kb.alliedtelesyn.com>. You can use the Knowledge Base to submit questions to our technical support staff and review answers to previously asked questions.

Email and Telephone Support

For Technical Support via email or telephone, refer to the Support & Services section of the Allied Telesyn web site: www.alliedtelesyn.com.

Returning Products

Products for return or repair must first be assigned a return materials authorization (RMA) number. A product sent to Allied Telesyn without an RMA number will be returned to the sender at the sender's expense.

To obtain an RMA number, contact Allied Telesyn Technical Support through our web site: www.alliedtelesyn.com.

Sales or Corporate Information

You can contact Allied Telesyn for sales or corporate information through our web site: www.alliedtelesyn.com. To find the contact information for your country, select Contact Us -> Worldwide Contacts.

Management Software Updates

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

- Allied Telesyn web site: www.alliedtelesyn.com
- Allied Telesyn FTP server: <ftp://ftp.alliedtelesyn.com>

If you prefer to download new software from the Allied Telesyn FTP server from your workstation's command prompt, you will need FTP client software and you must log in to the server. Enter "anonymous" for the user name and your email address for the password.

Chapter 1

Overview

This chapter describes the AT-S63 software functions, the methods you can use to access the software, and the management access levels. This chapter contains the following sections:

- ❑ “Management Overview” on page 22
- ❑ “Local Connection” on page 24
- ❑ “Remote Connection” on page 25
- ❑ “Management Access Levels” on page 27
- ❑ “Online Help” on page 28

Management Overview

The AT-S63 management software allows you to monitor and adjust the operating parameters of an AT-9400 Series switch and includes the following features:

- ❑ Basic operations such as configuring port and switch parameters, enhanced stacking, SNMPv1 and v2c, trunking, and mirroring
- ❑ Advanced operations including file uploads and downloads, event logging, traffic classifiers, access control lists, denial of service defense, Quality of Service (QoS), Class of Service (CoS), and IGMP
- ❑ SNMPv3
- ❑ Spanning tree protocols including STP, RSTP, and MSTP
- ❑ Virtual LANs
- ❑ Port security options such as 802.1x Port-based Network Access Control and MAC address tables
- ❑ Management security including encryption keys, PKI, SSL, Secure Shell, TACACS+, RADIUS, and management access control lists

The AT-S63 management software is preinstalled on the switch with default settings for all operating parameters. If the default settings are adequate for your network, you can use the device as an unmanaged switch by connecting it to your network, as explained in the hardware installation guide, and powering on the switch.

Note

The default settings for the management software are listed in Appendix A, “AT-S63 Default Settings” on page 439.

To actively manage a switch and adjust its operating parameters, you must connect to an AT-9400 Series switch and access the AT-S63 management software. There are two ways to connect to the switch:

- ❑ Locally
- ❑ Remotely

Depending upon the method you choose, specific AT-S63 software interfaces are available. When you have a local connection, you can use the menus, described in the *AT-S63 Management Software Menus Interface User's Guide*, or command line interface (CLI) described in the *AT-S63 Management Software Command Line Interface User's Guide*. With a remote connection you can use the menus, CLI, and web browser (as described in this guide), or a third-party network management application.

The following sections in this chapter briefly describe each type of connection.

Local Connection

You establish a local connection with an AT-9400 Series switch when you use the RJ-45 to RS-232 management cable included with the switch to connect a terminal or a PC with a terminal emulator program to the terminal port on the switch. The terminal port is located on the front panel of the AT-9400 Series switch.

This type of connection is referred to as “local” because you must be physically close to the switch, such as in the wiring closet where the switch is located.

With a local connection you can manage the switch using the command line or menus interfaces. The web browser and SNMP interfaces are not available through a local connection.

Note

For instructions on how to start a local management session, refer to Chapter 2, “Starting a Management Session” in the *AT-S63 Management Software Menus Interface User’s Guide*.

A switch does not need an Internet Protocol (IP) address for you to manage it locally. You can start a local management session on a switch at any time. It does not interfere with the device forwarding packets.

When you assign an IP address to an AT-9400 Series switch and designate it as a master switch, you can manage all of the switches that support enhanced stacking that reside in the same subnet, through the same local connection.

Note

For further information on enhanced stacking, refer to Chapter 5, “Enhanced Stacking” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Remote Connection

You can use any management station on your network that has the Telnet application to manage an AT-9400 Series switch. This is referred to as a remote connection.

To establish a remote connection to a switch, there must be at least one enhanced stacking switch in the subnet to which you assigned an IP address. Only one switch in a subnet needs to have an IP address. After you have established a Telnet management session with the switch that has an IP address, you can use the enhanced stacking feature of the management software to access all other switches that support enhanced stacking that reside in the same subnet.

Note

For further information on enhanced stacking, refer to Chapter 5, "Enhanced Stacking" in the *AT-S63 Management Software Menus Interface User's Guide*.

Note

For instructions on how to start a remote management session, refer to Chapter 2, "Starting a Management Session" in the *AT-S63 Management Software Menus Interface User's Guide*.

A remote connection allows you to use any of the AT-S63 management software user interfaces—CLI, menus, and web browser—as well as a third-party network management application to manage the switch.

Using an SNMP Network Management Application

You can use the Simple Network Management Protocol (SNMP) to run a network management application such as AT-View to manage the switch through t. A familiarity with how to use management information base (MIB) objects is necessary for this type of management.

The AT-S63 software supports the following MIBs:

- SNMP MIB-II (RFC 1213)
- Bridge MIB (RFC 1493)
- Interface Group MIB (RFC 1573)
- Ethernet MIB (RFC 1643)
- Remote Network MIB (RFC 1757)
- Allied Telesyn managed switch MIBs

You must download the Allied Telesyn managed switch MIBs (atistackinfo.mib and atiswitch.mib) file from the Allied Telesyn web site

and compile the files with your SNMP application. For instructions, refer to your third-party application's documentation.

Note

Third-party network management applications such as HP OpenView cannot use the enhanced stacking feature of the AT-S63 management software. Therefore, you must assign an IP address to each switch that you want to manage with one of these applications.

Management Access Levels

There are two levels of management access in the AT-S63 management software: manager and operator. When you log in as a manager, you can view and configure all of a switch's operating parameters. When you log in as an operator, you can only view the operating parameters; you cannot change any values.

You log in as a manager or an operator when you enter the appropriate username and password when you start an AT-S63 management session. To log in as a manager, type "manager" as the login name. The default password is "friend." The username for operator is "operator" and the default password is also "operator." The usernames and passwords are case sensitive.

Online Help

The AT-S63 management software web browser interface provides online help for all tabs and pages in the software. To access the online help, select the **Help** option from either the Configuration or Monitoring menu. To exit the help, select the Exit Help option.

Section I

Basic Operations

The chapters in this section provide information and procedures for basic switch setup using the AT-S63 management software. The chapters include:

- ❑ Chapter 2, “Starting a Web Browser Management Session” on page 31
- ❑ Chapter 3, “Basic Switch Parameters” on page 39
- ❑ Chapter 4, “SNMPv1 and SNMPv2c” on page 53
- ❑ Chapter 5, “Enhanced Stacking” on page 67
- ❑ Chapter 6, “Port Parameters” on page 77
- ❑ Chapter 7, “Port Trunking” on page 93
- ❑ Chapter 8, “Port Mirroring” on page 103

Chapter 2

Starting a Web Browser Management Session

This chapter contains the procedure for starting, using, and quitting a web browser management session on an AT-9400 Series switch. Sections in the chapter include:

- ❑ “Establishing a Remote Connection to Use the Web Browser Interface” on page 32
- ❑ “Web Browser Tools” on page 36
- ❑ “Saving Your Parameter Changes” on page 37
- ❑ “Quitting a Web Browser Management Session” on page 38

Establishing a Remote Connection to Use the Web Browser Interface

To establish a remote connection and use the web browser interface to manage an AT-9400 Series switch, there must be at least one switch in the subnet that has been assigned an IP address and whose stacking status has been changed to master switch. After you start a remote management session on the master switch, you can manage all the enhanced stacking switches that reside in the same subnet.

If the subnet does not contain an enhanced stacking switch with an IP address, then you must use the menus or the command line interface (CLI) to give the switch an IP address and subnet mask. Then you can connect to that switch and start a web browser management session.

Note

For background information on enhanced stacking, refer to Chapter 5, “Enhanced Stacking,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

To start a web browser management session, perform the following procedure:

1. Start your web browser.

Note

If your PC with the web browser is connected directly to the switch to be managed or is on the same side of a firewall as the switch, you must configure your browser’s network options not to use proxies. Consult your web browser’s documentation on how to configure the switch’s web browser to not use proxies.

2. In the URL field of the browser, enter the IP address of the switch you want to manage or of the master switch of the enhanced stack.

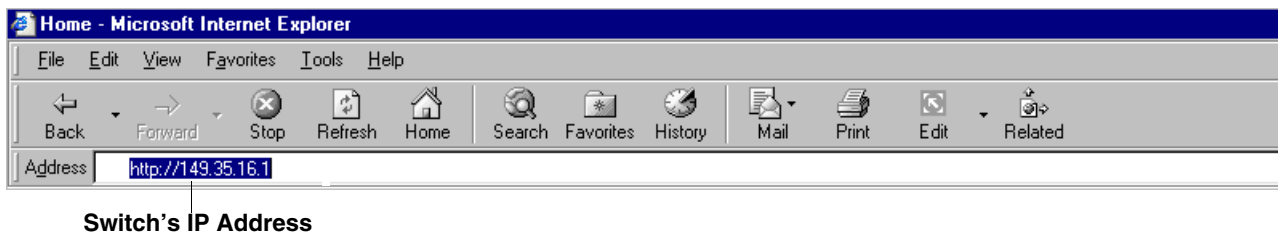
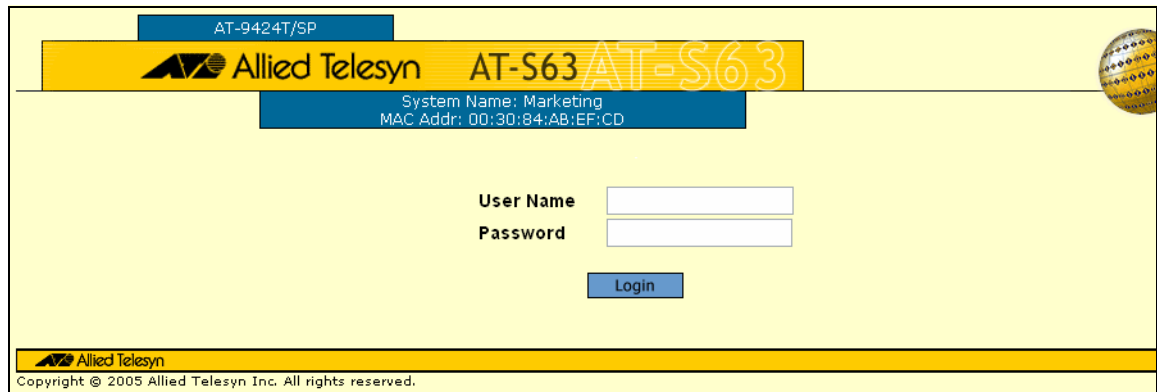


Figure 1. Entering a Switch’s IP Address in the URL Field

The AT-S63 management software displays the login page, as shown in Figure 2.



AT-9424T/SP

Allied Telesyn AT-S63

System Name: Marketing
MAC Addr: 00:30:84:AB:EF:CD

User Name

Password

Login

Allied Telesyn
Copyright © 2005 Allied Telesyn Inc. All rights reserved.

Figure 2. AT-S63 Login Page

3. Enter a user name and password. For manager access, enter “manager” as the user name. The default password is “friend.” For operator access, enter “operator” as the user name. The default password is “operator.” Login names and passwords are case-sensitive. (For information about the two access levels, refer to “Management Access” in Chapter 1, “Overview,” of the *AT-S63 Management Software Menus Interface User’s Guide*.)

You cannot change the user names. To change a password, refer to “Configuring the Manager and Operator Passwords” on page 46.

The home page is shown in Figure 3.

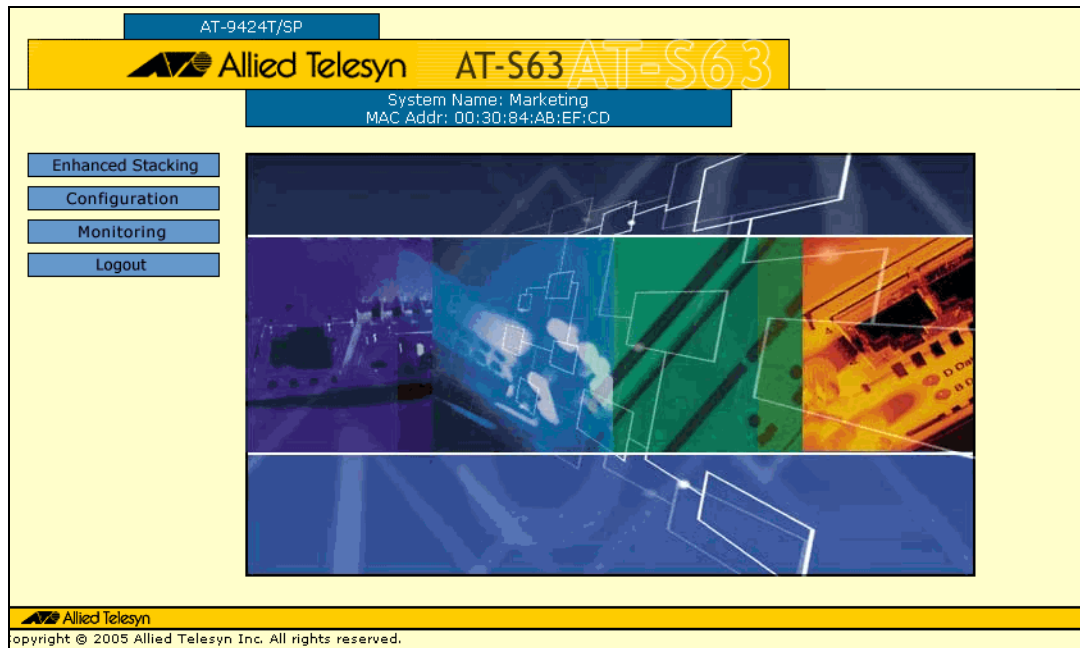


Figure 3. Home page

The main menu is on the left side of the home page. It consists of the following selections:

- Enhanced Stacking
- Configuration
- Monitoring
- Logout

Note

The Enhanced Stacking selection is included in the menu only if the switch you accessed is a master switch.

A web browser management session remains active even if you link to other sites. You can return to the management web pages anytime as long as you do not quit the browser.

If you attempt to log in with a web browser management session before the console timer expires, you will not be successful. To configure the timer, refer to Chapter 3, "Basic Switch Parameters" in the *AT-S63 Management Software Menus Interface User's Guide*.

You should always log out from a web browser management session (see "Quitting a Web Browser Management Session" on page 38) when you are finished managing the switch. Logging out prevents unauthorized

individuals from making changes to a switch's configuration if you leave your management station unattended. Also, as long as you are logged in, no one else can access the switch through another local or remote connection.

Web Browser Tools

You can use the web browser tools to move around the management pages. Selecting **Back** on your browser's toolbar returns you to the previous display. You can also use the browser's **bookmark** feature to save the link to the switch.

Saving Your Parameter Changes

When you make a change to a switch parameter, the change is, in most cases, immediately activated as soon as you click the Apply button on the page. However, a change to a switch parameter is initially saved only to temporary memory. It is lost the next time you reset or power cycle the unit. To permanently save a change, you must click the **Save Config** option on the Configuration menu. This option is displayed only after you have made configuration changes, as shown in Figure 4. After you click **Save Config**, the option is removed from the menu and your changes are permanently saved.

The screenshot displays the Configuration page for an AT-9424T/SP device. The page title is "Configuration" and it shows system information: System Name: Marketing, MAC Addr: 00:30:84:AB:EF:CD. The main content area is divided into three sections: Administration, Passwords, and Configuration. The Administration section includes fields for System Name (Marketing), Administrator (Ralph), Comments (In closet 2), IP Address (149.35.8.45), Subnet Mask (255.255.255.0), and Default Gateway (149.35.8.1). The Passwords section has fields for Manager Password, Confirm Manager Password, Operator Password, and Confirm Operator Password. The Configuration section has radio buttons for BOOTP/DHCP (Enable DHCP is selected) and MAC Address Aging Time (300 second(s)). At the bottom are buttons for Apply, Defaults, and Reset. On the left-hand menu, the "Save Config" option is highlighted with a red box and labeled "Save Config Option".

Figure 4. Save Option in the Configuration Menu

Quitting a Web Browser Management Session

To exit a web browser management session, select the **Logout** option from the main menu.

Chapter 3

Basic Switch Parameters

This chapter contains the following sections:

- ❑ “Configuring an IP Address and Switch Name” on page 40
- ❑ “Activating the BOOTP and DHCP Client Software” on page 43
- ❑ “Displaying System Information” on page 44
- ❑ “Configuring the Manager and Operator Passwords” on page 46
- ❑ “Rebooting a Switch” on page 48
- ❑ “Pinging a Remote System” on page 49
- ❑ “Returning the AT-S63 Management Software to the Factory Default Values” on page 51

Configuring an IP Address and Switch Name

Note

For guidelines about when to assign an IP address, subnet address, and gateway address to an AT-9400 Series switch, refer to “When Does a Switch Need an IP Address?” in Chapter 3, “Basic Switch Parameters,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

To set basic switch parameters for an AT-9400 Series switch, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5.

The screenshot shows the configuration interface for an AT-9424T/SP switch. The main title is "Configuration" with a yellow background. Below the title, the system name is "Marketing" and the MAC address is "00:30:84:AB:EF:CD". The interface has a left sidebar with navigation buttons: Home, System, Layer 1, Layer 2, Mgmt. Security, Mgmt. Protocols, Network Security, Services, Multicast, Utilities, Help, and Logout. The main content area has three tabs: General (selected), Event Log, and System Time. The General tab is divided into three sections: Administration, Passwords, and Configuration. The Administration section includes fields for System Name (Marketing), Administrator (Ralph), and Comments. It also displays IP Address (149.35.8.45), Subnet Mask (255.255.255.0), and Default Gateway (149.35.8.1). The Passwords section has fields for Manager Password, Confirm Manager Password, Operator Password, and Confirm Operator Password. The Configuration section has radio buttons for BOOTP/DHCP (Enable DHCP is selected) and MAC Address Aging Time (300 seconds). At the bottom, there are buttons for Apply, Defaults, and Reset.

Figure 5. General Tab (Configuration)

Note

This procedure describes the parameters in the Administration section of the tab. The Passwords section is described in “Configuring the Manager and Operator Passwords” on page 46. The BOOTP/DHCP parameters are described in “Activating the BOOTP and DHCP Client Software” on page 43. The MAC Address Aging Time parameter is described in “Changing the Aging Time” on page 405.

Note

The Defaults button returns all parameters in this tab to their default settings. The Reset button resets the switch. For instructions, refer to “Rebooting a Switch” on page 48.

2. Configure the following parameters as necessary:

System Name

This parameter specifies a name for the switch (for example, Sales Ethernet switch). The name is displayed at the top of the AT-S63 management pages and tabs. The name can be from 1 to 39 characters. The name can include spaces and special characters, such as exclamation points and asterisks. The default is no name. This parameter is optional.

Note

Allied Telesyn recommends assigning each switch a name. Names make it easier for you to identify the various switches when you manage them, and they can help you avoid performing a configuration procedure on the wrong switch.

Administrator

This parameter specifies the name of the network administrator responsible for managing the switch. The name can be from 1 to 20 characters. It can include spaces and special characters, such as dashes and asterisks. The default is no name. This parameter is optional.

Comments

This parameter specifies the location of the switch, (for example, 4th Floor - rm 402B). The location can be from 1 to 20 characters. The location can include spaces and special characters, such as dashes and asterisks. The default is no location. This parameter is optional.

Note

Another option for the IP Address, Subnet Mask, and Default Gateway parameters is to use DHCP or BOOTP to automatically assign them. See “Activating the BOOTP and DHCP Client Software” on page 43, and information in Chapter 3, “Basic Switch Parameters” in the *AT-S63 Management Software Menus Interface User’s Guide*.

IP Address

This parameter specifies the IP address of the switch. You must specify an IP address if you want the switch to function as the Master switch of an enhanced stack. The IP address must be entered in the format: xxx.xxx.xxx.xxx. The default value is 0.0.0.0.

Subnet Mask

This parameter specifies the subnet mask for the switch. You must specify a subnet mask if you assigned an IP address to the switch. The subnet mask must be entered in the format: xxx.xxx.xxx.xxx. The default value is 255.255.0.0.

Default Gateway

This parameter specifies the default router’s IP address. This address is required if you intend to remotely manage the switch from a management station that is separated from the switch by a router. The address must be entered in the format: xxx.xxx:xxx.xxx. The default value is 0.0.0.0.

3. Click **Apply** to activate your changes on the switch.

Note

A change to any of the above parameters is immediately activated on the switch.

A change to the IP address of the switch results in the loss of a remote management session. You can restart the management session using the switch’s new IP address.

4. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Activating the BOOTP and DHCP Client Software

For background information on BOOTP and DHCP, refer to Chapter 3, "Basic Switch Parameters," in the *AT-S63 Management Software Menus Interface User's Guide*.

To activate or deactivate the BOOTP and DHCP client software on the switch from a web browser management session, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. In the Configuration section, for the **BOOTP/DHCP** parameter, click one of the following:

Enable DHCP
Enables DHCP.

Enable BOOTP
Enables BOOTP.

Disable
Disables both DHCP and BOOTP.

3. Click **Apply** to activate your change on the switch.

Note

If you enabled BOOTP or DHCP, the switch immediately begins to query the network for a BOOTP or DHCP server. The switch continues to query the network for its IP configuration until it receives a response. If you manually assigned an IP address to the switch, that address is deleted and replaced by the IP address received from the BOOTP or DHCP server.

4. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying System Information

To view basic information about the switch, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6.

The screenshot shows the 'Monitoring' page for switch AT-9424T/SP. The 'General' tab is selected, displaying the following information:

System Name: Marketing
MAC Addr: 00:30:84:AB:EF:CD

General Information:

System Name Marketing	IP Address 149.35.8.45
Administrator Ralph	Subnet Mask 255.255.255.0
Comments	Default Gateway 149.35.8.1
BOOTP/DHCP Enabled(DHCP)	System Up Time 55Days 3 Hours 4 Minutes 36 Seconds
MAC Address Aging Time 300 second(s)	

System Software:

Application Software	ATS63 v1.1.0 (Jan 14 2005 17:02:34)
Bootloader	ATS63_LOADER v1.2.0 (Dec 6 2004 19:30:34)

Hardware:

Model Name	Serial Number	Temperature (Deg. C)	Upper Temp. Threshold (Deg. C)	Fan 1 Speed RPM/Status	Fan 2 Speed RPM/Status
AT-9424T/SP	S05525A023600001	29	60	3792	Off

Voltage: AT-9424T/SP S05525A023600001 29603792 Off

2.5 V	3.3 V	5.0 V	1.8 V	1.25 V	3.0 V	12.0 V
2.53V	3.36V	5.14V	1.80V	1.30V	1.80V	12.06V

Figure 6. General Tab (Monitoring)

The General section displays the following information:

System Name

The name of the switch.

Administrator

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

Comments

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

BOOTP/DHCP

The status of the BOOTP and DHCP client software. If enabled, the switch is obtaining its IP information from a BOOTP or DHCP server on the network.

MAC Address Aging Time

The time interval an inactive dynamic MAC address can remain in the MAC address table before it is deleted.

IP Address

The switch's IP address.

Subnet Mask

The switch's subnet mask.

Default Gateway

The IP address of a router for remote management.

System Up Time

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

The System Software section displays the following information:

Application Software

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

Bootloader

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

The Hardware section displays the following information:

Model Name

The model name.

Serial Number

The switch serial number.

Temperature (Deg.C)

The current system temperature.

Upper Temp. Threshold (Deg C)

The upper threshold for the switch temperature.

Fan 1 Speed RPM/Status**Fan 2 Speed RPM/Status**

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

The Voltage section provides the current voltage of the six power supplies in the switch, identified as 2.5 V, 3.3 V, 5 V, 1.8 V, 1.25 V, and 12 V.

Configuring the Manager and Operator Passwords

There are two levels of management access on an AT-9400 Series switch: manager and operator. When you log in as a manager, you can view and configure all of a switch's operating parameters. When you log in as an operator, you can only view the operating parameters; you cannot change any values.

You log in as a manager or an operator by entering the appropriate username and password when you start an AT-S63 management session. The default password for manager access is "friend." The default password for operator access is "operator." Passwords are case sensitive.

To change the manager or operator password, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. In the Passwords section, enter the new values. The parameters are described below.

Manager Password

Confirm Manager Password

You use these parameters to change the manager's login password for the switch. The password can be from 0 to 16 characters in length. The same password is used for both local and remote management sessions. To create a new password, enter the new password into both fields. The default password is "friend." The password is case sensitive.



Caution

Do not use spaces or special characters, such as asterisks (*) and exclamation points (!), in a password if you are managing the switch from a web browser. Many web browsers cannot handle special characters in passwords.

Operator Password Confirm Operator Password

Use these parameters to change the operator's login password for the switch. The password can be from 0 to 16 characters in length. The same password is used for both local and remote management sessions. To create a new password, enter the new password into both fields. The default password for operator is "operator." The password is case sensitive.



Caution

Do not use spaces or special characters, such as asterisks (*) and exclamation points (!), in a password if you are managing the switch from a web browser. Many web browsers cannot handle special characters in passwords.

Note

A change to a password is immediately activated on the switch. You are prompted for the new password the next time you log in.

3. Click **Apply** to activate your change on the switch.
4. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Rebooting a Switch

Note

Any parameters changes that have not been saved are discarded when a system is reset. To save parameter changes, refer to “Saving Your Parameter Changes” on page 36.

To reboot a switch, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Click **Reset** at the bottom of the tab.

A confirmation prompt is displayed.

3. Click **OK** to reset the switch or **Cancel** to cancel the procedure:

Note

The switch does not forward packets while it reloads the AT-S63 management software, a process that takes approximately 20 seconds to complete.

Resetting the switch ends your web browser management session. You must restart the session to continue managing the switch.

Pinging a Remote System

You can instruct the switch to ping a node on your network. This procedure is useful in determining whether a valid link exists between the switch and another device.

To ping a network device, perform the following procedure:

1. From the home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Utilities** option.

The Utilities tab is displayed with the File System tab selected by default, as shown in Figure 7.

The screenshot shows the web browser interface for the AT-9424T/SP switch. The main heading is "Monitoring". Below it, the system name is "Marketing" and the MAC address is "00:30:84:AB:EF:CD". A left-hand navigation menu includes options like Home, System, Layer 1, Layer 2, Mgmt. Security, Mgmt. Protocols, Network Security, Services, Multicast, Utilities, Help, and Logout. The "Utilities" option is selected. The main content area shows the "File System" tab with a sub-tab "Ping Client". It displays "Current Drives" as "Flash" and "Default Cfg. File" as "boot.cfg [Exists]". A table titled "Current Files" shows a single file named "boot.cfg" on the "flash" device, with a size of 2736 bytes, modified on 01/20/2005 at 13:44:42, and an attribute of "Archive". There are "View" and "Refresh" buttons at the bottom of the table.

File Name	Device	Size	Modified	Attributes
boot.cfg	flash	2736	01/20/2005 13:44:42	Archive

Figure 7. File System Tab (Monitoring)

3. Select the **Ping Client** tab.

The Ping Client tab is shown in Figure 8.

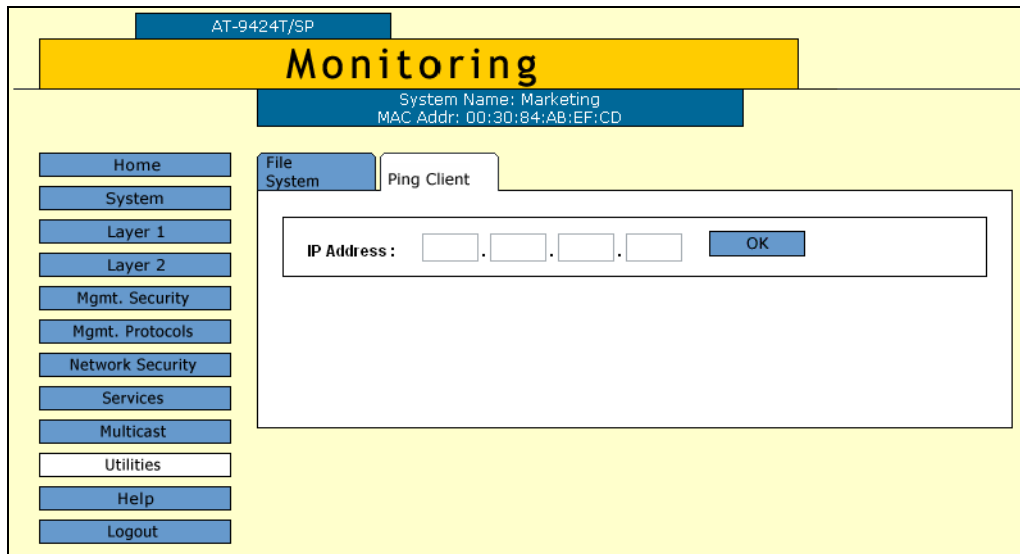


Figure 8. Ping Client Tab (Monitoring)

4. Enter the IP address of the end node you want the switch to ping.
5. Click **OK**.

The results of the ping are displayed in a popup window.

6. To stop the ping, click **OK**.

Returning the AT-S63 Management Software to the Factory Default Values

The procedure in this section returns all AT-S63 management software parameters to their default values. Please note the following before you perform this procedure:

- ❑ Returning all parameter settings to their default values also deletes any port-based or tagged VLANs you created on the switch.
- ❑ This procedure does not delete files from the AT-S63 file system. To delete files, refer to Chapter 10, "File System," in the *AT-S63 Management Software Menus Interface User's Guide*.
- ❑ This procedure does not delete any encryption keys stored in the key database. To delete encryption keys, refer to "Deleting a Key," in Chapter 26, "Encryption Keys," in the *AT-S63 Management Software Menus Interface User's Guide*.
- ❑ Returning a switch to its default values deletes all configuration commands in the active boot configuration file. If you want to keep the file, you should either create a copy of it, as explained in Chapter 10, "File System," in the *AT-S63 Management Software Menus Interface User's Guide*. Or, you can assign another configuration file, one whose configuration you do not want to retain, as the active boot configuration file. The latter procedure is described in the same chapter.

Note

The AT-S63 management software default values are listed in Appendix A, "AT-S63 Default Settings" on page 439.

Note

When you return a switch to its default values, the IP address is set to all zeros and DHCP is not enabled. Therefore, you will not be able to access the switch through the web browser interface or through enhanced stacking.

To return the AT-S63 management software to the default settings, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuring System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Utilities** option.

The Utilities page is displayed with the System Utilities tab selected by default, as shown in Figure 9.

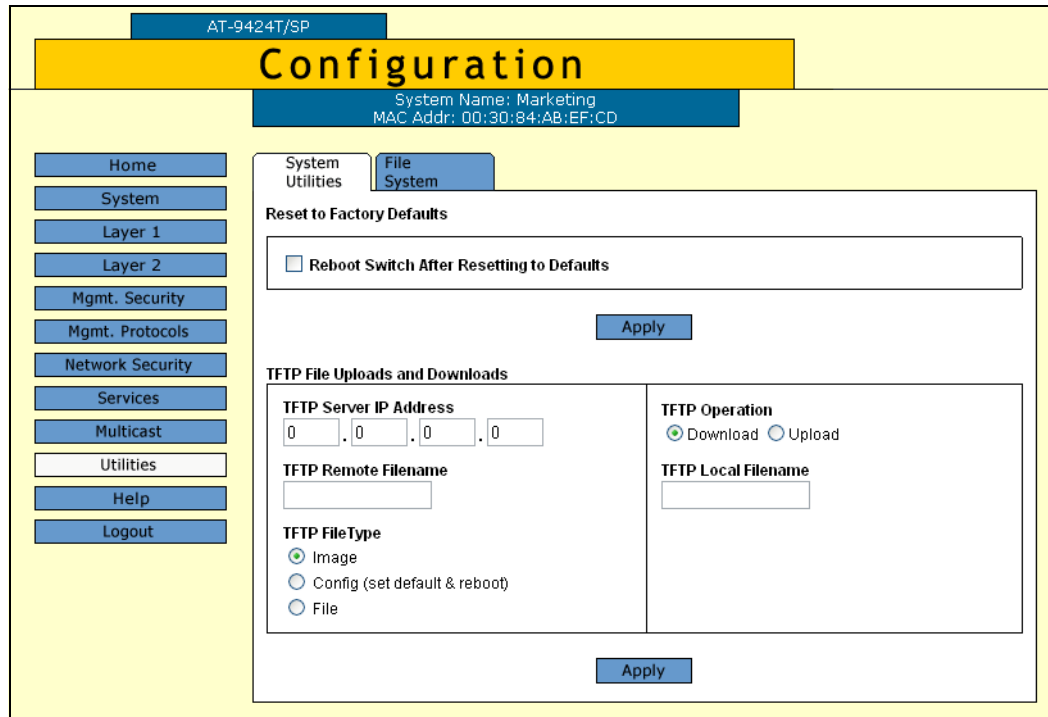


Figure 9. System Utilities Tab (Configuration)

3. Click the **Reboot Switch After Resetting to Defaults** checkbox.
4. Click **Apply**.

The web browser displays the following prompt:

This page may no longer be available while the switch reboots. Do you want to continue?

5. Click **OK** to continue, or **Cancel** to cancel the procedure.

Chapter 4

SNMPv1 and SNMPv2c

This chapter explains how to activate SNMP management on the switch and how to create, modify, and delete SNMPv1 and SNMPv2c community strings. This chapter contains the following procedures:

- ❑ “Enabling or Disabling SNMP Management” on page 54
- ❑ “Creating a New SNMPv1 and SNMPv2c Community” on page 56
- ❑ “Modifying an SNMPv1 and SNMPv2c Community” on page 59
- ❑ “Deleting an SNMPv1 and SNMPv2c Community” on page 62
- ❑ “Displaying the SNMPv1 and SNMPv2c Communities” on page 63

Note

For background information about SNMPv1 and SNMPv2c, refer to Chapter 4, “SNMPv1 and SNMPv2c,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Enabling or Disabling SNMP Management

To enable or disable SNMP management on the switch, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Mgmt. Protocols** option.

The Mgmt. Protocols page is displayed with the Server-based Authentication tab selected by default, as shown in Figure 10.

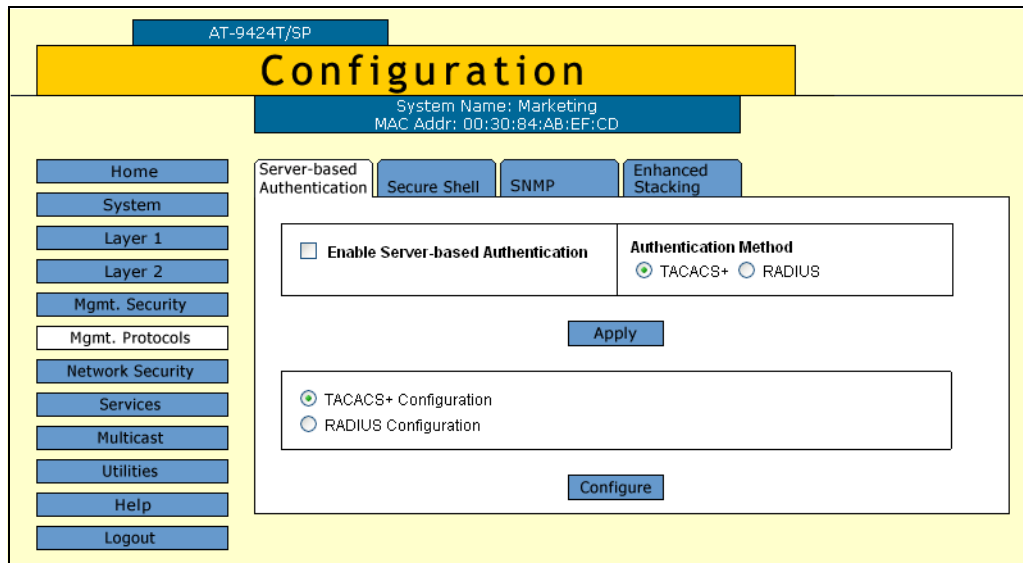


Figure 10. Server-based Authentication Tab (Configuration)

3. Select the **SNMP** tab.

The SNMP tab is shown in Figure 11.

Figure 11. SNMP Tab (Configuration)

4. Click the **Enable SNMP Access** checkbox to enable or disable SNMP management. A check in the box indicates that the feature is enabled, meaning that the switch can be managed from an SNMP management station. No check indicates that the feature is disabled. The default is disabled.
5. If you want the switch to send authentication failure traps, click the **Enable Authentication Failure Traps** checkbox. A check in the box indicates that the switch sends the trap.
6. Click **Apply**.

A change to SNMP access is immediately activated on the switch.

The community strings that already exist on the switch are displayed in a table.

7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Creating a New SNMPv1 and SNMPv2c Community

To create a new SNMPv1 and SNMPv2c community, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Mgmt. Protocols** option.

The Mgmt. Protocols page is displayed with the Server-based Authentication tab selected by default, as shown in Figure 10 on page 54.

3. Select the **SNMP** tab.

The SNMP tab is shown in Figure 11 on page 55.

4. In the SNMPv1 & SNMPv2c section, click **Configure**.

The SNMPv1 & SNMPv2c Communities tab is shown in Figure 12.

AT-9424T/SP

Configuration

System Name: Marketing
MAC Addr: 00:30:84:AB:EF:CD

Server-based Authentication | Secure Shell | **SNMP** | Enhanced Stacking

SNMPv1 & SNMPv2c Communities

Total Entries: 3. Page 1 of 1

	Community Name	Access Mode	Manager Stations	Trap Receivers	Open Access	Status
<input checked="" type="radio"/>	lemondrop19	Read Only			Yes	Enabled
<input type="radio"/>	rootbeer14	Read Only	198.1.1.9	198.1.1.9	No	Enabled
<input type="radio"/>	sassafra12	Read/Write	198.1.1.1, 198.20.2.2, 198.30.3.3	198.1.1.1, 198.20.2.2, 198.30.3.3	No	Enabled

Refresh Add Remove Modify

Back

Figure 12. SNMPv1 & SNMPv2c Communities Tab

5. Click **Add**.

The Add New SNMPv1 & SNMPv2c Community page is shown in Figure 13.

Figure 13. Add New SNMPv1 & SNMPv2c Community Page

6. Configure the following parameters:

Community Name

Enter an SNMP community name that consists of up to 15 alphanumeric characters.

Status

Click Enable to enable the SNMP community. Click Disable to disable the SNMP community.

Access Mode

Click Read Only to allow read access to the SNMP community. To allow read-write access to the SNMP community, click Read-Write.

Allow Any Station

Click this option to allow any SNMP manager to access the switch. When you click this option, a warning message appears on the screen. Click OK to continue.

Manager IP Address 1 through Manager IP Address 8

Enter an IP Address of a switch that is permitted SNMP manager access to the current switch. You can enter up to eight Manager IP Addresses.

Trap Receiver IP Address 1 through Trap Receiver IP Address 8

Use the above selections to specify the IP addresses of up to eight trap receivers on your network that can receive traps from the switch.

7. Click **Apply**.
8. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Modifying an SNMPv1 and SNMPv2c Community

To modify an SNMPv1 and SNMPv2c community, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Mgmt. Protocols** option.

The Mgmt. Protocols page is displayed with the Server-based Authentication tab selected by default, as shown in Figure 10 on page 54.

3. Select the **SNMP** tab.

The SNMP tab is shown in Figure 11 on page 55.

4. In the SNMPv1 & SNMPv2c section, click **Configure**.

The SNMPv1 & SNMPv2c Communities tab is shown in Figure 12 on page 56.

5. Click the button next to the community name and click **Modify**.

The Modify SNMPv1 & SNMPv2c Community page is shown in Figure 14.

Figure 14. Modify SNMPv1 & SNMPv2c Community Page

6. Modify the following parameters:

Community Name

This field is not configurable from this page. It is the name of the SNMP community.

Status

Click Enable to enable the SNMP community. Click Disable to disable the SNMP community.

Access Mode

Click Read Only to allow read access to the SNMP community. Click Read-Write to allow read-write access to the SNMP community.

Allow Any Station

Click this option to allow any SNMP manager to access the switch. When you click this option, a warning message appears on the screen. Click OK to continue.

Manager IP Address1 through Manager IP Address 8

Enter an IP Address of a switch that is permitted SNMP manager

access to the current switch. You can enter up to 8 Manager IP Addresses.

Trap Receiver IP Address 1 through **Trap Receiver IP Address 8**

Use the above selections to specify the IP addresses of up to 8 trap receivers on your network that can receive traps from the switch.

7. Click **Apply**.
8. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting an SNMPv1 and SNMPv2c Community

To delete an existing SNMPv1 and SNMPv2c community, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Mgmt. Protocols** option.

The Mgmt. Protocols page is displayed with the Server-based Authentication tab selected by default, as shown in Figure 10 on page 54.

3. Select the **SNMP** tab.

The SNMP tab is shown in Figure 11 on page 55.

4. In the SNMPv1 & SNMPv2c section, click **Configure**.

The SNMPv1 & SNMPv2c Communities tab is shown in Figure 12 on page 56.

5. Click the button next to the community name and click **Remove**.

A warning message is displayed.

6. Click **OK**.

7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying the SNMPv1 and SNMPv2c Communities

To display the SNMPv1 and SNMPv2c communities, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Mgmt. Protocols** option.

The Mgmt. Protocols page is displayed with the Server-based Authentication tab displayed by default, as shown in Figure 15.

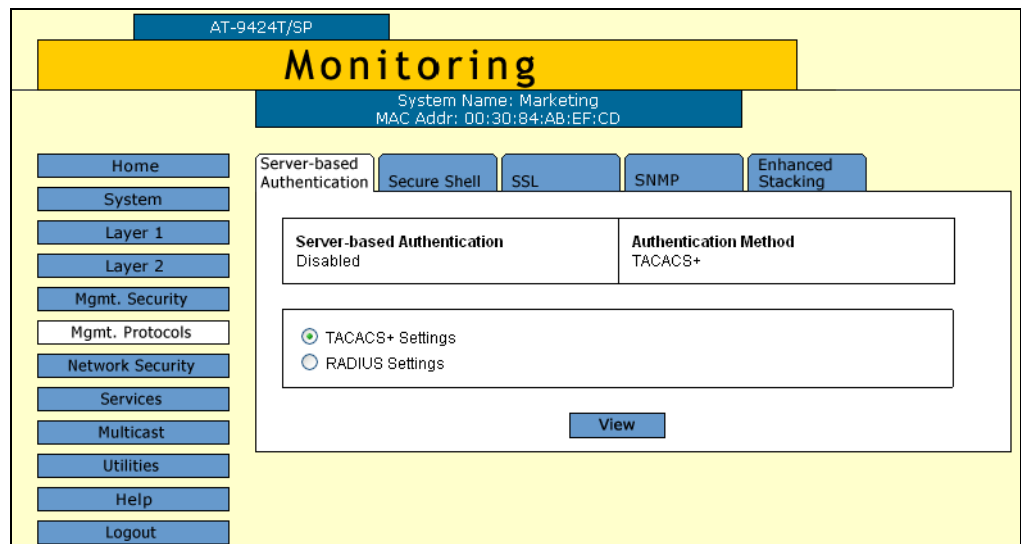


Figure 15. Server-based Authentication Tab (Configuration)

3. Select the **SNMP** tab.

The SNMP tab is shown in Figure 16.

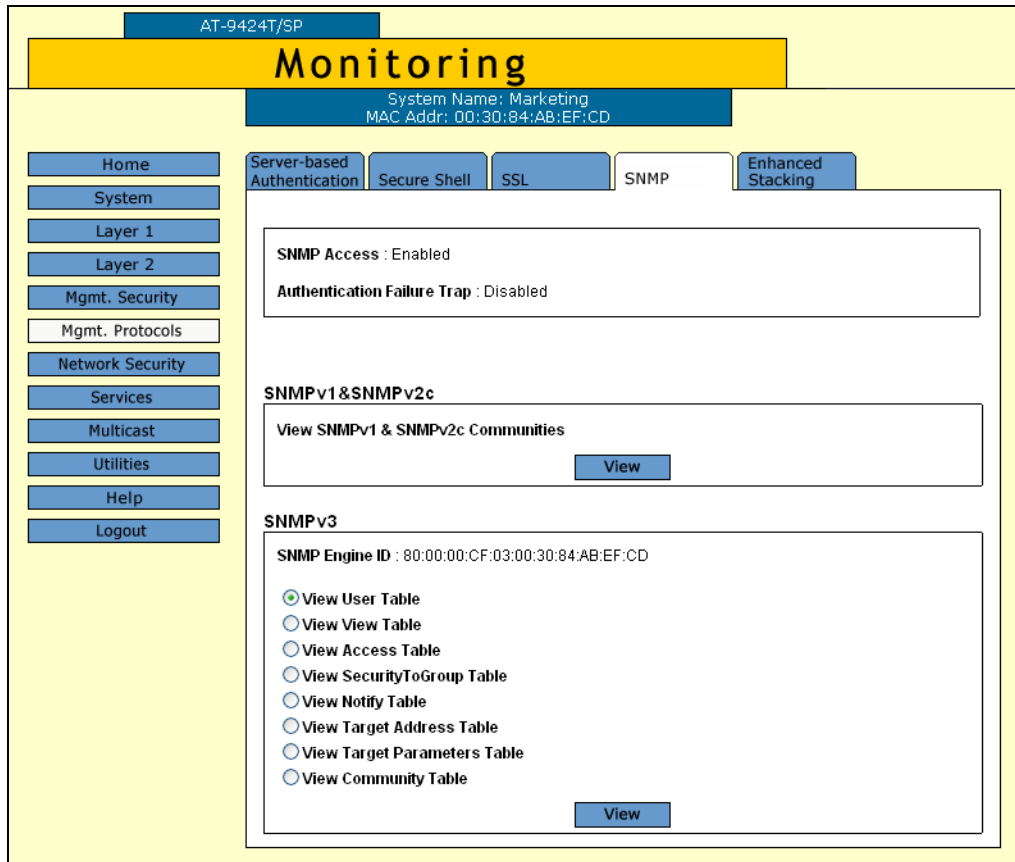


Figure 16. SNMP Tab (Monitoring)

4. In the SNMPv1 & SNMPv2c section, click **View**.

The SNMPv1 & SNMPv2c Communities tab is shown in Figure 17.

The screenshot shows the 'Monitoring' tab in the web browser interface. The main content area displays the 'SNMP v1/v2c Communities' configuration page. The page includes a table with the following data:

Community Name	Access Mode	Manager Stations	Trap Receivers	Open Access	Status
ati54sunwale	Read Write	198.12.19.1, 198.12.20.1	196.1.1.1, 198.12.19.1, 198.12.20.1	Yes	Enabled
bothell99	Read Only	196.1.1.1	196.1.1.1	No	Enabled
miami77	Read Only	145.2.2.2, 145.2.34.4	145.2.2.2, 145.2.34.4	No	Enabled
milan	Read Only	198.10.10.10, 198.10.10.11	198.10.10.10, 198.10.10.11	No	Enabled

The interface also includes a navigation menu on the left with options like Home, System, Layer 1, Layer 2, Mgmt. Security, Mgmt. Protocols, Network Security, Services, Multicast, Utilities, Help, and Logout. The top navigation bar shows 'Monitoring' as the active tab. The main content area has buttons for 'Refresh', 'Next', and 'Back'.

Figure 17. SNMPv1 & SNMPv2c Communities Tab (Monitoring)

The SNMPv1 & SNMPv2c Communities tab displays a table that contains the following columns of information:

Community Name

The SNMP community name.

Access Mode

The access mode for access to that community. The possible settings are Read Only and Read/Write.

Manager Stations

The IP addresses of the management stations that are allowed SNMP access to the switch.

Trap Receivers

The IP addresses of up to 8 trap receivers on your network that can receive traps from the switch.

Open Access

The status of access to the SNMP community by a management station, one of the following settings:

Yes - Any management station can access the SNMP community.

No - Access to the SNMP community is only available to a management station configured within this community.

Status

The community status, one of the following settings:

Enabled - The community is enabled.

Disabled - The community is disabled.

Chapter 5

Enhanced Stacking

This chapter contains the following procedures for setting up enhanced stacking:

- ❑ “Setting a Switch’s Enhanced Stacking Status” on page 68
- ❑ “Selecting a Switch in an Enhanced Stack” on page 71
- ❑ “Returning to the Master Switch” on page 74
- ❑ “Displaying the Enhanced Stacking Status” on page 75

Note

For background information on enhanced stacking, refer to Chapter 5, “Enhanced Stacking,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Setting a Switch's Enhanced Stacking Status

The enhanced stacking status of the switch can be master, slave, or unavailable. Each status is described below:

- ❑ **Master** - A master switch of a stack can be used to manage other enhanced stacking switches in a subnet. After you have established a local or remote management session with the master switch, you can access and manage the other enhanced stacking switches in the subnet.
- ❑ A master switch must have a unique IP address. You can manually assign a master switch an IP address or activate the BOOTP and DHCP client software on the switch so that the switch automatically obtains an IP address from a BOOTP or DHCP server on your network. Refer to “Configuring an IP Address and Switch Name” on page 40 and “Activating the BOOTP and DHCP Client Software” on page 43 for further information.
- ❑ **Slave** - A slave switch can be remotely managed through a master switch. It does not need an IP address or subnet mask.
- ❑ **Unavailable** - A switch with an unavailable stacking status cannot be remotely managed through a master switch. A switch with this designation can be managed locally. To be managed remotely, a switch with an unavailable stacking status must be assigned a unique IP address.

Note

The default setting for a switch is slave.

To configure a switch's enhanced stacking status, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Mgmt. Protocols** option.

The Mgmt. Protocols page is displayed with the Server-based Authentication tab selected by default, as shown in Figure 18.

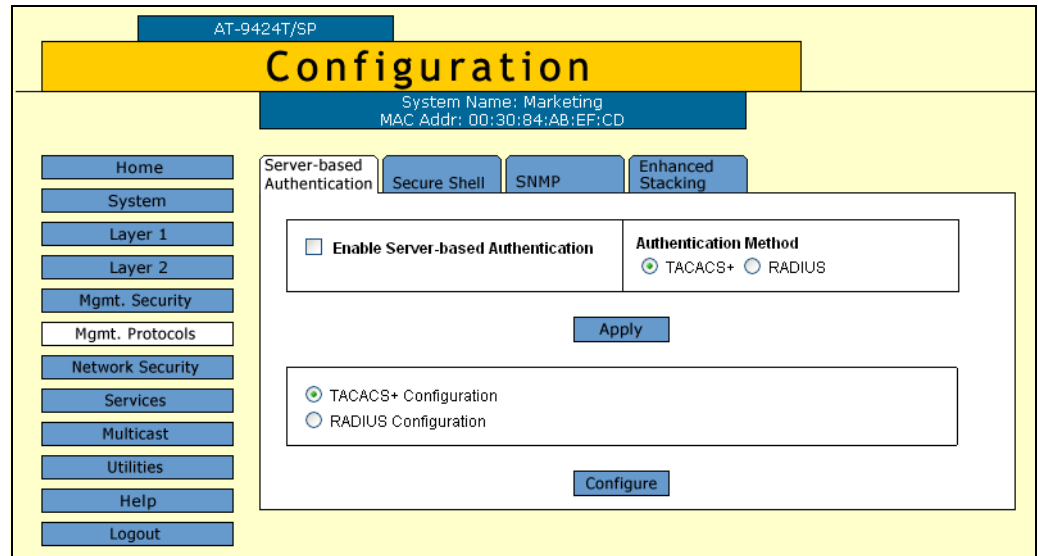


Figure 18. Server-based Authentication Tab (Configuration)

3. Select the **Enhanced Stacking** tab.

The Enhanced Stacking tab is shown in Figure 19.

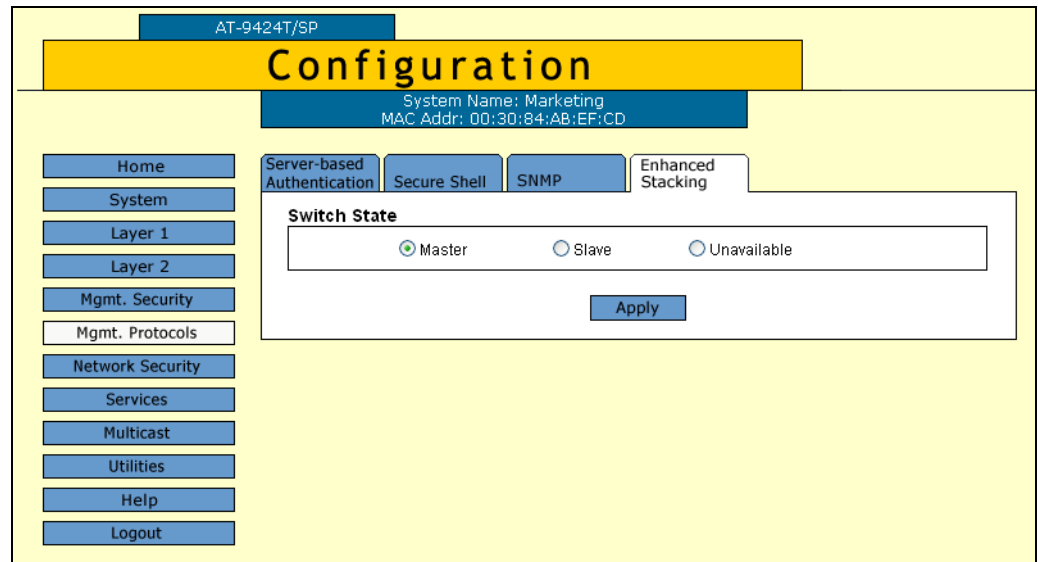


Figure 19. Enhanced Stacking Tab (Configuration)

4. Click the desired enhanced stacking status for the switch. The default is Slave.
5. Click **Apply**.

The new enhanced stacking status is immediately activated on the switch.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Selecting a Switch in an Enhanced Stack

Before you perform any procedure on a switch in an enhanced stack, check to be sure that you are performing it on the correct switch. If you assigned system names to your switches, identifying your switches is easy. The AT-S63 management software displays the name of the switch being managed at the top of every management menu.

When you start a web browser management session on the master switch of the enhanced stack, you are by default addressing that particular switch. The management tasks that you perform affect only the master switch.

To manage a slave switch or another master switch in the same stack, you need to select it from the management software.

To select a switch to manage in an enhanced stack, perform the following procedure:

1. From the home page, select **Enhanced Stacking**.

Note

If the Home page does not have an Enhanced Stacking menu option, the switch's enhanced stacking status is either slave or unavailable. For instructions on how to change a switch's stacking status, refer to the previous procedure:

The master switch polls the network for the slave and master enhanced stacking switches in the subnet and displays a list of the

switches in the Stacking Switches page. An example is shown in Figure 20.

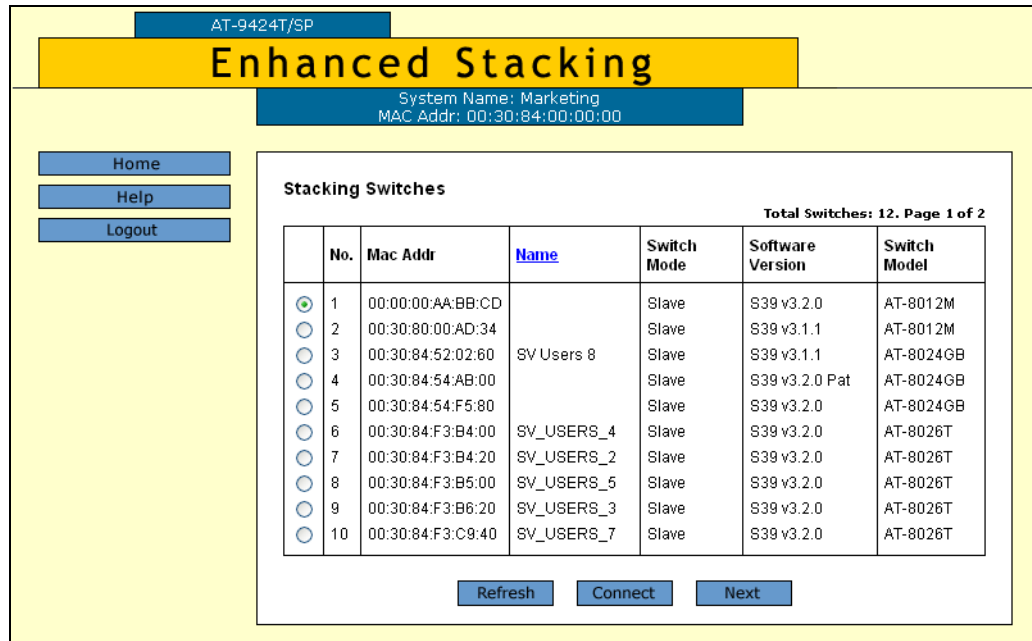


Figure 20. Stacking Switches Page

Note

The master switch on which you started the management session is not included in the list, nor are any switches with an enhanced stacking status of Unavailable.

You can sort the switches in the list by switch name or MAC address by clicking on the column headers. By default, the list is sorted by MAC address.

To refresh the list, click **Refresh**. This instructs the master switch to again poll the subnet for all switches.

2. To manage another switch in an enhanced stack, click the button to the left of the appropriate switch in the list. You can select only one switch at a time.

Note

If the web server on the master switch is operating in the secure HTTPS mode, you can manage only those enhanced stacking switches that are also operating HTTPS. You cannot manage a switch whose web server is operating in the non-secure HTTP mode.

3. Click **Connect**.
4. Enter a user name and password for the switch when prompted.

The home page of the selected switch is displayed. You can now manage the switch.

Returning to the Master Switch

When you are finished managing a slave switch and want to manage another switch in the stack, return to the Home page of the switch and select **Disconnect** from the menu. This returns you to the Enhanced Stacking page in Figure 20 on page 72. When you see that page, you are again addressing the master switch from which you started the management session.

You can select another switch in the list to manage or, if you want to manage the master switch, select **Home** to return to the master switch's home page.

Displaying the Enhanced Stacking Status

To display the enhanced stacking status of the switch, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Mgmt. Protocols** option.

The Mgmt. Protocols page is displayed with the Server-based Authentication tab selected by default, as shown in Figure 21.

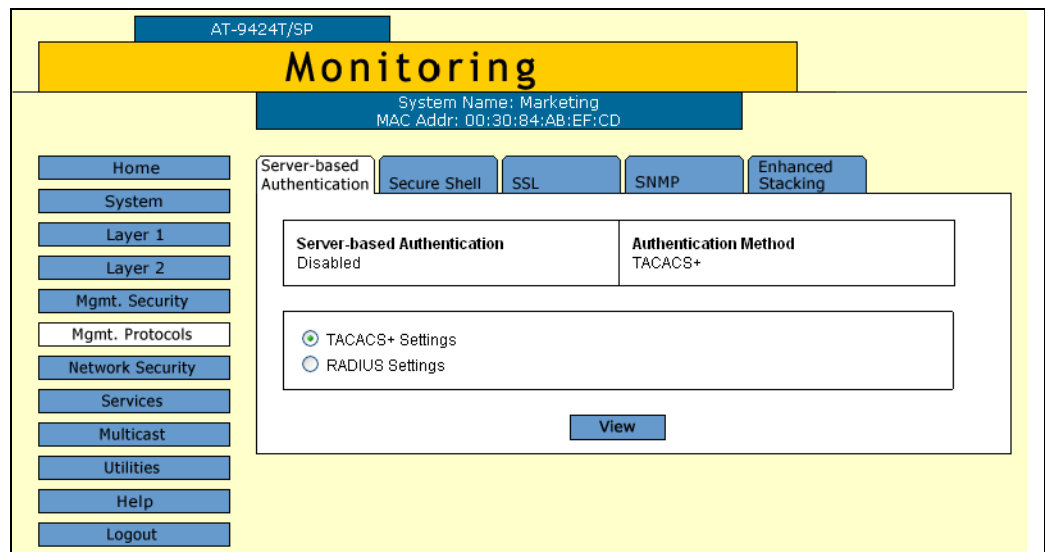


Figure 21. Server-based Authentication Tab (Monitoring)

3. Select the **Enhanced Stacking** tab.

The Enhanced Stacking tab is shown Figure 22.

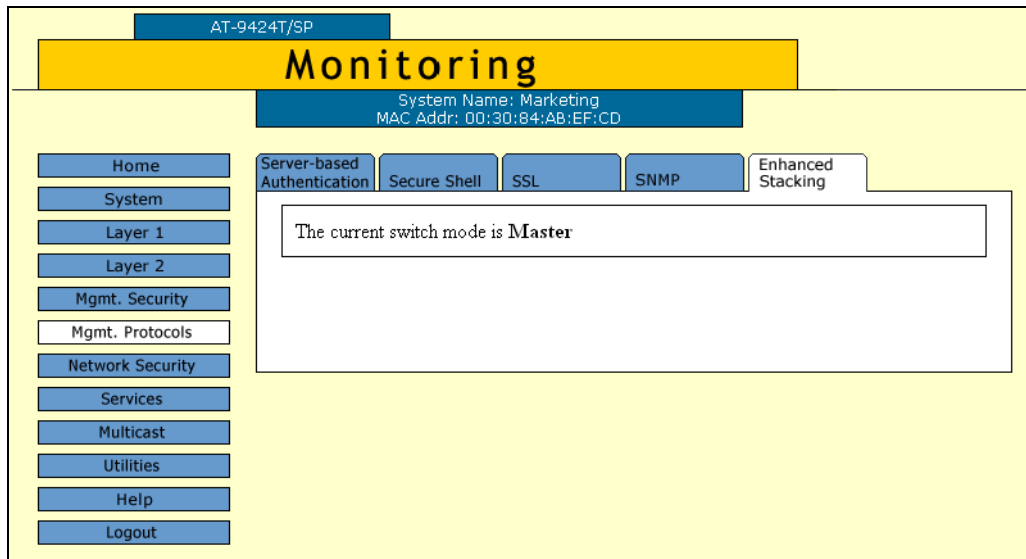


Figure 22. Enhanced Stacking Tab (Monitoring)

The information in the tab states the current enhanced stacking status of the switch as master, slave, or unavailable.

Chapter 6

Port Parameters

This chapter explains how to view and change the parameter settings for the individual ports on a switch. Examples of the parameters that you can adjust include port speed and duplex mode.

This chapter contains the following procedures:

- ❑ “Configuring Port Parameters” on page 78
- ❑ “Displaying Port Status” on page 85
- ❑ “Displaying Port Statistics” on page 89
- ❑ “Resetting a Port to the Default Settings” on page 92

Note

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

Configuring Port Parameters

To configure the parameter settings of a port on the switch, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 1** option.

The Layer 1 page is displayed with the Port Settings tab selected by default, as shown in Figure 23.

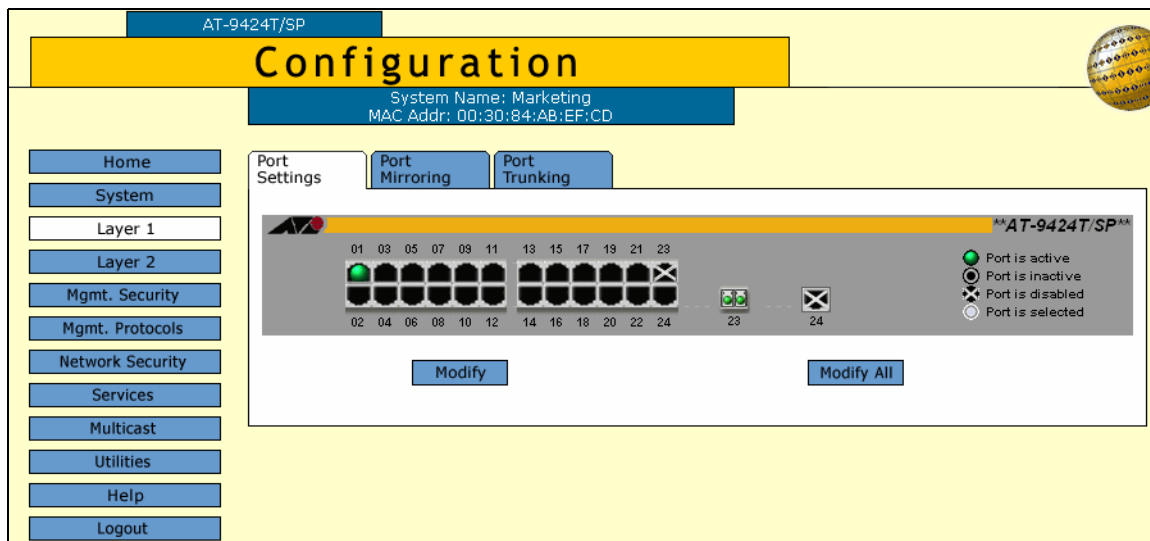


Figure 23. Port Settings Tab (Configuration)

3. Click the port in the graphical switch image that you want to configure. The selected port turns white. You can select more than one port at a time to configure. (To deselect a port, click it again.)
4. Click **Modify**. To configure all the ports, click **Modify All**.

Note

If you select Modify All, you cannot configure the port name or set the speed and duplex mode. The speed and duplex mode are set to autonegotiate.

The Port Configuration page is shown Figure 24.

The screenshot shows a web browser interface for configuring a port. The title bar reads "Port Configuration - 5". The main content area is divided into two columns of settings, each with a label and a corresponding input field or dropdown menu. At the bottom, there are three buttons: "Apply", "Defaults", and "Close".

Parameter	Value
Name	Port_05
Status	Enabled
Speed and Duplex	Auto-Negotiate
MDI/MDIX Crossover	Auto
Ingress Broadcast Filter	Disabled
Egress Broadcast Filter	Disabled
Ingress Unknown Unicast Filter	Disabled
Egress Unknown Unicast Filter	Disabled
Ingress Unknown Multicast Filter	Disabled
Egress Unknown Multicast Filter	Disabled
Flow Control	Disabled
Back Pressure	Disabled
Flow Control/Back Pressure Limit	7935 [1-7935] Cells
HOL Blocking	682 [0-8191] Cells
Broadcast Rate Limiting	Disabled
Broadcast Rate	262143 [0-262143] Pkts/Sec
Unknown Unicast Rate Limiting	Disabled
Unknown Unicast Rate	262143 [0-262143] Pkts/Sec
Multicast Rate Limiting	Disabled
Multicast Rate	262143 [0-262143] Pkts/Sec

Figure 24. Port Configuration Page

- Configure the following parameters as necessary.

Name

Use this selection to assign a name to a port, from 1 to 15 alphanumeric characters. Spaces are allowed, but you should not use special characters, such as asterisks or exclamation points. (You cannot assign a name when you are configuring more than one port.)

Status

Use this selection to enable or disable a port. When disabled, a port does not accept or forward frames.

You might want to disable a port and prevent packets from being forwarded if a problem occurs with the node or cable connected to the port. After the problem has been fixed, you can enable the port again to resume normal operation.

You might also want to disable a port that is not being used to secure it from unauthorized connections.

The possible settings are:

Enabled - The port receives and forwards packets. This is the default setting.

Disabled - The port does not receive or forward packets.

Speed and Duplex

You use this selection to configure a port for autonegotiation or to manually set a port's speed and duplex mode.

If you select Auto-Negotiate for autonegotiation, which is the default setting, the switch sets both speed and duplex mode for the port automatically.

Note the following about the operation of autonegotiation on the switch port:

- ❑ In order for a switch port to successfully autonegotiate its duplex mode with an end node, the end node should also be using autonegotiation. Otherwise, a duplex mode mismatch can occur. A switch port using autonegotiation defaults to half-duplex if it detects that the end node is not using autonegotiation. This results in a mismatch if the end node is operating at a fixed duplex mode of full-duplex.

To avoid this problem, when connecting an end node with a fixed duplex mode of full-duplex to a switch port, you should disable autonegotiation on the port and set the port's speed and duplex mode manually.

- ❑ If you disable autonegotiation on a port, the auto-MDI/MDI-X feature on a port is also disabled, and the port defaults to the MDI-X configuration. Consequently, if you disable autonegotiation and set a port's speed and duplex mode manually, you might also need to set the port's MDI/MDI-X setting as well.

Auto-Negotiate: The port autonegotiates both speed (10/100/1000 Mbps) and duplex mode. This is the default.

The other possible settings are:

10Mbps - Half Duplex

10Mbps - Full Duplex

100Mbps - Half Duplex

100Mbps - Full Duplex

Note

When a transceiver is inserted into an uplink slot in an AT-9424 switch and a link is established, that slot becomes a primary uplink port and the corresponding backup port, 23R or 24R, automatically transitions to redundant uplink status. The speed and duplex mode of the redundant port automatically transitions to Auto-Negotiate to match the speed of the primary uplink port and you cannot configure the MDI/MDIX crossover parameter.

Note

1000 Mbps speed is only available when you set the port to autonegotiate. You cannot set this manually.

If you select all ports, the Speed and Duplex setting displays "Not Configurable," because all ports are set to autonegotiate.

MDI/MDIX Crossover

The wiring configuration of the port. The possible settings are:

Auto - The port automatically configures itself as MDI or MDIX, depending upon the end node. This is the default.

MDI - The port uses straight through cable.

MDIX - The port uses a crossover cable.

Note

Ports 23 and 24 on an AT-9424 switch are always set to Auto, and you cannot change the setting.

Note

The Auto setting is not available if you set a port's speed and duplex mode manually.

Ingress Broadcast Filter

Use this parameter to allow or disallow the port to receive ingress broadcast packets. The possible settings are:

Enabled - The port does not receive any broadcast packets.

Disabled - The port receives broadcast packets. This is the default setting.

Egress Broadcast Filter

Use this parameter to allow or disallow egress the port to send broadcast packets. The possible settings are:

Enabled - The port does not send any broadcast packets.

Disabled - The port sends broadcast packets. This is the default setting.

For further information about filters, refer to Chapter 6, "Port Parameters," in the *AT-S63 Management Software Menu Interface User's Guide*.

Ingress Unknown Unicast Filter

Use this parameter to allow or disallow the port to receive ingress unknown unicast packets. The possible settings are:

Enabled - The port does not receive any unknown unicast packets.

Disabled - The port receives unknown unicast packets. This is the default setting.

Egress Unknown Unicast Filter

Use this parameter to allow or disallow the port to send egress unknown unicast packets. The possible settings are:

Enabled - The port does not send any unknown unicast packets.

Disabled - The port sends unknown unicast packets. This is the default setting.

Ingress Unknown Multicast Filter

Use this parameter to allow or disallow the port to receive ingress unknown multicast packets. The possible settings are:

Enabled - The port does not receive any unknown multicast packets.

Disabled - The port receives unknown multicast packets. This is the default setting.

Egress Unknown Multicast Filter

Use this parameter to allow or disallow the port to send egress unknown multicast packets. The possible settings are:

Enabled - The port does not send any unknown multicast packets.

Disabled - The port sends unknown multicast packets. This is the default setting.

Flow Control

Sets flow control on a port. This option only applies to ports operating in full-duplex mode. A switch port uses back pressure to control the flow of ingress packets. The switch sends a special pause packet to stop the end node from sending frames. The pause packet notifies the

end node to stop transmitting for a specified period of time. The possible settings are:

Auto - The port uses flow control if it detects that the end node is using it.

Disabled - No flow control on the port. This is the default.

Enabled - Flow control is activated.

For further information about flow control, refer to Chapter 6, "Port Parameters," in the *AT-S63 Management Software Menus Interface User's Guide*.

Back Pressure

Use this parameter to set back pressure on a port. This option only appears for ports operating in half-duplex mode. A switch port uses back pressure to control the flow of ingress packets. The possible settings are:

Enabled - Back pressure is enabled.

Disabled - Back pressure is disabled. This is the default.

For further information about back pressure, refer to Chapter 6, "Port Parameters," in the *AT-S63 Management Software Menus Interface User's Guide*.

Flow Control/Back Pressure Limit

Use this parameter to specify the maximum number of ingress packets that a port receives within a one second period before initiating flow control or back pressure. A cell equals 128 bytes. The range is 1 to 7935. The default is 7935 cells.

The following three parameters allow you to set rate limiting, the maximum number of ingress packets a port accepts each second. Packets exceeding the threshold are discarded.

HOL Blocking

HOL blocking sets a threshold on the utilization of a port's egress queue. When the threshold for a port is exceeded, the switch signals other ports to discard packets to the oversubscribed port. The possible settings are:

Enabled - HOL blocking prevention is activated.

Disabled - HOL blocking is inactivated on this port.

You also set the rate limit in number of cells. A cell is 128 bytes. The range is 1 to 8191. The default is 682. For more information about HOL blocking, refer to Chapter 6, "Port Parameters," in the *AT-S63 Management Software Menus Interface User's Guide*.

Broadcast Rate Limiting

Use this parameter to enable or disable ingress broadcast packet limits. The possible settings are:

Enabled - Broadcast packet ingress rate limiting is enabled.

Disabled - Broadcast packet ingress rate limiting is disabled. This is the default.

Broadcast Rate

Use this parameter to set the broadcast rate limit in packets per second. The range is 0 to 262143. The default is 262143.

Unknown Unicast Rate Limiting

Use this parameter to enable or disable ingress unknown unicast packet limits. The possible settings are:

Enabled - Unknown unicast packet ingress rate limiting is enabled.

Disabled - Unknown unicast packet ingress rate limiting is disabled. This is the default.

Unknown Unicast Rate

Use this parameter to set the unknown unicast rate limit in packets per second. The range is 0 to 262143. The default is 262143.

Multicast Rate Limiting

Use this parameter to enable or disable ingress multicast packet limits. The possible settings are:

Enabled - Multicast packet ingress rate limiting is enabled.

Disabled - Multicast packet ingress rate limiting is disabled. This is the default.

Multicast Rate

Use this parameter to set the multicast rate limit in packets per second. The range is 0 to 262143. The default is 262143.

6. After you have made the desired changes, click **Apply**.

The switch activates the parameter changes on the port.

7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying Port Status

To display the status of a switch port, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Layer 1** option.

The Layer 1 page is displayed with the Port Settings tab selected by default, as shown in Figure 25.

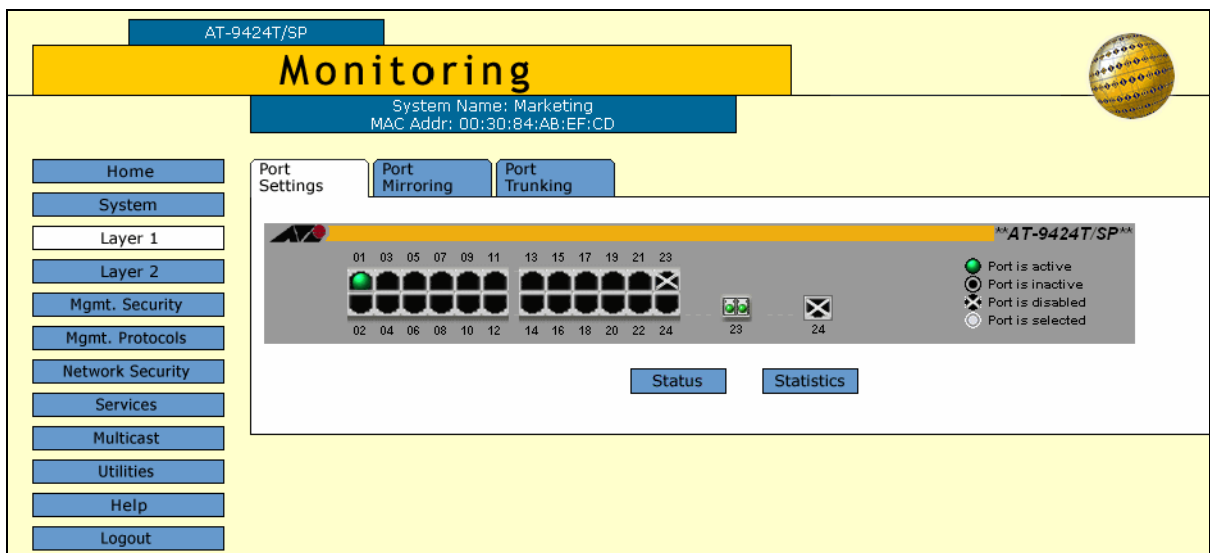


Figure 25. Port Settings Tab (Monitoring)

The Port Settings tab displays a graphical image of the front of the switch. Ports with valid links to end nodes have a green light.

3. Click a port. You can select more than one port at a time when you want to display port status. However, you can select only one port when displaying statistics. A selected port turns white. (To deselect a port, click it again.)
4. Click **Status**.

The Port Status page is shown in Figure 26.

Port Status - 3	
Name Port_03	Status Enabled
Vlan Id 1	Link Status Down
Speed and Duplex Auto	MDI/MDIX Crossover MDIX
Ingress Broadcast Filter Disabled	Egress Broadcast Filter Disabled
Ingress Unknown Unicast Filter Disabled	Egress Unknown Unicast Filter Disabled
Ingress Unknown Multicast Filter Disabled	Egress Unknown Multicast Filter Disabled
Flow Control Disabled	Back Pressure Disabled
Flow Control/Back Pressure Limit 7935	HOL Blocking 682
Broadcast Rate Limiting Disabled	Broadcast Rate 262143
Unknown Unicast Rate Limiting Disabled	Unknown Unicast Rate 262143
Multicast Rate Limiting Disabled	Multicast Rate 262143

Figure 26. Port Status Page

The Port Status page displays the following information:

Name

The name of the port.

Status

The status of the port, enabled or disabled.

VLAN ID

The VLAN identifier (VID) of the VLAN in which the port is an untagged member.

Link Status

The status of the link between the port and the end node connected to the port, up or down.

Speed and Duplex

The speed and duplex mode.

MDI/X Crossover

The operating configuration of the port. The possible settings are MDI and MDI-X.

Ingress Broadcast Filter

Status of the filter on ingress broadcast packets.

Ingress Unknown Unicast Filter

Status of the filter on ingress unknown unicast packets.

Ingress Unknown Multicast Filter

Status of the filter on ingress unknown multicast packets.

Flow Control

Status of flow control, enabled or disabled.

Flow Control/Back Pressure Limit

The flow control/back pressure limit.

Broadcast Rate Limiting

The status of rate limiting on broadcast packets.

Unknown Unicast Rate Limiting

The status of rate limiting on broadcast packets.

Multicast Rate Limiting

The status of rate limiting on broadcast packets.

Status

The overall status of the port, enabled or disabled.

Egress Broadcast Filter

The status of the filter on egress broadcast packets.

Egress Unknown Unicast Filter

The status of the filter on egress unknown unicast packets.

Egress Unknown Multicast Filter

The status of the filter on egress unknown multicast packets.

Back Pressure

The status of back pressure on the port, enabled or disabled.

Flow Control/Back Pressure Limit

The flow control and back pressure limit.

HOL Blocking

The Head of Line Blocking setting.

Broadcast Rate Limiting

The status of broadcast rate limiting, enabled or disabled.

Broadcast Rate

The rate on broadcast packets.

Unknown Unicast Rate Limiting

The status of unknown unicast rate limiting, enabled or disabled.

Unknown Unicast Rate

The rate on unknown unicast packets.

Multicast Rate Limiting

The status of multicast rate limiting, enabled or disabled.

Multicast Rate

The rate on multicast packets.

Displaying Port Statistics

To display the statistics of a switch port, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Layer 1** option.

The Layer 1 page is displayed with the Port Settings tab selected by default, as shown in Figure 25 on page 85

The Port Setting tab displays a graphical image of the front of the switch. Ports with valid links to end nodes have a green light.

3. Click a port. You can select more than one port at a time when you want to display port status. However, you can select only one port when displaying statistics. A selected port turns white. (To deselect a port, click it again.)
4. Click **Statistics**.

The Port Statistics page is shown in Figure 27.

The screenshot shows a web browser window titled "Port Statistics - 1". Inside the window, there is a table with the following data:

Current Port: 1. Total Ports Selected: 1. Page 1 of 1			
Bytes Received	62591	Bytes Sent	244962
Frames Received	571	Frames Sent	292
Broadcast Frames Received	358	Broadcast Frames Sent	4
Multicast Frames Received	45	Multicast Frames Sent	72
Frames 64 Bytes	211	Frames 65-127 Byte	348
Frames 128-255 Bytes	105	Frames 256-511 Bytes	33
Frames 512-1023 Bytes	19	Frames 1024-1518 Bytes	147
Frames 1519-1522 Bytes	0	Dropped Frames	0
CRC Error	6	Jabber	0
No. of Rx Errors	6	No. of Tx Errors	0
UnderSize Frames	0	OverSize Frames	0
Fragments	0	TX Collisions	0

At the bottom of the table, there are five buttons: Refresh, Clear, Clear All, Status, and Close.

Figure 27. Port Statistics Page

The Port Statistics page displays a table that contains the following columns of information:

Bytes Received

Number of bytes received on the port.

Bytes Sent

Number of bytes transmitted from the port.

Frames Received

Number of frames received on the port.

Frames Sent

Number of frames transmitted from the port.

Broadcast Frames Received

Number of broadcast frames received on the port.

Broadcast Frames Sent

Number of broadcast frames transmitted from the port.

Multicast Frames Received

Number of multicast frames received on the port.

Multicast Frames Sent

Number of multicast frames transmitted from the port.

Frames 64 Bytes

Frames 65 - 127 Bytes

Frames 128 - 255 Bytes

Frames 256 - 511 Bytes

Frames 512 - 1023 Bytes

Frames 1024 - 1518 Bytes

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 on the port.

Jabber

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

No. of Rx Errors

Total number of frames received on the port containing errors.

Undersize Frames

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

Oversize Frames

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

Fragments

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

TXCollisions

Number of transmit collisions.

5. To clear all the counters for the selected port, click **Clear**. To clear the counters for all ports on the switch, click **Clear All**.

Resetting a Port to the Default Settings

To reset a port to the default settings, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 1** option.

The Layer 1 page is displayed with the Port Settings tab selected by default, as shown in Figure 23 on page 78.

3. Click the port in the graphical switch image that you want to configure. The selected port turns white. You can select more than one port at a time to configure. (To deselect a port, click it again.)

4. Click **Modify**. To configure all of the ports, click **Modify All**.

The Port Configuration page is displayed, as shown Figure 24 on page 79.

5. Click **Defaults**.

The port(s) are returned to the default settings listed in Appendix A, "AT-S63 Default Settings" on page 439.

Chapter 7

Port Trunking

This chapter contains the procedure for creating, modifying, or deleting a port trunk. The sections in this chapter are:

- “Creating a Port Trunk” on page 94
- “Modifying a Port Trunk” on page 97
- “Deleting a Port Trunk” on page 99
- “Displaying the Port Trunks” on page 100

Note

For background information on port trunking, refer to Chapter 7, “Static and LACP Port Trunks,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Creating a Port Trunk



Caution

Do not connect the cables of a port trunk to the ports on the switch until after you have configured the ports on both the switch and the end node. Connecting the cables prior to configuring the ports can create loops in your network topology. Loops can result in broadcast storms, which can adversely effect the operation of your network.

If you are deleting a port trunk, disconnect the cables from the ports before you delete the trunk. Deleting the trunk without first disconnecting the data cables can create a loop in your network topology, which can result in broadcast storms.

To create a port trunk, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 1** option.

The Layer 1 page opens with the Port Settings tab displayed by default, as shown in Figure 23 on page 78.

3. Select the **Port Trunking** tab.

The Port Trunking tab is shown in Figure 28 and displays any existing trunks in a table.

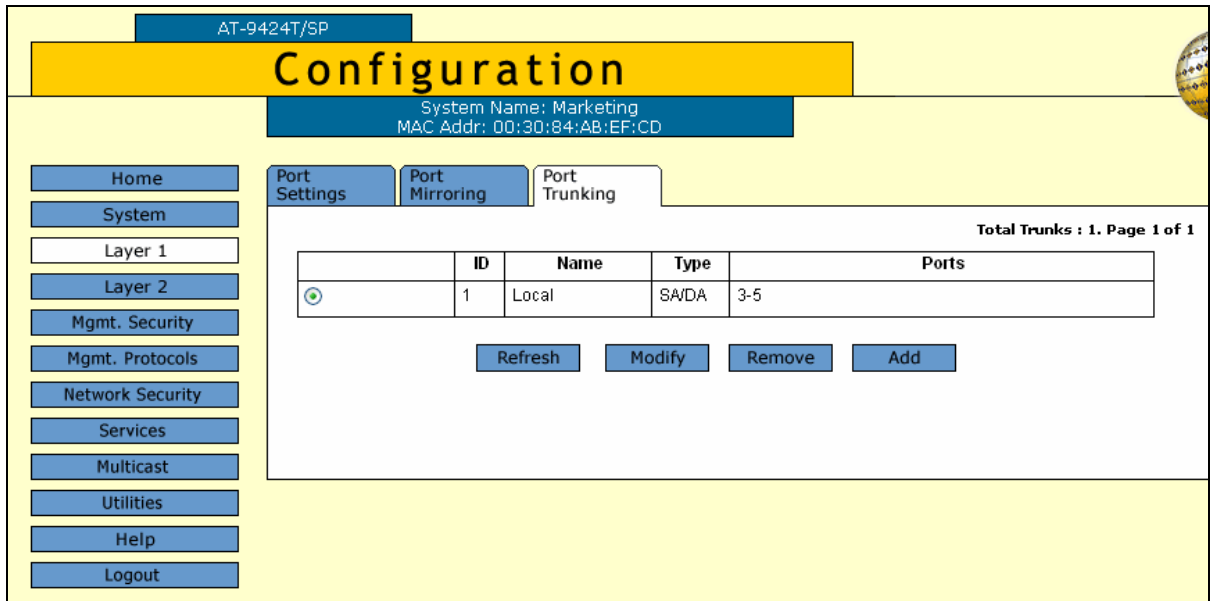


Figure 28. Port Trunking Tab (Configuration)

4. Click **Add**.

The Add New Trunk page is shown in Figure 29.

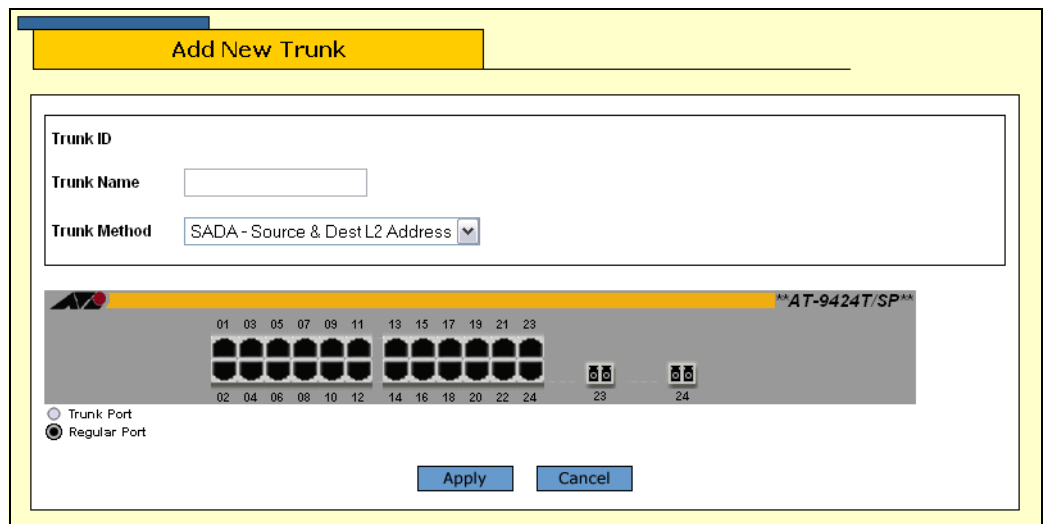


Figure 29. Add New Trunk Page

5. Configure the following parameters as necessary.

Trunk Name

The name for the port trunk. The name can be up to 16 alphanumeric characters. No spaces or special characters, such as asterisks and

exclamation points, are allowed. Each trunk must be given a unique name.

Trunk Method

Select a load distribution method. The possible settings are:

SA - Source MAC address (Layer 2)

DA - Destination MAC address (Layer 2)

SA/DA - Source MAC address /destination MAC address (Layer 2)

SI - Source IP address (Layer 3)

DI - Destination IP address (Layer 3)

SI/DI - Source IP address /destination IP address (Layer 3)

6. Click the ports that are to make up the port trunk. A selected port changes to white. An unselected port is black. A port trunk can contain up to eight ports.

Note

All ports in a trunk must operate at the same speed. When you include port 23R or 24R on an AT-9424 switch in a trunk and the port transitions to redundant uplink status, the port speed is automatically adjusted to 1000 Mbps. If the other ports in the trunk are operating at a different speed, port trunking may be unpredictable. Because of these port speed variables, Allied Telesyn suggests that you not include port 23R or 24R in a port trunk.

7. Click **Apply**.

The new port trunk is now active on the switch.

8. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)
9. Configure the ports on the remote switch for port trunking.
10. Connect the cables to the ports of the trunk on the switch.

The port trunk is ready for network operations.

Modifying a Port Trunk

This section contains the procedure for modifying a port trunk on the switch. You can change the name of a trunk and the ports that constitute the trunk. You cannot change the load distribute method. Be sure to review the guidelines in Chapter 7, "Static and Dynamic Port Trunking," in the *AT-S63 Management Software Menus Interface User's Guide* before you perform the procedure:



Caution

If you are adding or removing ports from the trunk, you should disconnect all data cables from the ports of the trunk on the switch before performing the procedure. Adding or removing ports from a port trunk without first disconnecting the cables may result in loops in your network topology. Loops can produce broadcast storms and poor network performance.

Note

Before you modify a port trunk, examine the speed, duplex mode, and flow control settings of the lowest numbered port that are to be in the trunk. Check to be sure that the settings are correct for the end node to which the trunk is to be connected. When you modify a 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.

To modify a port trunk, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 1** option.

The Layer 1 page opens with the Port Settings tab displayed by default, as shown in Figure 18 on page 74.

3. Select the **Port Trunking** tab.

The Port Trunking tab is shown in Figure 28 on page 95.

- Click the button next to the port trunk you want to modify and click **Modify**.

The Modify Trunk page is shown in Figure 30.

Figure 30. Modify Trunk Page

Note

You cannot change the Trunk ID number or the load distribution method of a port trunk.

- Configure the following parameter as necessary.

Trunk Name

The name can be up to 16 alphanumeric characters. No spaces or special characters, such as asterisks and exclamation points, are allowed. Each trunk must have a unique name.

- To add or remove ports from a trunk, click the ports in the graphical image of the switch. A selected port changes to white. An unselected port is black. A port trunk can contain up to eight ports.
- Click **Apply**.
Changes to a port trunk are activated on the switch.
- From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)
- Reconnect the cables to the ports of the trunk.

Deleting a Port Trunk



Caution

Disconnect the cables from the port trunk on the switch before performing the following procedure. 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.

To delete a port trunk from the switch, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 1** option.

The Layer 1 page opens with the Port Settings tab displayed by default, as shown in Figure 18 on page 74.

3. Select the **Port Trunking** tab.

The Port Trunking tab is shown in Figure 28 on page 95.

4. Click the button next to the port trunk you want to delete and click **Remove**.

The port trunk is deleted from the switch.

5. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying the Port Trunks

To display the port trunks, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Layer 1** option.

The Layer 1 page is displayed with the Port Settings tab selected by default, as shown in Figure 25 on page 85.

3. Select the **Port Trunking** tab.

The Port Trunking tab is shown in Figure 31.

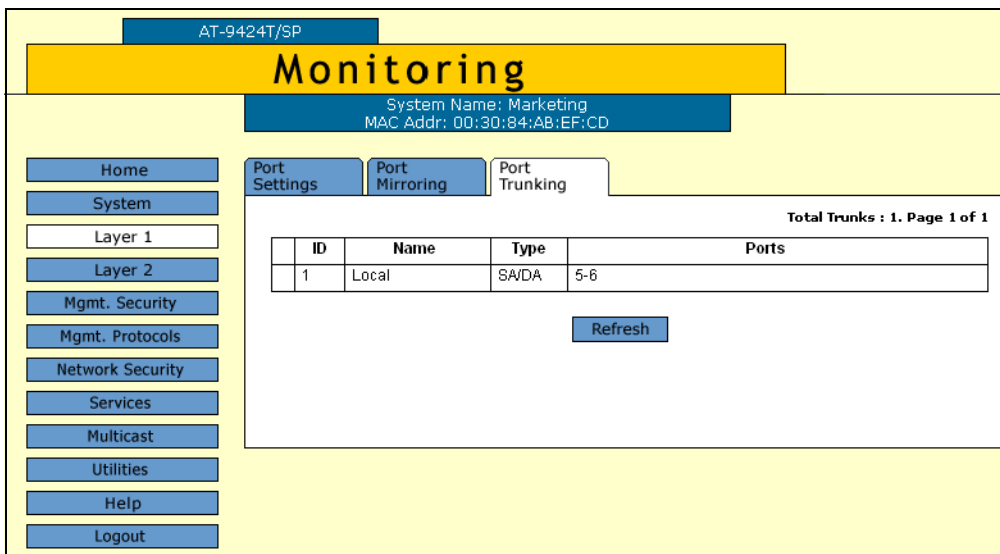


Figure 31. Port Trunking Tab (Monitoring)

The Port Trunking tab displays a table that contains the following columns of information:

ID

The ID number of the trunk.

Name

The name of the trunk.

Type

The load distribution method. The possible settings are:

SA - Source MAC address (Layer 2)

DA - Destination MAC address (Layer 2)

SA/DA - Source MAC address /destination MAC address (Layer 2)

SI - Source IP address (Layer 3)

DI - Destination IP address (Layer 3)

SI/DI - Source IP address /destination IP address (Layer 3)

Ports

The ports of the trunk.

Chapter 8

Port Mirroring

This chapter contains the procedures for creating or deleting a port mirror. The sections in the chapter include:

- ❑ “Creating a Port Mirror” on page 104
- ❑ “Modifying a Port Mirror” on page 107
- ❑ “Disabling a Port Mirror” on page 108
- ❑ “Deleting a Port Mirror” on page 109
- ❑ “Displaying the Port Mirror” on page 110

Note

For background information on port mirroring, refer to Chapter 8, “Port Mirroring,” in the *AT-S63 Management Software Menu Interface User’s Guide*.

Creating a Port Mirror

To create a port mirror, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 1** option.

The Layer 1 page opens with the Port Settings tab displayed by default, as shown in Figure 23 on page 78.

3. Select the **Port Mirroring** tab.

The Port Mirroring tab is shown in Figure 32 with any configured mirror.

AT-9424T/SP

Configuration

System Name: Marketing
MAC Addr: 00:30:84:AB:EF:CD

Port Settings | **Port Mirroring** | Port Trunking

Total Mirrors: 1. Page 1 of 1

	Mirror to Port	Ingress Port(s)	Egress Port(s)	Status
<input checked="" type="checkbox"/>	14	7-8	11	Enabled

Refresh Modify

Home
System
Layer 1
Layer 2
Mgmt. Security
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Help
Logout

Figure 32. Port Mirroring Tab (Configuration)

This tab displays any port mirror already existing on the switch. If the Mirror to Port column contains a 0 (zero), there is no port mirror.

4. Click **Modify**.

The Modify Mirror page is shown in Figure 33.

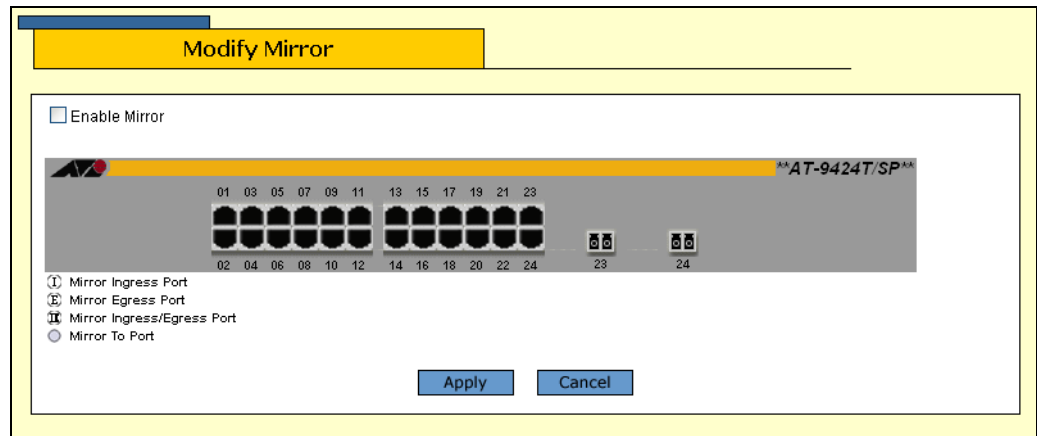


Figure 33. Modify Mirror Page

- Click the ports of the port mirror. Clicking a port toggles it through the possible settings, which are as follows:



The destination (mirror) port. There can be only one destination port.



A source port. The port's ingress traffic is mirrored to the destination port.



A source port. The port's egress traffic is mirrored to the destination port.



A source port. The port's ingress and egress traffic is mirrored to the destination port.

You can mirror just one port, a few ports, or all of the ports on the switch, with the exception, of course, of the destination port.

Note

When a transceiver is inserted into an uplink slot and a link is established, that slot becomes a primary uplink port and the corresponding backup port on an AT-9424 switch, 23R or 24R, automatically transitions to redundant uplink status. Any settings for port mirroring remain intact when the backup port makes the transition to a redundant uplink state.

Figure 34 shows an example of the Modify Mirror page configured for a port mirror. The egress traffic on ports 11 and 12 is being mirrored to the destination port 5.

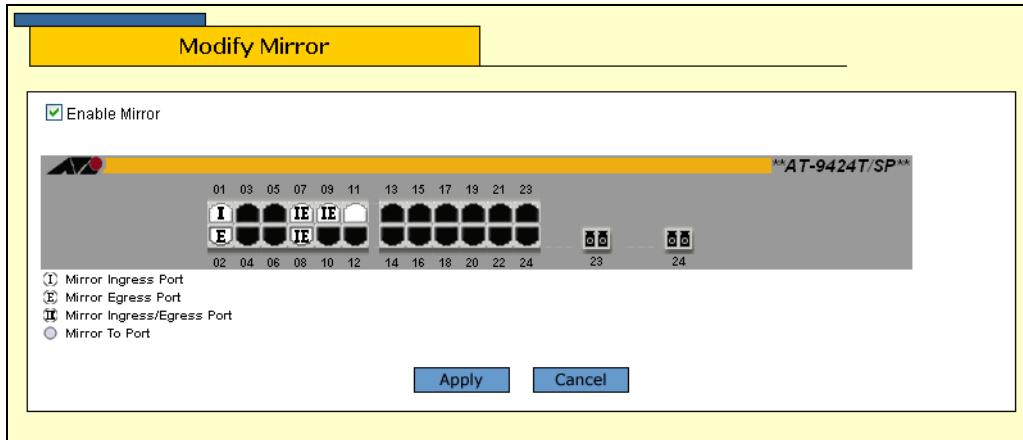


Figure 34. Example of a Modify Mirror Page

6. After selecting the destination and source ports, click the **Enable Mirror** check box.
7. Click **Apply**.

The port mirror is now active on the switch. You can connect a data analyzer to the destination port to monitor the traffic on the source ports.

8. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Modifying a Port Mirror

To modify a port mirror, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 1** option.

The Layer 1 page opens with the Port Settings tab displayed by default, as shown in Figure 18 on page 74.

3. Select the **Port Mirroring** tab.

The Port Mirroring tab is shown in Figure 32 on page 104.

4. Click **Modify**.

The Modify Mirror page is shown in Figure 33 on page 105.

5. Click the ports of the port mirror to change its type. Clicking a port toggles it through the possible settings, which are as follows:



The destination (mirror) port. There can be only one destination port.



A source port. The port's ingress traffic is mirrored to the destination port.



A source port. The port's egress traffic is mirrored to the destination port.



A source port. The port's ingress and egress traffic is mirrored to the destination port.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Disabling a Port Mirror

To disable a port mirror, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 1** option.

The Layer 1 page opens with the Port Settings tab displayed by default, as shown in Figure 18 on page 74.

3. Select the **Port Mirroring** tab.

The Port Mirroring tab is shown in Figure 32 on page 104.

4. Click **Modify**.

The Modify Mirror page is shown in Figure 33 on page 105.

5. Click the **Enable Mirror** checkbox to remove the check and disable the mirror.

6. Click **Apply**.

7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting a Port Mirror

To delete a port mirror, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 1** option.

The Layer 1 page opens with the Port Settings tab displayed by default, as shown in Figure 18 on page 74.

3. Select the **Port Mirroring** tab.

The Port Mirroring tab is shown in Figure 32 on page 104.

4. Click **Modify**.

The Modify Mirror page is shown in Figure 33 on page 105.

5. Click the **Enable Mirror** checkbox to remove the check and disable the mirror.

6. Click **Apply**.

7. Click the destination port, which is white, so that it is black.

8. Click **Apply**.

9. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying the Port Mirror

To display the port mirror, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Layer 1** option.

The Layer 1 page is displayed with the Port Settings tab selected by default, as shown in Figure 25 on page 85.

3. Select the **Port Mirroring** tab.

The Port Mirroring tab is shown in Figure 35.

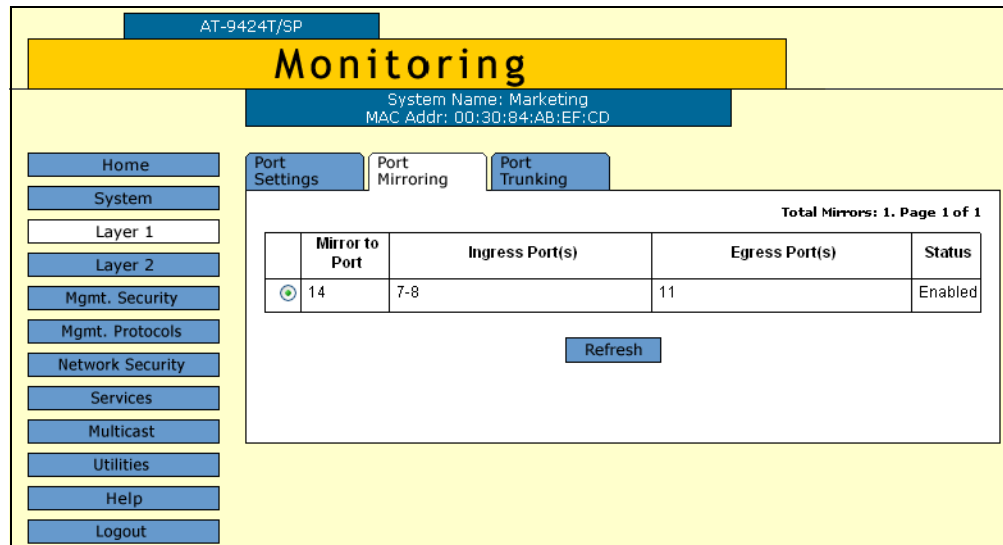


Figure 35. Port Mirroring Tab (Monitoring)

The Port Mirroring tab displays a table that contains the following columns of information:

Mirror to Port

The destination port to which the traffic is copied and where the network analyzer is located.

Ingress Port(s)

The source ports whose ingress traffic is mirrored to the destination port.

Egress Port(s)

The source ports whose egress traffic is mirrored to the destination port.

Status

The status of the mirroring feature. The possible settings are:

Enabled - Traffic is being copied to the destination port.

Disabled - No traffic is being mirrored.

Section II

Advanced Operations

The chapters in this section provide information and procedures for advanced switch setup using the AT-S63 management software. The chapters include:

- ❑ Chapter 9, “File System” on page 115
- ❑ Chapter 10, “File Downloads and Uploads” on page 121
- ❑ Chapter 11, “Event Log” on page 127
- ❑ Chapter 12, “Classifiers” on page 145
- ❑ Chapter 13, “Access Control Lists” on page 155
- ❑ Chapter 14, “Denial of Service Defense” on page 163
- ❑ Chapter 15, “Quality of Service” on page 169
- ❑ Chapter 16, “Class of Service” on page 191
- ❑ Chapter 17, “IGMP Snooping” on page 203

Chapter 9

File System

This chapter contains procedures for working with the file system and contains the following sections:

- ❑ “Listing the Files in Flash Memory” on page 116
- ❑ “Listing Files on the Compact Flash Card” on page 118

Listing the Files in Flash Memory

To display a list of the system files stored in flash memory as well as on a compact flash card (if the switch supports this and a compact flash card is inserted in the slot), perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Utilities** option.

The Utilities page is displayed with the System Utilities tab displayed by default, as shown in Figure 9 on page 52.

3. Select the **File System** tab.

The File System tab for an AT-9400 Series switch without a flash memory card drive is shown in Figure 36.

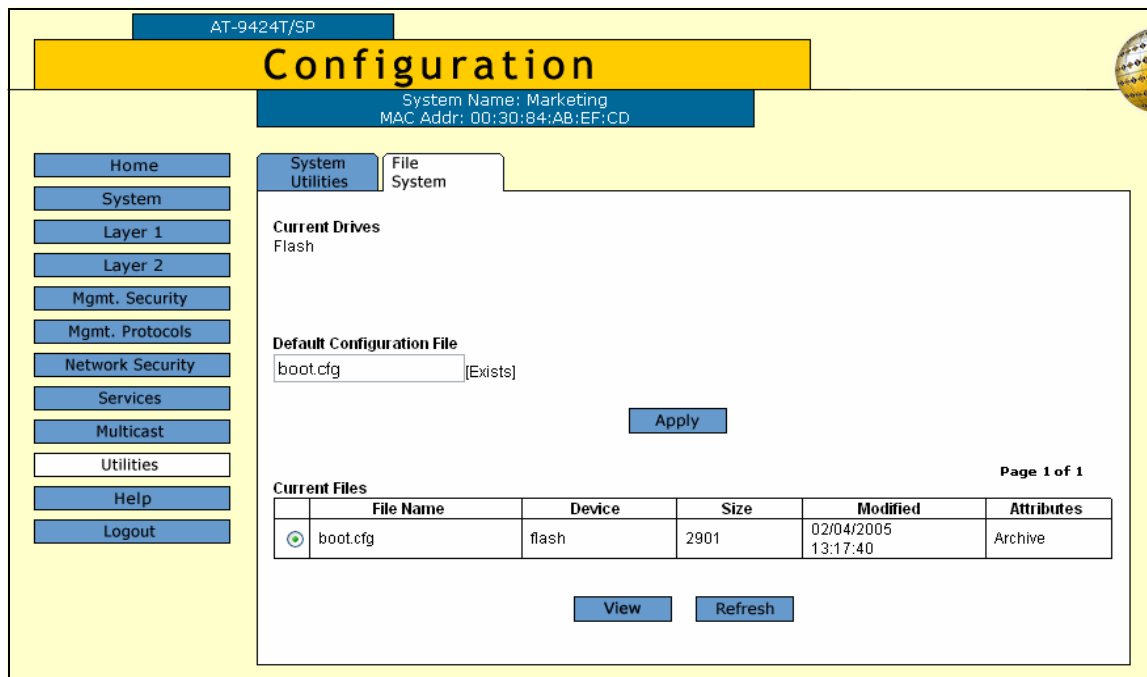


Figure 36. File System Tab (Configuration)

The columns in the List Files table are described below. This information is for viewing purposes only.

File Name

Name of the system file.

Device

The device type, either “flash” for flash memory or “cflash” for compact flash card.

Size

Size of the file, in bytes.

Modified

The time the file was created or last modified, in the following date and time format: month/day/year hours:minutes:seconds.

Attributes

The file type, one of the following:

- Normal
- Read Only
- Hidden
- System
- Volume
- Directory
- Archive
- Invalid

4. In the Current Files section, click a file and click **View**.

The Viewing File page for a portion of a configuration file is shown in Figure 37.

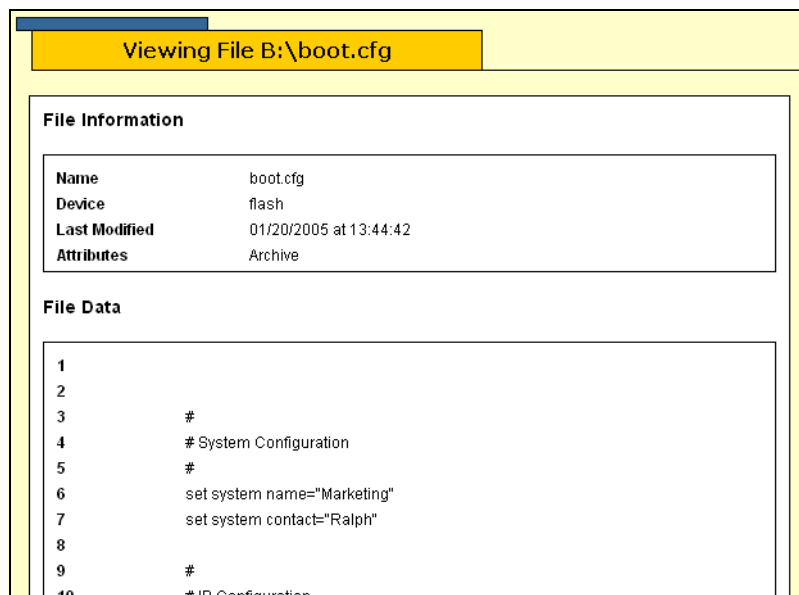


Figure 37. List Files Page

Listing Files on the Compact Flash Card

To view the files on the compact flash card, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Utilities** option.

The Utilities page is displayed with the System Utilities tab displayed by default, as shown in Figure 9 on page 52.

3. Select the **File System** tab.

The File System tab for an AT-9400 series switch with a compact flash card is shown in Figure 38.

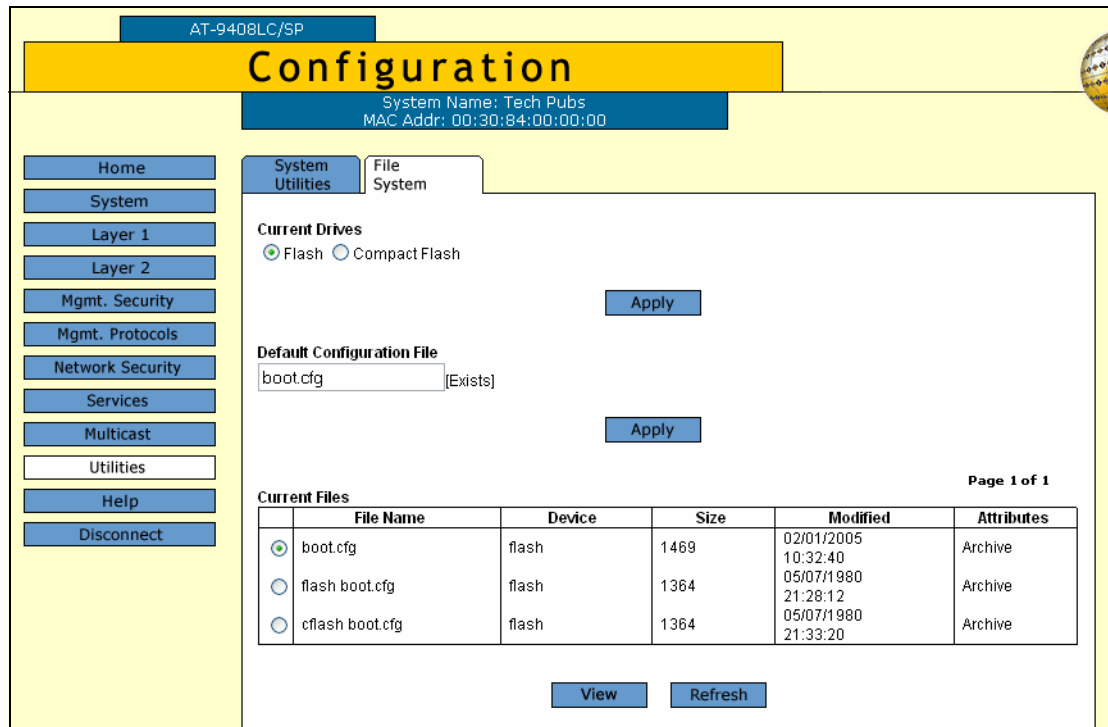


Figure 38. File System Tab (Configuration) with Compact Flash

4. In the Current Drives section, click **Compact Flash** and click **Apply**.

The system displays files on the compact flash card, as shown in Figure 39.

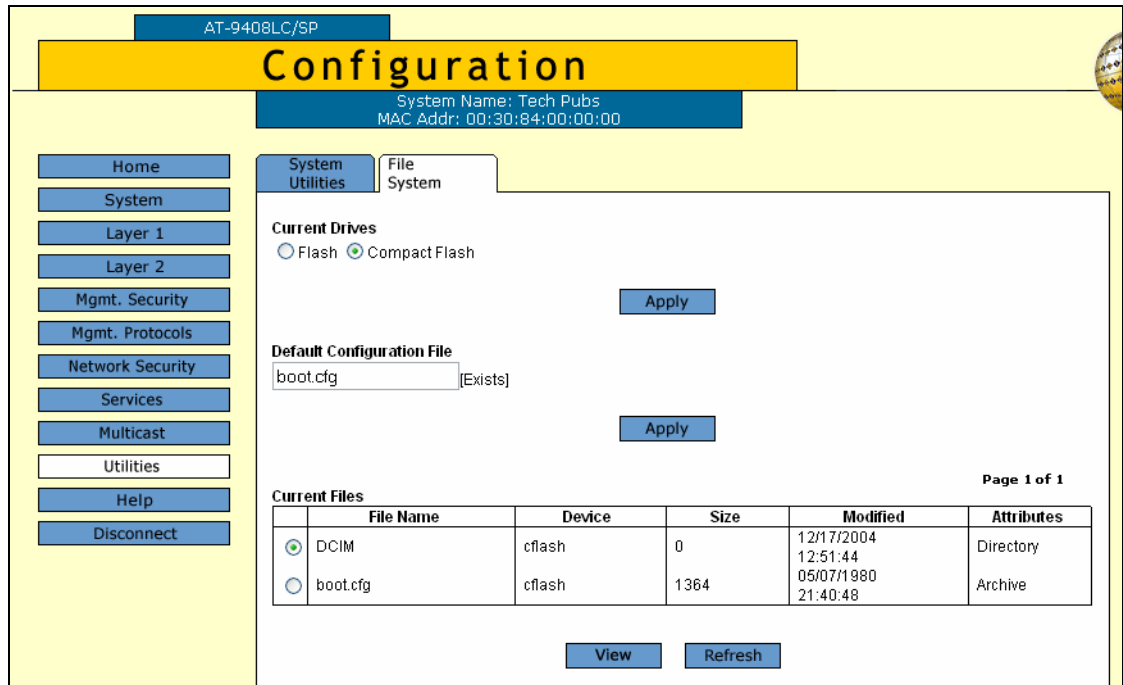


Figure 39. List Files Menu for a Compact Flash Card

The columns in the List Files table are described below. This information is for viewing purposes only.

File Name

Name of the system file.

Device

The device type, either “flash” for flash memory or “cflash” for compact flash card.

Size

Size of the file, in bytes.

Modified

The time the file was created or last modified, in the following date and time format: month/day/year hours:minutes:seconds.

Attributes

The file type, one of the following:

- Normal
- Read Only
- Hidden
- System
- Volume

- Directory
- Archive
- Invalid

5. In the Current Files section, click a file and click **View**.

The Viewing File page for that file is displayed. An example is shown in Figure 37 on page 117.

Chapter 10

File Downloads and Uploads

This chapter contains the procedure for downloading a new AT-S63 image file onto the switch. This chapter also contains procedures for uploading and downloading system files, such as a boot configuration file, from the file system in the switch. This chapter contains the following sections:

- ❑ “Downloading a File” on page 122
- ❑ “Uploading a File” on page 125

Downloading a File

This procedure explains how to download a file from a TFTP server on your network to the switch using the web browser interface. You can download any of the following files:

- AT-S63 image file
- Boot configuration file
- Public key
- CA certificate

Note

The public key and CA certificate are supported only on the version of AT-S63 management software that features SSL, PKI, and SSH security.

Note the following before you begin this procedure:

- You must use TFTP to upload a file from a web browser management session.
- To use TFTP, there must be a node on your network that contains the TFTP server software.
- The file that you are downloading must be stored on the TFTP server node.
- You should start the TFTP server before you begin the download procedure:
- The AT-S63 image file contains the bootloader for the switch. You cannot load the image file and bootloader separately.
- Installing a new AT-S63 software image does not change the current configuration of a switch (for instance, IP address, subnet mask, and virtual LANs). If you want to return a switch to its default configuration values, refer to “Returning the AT-S63 Management Software to the Factory Default Values” on page 50.

**Caution**

The switch stops forwarding Ethernet traffic after it has downloaded an AT-S63 image file and begun to initialize the software. Some network traffic may be lost.

To download a file, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Utilities** option.

The Utilities page is displayed with the System Utilities tab displayed by default, as shown in Figure 9 on page 52.

Note

You use the top portion of the System Utilities tab to return the switch to its factory default settings. For instructions, refer to “Returning the AT-S63 Management Software to the Factory Default Values” on page 50.

3. In the TFTP File Uploads and Downloads section, in the TFTP Server IP Address field, enter the IP address of the network node that contains the TFTP server software.
4. For TFTP Operation parameter, click **Download**.
5. In the TFTP Remote Filename field, enter the filename of the file on the TFTP server to be downloaded to the switch.
6. In the TFTP Local Filename field, enter a name for the file. This is the name that the switch uses to store the file in its file system. If you are downloading the AT-S63 image file, enter “ats63.img” as the filename.
7. For the TFTP File Type, select one of the following:

Image

Select this option if you are downloading the AT-S63 image file.

Config

Select this option if you are downloading a configuration file and you want the file to be designated as the active boot configuration file.

File

Select this option if you are downloading a CA certificate or encryption key, or a configuration file that you do not want designated as the active boot configuration file.

8. Click **Apply**.

The management software notifies you after the download is complete.



Caution

After an AT-S63 switch image file is downloaded, the switch must decompress it and write it to flash memory. This can require one to two minutes to complete. Do not reset or power off the unit while it is decompressing the file. After the file has been decompressed, the

switch automatically resets. Your web browser management session ends. To continue managing the switch, you must reestablish the management session.

Uploading a File

This procedure explains how to upload a file from the switch's file system to a TFTP server on your network using the web browser interface. You can upload any of the following files:

- Boot configuration file
- Public encryption key
- CA certificate
- CA enrollment request

Note

The public key, CA certificate, and CA enrollment request are supported only on the version of AT-S63 management software that features SSL, PKI, and SSH security.

Note the following before you begin this procedure:

- You must use TFTP to download a file from a web browser management session.
- There must be a node on your network that contains the TFTP server software.
- You should start the TFTP server before you begin the upload procedure:

To upload a file, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Utilities** option.

The Utilities page is displayed with the System Utilities tab displayed by default, as shown in Figure 9 on page 52.

Note

The top portion of the tab is used to return the switch to its factory default settings. For instructions, refer to "Returning the AT-S63 Management Software to the Factory Default Values" on page 50.

3. In the TFTP File Uploads and Downloads section, in the TFTP Server IP Address field, enter the IP address of the network node that contains the TFTP server software.
4. For the TFTP Operation parameter, click **Upload**.
5. In the TFTP Remote Filename field, enter a name for the file. This is the name that the file is stored as on the TFTP server.
6. In the TFTP Local Filename field, enter the name of the file in the switch's file system that you want to upload to the TFTP server.

Note

The TFTP File Type options are not used when uploading a file.

7. Click **Apply**.

The management software notifies you when the upload is complete.

Chapter 11

Event Log

This chapter describes the event log that allows you to view information about network activity. Sections in the chapter include:

- “Working with the Event Log” on page 128
- “Working with Log Outputs” on page 138

For more information about the event log and log outputs, refer to Chapter 12, “Event Log,” in the *AT-S63 Management Software Menu Interface User’s Guide*.

Note

The event log, even when disabled, logs all AT-S63 initialization events that occur when the switch is reset or power cycled. Any switch events that occur after AT-S63 initialization are entered into the log only if you enable the event log. The default setting for the event log is disabled.

Working with the Event Log

This section includes the following topics:

- “Enabling or Disabling the Event Log,” next
- “Displaying Events” on page 130
- “Disabling the Event Log” on page 136
- “Clearing the Event Log” on page 136
- “Saving the Event Log to a File” on page 136

Enabling or Disabling the Event Log

To enable or disable the event log, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **Event Log** tab.

The Event log tab is shown in Figure 40.

AT-9424T/SP

Configuration

System Name: Marketing
MAC Addr: 00:30:84:AB:EF:CD

Home
System
Layer 1
Layer 2
Mgmt. Security
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Help
Logout

General | **Event Log** | System Time

Log Settings

Status <input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	Clear Log <input type="checkbox"/> Clear Log <input type="radio"/> Permanent <input checked="" type="radio"/> Temporary
---	---

Apply

Page 1 of 1

Configure Log Outputs

ID	Type	Status	Details
<input checked="" type="radio"/> 0	Permanent	Enabled	Wrap on Full
<input type="radio"/> 1	Temporary	Enabled	Wrap on Full
<input type="radio"/> 3	Syslog	Enabled	149.35.8.45
<input type="radio"/> 5	Syslog	Disabled	0.0.0.0

Display Filter Settings

Log Location <input checked="" type="radio"/> Temporary (RAM) <input type="radio"/> Permanent(NVS)	Mode <input checked="" type="radio"/> Normal <input type="radio"/> Full
Severity Selections D-Debug E-Error W-Warning I-Information	Module Selections SYSTEM CLI EVTLOG MAC
Display Order <input checked="" type="radio"/> Chronological <input type="radio"/> Reverse Chronological	Save Filename <input type="text"/>

Figure 40. Event Log Tab (Configuration)

- In the Log Settings section, for the Status, click **Enabled** to enable the event log, or **Disabled** to disable the event log.

The event log is enabled by default.

- Click **Apply** to activate the settings on the switch.
- Select the **General** tab.
- From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying Events

Each time that you want to view the event log, you must choose how and what you want displayed. The event log settings are not saved.

To specify the type of events you want to display in the event log, perform the following procedure:

1. From the home page, select **Monitoring**.

The System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

Note

You can also display events by selecting Configuration from the home page and then the Event Log tab. The tab contains the same Filter Settings and Actions section as described in this procedure:

2. Select the **Event Log** tab.

The Event log tab is shown in Figure 41.

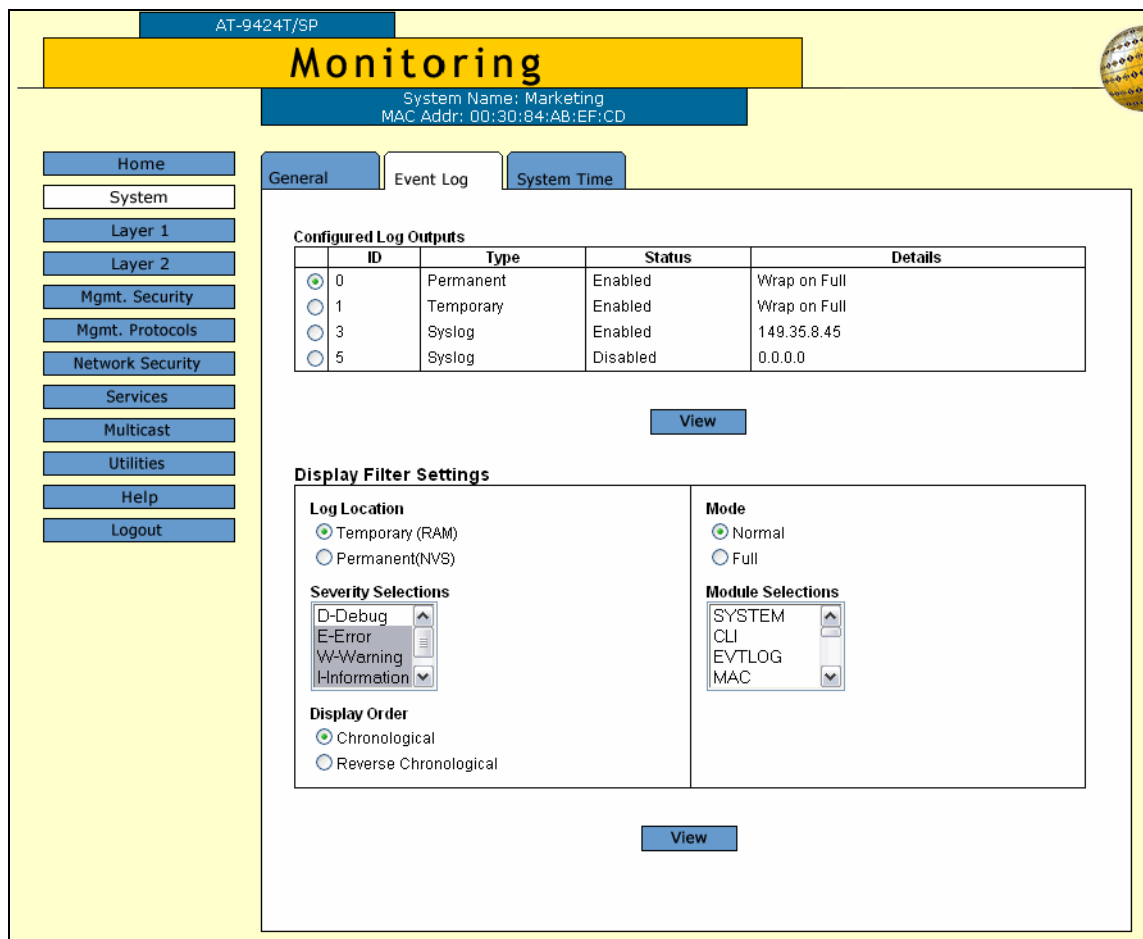


Figure 41. Event Log Tab (Monitoring)

3. In the Display Filter Settings section, for **Log Location**, click one of the following:

Temporary (Memory)

Displays the events stored in temporary memory. This selection stores approximately 4,000 events. If the switch has been running for some time without a reset or power cycle, select Temporary. This is the default.

Permanent (NVS)

Displays events stored in nonvolatile memory, which stores no more than 2,000 events. If the switch was recently reset or power cycled and you want to view the events that occurred prior to the reset, select Permanent.

4. To display events of a selected severity, in the **Severity Selections** list, select one or more of the following severity types:

D - Debug

Debug messages provide detailed high-volume information that is intended only for technical support personnel.

E - Error

Only error messages are displayed. Error messages indicate that the switch operation is severely impaired.

W - Warning

Only warning messages are displayed. These messages indicate that an issue may require manager attention.

I - Information

Only informational messages are displayed. Informational messages display useful information that you can ignore during normal operation.

ALL

All messages of any type are displayed.

To select more than one severity, use <Ctrl> click.

5. To choose the chronological order of events in the display, for **Display Order**, click one of the following:

Chronological

Displays the events in the order from the oldest event to the most recent event. This is the default.

Reverse Chronological

Displays the events in from the most recent event to the oldest event.

6. To select the format of the event log, for **Mode**, click one of the following:

Normal

Displays the time, module, severity, and description for each event. This is the default. An example of Normal mode is shown in Figure 42 on page 134.

Full

Displays the same information as Normal, plus the file name, line number, and event ID. An example of Full mode is shown in Figure 43 on page 135.

- To display events of a particular AT-S63 software module, from the **Module Selections** list, select one or more of the modules listed in Table 1. To select more than one module, use <Ctrl> click.

Table 1. AT-S63 Software Modules

Name	Description
ACL	Access control lists
ALL	All modules
CFG	Configuration file
CLI	Command line interface commands
DOS	Denial of Service defense
ENCO	Encryption keys
ESTACK	Enhanced stacking
EVTLOG	Event log
FILE	File system
GARP	GARP VLAN Registration Protocol
HTTP	Web server
IGMPSNOOP	IGMP snooping
IP	IP configuration
MAC	MAC address table
MGMTACL	Management ACL
PACCESS	802.1X Port-based Access Control
PCFG	Port configuration
PKI	Public Key Infrastructure
PMIRR	Port mirroring
PSEC	Port security

Table 1. AT-S63 Software Modules (Continued)

Name	Description
PTRUNK	Port trunking
QOS	Quality of Service
RADIUS	RADIUS authentication protocol
RRP	RRP Snooping
SNMP	Simple Network Management Protocol
SSH	Secure Shell protocol
SSL	Secure Sockets Layer protocol
STP	Spanning Tree, Rapid Spanning Tree, and Multiple Spanning Tree protocols
SYSTEM	Hardware status; Manager and Operator log in and log off events.
TACACS	TACACS+ authentication protocol
TELNET	TELNET
TFTP	Trivial File Transfer Protocol
TIME	System Time and SNTP
VLAN	Port-based and tagged VLANs, and multiple VLAN modes

8. Click **View**.

Figure 42 shows an example of an event log in Normal mode.

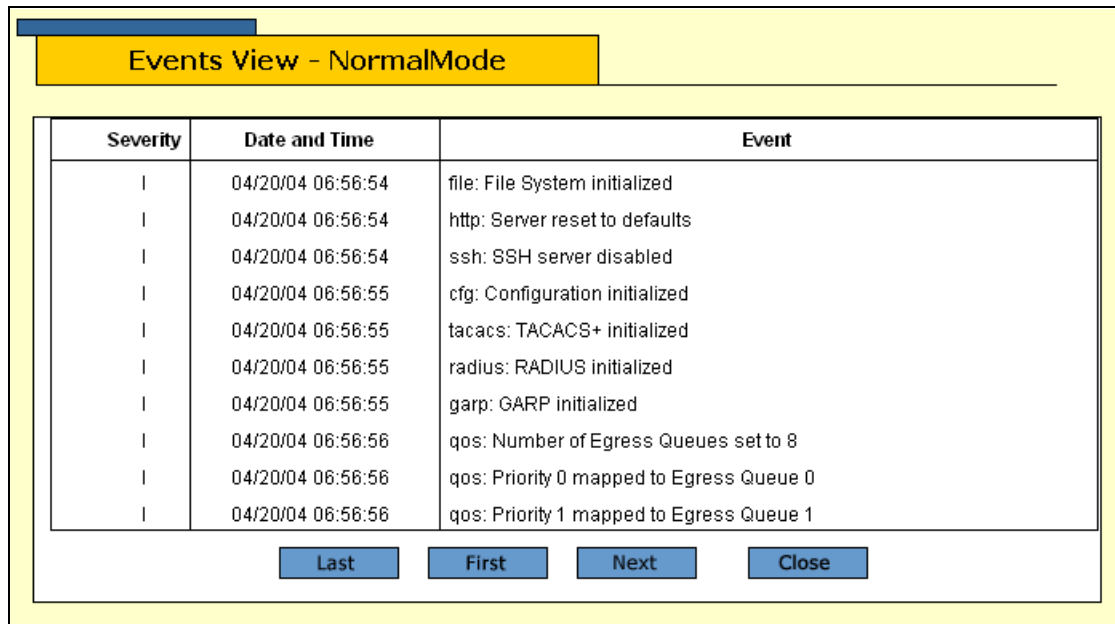


Figure 42. Event Log Example Displayed in Normal Mode

The events are displayed in a table. The columns in the table shown in normal display mode are described below:

S (Severity)

The event’s severity. The severity codes and their corresponding severity level and description are shown in Table 2.

Table 2. Event Severity Levels

Severity Code	Severity Level	Description
E	Error	Switch operation is severely impaired.
W	Warning	An issue that may require network manager attention.
I	Information	Useful information that can be ignored during normal operation.
D	Debug	Messages intended for technical support and software development.

Date and Time

The date and time the event occurred.

Event

This item contains two parts. The first part is the name of the module

within the AT-S63 management software that generated the event. The second part is a description of the event.

When you display the events in full mode, more information is included. Figure 43 shows the same portion of the event log in Figure 42 on page 134 but displayed in full mode.

Events View - FullMode				
Severity	Date and Time	EventID	Filename:Line	Event
I	04/20/04 06:56:54	183001	fileapp.c:131	file: File System initialized
I	04/20/04 06:56:54	243004	webserv.c:79	http: Server reset to defaults
I	04/20/04 06:56:54	323003	atiss.c:535	ssh: SSH server disabled
I	04/20/04 06:56:55	363001	cfgmain.c:159	cfg: Configuration initialized
I	04/20/04 06:56:55	283001	tacacs.c:830	tacacs: TACACS+ initialized
I	04/20/04 06:56:55	273001	radiusclient.c:1280	radius: RADIUS initialized
I	04/20/04 06:56:55	073001	garpmain.c:259	garp: GARP initialized
I	04/20/04 06:56:56	203002	qosapp.c:711	qos: Number of Egress Queues set to 8
I	04/20/04 06:56:56	203003	qosapp.c:787	qos: Priority 0 mapped to Egress Queue 0
I	04/20/04 06:56:56	203003	qosapp.c:787	qos: Priority 1 mapped to Egress Queue 1

[Close](#)

Figure 43. Event Log Example Displayed in Full Mode

In addition to the information displayed in Normal mode, the Full mode also displays additional columns in the table, as described below:

Event ID

A unique, random number assigned to each event.

Filename:Line

The AT-S63 software source file name and the line number in that source file that produced the event.

- Click one of the following buttons to scroll through the event log:

Last - Last page

First - First page

Next - Next page

Previous - Previous page

Close - Closes the log

To clear the current event log, go to “Clearing the Event Log” on page 136.

Disabling the Event Log

To activate or deactivate the event log, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **Event Log** tab.

The Event log tab is shown in Figure 40 on page 129.

3. In the Log Settings section, for the Status, click **Disabled**.
4. Click **Apply** to activate the settings on the switch.
5. Select the **General** tab.
6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Clearing the Event Log

You can clear the event log to remove old events and start fresh. To clear the event log, do the following:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **Event Log** tab.

The Event log tab is shown in Figure 40 on page 129.

3. In the Log Settings section, click the **Clear Log** checkbox.
4. Click the button next to the location of the log you want to clear, either Permanent or Temporary.
5. Click **Apply** to activate the settings on the switch.

Saving the Event Log to a File

You can save the event log to a file to review later. The file is saved as an ASCII file so that you can also email the file to someone else for troubleshooting.

To save the event log to a file, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **Event Log** tab.

The Event log tab is shown in Figure 40 on page 129.

3. In the **Filter Settings and Actions** section, select the type of events you want to save to the file.
4. In the **Save Filename** field, enter a name for the file with a .log file name extension.
5. Click **Save**.

The log file is saved on the switch as an ASCII file.

6. To upload the file to your management station for viewing or sending with an email, refer to “Uploading a File” on page 125.

Working with Log Outputs

Instead of checking the log files on each individual switch, you can create an output definition that defines the events that are sent to a syslog server. From this central point, you can monitor all the AT-9400 Series switches in your network. This is called a log output file. For more information about log output files, refer to Chapter 12, “Event Log,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

This section contains the following topics:

- ❑ “Configuring a Log Output Definition,” next
- ❑ “Viewing a Log Output Definition” on page 140
- ❑ “Modifying a Log Output Definition” on page 142
- ❑ “Deleting a Log Output Definition” on page 144

Configuring a Log Output Definition

To configure a log output, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **Event Log** tab.

The Event log tab is shown in Figure 40 on page 129.

3. In the Configure Log Outputs section, click **Create**.

The Create Log Output page is shown in Figure 44.

Figure 44. Create Event Log Output Page

4. Configure the following parameters as necessary:

Output ID

An ID number for the log output.

Output Status

Specifies whether or not the output is sent to the syslog server. The options are:

Enabled - Sends the output to the syslog server. Message generation is automatically enabled when you specify the IP address for the syslog server.

Disabled - The output is not sent to the syslog server even if an IP address is defined.

Message Format

Specifies the format of the messages sent to the syslog server. The options are:

Extended - Displays the time, module, severity, description, file name, line number, and event ID. This is the default.

Normal - Displays the time, module, severity, and description for each event.

Severity Selections

Specifies the severity of events you want to send to the syslog server. The possible options are:

ALL - All messages of the following types are displayed. This is the default.

Error - Only error messages are displayed. Error messages indicate that the switch operation is severely impaired.

Warning - Only warning messages are displayed. These messages indicate that an issue may require manager attention.

Information - Only informational messages are displayed. Informational messages display useful information that you can ignore during normal operation.

Debug - Debug messages provide detailed high-volume information that is intended only for technical support personnel.

Use <Ctrl>+click to select more than one severity at a time.

Type

The only available type is Syslog and you cannot change this.

Syslog Server IP Address

The IP address of the syslog server.

Facility Level

The numerical code to be added to the entries sent to the syslog server to group the entries according to the module or switch that produced them.

The facility levels are described in Table 3.

Table 3. Default Syslog Facilities

Facility	Mapped Event Log Modules and Events
Default	This facility number applies the functional groupings defined in the RFC 3164 standard.
local 1 through local 7	An identifier to assign to specific switches or groups of switches.

Note

For further information about the syslog facility levels, refer to Chapter 12, “Event Log” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Module Selections

Specifies the AT-S63 management software module(s) whose events you want to send to the syslog server. To select more than one, use <Ctrl>+click. For a list of modules, refer to Table 1 on page 132.

5. Click **Apply**.
6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Viewing a Log Output Definition

To view an existing log output definition, perform the following procedure:

1. From the home page, select **Monitoring**.

The System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. Select the **Event Log** tab.

The Event Log tab is shown in Figure 41 on page 130.

3. In the Configured Log Outputs section, select a log output from the list and click **View**.

The View Log Output page is shown in Figure 45.

Output ID	Type
3	Syslog
Output Status	Syslog Server IP Address
Enabled	149.35.8.45
Message Format	Facility Level
Extended	LOCAL_1
Severity Selections	Module Selections
D-Debug	SYSTEM
E-Error	CLI
W-Warning	EVTLOG
I-Information	MAC

[Close](#)

Figure 45. View Event Log Output Page

This page displays the following information:

Output ID

An ID number for the log output.

Output Status

Whether or not the output is sent to the syslog server, either enabled or disabled.

Message Format

The format of the messages sent to the syslog server.

Severity Selections

The severity of events sent to the syslog server. Scroll the list to view all the selections.

Type

The only available type is Syslog and you cannot change this.

Syslog Server IP Address

The IP address of the syslog server.

Facility Level

The numerical code to be added to the entries sent to the syslog server to group the entries according to the module or switch that produced them.

Module Selections

Specifies the AT-S63 management software module(s) whose events you want to send to the syslog server. Scroll the list to view all the modules that have been selected for this log output.

4. When you are done, click **Close**.

Modifying a Log Output Definition

To modify a log output definition, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **Event Log** tab.

The Event log tab is shown in Figure 40 on page 129.

3. In the Configure Log Outputs section, Select the log output file that you want to modify and click **Modify**.

The Configure Log Outputs section is shown in Figure 46.

ID	Type	Status	Details
0	Permanent	Enabled	Wrap on Full
1	Temporary	Enabled	Wrap on Full
3	Syslog	Enabled	149.35.8.45
5	Syslog	Disabled	0.0.0.0

Buttons: Create, Modify, Delete, Refresh

Figure 46. Configure Log Outputs Section

The Modify Event Log Output page is shown in Figure 47.

Modify Event Log Output 3

Output ID: 3

Output Status: Disabled

Message Format: Normal

Severity Selections: D-Debug, E-Error, W-Warning, Information

Type: Syslog

Syslog Server IP Address: 149 . 35 . 8 . 45

Facility Level: LOCAL_1

Module Selections: SYSTEM, CLI, EVTLOG, MAC

Buttons: Apply, Close

Figure 47. Modify Event Log Output Page

4. Modify the following parameters as necessary:

Output ID

An ID number for the log output.

Output Status

Specifies whether or not the output is sent to the syslog server. The options are:

Enabled - Sends the output to the syslog server. Message generation is automatically enabled when you specify the IP address for the syslog server.

Disabled - The output is not sent to the syslog server even if an IP address is defined.

Message Format

Specifies the format of the messages sent to the syslog server. The options are:

Extended - Displays the time, module, severity, description, file name, line number, and event ID. This is the default.

Normal - Displays the time, module, severity, and description for each event.

Severity Selections

Specifies the severity of events you want to send to the syslog server. The possible options are:

ALL - All messages of the following types are displayed. This is the default.

Error - Only error messages are displayed. Error messages indicate that the switch operation is severely impaired.

Warning - Only warning messages are displayed. These messages indicate that an issue may require manager attention.

Information - Only informational messages are displayed. Informational messages display useful information that you can ignore during normal operation.

Debug - Debug messages provide detailed high-volume information that is intended only for technical support personnel.

Use <Ctrl>+click to select more than one severity at a time.

Type

The only available type is Syslog and you cannot change this.

Syslog Server IP Address

The IP address of the syslog server.

Facility Level

The numerical code to be added to the entries sent to the syslog server to group the entries according to the module or switch that produced them.

The facility levels are described in Table 3 on page 140.

Module Selections

Specifies the AT-S63 management software module(s) whose events you want to send to the syslog server. To select more than one, use <Ctrl>+click. For a list of modules, refer to Table 1 on page 132.

5. Click **Apply** to apply the changes or **Close** to close the page without making changes.
6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting a Log Output Definition

To delete a log output, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **Event Log** tab.

The Event log tab is shown in Figure 40 on page 129.

3. In the Configure Log Outputs section, Select the log output file that you want to modify and click **Delete**.

The log output definition is deleted from the list.

Chapter 12

Classifiers

You use classifiers to define traffic flows. This chapter contains the following sections:

- ❑ “Configuring a Classifier” on page 146
- ❑ “Modifying a Classifier” on page 149
- ❑ “Deleting a Classifier” on page 151
- ❑ “Displaying the Classifiers” on page 152

Note

For background information about classifiers, refer to Chapter 13, “Classifiers,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Configuring a Classifier

To configure a classifier, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Network Security** option.

The Network Security page is displayed with the Port Security tab selected by default, as shown in Figure 48.

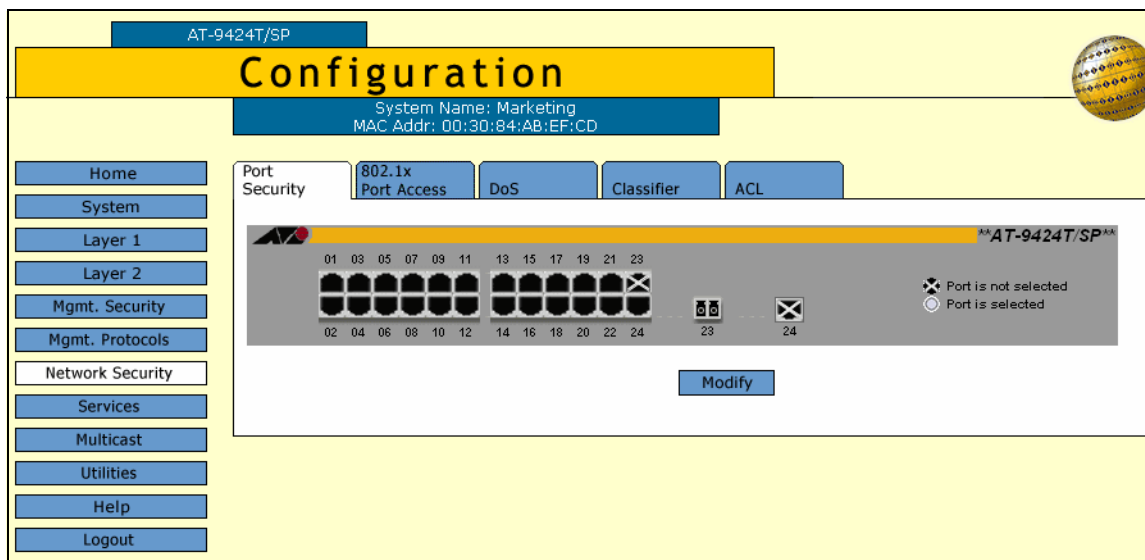


Figure 48. Port Security Tab (Configuration)

3. Select the **Classifier** tab.

The Classifier tab is shown in Figure 49.

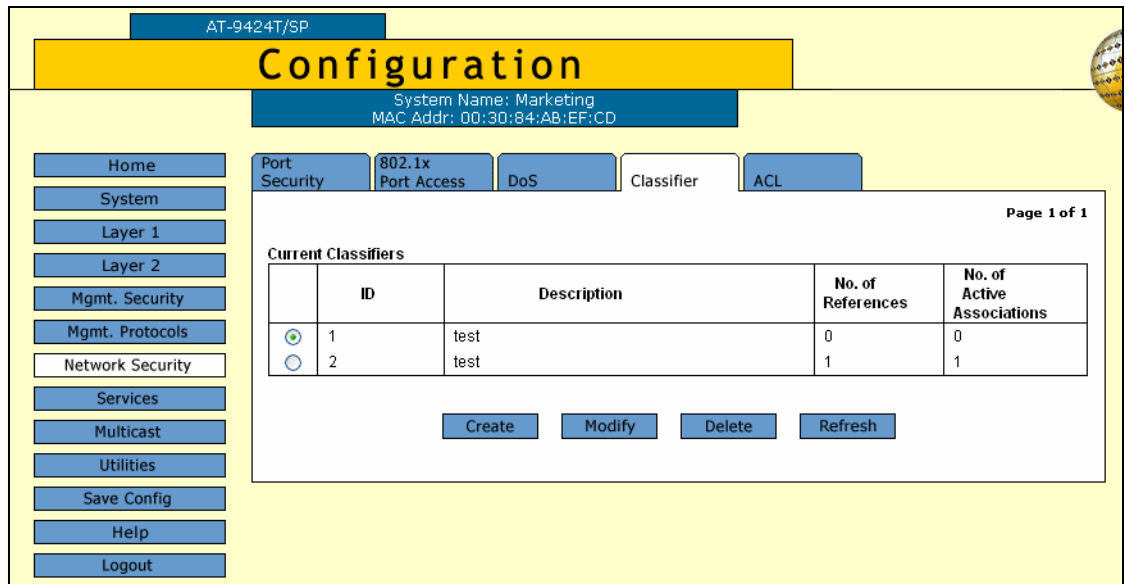


Figure 49. Classifier Tab (Configuration)

4. Click **Create**.

The Create Classifier page is shown in Figure 50.

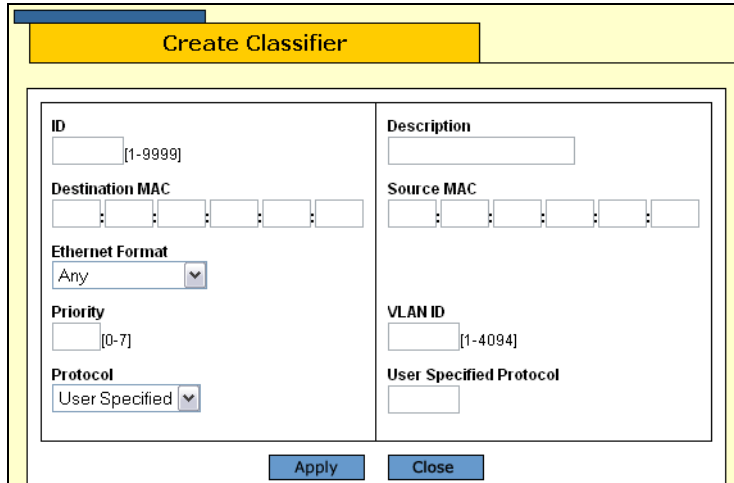


Figure 50. Create Classifier Page

5. Configure the following parameters as desired:

ID

The ID number of the classifier, a number between 1 and 9999. The default is the lowest available number.

Destination MAC

The destination MAC address for this traffic flow.

Ethernet Format

Specifies the type of Ethernet frame that needs to be classified. Select one of the following from the list:

- Any
- Untagged
- Tagged
- 802.2 Untagged
- 802.2 Tagged

Priority

Specifies the priority value in the IEEE 802.1p tag control field that traffic belonging to this traffic class is assigned. The range is 0 to 7 with 0 (zero) as the lowest priority.

Protocol

Specifies the protocol used to identify the traffic flow. Select one of the following from the list:

- User specified
- IP
- ARP
- RARP

Description

A description of the classifier, up to 15 alphanumeric characters including spaces.

User Specified Protocol

Specifies a protocol other than one of those listed in the Protocol list.

6. Click **Apply**.
7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Modifying a Classifier

To modify a classifier, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Network Security** option.

The Network Security page is displayed with the Port Security tab selected by default, as shown in Figure 48 on page 146.

3. Select the **Classifier** tab.

The Classifier tab is shown in Figure 49 on page 147.

4. Click **Modify**.

The Modify Classifier page is shown in Figure 51.

Modify Classifier	
ID 1	Description test
Destination MAC [][] : [][] : [][] : [][] : [][]	Source MAC [][] : [][] : [][] : [][] : [][]
Ethernet Format Any	VLAN ID [] [1-4094]
Priority [] [0-7]	User Specified Protocol []
Protocol User Specified	
<input type="button" value="Apply"/> <input type="button" value="Close"/>	

Figure 51. Modify Classifier Page

Note

You can modify a classifier if it has references associated with it, but not if it has active associations.

5. Modify the following parameters as necessary:

ID

The ID number of the classifier, a number between 1 and 9999. The default is the lowest available number.

Destination MAC

The destination MAC address for this traffic flow.

Ethernet Format

Specifies the type of Ethernet frame that needs to be classified. Select one of the following from the list:

- Any
- Untagged
- Tagged
- 802.2 Untagged
- 802.2 Tagged

Priority

Specifies the priority value in the IEEE 802.1p tag control field that traffic belonging to this traffic class is assigned. The range is 0 to 7 with 0 (zero) as the lowest priority.

Protocol

Specifies the protocol used to identify the traffic flow. Select one of the following from the list:

- User specified
- IP
- ARP
- RARP

Description

A description of the classifier, up to 15 alphanumeric characters including spaces.

VLAN ID

The ID number of the VLAN that identifies a traffic flow.

User Specified Protocol

Specifies a protocol other than one of those listed in the Protocol list.

6. Click **Apply**.
7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting a Classifier

To delete a classifier, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Network Security** option.

The Network Security page is displayed with the Port Security tab selected by default, as shown in Figure 48 on page 146.

3. Select the **Classifier** tab.

The Classifier tab is shown in Figure 49 on page 147.

4. Click the button next to the classifier you want to delete and click **Delete**.

Note

You cannot delete a classifier if it belongs to an ACL or QoS policy that has already been assigned to a port. You must first remove the port assignments from the ACL or policy before you can delete the classifier.

5. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying the Classifiers

To display the classifiers, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

Note

You can access the Classifiers tab either through the Network Security menu option or through the Services menu option. This procedure uses the path through the Services menu option.

2. From the Monitoring menu, select **Services**.

The Services menu is displayed with the CoS tab selected by default, as shown in Figure 52.

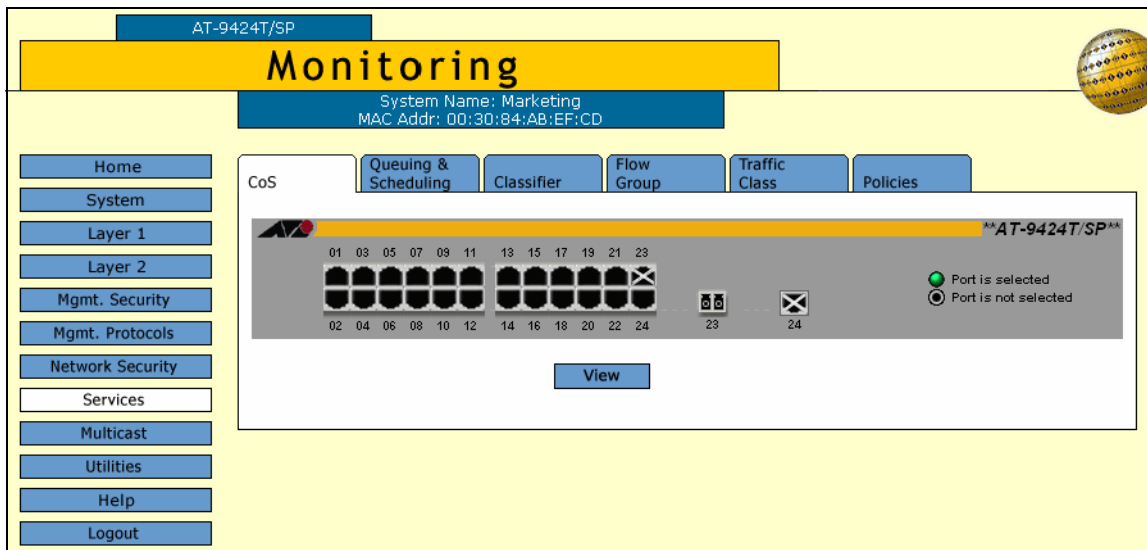


Figure 52. CoS Tab (Monitoring)

3. Select the **Classifiers** tab.

The Classifiers tab is shown in Figure 53.

The screenshot shows the AT-S63 Management Software Web Browser Interface. The top navigation bar includes 'AT-9424T/SP' and a yellow 'Monitoring' header. Below the header, system information is displayed: 'System Name: Marketing' and 'MAC Addr: 00:30:84:AB:EF:CD'. The main navigation menu on the left includes 'Home', 'System', 'Layer 1', 'Layer 2', 'Mgmt. Security', 'Mgmt. Protocols', 'Network Security', 'Services', 'Multicast', 'Utilities', 'Help', and 'Logout'. The main content area has tabs for 'CoS', 'Queuing & Scheduling', 'Classifier', 'Flow Group', 'Traffic Class', and 'Policies'. The 'Classifier' tab is active, showing 'Page 1 of 1' and a table of 'Current Classifiers'.

	ID	Description	No. of References	No. of Active Associations
<input checked="" type="radio"/>	1	test	0	0
<input type="radio"/>	2	test	1	1

A 'View' button is located below the table.

Figure 53. Classifier Tab (Monitoring)

The Classifier tab displays a table of the currently configured classifiers that contains the following columns of information:

ID

The ID of the classifier.

Description

A description of the classifier.

No. of References

The number of times the classifier has been referred to by an ACL or a flow group.

No. of Active Associations

A classifier is active if the corresponding ACL or flow group to which it is attached is active. This item shows the number of such associations that are active.

- To display detailed information about a classifier, select the classifier and click **View**.

The View Classifier page opens, as shown in Figure 54.

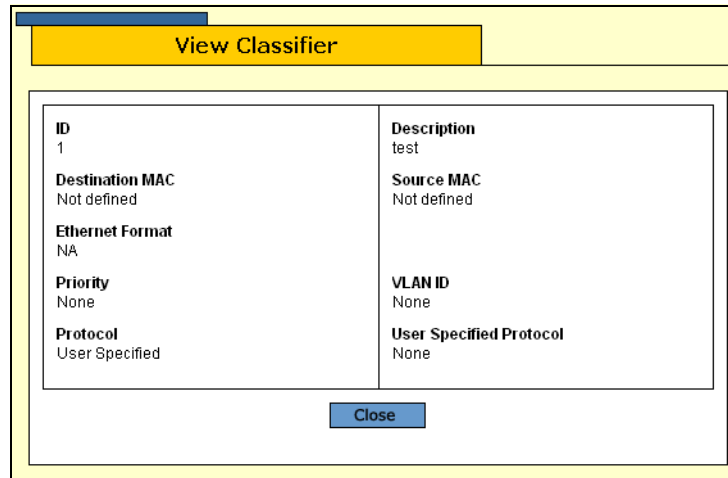


Figure 54. View Classifier Page

The View Classifier page displays the following information:

ID

The classifier ID.

Destination MAC

The destination MAC address for this traffic flow.

Ethernet Format

The type of Ethernet frames that will be classified.

Priority

The priority value in the IEEE 802.1p tag control field that traffic belonging to this traffic class is assigned.

Protocol

The protocol used to identify the traffic flow.

Description

A description of the classifier.

Source MAC

The source MAC address.

VLAN ID

The ID number of the VLAN that identifies a traffic flow.

User Specified Protocol

A protocol other than one of those listed in the Protocol list, if any.

5. Click **Close** to close the page.

Chapter 13

Access Control Lists

An access control list (ACL) is a tool for managing network traffic. This chapter contains the following sections:

- ❑ “Configuring an Access Control List” on page 156
- ❑ “Modifying an Access Control List” on page 158
- ❑ “Displaying the Access Control Lists” on page 160

Note

For background information about access control lists, refer to Chapter 14, “Access Control Lists,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Configuring an Access Control List

To configure an access control list, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Network Security** option.

The Network Security page is displayed with the Port Security tab selected by default, as shown in Figure 48 on page 146.

3. Select the **ACL** tab.

The ACL tab is shown in Figure 55.

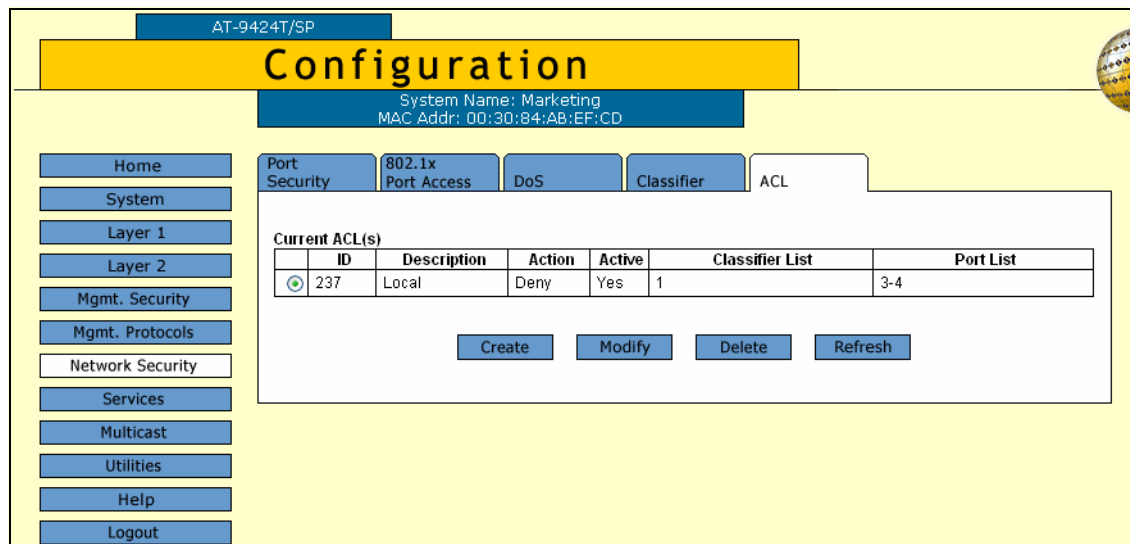


Figure 55. ACL Tab (Configuration)

4. Click **Create**.

The Create ACLs page is displayed, as shown in Figure 56.

Figure 56. Create ACLs Page

5. Configure the following parameters:

ID

Specifies the ID number for the ACL. Every ACL on the switch must have a unique ID number. The range is 0 to 255 and the default is the lowest unused number.

Classifier List

The classifiers assigned to this ACL. You must create the classifiers before you assign them to an ACL.

Action

Specifies whether the ACL discards (0) or accepts (1) the ingress packets. The default is to discard the packets.

Description

Specifies a description for the ACL. A description can be up to 15 alphanumeric characters, including spaces.

Port List

Specifies the ports where the ACL is assigned. Select the ports from the list using <Ctrl> click to select more than one.

6. Click **Apply**.
7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Modifying an Access Control List

To modify an access control list, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Network Security** option.

The Network Security page is displayed with the Port Security tab selected by default, as shown in Figure 48 on page 146.

3. Select the **ACL** tab.

The ACL tab is shown in Figure 55 on page 156.

4. Select the ACL you want to modify and click **Modify**.

The Modify ACLs page is displayed, as shown in Figure 57.

The screenshot shows a web-based configuration interface for modifying an ACL. The window title is 'Modify ACL(s)'. The form contains the following elements:

- ID:** 237
- Description:** Local
- Classifier List:** A list box containing '1' and '2'.
- Port List:** A list box containing '1', '2', '3', and '4'.
- Action:** A dropdown menu set to 'DENY'.
- Buttons:** 'Apply' and 'Close' buttons at the bottom.

Figure 57. Modify ACLs Page

5. Configure the following parameters as necessary:

ID

Specifies the ID number for the ACL. Every ACL on the switch must have a unique ID number. The range is 0 to 255 and the default is the lowest unused number.

Classifier List

The classifiers assigned to this ACL. You must create the classifiers before you assign them to an ACL.

Action

Specifies whether the ACL discards (0) or accepts (1) the ingress packets. The default is to discard the packets.

Description

Specifies a description for the ACL. A description can be up to 15 alphanumeric characters, including spaces.

Port List

Specifies the ports where the ACL is assigned. Select the ports from the list using <Ctrl> click to select more than one.

6. Click **Apply**.
7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying the Access Control Lists

To display the current ACLs, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select **Network Security**.

The Network Security page is displayed with the Port Security tab selected by default, as shown in Figure 58.

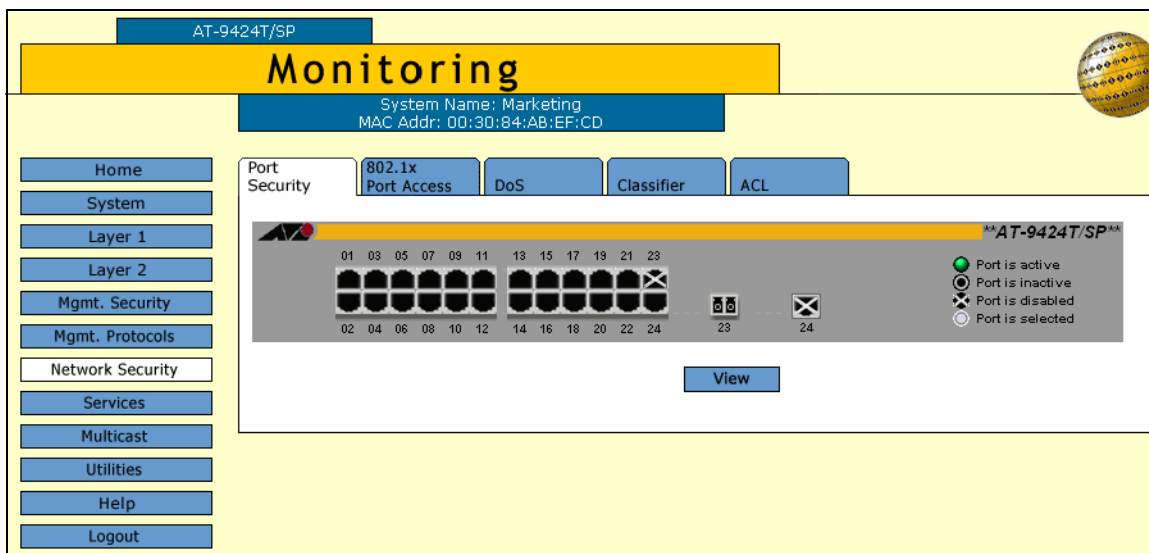


Figure 58. Port Security Tab (Monitoring)

3. Select the **ACL** tab.

The ACL tab is shown in Figure 59.

The screenshot shows the AT-S63 Management Software Web Browser Interface. The top navigation bar is yellow and contains the text 'Monitoring' and 'System Name: Marketing MAC Addr: 00:30:84:AB:EF:CD'. Below this, there is a blue bar with 'AT-9424T/SP'. The main content area is divided into several sections. On the left, there is a vertical navigation menu with buttons for 'Home', 'System', 'Layer 1', 'Layer 2', 'Mgmt. Security', 'Mgmt. Protocols', 'Network Security', 'Services', 'Multicast', 'Utilities', 'Help', and 'Logout'. The main content area has a blue bar with 'Port Security', '802.1x Port Access', 'DoS', 'Classifier', and 'ACL'. Below this, there is a table titled 'Current ACL(s)' with the following columns: ID, Description, Action, Active, Classifier List, and Port List. The table contains one row with the following data: ID: 237, Description: Local, Action: Deny, Active: Yes, Classifier List: 1, and Port List: 3-4. Below the table is a 'View' button.

ID	Description	Action	Active	Classifier List	Port List
237	Local	Deny	Yes	1	3-4

Figure 59. ACL Tab (Monitoring)

The ACL tab displays a table of the currently configured ACLs that contains the following columns of information:

ID

The ID number for the ACL.

Description

A description of the ACL.

Action

Shows whether the ACL discards (0) or accepts (1) the packets.

Active

Whether or not the ACL is active on the ports.

Classifier List

The classifiers assigned to this ACL.

Port List

The ports where the ACL is assigned.

- To view detailed information about an ACL, select the ACL and click **View**.

The View ACLs page opens, as shown in Figure 60.

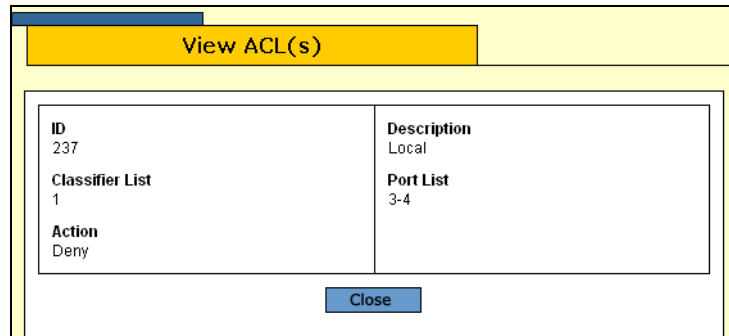


Figure 60. View ACLs Page

The View ACLs page displays the following information:

ID

The ID number for the ACL.

Description

A description of the ACL.

Classifier List

The classifiers assigned to this ACL.

Port List

The ports where the ACL is assigned.

Action

Shows whether the ACL discards (0) or accepts (1) the packets.

5. Click **Close**.

Chapter 14

Denial of Service Defense

This chapter contains instructions on how to configure the Denial of Service defense feature on the switch. The sections include:

- “Configuring Denial of Service Defense” on page 164
- “Displaying the DoS Settings” on page 167

Note

For background information on denial of service defense, refer to Chapter 15, “Denial of Service Defense,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Configuring Denial of Service Defense

To configure the ports on the switch for Denial of Service attack defense, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Network Security** option.

The Network Security page is displayed with the 802.1x Port Access tab selected by default, as shown in Figure 48 on page 146.

3. Select the **DoS** tab.

The DoS tab is shown in Figure 61.

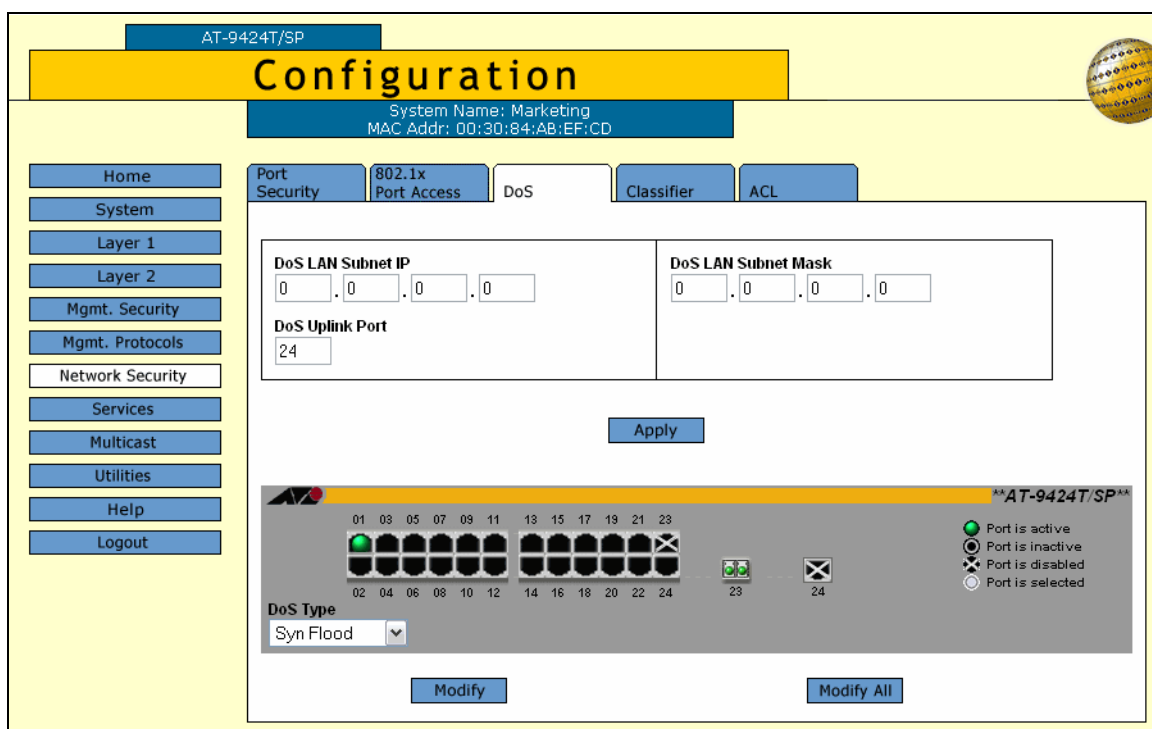


Figure 61. DoS Tab (Configuration)

4. If you are implementing the SMURF or Land defense, you must provide an IP address and mask for your LAN. To do this, complete the following procedure: Otherwise, skip ahead to Step 5.
 - a. In the DoS LAN Subnet IP field, enter the IP address of one of the devices connected to the switch, preferably the lowest IP address.

- b. In the DoS Subnet Mask field, enter the LAN's mask. enter the mask. A binary "1" indicates the switch should filter on the corresponding bit of the IP address, while a "0" indicates that it should not. As an example, assume that the devices connected to a switch are using the IP address range 149.11.11.1 to 149.11.11.50. The mask would be 0.0.0.63.
 - c. If you are activating the Land defense, in the DoS Uplink Port field enter the number of the port connected to the device (e.g., DSL router) that leads outside your network. You can specify only one uplink port.
5. Click the ports in the switch image where you want to enable or disable a defense mechanism.
 6. Using the DoS Type list, select the type of denial of service attack you want to either enable or disable on the ports. The possible selections are:
 - Syn Flood attack
 - Smurf attack
 - Land attack
 - Tear drop attack
 - Ping of death attack
 - IP Options
 7. Click **Modify**. To configure all the ports, click **Modify All**.

The DoS Configuration for Ports page opens. The page shown in Figure 62 is for IP Options.

Figure 62. DoS Configuration for Ports Page

8. Configure the following parameters as necessary:

Status

Click Enable or Disable to enable or disable DoS on the selected ports.

Action

The action a port takes when an intruder packet is received. Although five possible selections are shown in the Action list box, they all do the same thing: block the packet, record the event, and drop the packet. This option applies only to the IP Options defense.

Mirror Port

This option applies to the Land, Tear Drop, Ping of Death, and IP Options. You can use this option to copy offending traffic to another port on the switch. You can specify only one mirror port. Specifying a mirror port is not required.

9. Click **Apply**.

The defense is immediately activated on the ports.

10. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying the DoS Settings

To display the DoS settings, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select **Network Security**.

The Network Security page is displayed with the Port Security tab selected by default, as shown in Figure 58 on page 160.

3. Select the **DoS** tab.

The DoS tab is shown in Figure 63.

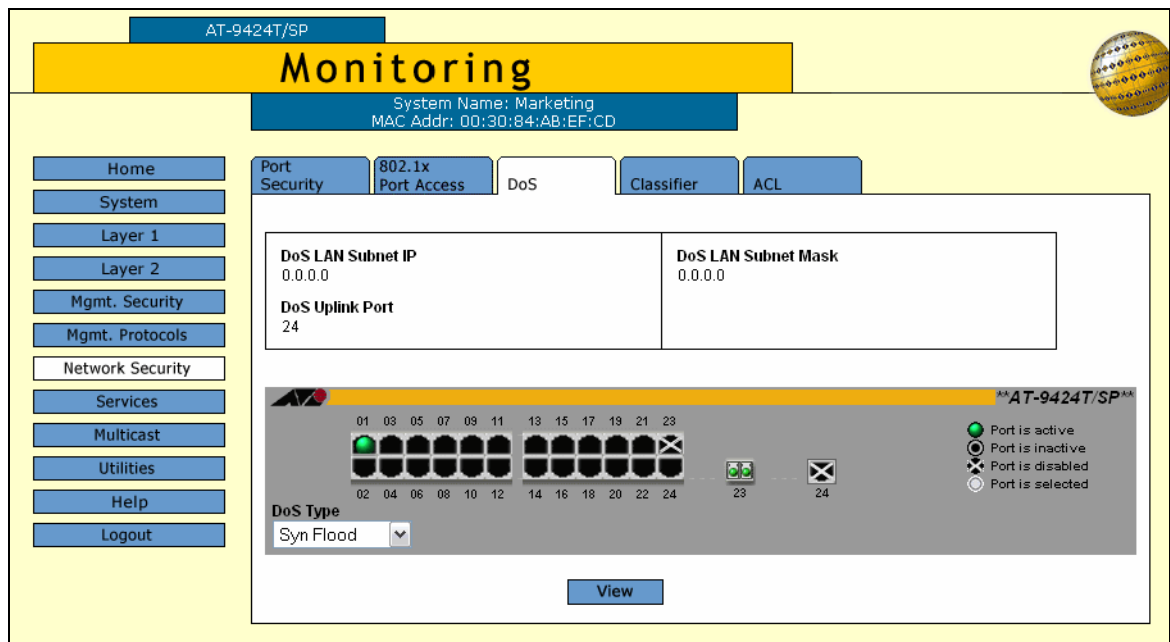


Figure 63. DoS Tab (Monitoring)

4. Click the port whose DoS settings you want to view. You can select more than one port at a time.
5. Using the DoS Type list, select the type of denial of service defense whose settings you want to view.
6. Click **View**.

The DoS Monitor for Port page opens, as shown in Figure 64.

Port	Status	Type	Action	Mirror Port
5	Disable	SYN_FLOOD	Block	--

[Close](#)

Figure 64. DoS Monitor for Ports Page

The page displays a table that contains the following columns of information:

Port

The port number.

Status

Whether DoS is enabled or disabled on the port.

Type

The type of DoS prevention.

Action

The action a port takes when an intruder packet is received. Although five possible selections are shown in the Action list box, they all do the same thing: block the packet, record the event, and drop the packet. This column is only displayed for the IP Options defense.

Mirror Port

The port on the switch to which offending traffic is copied.

Chapter 15

Quality of Service

This chapter contains instructions on how to configure Quality of Service (QoS). This chapter contains the following procedures:

- ❑ “Managing Flow Groups” on page 170
- ❑ “Managing Traffic Classes” on page 176
- ❑ “Managing Policies” on page 184

Note

For background information on QoS, refer to Chapter 16, “Quality of Service,” in the *AT-S63 Management Software Menu Interface User’s Guide*.

Managing Flow Groups

Flow groups are groups of classifiers that group together similar traffic flows. This section contains the following procedures:

- ❑ “Configuring Flow Groups,” next
- ❑ “Modifying a Flow Group” on page 172
- ❑ “Deleting a Flow Group” on page 173
- ❑ “Displaying Flow Groups” on page 173

Configuring Flow Groups

To configure a flow group, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Services** option.

The Services page is displayed with the CoS tab selected by default, as shown in Figure 65.

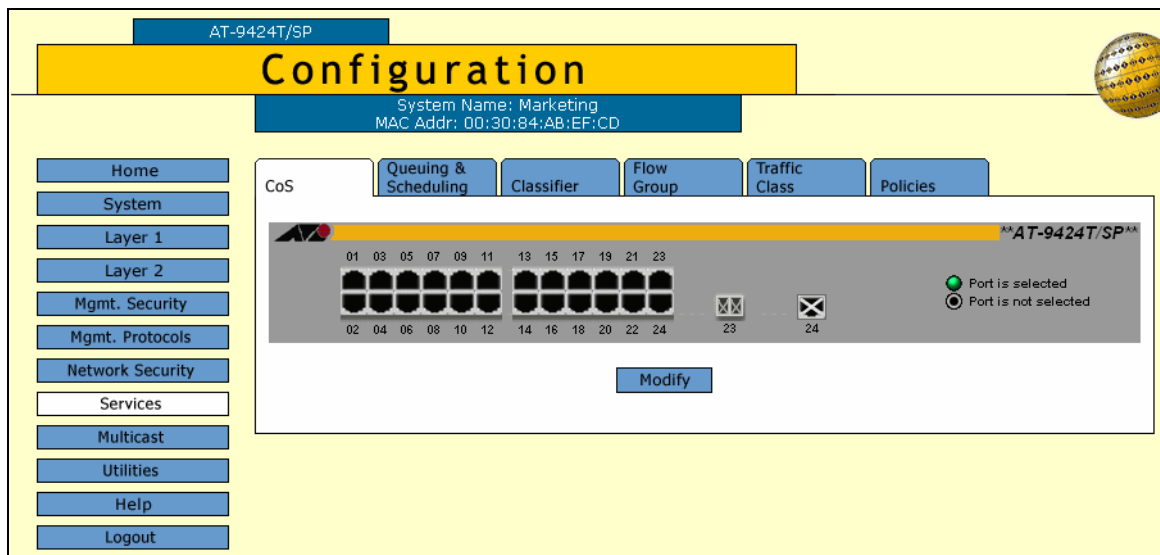


Figure 65. CoS Tab (Configuration)

3. Select the **Flow Group** tab.

The Flow Group tab is shown in Figure 66.

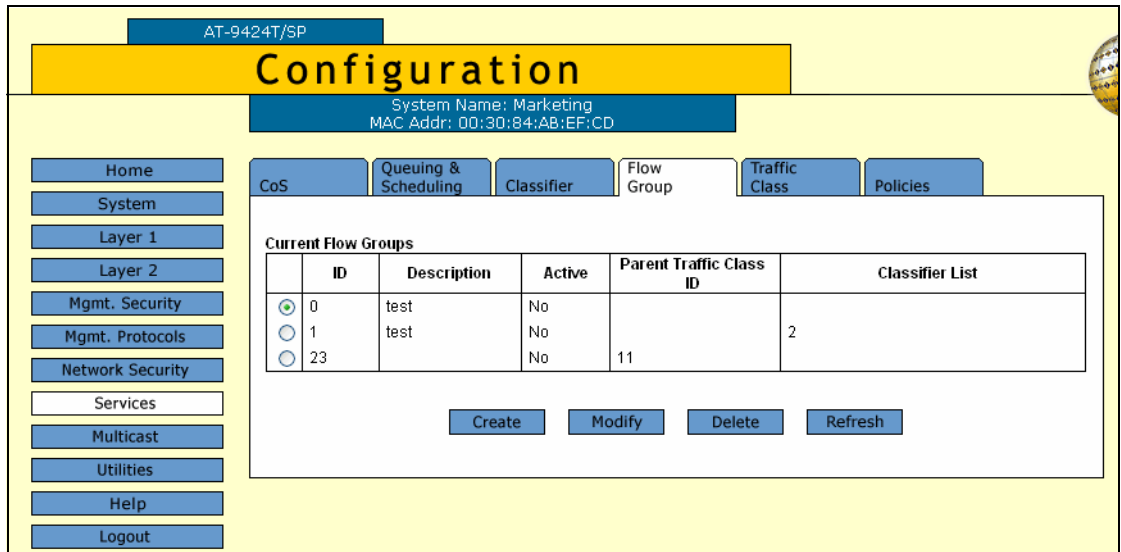


Figure 66. Flow Group Tab (Configuration)

4. Click **Create**.

The Create Flow Group page opens, as shown in Figure 67.

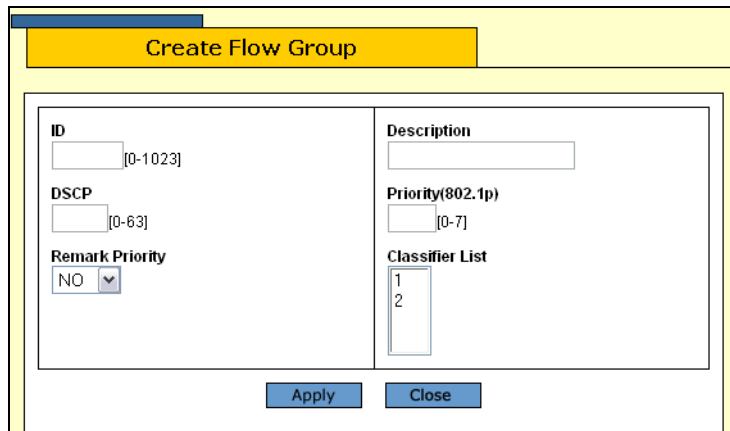


Figure 67. Create Flow Group Page

5. Configure the following parameters as necessary:

ID

Specifies the ID number for this flow group. The range is 0 to 1023.

DSCP

Specifies a replacement value to write into the DSCP (TOS) field of the packets. The range is 0 to 63.

Remark Priority

Replaces the user priority value in the packets with the new value specified in the Priority parameter.

Description

Specifies the flow group description. A description can be up to 15 alphanumeric characters, including spaces.

Priority (802.1p)

Specifies a new user priority value for the packets. The range is 0 to 7.

Classifier List

The classifiers to be assigned to the policy. The specified classifiers must already exist. To select more than one classifier, use <Ctrl> click.

6. Click **Apply**.
7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Modifying a Flow Group

To modify a flow group, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Services** option.

The Services page is displayed with the CoS tab selected by default, as shown in Figure 65 on page 170.

3. Select the flow group you want to modify and click **Modify**.

The Modify Flow Group page is displayed, as shown in Figure 68.

Figure 68. Modify Flow Group Page

4. Configure the following parameters as necessary:

ID

Specifies the ID number for this flow group. The range is 0 to 1023.

DSCP

Specifies a replacement value to write into the DSCP (TOS) field of the packets. The range is 0 to 63.

Remark Priority

Replaces the user priority value in the packets with the new value specified in the Priority parameter.

Description

Specifies the flow group description. A description can be up to 15 alphanumeric characters, including spaces.

Priority (802.1p)

Specifies a new user priority value for the packets. The range is 0 to 7.

Classifier List

The classifiers to be assigned to the policy. The specified classifiers must already exist. To select more than one classifier, use <Ctrl> click.

5. Click **Apply**.
6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting a Flow Group

To delete a flow group, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Services** option.

The Services page is displayed with the CoS tab selected by default, as shown in Figure 65 on page 170.

3. Select the flow group you want to delete and click **Delete**.

The flow group is deleted from the list.

Displaying Flow Groups

To display the flow groups, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

Note

You can access the Classifiers tab either through the Network Security menu option or through the Services menu option. This procedure uses the path through the Services menu option.

- From the Monitoring menu, select the **Services** option.

The Services menu is displayed with the CoS tab selected by default, as shown in Figure 52 on page 152.

- Select the **Flow Group** tab.

The Flow Group tab is shown in Figure 69.

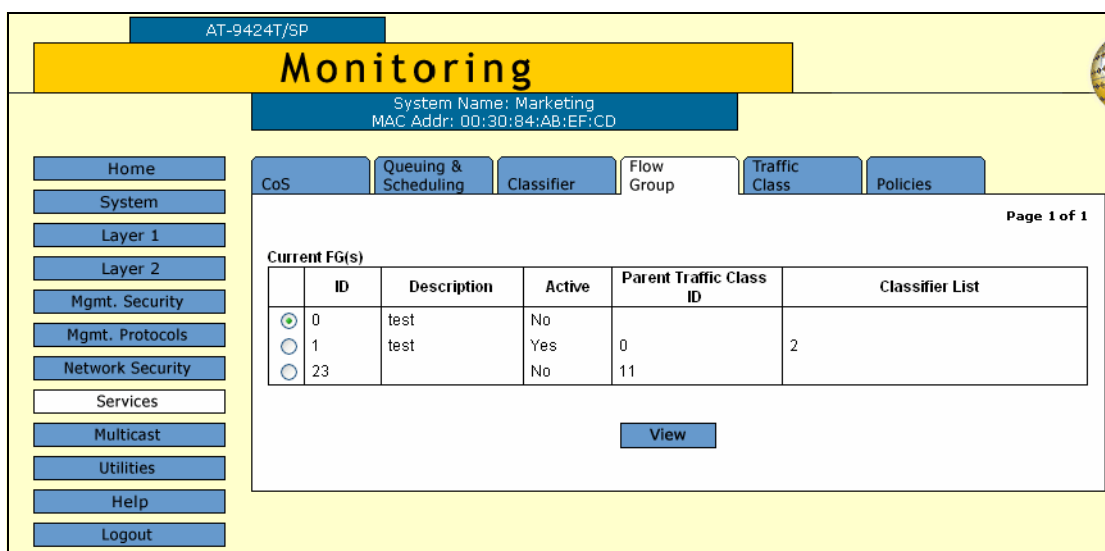


Figure 69. Flow Group Tab (Monitoring)

The Flow Group tab displays the currently configured flow groups in a table that contains the following columns of information:

ID

The ID number for this flow group.

Description

The flow group description.

Active

Whether or not the flow group is active.

Parent Traffic Class ID

The traffic class associated with this flow group. This information is for display only.

Classifier List

The classifiers assigned to the flow group.

- To display detailed information about a flow group, select the flow group and click **View**.

The View Flow Group page is shown in Figure 70.

View Flow Group	
ID 23	Description Local
DSCP 4	Priority(802.1p) None
Remark Priority No	Classifier List None
<input type="button" value="Close"/>	

Figure 70. View Flow Group Page

The View Flow Group page displays the following information:

ID

The ID number for this flow group.

Description

The flow group description.

DSCP

The replacement value to write into the DSCP (TOS) field of the packets.

Priority

The new user priority value for the packets.

Remark Priority

Replaces the user priority value in the packets with the new value specified in the Priority parameter.

Classifier List

The classifiers assigned to the flow group.

- Click **Close**.

Managing Traffic Classes

Traffic classes consist of a set of QoS parameters and a group of QoS flow groups. This section contains the following procedures:

- ❑ “Configuring Traffic Classes,” next
- ❑ “Modifying a Traffic Class” on page 178
- ❑ “Deleting a Traffic Class” on page 180
- ❑ “Displaying the Traffic Classes” on page 180

Configuring Traffic Classes

To configure a traffic class, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Services** option.

The Services page is displayed with the CoS tab selected by default, as shown in Figure 65 on page 170.

3. Select the **Traffic Class** tab.

The Traffic Class tab is shown in Figure 71.

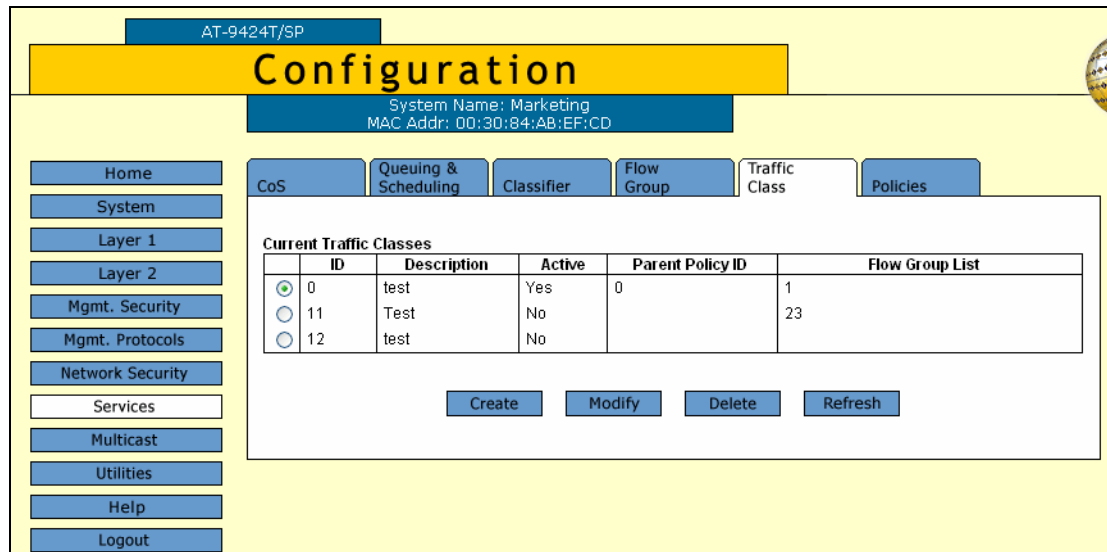


Figure 71. Traffic Class Tab

4. Click **Create**.

The Create Traffic Class page is shown in Figure 72.

Figure 72. Create Traffic Class Page

5. Configure the following parameters:

ID

Specifies the ID number for this traffic class. The range is 0 to 1023.

Exceed Action

Specifies the action to be taken if the traffic of the traffic class exceeds the maximum bandwidth specified by the Max Bandwidth parameter. The possible options are drop and remark.

DSCP

Specifies a replacement value to write into the DSCP (TOS) field of the packets. The range is 0 to 63.

Burst Size

Specifies the size of a token bucket for the traffic class. The range is 4 to 512 Kbps. You must also specify the Max Bandwidth.

Remark Priority

Replaces the user priority value in the packets with the new value specified in the Priority parameter.

Description

Specifies the traffic class description. A description can be up to 15 alphanumeric characters, including spaces.

Exceed Remark Value

Specifies the DSCP replacement value for traffic that exceeds the maximum bandwidth. This value takes precedence over the DSCP value. The default is 0.

Max Bandwidth

Specifies the maximum bandwidth available for the traffic class. The range is 0 to 1016 Mbps. If you set this parameter to 0 (zero), all traffic that matches that traffic class is dropped.

Priority

Specifies the priority value in the IEEE 802.1p tag control field that traffic belonging to this traffic class is assigned. The range is 0 to 7 with 0 (zero) as the lowest priority.

Flow Group List

The flow groups assigned to this traffic class. Use <Ctrl> click to select more than one.

6. Click **Apply**.
7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Modifying a Traffic Class

To modify a traffic class, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Services** option.

The Services page is displayed with the CoS tab selected by default, as shown in Figure 65 on page 170.

3. Select the **Traffic Class** tab.

The Traffic Class tab is shown in Figure 71 on page 176

4. Select the traffic class you want to modify and click **Modify**.

The Modify Traffic Class page is shown in Figure 73.

Modify Traffic Class	
ID 11	Description Test
Exceed Action DROP	Exceed Remark value 0 [0-63]
DSCP Value 0 [0-63]	Max Bandwidth [0-1016]
Burst Size [4-512]	Priority [0-7]
Remark Priority NO	Flow Group List 0 1 23
<input type="button" value="Apply"/> <input type="button" value="Close"/>	

Figure 73. Modify Traffic Class Page

- Configure the following parameters as necessary:

ID

Specifies the ID number for this traffic class. The range is 0 to 1023.

Exceed Action

Specifies the action to be taken if the traffic of the traffic class exceeds the maximum bandwidth specified by the Max Bandwidth parameter. The possible options are drop and remark.

DSCP

Specifies a replacement value to write into the DSCP (TOS) field of the packets. The range is 0 to 63.

Burst Size

Specifies the size of a token bucket for the traffic class. The range is 4 to 512 Kbps. You must also specify the Max Bandwidth.

Remark Priority

Replaces the user priority value in the packets with the new value specified in the Priority parameter.

Description

Specifies the traffic class description. A description can be up to 15 alphanumeric characters, including spaces.

Exceed Remark Value

Specifies the DSCP replacement value for traffic that exceeds the maximum bandwidth. This value takes precedence over the DSCP value. The default is 0.

Max Bandwidth

Specifies the maximum bandwidth available for the traffic class. The range is 0 to 1016 Mbps. If you set this parameter to 0 (zero), all traffic that matches that traffic class is dropped.

Priority

Specifies the priority value in the IEEE 802.1p tag control field that traffic belonging to this traffic class is assigned. The range is 0 to 7 with 0 (zero) as the lowest priority.

Flow Group List

The flow groups assigned to this traffic class. Use <Ctrl> click to select more than one.

6. Click Apply.
7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting a Traffic Class

To delete a traffic class, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Services** option.

The Services page is displayed with the CoS tab selected by default, as shown in Figure 65 on page 170.

3. Select the **Traffic Class** tab.

The Traffic Class tab is shown in Figure 71 on page 176

4. Select the traffic class you want to delete and click **Delete**.

The traffic class is deleted from the list.

Displaying the Traffic Classes

To display the traffic classes, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select **Services**.

The Services menu is displayed with the CoS tab selected by default, as shown in Figure 52 on page 152.

3. Select the **Traffic Class** tab.

The Traffic Class tab is shown in Figure 74.

AT-9424T/SP

Monitoring

System Name: Marketing
MAC Addr: 00:30:84:AB:EF:CD

Home System Layer 1 Layer 2 Mgmt. Security Mgmt. Protocols Network Security Services Multicast Utilities Help Logout

CoS Queuing & Scheduling Classifier Flow Group **Traffic Class** Policies

Page 1 of 1

Current Traffic Classes

	ID	Description	Active	Parent Policy ID	Flow Group List
<input checked="" type="radio"/>	0	test	Yes	0	
<input type="radio"/>	11	Test	No		1 23
<input type="radio"/>	12	test	No		

View

Figure 74. Traffic Class Tab (Monitoring)

The Traffic Class tab displays the currently configured flow groups in a table that contains the following columns of information:

ID

The ID of the traffic class.

Description

A description of the traffic class.

Active

Whether or not this traffic class is active on the switch.

Parent Policy ID

The policy associated with this traffic class. This information is for display only.

Flow Group List

The flow groups assigned to this traffic class.

4. To display detailed information about a traffic class, select the traffic class and click **View**.

The View Traffic Class page is shown in Figure 75.

The screenshot shows a window titled "View Traffic Class" with a yellow header. Inside, there is a table with two columns. The left column contains the following items: ID (11), Exceed Action (Drop), DSCP Value (0), Burst Size (None), and Remark Priority (No). The right column contains: Description (Test), Exceed Remark value (0), Max Bandwidth (None), Priority (None), and Flow Group List (23). At the bottom of the window are two buttons: "Apply" and "Close".

ID 11	Description Test
Exceed Action Drop	Exceed Remark value 0
DSCP Value 0	Max Bandwidth None
Burst Size None	Priority None
Remark Priority No	Flow Group List 23

Figure 75. View Traffic Class Page

The View Traffic Class page displays the following information:

ID

The ID of the traffic class.

Exceed Action

The action to be taken if the traffic of the traffic class exceeds the maximum bandwidth specified by the Max Bandwidth parameter.

DSCP Value

The replacement value to write into the DSCP (TOS) field of the packets.

Burst Size

The size of a token bucket for the traffic class.

Remark Priority

Replaces the user priority value in the packets with the new value specified in the Priority parameter.

Description

A description of the traffic class.

Exceed Remark Value

The DSCP replacement value for traffic that exceeds the maximum bandwidth.

Max Bandwidth

The maximum bandwidth available for the traffic class.

Priority

The priority value in the IEEE 802.1p tag control field that traffic belonging to this traffic class is assigned.

Flow Group List

The flow groups assigned to this traffic class.

5. Click **Close**.

Managing Policies

QoS policies consist of a collection of user-defined traffic classes. This section contains the following procedures:

- ❑ “Configuring a Policy,” next
- ❑ “Modifying a Policy” on page 186
- ❑ “Deleting a Policy” on page 188
- ❑ “Displaying Policies” on page 188

Configuring a Policy

To configure a policy, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Services** option.

The Services page is displayed with the CoS tab selected by default, as shown in Figure 65 on page 170.

3. Select the **Policies** tab.

The Policies tab is shown in Figure 76.

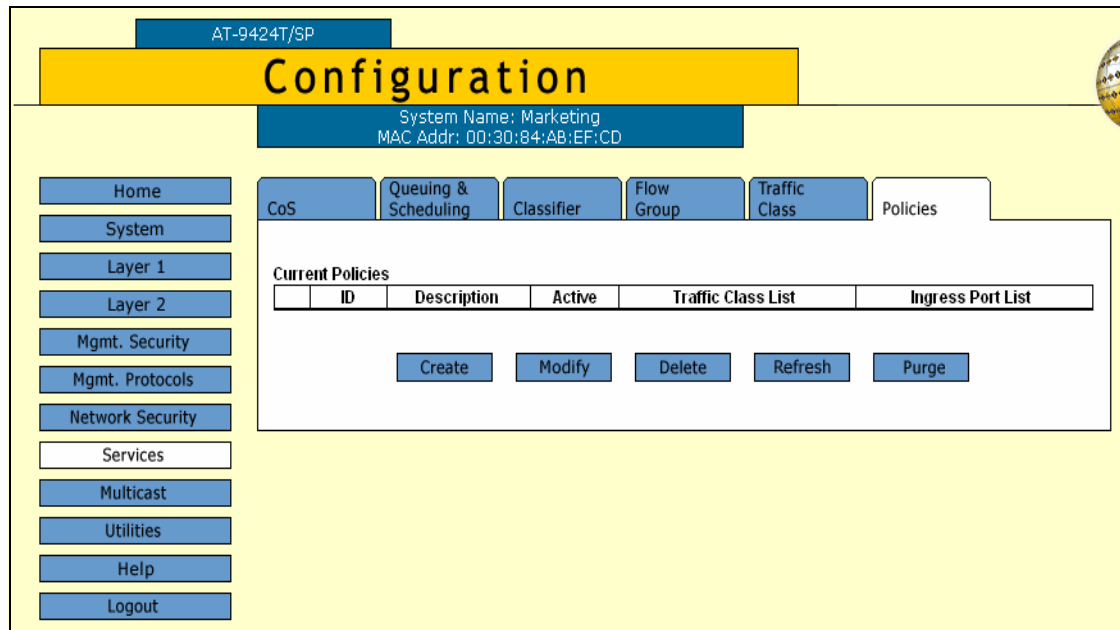


Figure 76. Policies Tab (Configuration)

The Policies tab displays the existing policies in a table that contains the following columns of information:

ID

The ID of the policy.

Description

A description of the policy.

Active

Whether or not this policy is active on the switch.

Traffic Class List

The traffic classes assigned to the policy.

Ingress Port List

The ingress ports to which the policy is assigned.

4. Click **Create**.

The Create Policy page opens, as shown in Figure 77.

Figure 77. Create Policy Page

5. Configure the following parameters as necessary:

ID

Specifies the ID number for this policy. The range is 0 to 255.

Description

Specifies the policy description. A description can be up to 15 alphanumeric characters, including spaces.

Remark DSCP

Specifies the conditions under which the ingress DSCP value is overwritten. Select one of the following options from the list:

None - Disables this function.

All - All packets are remarked.

DSCP Value

Specifies a replacement value to write into the DSCP (TOS) field of the packets. The range is 0 to 63.

Traffic Class List

Specifies the traffic classes to be assigned to the policy. The traffic classes must already exist. Select the classes from the list. To select more than one, use <Ctrl> click.

Ingress Port List

Specifies the ingress ports to which the policy is to be assigned. Select the ports from the list. To select more than one, use <Ctrl> click. A port can be an ingress port of only one policy at a time.

Egress Port

Specifies the egress port to which the policy is to be assigned. A port can be an egress port of only one policy at a time.

Redirect Port

Specifies the port to which the classified traffic from the ingress ports is redirected.

6. Click **Apply**.
7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Modifying a Policy

To modify a policy, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Services** option.

The Services page is displayed with the CoS tab selected by default, as shown in Figure 65 on page 170.

3. Select the **Policies** tab.

The Policies tab is shown in Figure 76 on page 184.

4. Select a policy from the list and click **Modify**.

The Modify Policy page is shown in Figure 78.

Figure 78. Modify Policy Page

5. Modify the following parameters as necessary:

ID

Specifies the ID number for this policy. The range is 0 to 255.

Description

Specifies the policy description. A description can be up to 15 alphanumeric characters, including spaces.

Remark DSCP

Specifies the conditions under which the ingress DSCP value is overwritten. Select one of the following options from the list:

None - Disables this function.

All - All packets are remarked.

DSCP Value

Specifies a replacement value to write into the DSCP (TOS) field of the packets. The range is 0 to 63.

Traffic Class List

Specifies the traffic classes to be assigned to the policy. The traffic classes must already exist. Select the classes from the list. To select more than one, use <Ctrl> click.

Ingress Port List

Specifies the ingress ports to which the policy is to be assigned. Select the ports from the list. To select more than one, use <Ctrl> click. A port can be an ingress port of only one policy at a time.

Egress Port

Specifies the egress port to which the policy is to be assigned. A port can be an egress port of only one policy at a time.

Redirect Port

Specifies the port to which the classified traffic from the ingress ports is redirected.

6. Click **Apply**.
7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting a Policy

To delete a policy, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Services** option.

The Services page is displayed with the CoS tab selected by default, as shown in Figure 65 on page 170.

3. Select the **Policies** tab.

The Policies tab is shown in Figure 76 on page 184.

4. Do one of the following:

- Select a policy from the list and click **Delete**.
- Click **Purge** to delete all the policies

Displaying Policies

To display the policies, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select **Services**.

The Services menu is displayed with the CoS tab selected by default, as shown in Figure 52 on page 152.

3. Select the **Policies** tab.

The Policies tab is shown in Figure 79.

The screenshot shows the 'Monitoring' section of the web browser interface. At the top, there is a yellow header with the text 'Monitoring'. Below this, a blue bar displays 'System Name: Marketing' and 'MAC Addr: 00:30:84:AB:EF:CD'. A navigation menu on the left includes options like Home, System, Layer 1, Layer 2, Mgmt. Security, Mgmt. Protocols, Network Security, Services, Multicast, Utilities, Help, and Logout. The main content area has tabs for CoS, Queuing & Scheduling, Classifier, Flow Group, Traffic Class, and Policies. The 'Policies' tab is active, showing a table of 'Current Policies' with columns for ID, Description, Active, Traffic Class List, and Ingress Port List. A 'View' button is located below the table.

Current Policies					
	ID	Description	Active	Traffic Class List	Ingress Port List
	0	test	Yes	0	22

Figure 79. Policies Tab (Monitoring)

The Policies tab displays the existing policies in a table that contains the following columns of information:

ID

The ID of the policy.

Description

A description of the policy.

Active

Whether or not this policy is active on the switch.

Traffic Class List

The traffic classes assigned to the policy.

Ingress Port List

The ingress ports to which the policy is assigned.

- To view the details of a specific policy, select the policy and click View.

The View Policy page is shown in Figure 80.

View Policy	
ID 0	Description audio
Remark DSCP None	DSCP Value None
Traffic Class List 0	Ingress Port List 22
Egress Port 3	Redirect Port 1

Figure 80. View Policy Page

The View Policy page contains the following information:

ID

The ID of the policy.

Description

A description of the policy.

Remark DSCP

The conditions under which the ingress DSCP value is overwritten.

DSCP Value

A replacement value to write into the DSCP (TOS) field of the packets.

Traffic Class List

The traffic classes to be assigned to the policy.

Ingress Port List

The ingress ports to which the policy is to be assigned.

Egress Port

The egress port to which the policy is to be assigned.

Redirect Port

The port to which the classified traffic from the ingress ports is redirected.

5. Click **Close**.

Chapter 16

Class of Service

This chapter contains instructions on how to configure Class of Service (CoS). This chapter contains the following procedure:

- ❑ “Configuring CoS” on page 192
- ❑ “Mapping CoS Priorities to Egress Queues” on page 195
- ❑ “Configuring Egress Scheduling” on page 198
- ❑ “Displaying the CoS Settings” on page 200
- ❑ “Displaying the QoS Schedule” on page 202

Note

For background information on CoS, refer to Chapter 17, “Class of Service,” in the *AT-S63 Management Software Menu Interface User’s Guide*.

Configuring CoS

This procedure explains how to change the egress queue used to handle untagged ingress packets on a port. This procedure also overrides the priority levels in tagged ingress packets.

To configure CoS, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Services** option.

The Services page is displayed with the CoS tab selected by default, as shown in Figure 81.

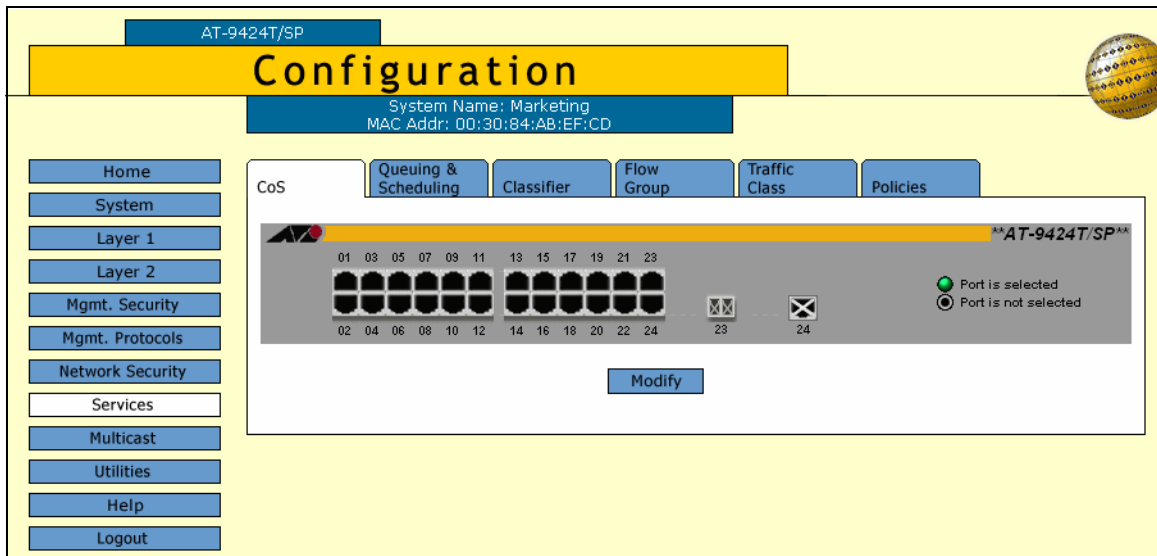


Figure 81. CoS Tab (Configuration)

3. Select the ports whose CoS settings you want to configure and click **Modify**.

The CoS Setting for Port page is shown in Figure 82.

Port	VLAN ID	Default Priority	Override Priority
5	1	0	No
7	1	0	No

Priority: Override Priority

Figure 82. CoS Setting for Port Page

- Use the Priority list to select a value from Level 1 to Level 7 that corresponds to the egress queue where you want all untagged ingress packets on the port to be stored. For example, if you select Level 4, all untagged packets received on the port are stored in egress queue Q2 of the egress port. The default is Level 0, which corresponds to Q0. (If you perform Step 6 and override the priority level in tagged packets, the selected egress queue is also used to store all tagged packets.) The default values are listed in Table 4.

Table 4. Default Mappings of IEEE 802.1p Priority Levels to Priority Queues

IEEE 802.1p Priority Level	Port Priority Queue
0 or 1	Q0 (lowest)
2 or 3	Q1
4 or 5	Q2
6 or 7	Q3 (highest)

- If you are configuring a tagged port and you want the port to ignore the priority tag in egress tagged packets, click the **Override Priority** option. A check in the box indicates this feature is activated. All tagged packets are directed to the egress queue specified in Step 6.

Note

The tagged information in a packet is not changed as the packet traverses the switch. A tagged packet exits the switch with the same priority level that it had when it entered.

The default for this parameter is No, meaning that the priority level of tagged packets is determined by the priority level specified in the packet itself.

6. Click **Apply**.

Configuration changes are immediately activated on the switch.

7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Mapping CoS Priorities to Egress Queues

This procedure explains how to change the default mappings of CoS priorities to egress priority queues, as shown in Table 4 on page 193. This is set at the switch level. You cannot set this on a per-port basis.

To change the mappings, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Services** option.

The Services page is displayed with the CoS tab selected by default, as shown in Figure 81 on page 192.

3. Select the **Queuing & Scheduling** tab.

The Queuing & Scheduling tab is shown in Figure 83.

Figure 83. Queuing & Scheduling Tab (Configuration)

Note

The Configure Egress Weights section in the tab is explained in the next procedure, “Configuring Egress Scheduling” on page 198.

- In the Configure CoS Queues to Egress Queues section of the tab, click the list for a CoS priority whose queue assignment you want to change and select the new queue.

For example, to direct all tagged packets with a CoS priority of 5 to egress queue Q3, you would use the list in **CoS 5 to PQ** and select **Q3 - QoS PriorityQ 3**.

- If desired, repeat Step 4 to change the egress queue assignment of other CoS priorities.
- Click **Apply**.

7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Configuring Egress Scheduling

This procedure explains how to select and configure a scheduling method for QoS. Scheduling determines the order in which the ports handle packets in their egress queues. For an explanation of the two scheduling methods, refer to “Scheduling” in Chapter 13, “Quality of Service,” in the *AT-S63 Management Software Menus Interface User’s Guide*. Scheduling is set at the switch level. You cannot set this at the port level.

To change scheduling, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Services** option.

The Services page is displayed with the CoS tab selected by default, as shown in Figure 81 on page 192.

3. Select the **Queuing & Scheduling** tab.

The Queuing & Scheduling tab is shown in Figure 83 on page 196.

Note

The Configure CoS Queues to Egress Queues section in the tab is explained in the previous procedure “Mapping CoS Priorities to Egress Queues” on page 195.

4. To select a scheduling method, click either **Strict Priority** or **Weighted Priority** in the Configure Egress Weights section of the tab. The default is Strict Priority.

Skip the next step if you select Strict Priority. Queue weights do not apply to Strict Priority scheduling.

5. If you selected Weighted Priority, use the Queue # Weight fields to specify for each queue the number of packets you want a port to transmit before it goes to the next queue. For an example, refer to Table 5.

Table 5. Example of Weighted Round Robin Priority

Port Egress Queue	Maximum Number of Packets
Q3	15
Q2	10

Table 5. Example of Weighted Round Robin Priority (Continued)

Port Egress Queue	Maximum Number of Packets
Q1	5
Q0	1

Leaving the default value of 1 for each queue results in all egress queues being given the same priority.

6. Click **Apply**.
7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying the CoS Settings

To display the CoS settings, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select **Services**.

The Services page is displayed with the CoS tab selected by default, as shown in Figure 84.

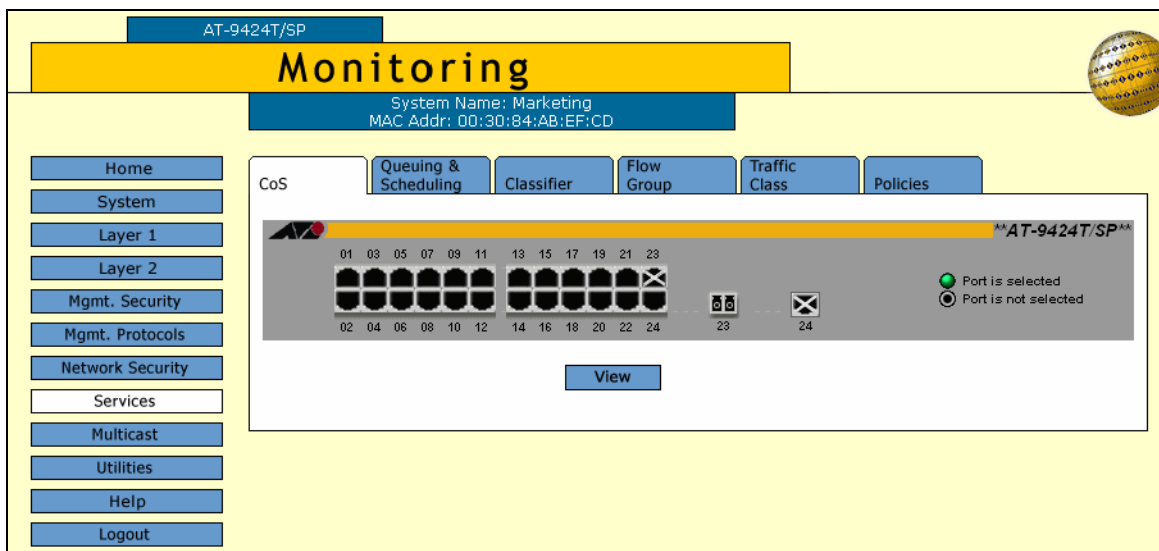
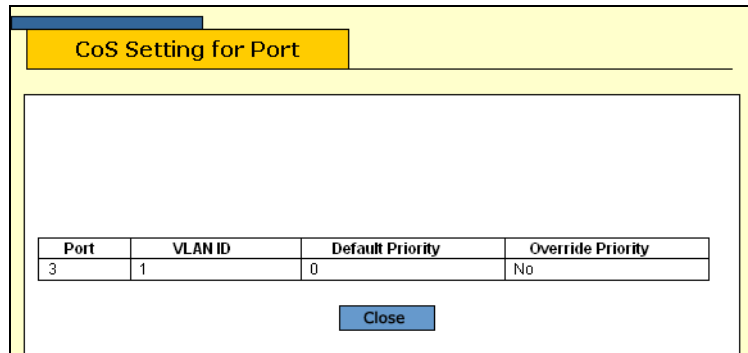


Figure 84. CoS Tab (Monitoring)

3. Click the port where you want to view the settings. You can select more than one port at a time. A selected port turns white. (To deselect a port, click it again.)
4. Click **View**.

The CoS Setting for Port page is shown in Figure 85.



Port	VLAN ID	Default Priority	Override Priority
3	1	0	No

Close

Figure 85. CoS Setting for Port Page

The CoS Setting for Port page displays a table that contains the following columns of information:

Port

The port number.

VLAN ID

The VLAN of which the port is a member.

Default Priority

The default priority level for this port.

Override Priority

Whether or not the default priority should be overridden.

5. Click **Close**.

Displaying the QoS Schedule

To display the QoS schedule, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Services** option.

The Services page is displayed with the CoS tab selected by default, as shown in Figure 52 on page 152.

3. Select the **Queuing and Scheduling** tab.

The Queuing and Scheduling tab is shown in Figure 86.

The screenshot shows the 'Monitoring' interface for a system named 'Marketing' with MAC address '00:30:84:AB:EF:CD'. The 'Queuing & Scheduling' tab is selected, showing the following configuration:

CoS Priority to Egress Queues	
CoS 0 to PQ QoS PriorityQ 1	CoS 1 to PQ QoS PriorityQ 0
CoS 2 to PQ QoS PriorityQ 2	CoS 3 to PQ QoS PriorityQ 3
CoS 4 to PQ QoS PriorityQ 4	CoS 5 to PQ QoS PriorityQ 5
CoS 6 to PQ QoS PriorityQ 6	CoS 7 to PQ QoS PriorityQ 7

Egress Weights	
Select Schedule Strict Priority	
Queue 0 Weight(Weighted) Weight 0	Queue 4 Weight(Weighted) Weight 0
Queue 1 Weight(Weighted) Weight 0	Queue 5 Weight(Weighted) Weight 0
Queue 2 Weight(Weighted) Weight 0	Queue 6 Weight(Weighted) Weight 0
Queue 3 Weight(Weighted) Weight 0	Queue 7 Weight(Weighted) Weight 0

Figure 86. QoS Scheduling Tab (Monitoring)

The upper section displays the CoS priority to egress queue assignments. The lower section displays the egress weight settings.

Chapter 17

IGMP Snooping

This chapter describes how to configure the IGMP snooping feature on the switch. The sections in the chapter include:

- ❑ “Configuring IGMP Snooping” on page 204
- ❑ “Displaying a List of Host Nodes” on page 207
- ❑ “Displaying a List of Multicast Routers” on page 210

Note

For background information, refer to Chapter 18, “IGMP Snooping,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Configuring IGMP Snooping

To configure IGMP snooping, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Multicast** option.

The Multicast page is displayed with the **IGMP** tab selected by default, as shown in Figure 87.

Figure 87. IGMP Tab (Configuration)

3. Configure the following parameters as necessary.

Enable IGMP Snooping Status

Enables and disables IGMP snooping on the switch. A check in the box indicates that IGMP is enabled.

Multicast Host Topology

Defines whether there is only one host node per switch port or multiple host nodes per port. Possible settings are Edge (Single-Host/Port) and Intermediate (Multi-Host/Port).

The Edge (Single-Host/Port) setting is appropriate when there is only one host node connected to each port on the switch. This setting causes the switch to immediately stop sending multicast packets out a switch port when a host node signals its desire to leave a multicast group by sending a leave request or when the host node stops sending

reports and times out. The switch forwards the leave request to the router and simultaneously ceases transmission of any further multicast packets out the port where the host node is connected.

The Intermediate (Multi-Host) setting is appropriate if there is more than one host node connected to a switch port, such as when a port is connected to an Ethernet hub to which multiple host nodes are connected. With this setting selected the switch continues sending multicast packets out a port even after it receives a leave request from a host node on the port. This ensures that the remaining active host nodes on the port continue to receive the multicast packets. Only after all of the host nodes connected to a switch port have transmitted leave requests (or have timed out) does the switch stop sending multicast packets out the port.

If a switch has a mixture of host nodes, that is, some connected directly to the switch and others through an Ethernet hub, you should select the Intermediate Multi-Host Port selection.

Multicast Router Ports Mode

Specifies whether the router ports are determined automatically or if you enter them manually. If you want the switch to determine the ports automatically, select Auto-Detect, which is the default. To enter them yourself, click Manual Select and enter the ports in the field.

Host/Router Timeout Interval

Specifies the time period in seconds after which the switch determines that a host node has become inactive. An inactive host node is a node that has not sent an IGMP report during the specified time interval. The range is from 1 second to 86,400 seconds (24 hours). The default is 260 seconds.

This parameter also specifies the time interval used by the switch in determining whether a multicast router is still active. The switch makes the determination by watching for queries from the router. If the switch does not detect any queries from a multicast router during the specified time interval, it assumes that the router is no longer active on the port.

Maximum Multicast Groups

Specifies the maximum number of multicast groups the switch learns. The range is 1 to 255 groups. The default is 64 multicast groups.

This setting is useful with networks that contain a large number of multicast groups. You can use the parameter to prevent the switch's MAC address table from filling up with multicast addresses, leaving no room for dynamic or static MAC addresses. The range is 1 address to 2048 addresses. The default is 256 multicast addresses.

4. Click **Apply**.

5. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying a List of Host Nodes

You can use the AT-S63 management software to display a list of the multicast groups on a switch, as well as the host nodes. You can also view the multicast routers. A multicast router is a router that is receiving multicast packets from a multicast application and transmitting the packets to host nodes.

To view host nodes, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Multicast** option.

The Multicast page is displayed with the IGMP tab as shown in Figure 88.

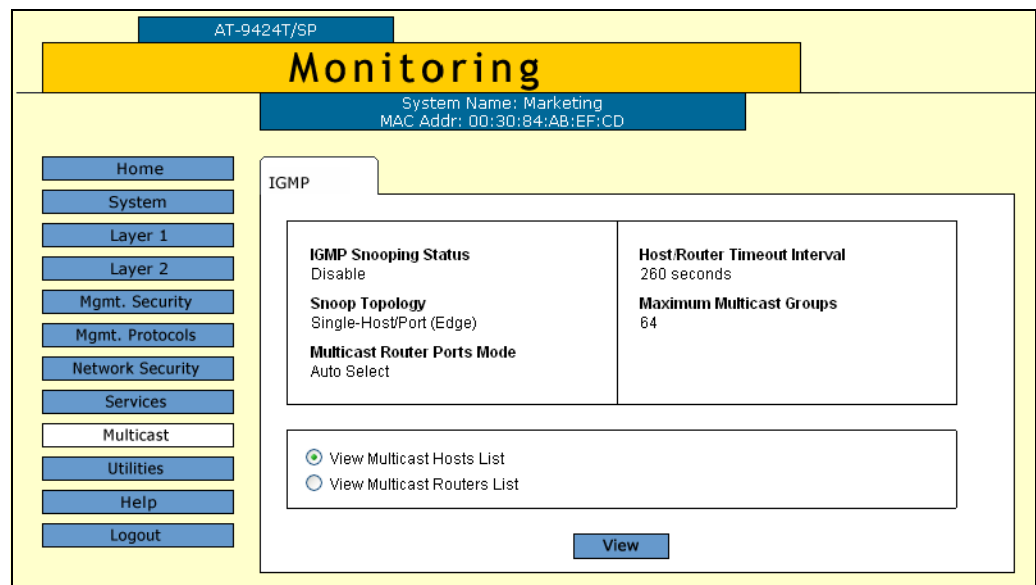


Figure 88. IGMP Tab (Monitoring)

The IGMP tab provides the following information:

Enable IGMP Snooping Status

The IGMP snooping status on the switch. Possible settings are Enabled and Disabled

Snoop Topology

Whether there is only one host node per switch port or multiple host nodes per port. The possible settings are Edge (Single-Host/Port) and Intermediate (Multi-Host/Port).

Multicast Router Ports Mode

How the router ports are determined. The possible settings are:

Auto-Detect - The switch determines the ports automatically.

Port number - The selected router ports.

Host/Router Timeout Interval

The time period in seconds after which the switch determines that a host node has become inactive.

Maximum Multicast Groups

The maximum number of multicast groups the switch learns.

3. To view the multicast addresses and the host nodes, click **View Multicast Hosts List** and then click **View**.

The View Multicast Hosts List is shown in Figure 89.

Total Multicast Groups: 4. Page 1 of 1				
Multicast Group	VLAN ID	Member Port	Host IP	Status
01:00:5E:00:01:01	1	6	172.16.10.51	Active
01:00:5E:7F:FF:FA	1	5	149.35.200.75	Active
			149.35.200.65	Active
01:00:5E:00:00:02	1	17	149.35.200.69	Active
01:00:5E:00:00:09	1	14	149.35.200.61	Active

Figure 89. View Multicast Hosts List Page

The View Multicast Hosts List page displays a table that contains the following columns of information:

Multicast Group

The multicast address of the group.

VLAN ID

The VID of the VLAN in which the port is an untagged member.

Member Port

The port(s) on the switch to which one or more host nodes of the multicast group are connected.

Host IP

The IP address(es) of the host node(s) connected to the port.

Status

Indicates IGMP group status of the port. The possible settings are:

Active - The port is active in the IGMP group.

Left Group - The port is not active in the IGMP group.

Displaying a List of Multicast Routers

To view multicast routers, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. Select the **IGMP** tab.

The IGMP tab is shown in Figure 88 on page 207.

3. To view the multicast routers, click **View Multicast Router List** and then click **View**.

The View Multicast Routers List is shown in Figure 90.

Total Multicast Routers: 1. Page 1 of 1		
Port	VLAN ID	Router IP
1	1	172.16.10.1

Figure 90. View Multicast Routers List Page

The View Multicast Routers List page displays a table that contains the following columns of information:

Port

The port on the switch where the multicast router is connected.

VLAN ID

The VID of the VLAN in which the port is an untagged member.

Router IP

The IP address of the port on the router.

If the routers are static routers (specified with the Manual Select option on the Configuration IGMP page), then the View Multicast Routers List

page opens, as shown in Figure 91.

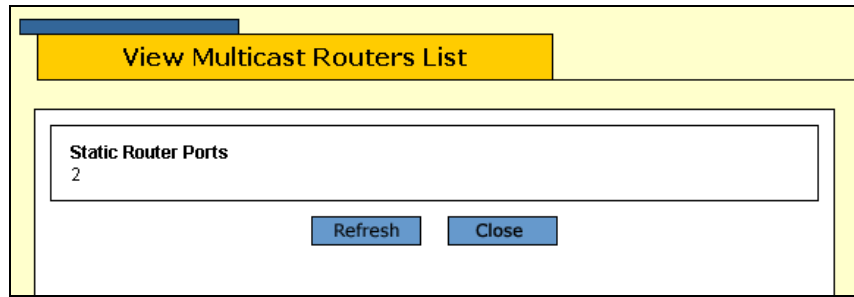


Figure 91. View (Static) Multicast Routers List Page

Section III

SNMPv3

The chapter in this section provides information and procedures for SNMPv3. The chapter is:

- Chapter 18, “SNMPv3” on page 215

Chapter 18

SNMPv3

This chapter provides the following procedures for configuring SNMPv3 parameters using a web browser management session:

- ❑ “Configuring the SNMPv3 Protocol” on page 216
- ❑ “Enabling or Disabling SNMP Management” on page 217
- ❑ “Configuring the SNMPv3 User Table” on page 220
- ❑ “Configuring the SNMPv3 View Table” on page 228
- ❑ “Configuring the SNMPv3 Access Table” on page 234
- ❑ “Configuring the SNMPv3 SecurityToGroup Table” on page 241
- ❑ “Configuring the SNMPv3 Notify Table” on page 247
- ❑ “Configuring the SNMPv3 Target Address Table” on page 252
- ❑ “Configuring the SNMPv3 Target Parameters Table” on page 259
- ❑ “Configuring the SNMPv3 Community Table” on page 266
- ❑ “Displaying SNMPv3 Tables” on page 272

Note

For background information on SNMPv3, refer to Chapter 20, “SNMPv3,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Configuring the SNMPv3 Protocol

To configure the SNMPv3 protocol, you need to first enable SNMP access on the switch. Then you configure the SNMPv3 tables. See the following procedures:

- ❑ “Enabling or Disabling SNMP Management” on page 217
- ❑ “Configuring the SNMPv3 User Table” on page 220
- ❑ “Configuring the SNMPv3 View Table” on page 228
- ❑ “Configuring the SNMPv3 Access Table” on page 234
- ❑ “Configuring the SNMPv3 SecurityToGroup Table” on page 241
- ❑ “Configuring the SNMPv3 Notify Table” on page 247
- ❑ “Configuring the SNMPv3 Target Address Table” on page 252
- ❑ “Configuring the SNMPv3 Target Parameters Table” on page 259
- ❑ “Configuring the SNMPv3 Community Table” on page 266

Note

Use the SNMPv3 Community Table only if you are configuring the SNMPv3 protocol with an SNMPv1 or an SNMPv2c implementation. Allied Telesyn does not recommend this configuration.

Enabling or Disabling SNMP Management

In order to allow an SNMP manager or host to access the switch you need to enable SNMP access. In addition, to allow the switch to send a trap when it receives a login attempt from an unauthenticated user, you need to enable authentication failure traps. This section provides a procedure to accomplish both of these tasks.

To enable SNMP access and authentication failure traps, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Mgmt. Protocols** option.

The Mgmt. Protocols page is displayed with the Server-based Authentication tab selected by default, as shown in Figure 10 on page 54.

3. Select the **SNMP** tab.

The SNMP tab is shown in Figure 92.

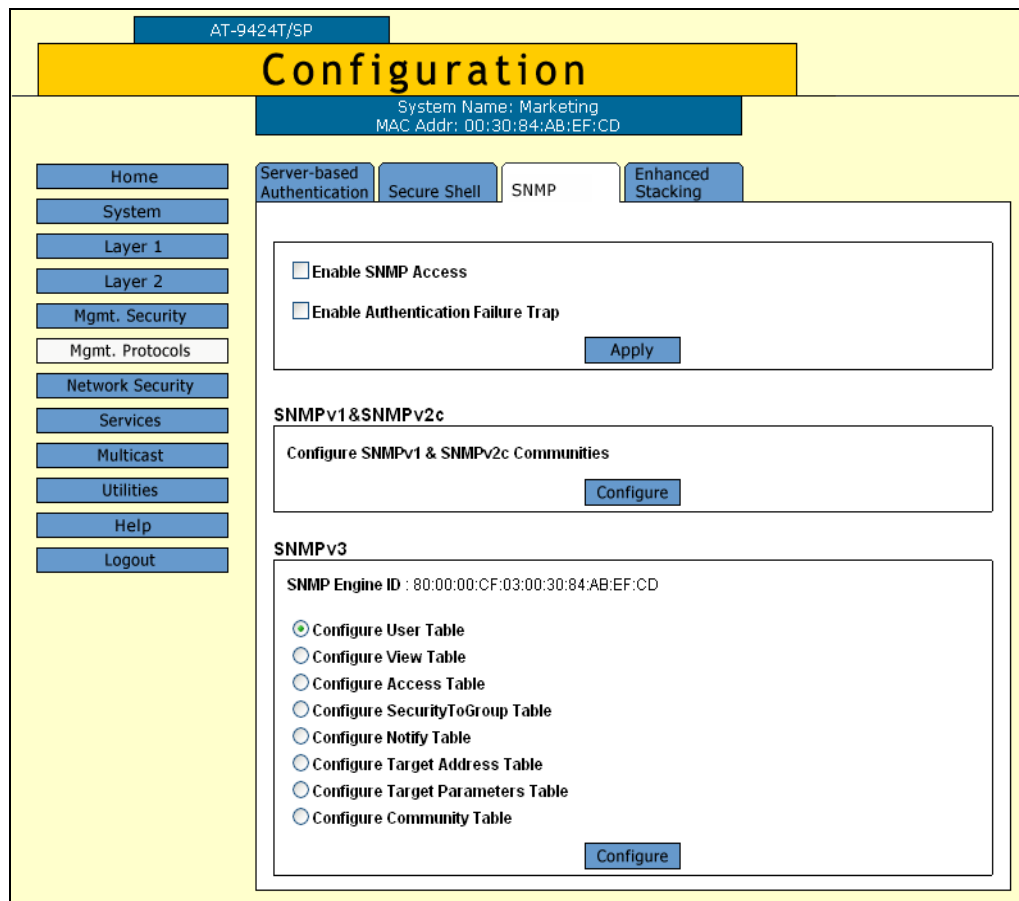


Figure 92. SNMP Tab (Configuration)

- Click the **Enable SNMP Access** checkbox to enable or disable SNMP management. A check in the box indicates that the feature is enabled, meaning that the switch can be managed from an SNMP management station. No check indicates that the feature is disabled. The default is disabled.

Use this parameter to enable the switch to be remotely managed with an SNMP application program.

Note

If the Enable SNMP Access check box is not checked, the switch cannot be managed through SNMP. This is the default.

- If you want the switch to send authentication failure traps, click the **Enable Authentication Failure Traps** checkbox. A check in the box indicates that the switch sends the trap.
- Click **Apply**.

7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Configuring the SNMPv3 User Table

You can create, delete, and modify an SNMPv3 User Table entry. See the following procedures:

- “Creating a User Table Entry” on page 220
- “Deleting a User Table Entry” on page 223
- “Modifying a User Table Entry” on page 224

For reference information about the SNMPv3 User Table, see Chapter 18, “SNMPv3” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Creating a User Table Entry

To create an entry in the SNMPv3 User Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 92 on page 218.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 92 on page 218.

3. In the SNMPv3 section, click the button next to **Configure User Table** and then click **Configure** at the bottom of the tab.

The SNMPv3 User Table tab is shown in Figure 93.

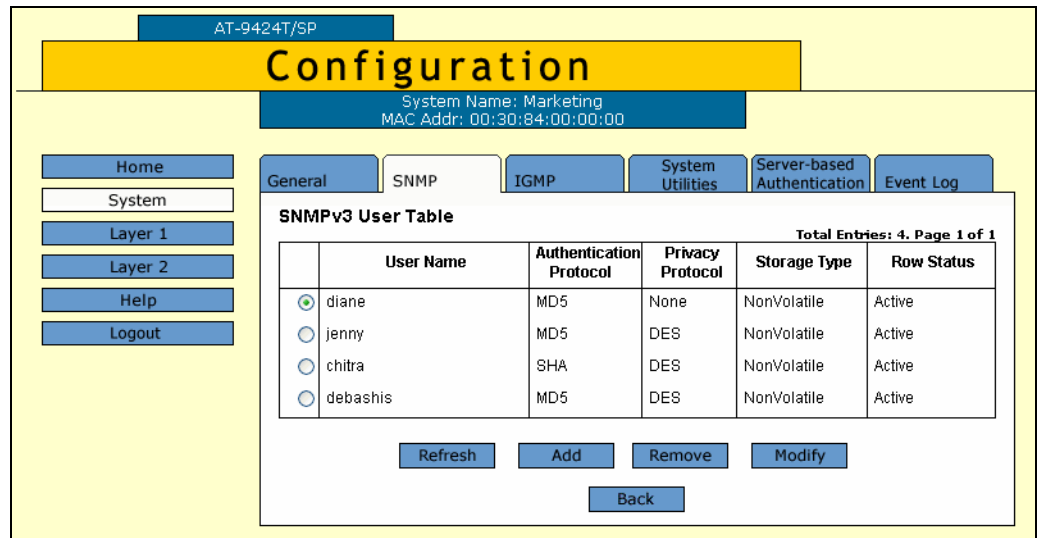


Figure 93. SNMPv3 User Table Tab (Configuration)

4. Click **Add**.

The Add New SNMPv3 User page is shown in Figure 94.

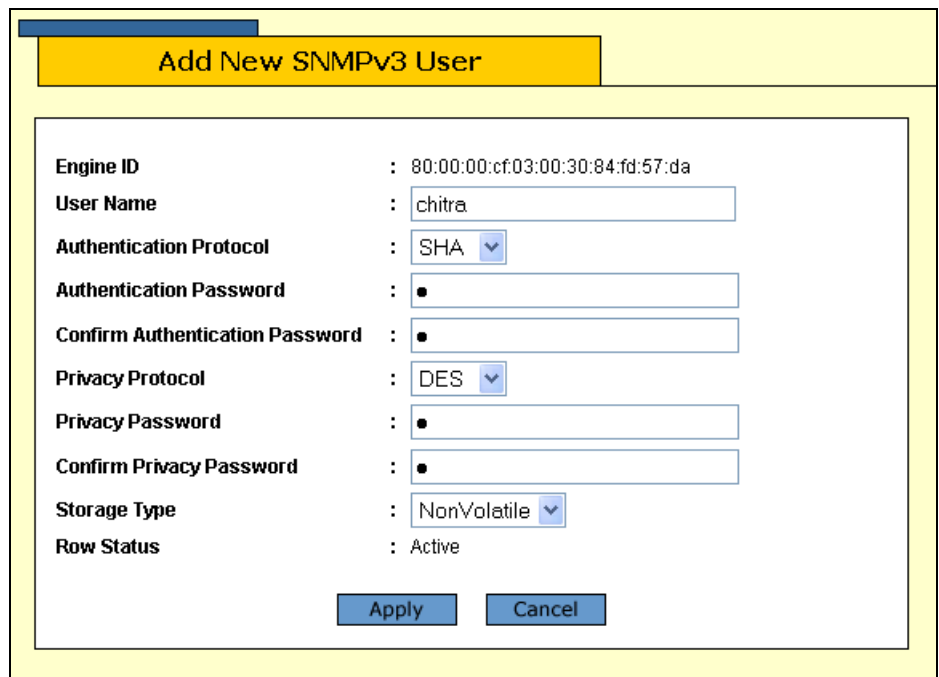


Figure 94. Add New SNMPv3 User Page

5. In the User Name field, enter a name, or logon id, that consists of up to 32 alphanumeric characters

6. In the Authentication Protocol field, enter an authentication protocol. This is an optional parameter.

Select one of the following:

MD5

This value represents the MD5 authentication protocol. With this selection, users (SNMP entities) are authenticated with the MD5 authentication protocol after a message is received. This algorithm generates the message digest. The user is authenticated when the authentication protocol checks the message digest. With the MD5 selection, you can configure a Privacy Protocol.

SHA

This value represents the SHA authentication protocol. With this selection, users are authenticated with the SHA authentication protocol after a message is received. This algorithm generates the message digest. The user is authenticated when the authentication protocol checks the message digest. With the SHA selection, you can configure a Privacy Protocol.

None

This value represents no authentication protocol. When messages are received, users are not authenticated. With the None selection, you cannot configure a Privacy Protocol.

Note

You may want to assign NONE to a super user.

7. In the Authentication Password field, enter an authentication password of up to 32 alphanumeric characters.
8. In the Confirm Authentication Password field, re-enter the authentication password.

Note

If you have the nonencrypted version of the AT-S60 software, then the Privacy Protocol field is read-only.

Note

You can only configure the Privacy Protocol if you have configured the Authentication Protocol with the MD5 or SHA values.

9. In the Privacy Protocol field, enter one of the following options:

DES

Select this value to make the DES privacy (or encryption) protocol the

privacy protocol for this User Table entry. With this selection, messages transmitted between the host and the switch are encrypted with the DES protocol.

None

Select this value if you do not want a privacy protocol for this User Table entry. With this selection, messages transmitted between the host and the switch are not encrypted.

10. In the Privacy Password field, enter a privacy password of up to 32 alphanumeric characters.
11. In the Confirm Privacy Password field, re-enter the privacy password.
12. In the Storage Type field, enter one of the following storage options for this table entry:

Volatile

Select this storage type if you do not want the ability to save an entry in the User Table. After making changes to an User Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

NonVolatile

Select this storage type if you want the ability to save an entry in the User Table. After making changes to an User Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesyn recommends this storage type.

Note

The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 User Table entry takes effect immediately.

13. Click **Apply** to update the SNMPv3 User Table.
14. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting a User Table Entry

To delete an entry in the SNMPv3 User Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 92 on page 218.

3. In the SNMPv3 section, click the button next to **Configure User Table** and then click **Configure**.

The SNMPv3 User Table tab is shown in Figure 93 on page 221.

4. Click the button next to the User Table entry that you want to delete and then click **Remove**.

A warning message is displayed.

5. Click **OK**.
6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Modifying a User Table Entry

To modify an entry SNMPv3 User Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 92 on page 218.

3. In the SNMPv3 section, click the button next to **Configure User Table** and then click **Configure**.

The SNMPv3 User Table tab is shown in Figure 93 on page 221.

4. Click the button next to the SNMPv3 user that you want to change and then click **Modify**.

The Modify SNMPv3 User page is shown in Figure 95.

Figure 95. Modify SNMPv3 User Page

- In the Authentication Protocol field, enter an authentication protocol. This is an optional parameter.

Select one of the following:

MD5

This value represents the MD5 authentication protocol. With this selection, users (SNMP entities) are authenticated with the MD5 authentication protocol after a message is received. This algorithm generates the message digest. The user is authenticated when the authentication protocol checks the message digest. With the MD5 selection, you can configure a Privacy Protocol.

SHA

This value represents the SHA authentication protocol. With this selection, users are authenticated with the SHA authentication protocol after a message is received. This algorithm generates the message digest. The user is authenticated when the authentication protocol checks the message digest. With the SHA selection, you can configure a Privacy Protocol.

None

This value represents no authentication protocol. When messages are received, users are not authenticated. With the None selection, you cannot configure a Privacy Protocol.

Note

You may want to assign NONE to a super user.

6. In the Authentication Password field, enter an authentication password of up to 32 alphanumeric characters.
7. In the Confirm Authentication Password field, re-enter the authentication password.

Note

If you have the nonencrypted version of the AT-S60 software, then the Privacy Protocol field is read-only.

Note

You can only configure the Privacy Protocol if you have configured the Authentication Protocol with the MD5 or SHA values.

8. In the Privacy Protocol field, enter one of the following options:

DES

Select this value to make the DES privacy (or encryption) protocol the privacy protocol for this User Table entry. With this selection, messages transmitted between the host and the switch are encrypted with the DES protocol.

None

Select this value if you do not want a privacy protocol for this User Table entry. With this selection, messages transmitted between the host and the switch are not encrypted.

9. In the Privacy Password field, enter a privacy password of up to 32 alphanumeric characters.
10. In the Confirm Privacy Password field, re-enter the privacy password.
11. In the Storage Type field, enter one of the following storage options for this User Table entry:

Volatile

Select this storage type if you do not want the ability to save an entry in the SNMPv3 User Table. After making changes to an SNMPv3 User Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

NonVolatile

Select this storage type if you want the ability to save an entry in the SNMPv3 User Table. After making changes to an SNMPv3 User Table

entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesyn recommends this storage type.

Note

The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 User Table entry takes effect immediately.

12. Click **Apply** to update the SNMPv3 User Table.
13. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Configuring the SNMPv3 View Table

You can create, delete, and modify an SNMPv3 View Table entry. See the following procedures:

- “Creating a View Table Entry” on page 228
- “Deleting a View Table Entry” on page 231
- “Modifying a View Table Entry” on page 231

For reference information about the SNMPv3 View Table, see Chapter 20, “SNMPv3” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Creating a View Table Entry

To create an entry in the SNMPv3 View Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 92 on page 218.

3. In the SNMPv3 section, click the button next to **Configure View Table** and then click **Configure** at the bottom of the tab.

The SNMPv3 View Table tab is shown in Figure 96.

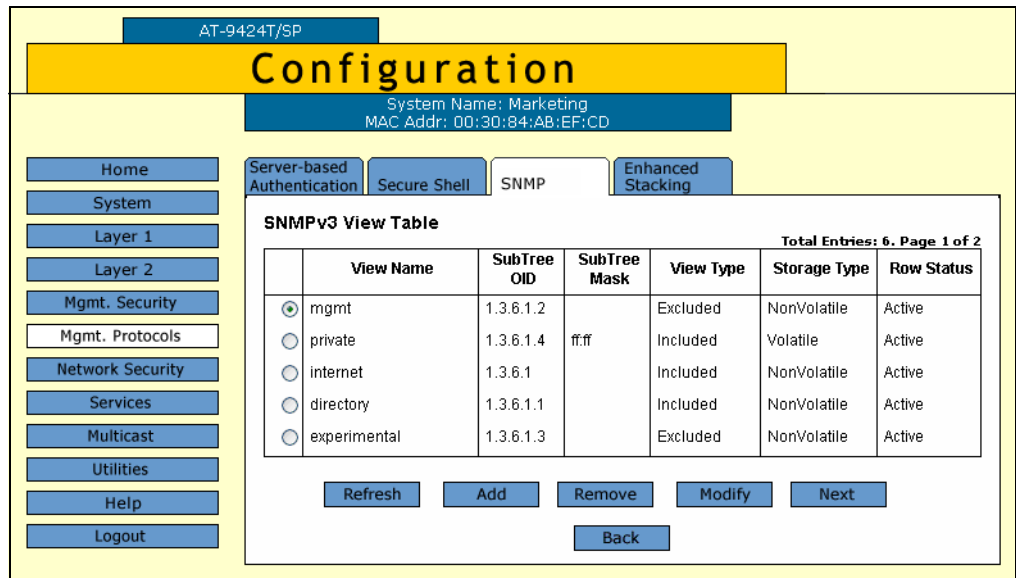


Figure 96. SNMPv3 View Table Tab (Configuration)

4. Click **Add**.

The Add New SNMPv3 View page is shown in Figure 97.

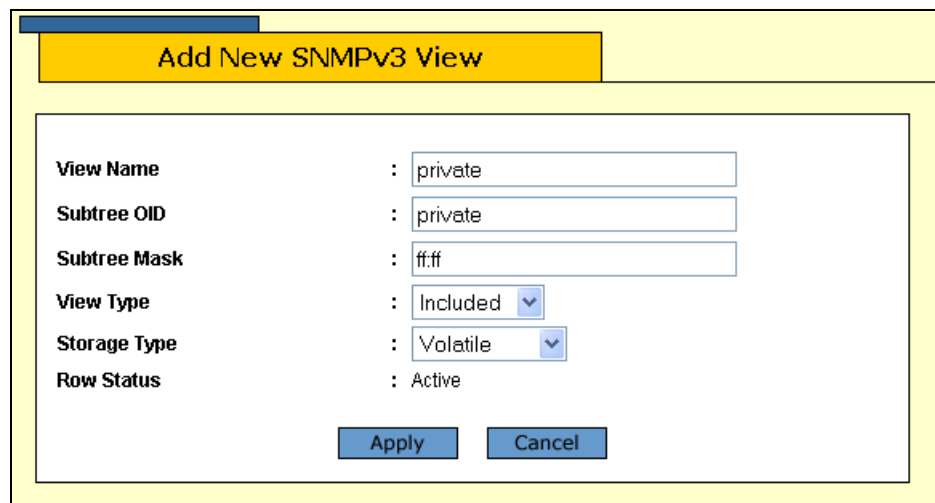


Figure 97. Add New SNMPv3 View Page

5. In the View Name field, enter a descriptive name for this view.

Assign a name that reflects the subtree OID, for example, "internet."
Enter a unique name of up to 32 alphanumeric characters.

Note

The “defaultViewAll” value is the default entry for the SNMPv1 and SNMPv2c configuration. You cannot use the default value for an SNMPv3 View Table entry.

6. In the Subtree OID field, enter a subtree that this view will or will not be permitted to display.

You can enter either a numeric value in hex format or the equivalent text name. For example, the OID hex format for TCP/IP is:

1.3.6.1.2.1.6

The text format is for TCP/IP is:

tcp

7. In the Subtree Mask field, enter a subtree mask in hexadecimal format.

This is an optional parameter that is used to further refine the value of the Subtree OID parameter.

The Subtree OID parameter defines a MIB View and the Subtree Mask parameter further restricts a user’s view to a specific the column and row of the MIB View. The value of the Subnet Mask parameter is dependent on the subtree you select. For example, if you configure the View Subtree parameter as MIB ifEntry.0.3, it has the following value:

1.3.6.1.2.1.2.2.1.0.3

To restrict the user’s view to the third row (all columns) of the MIB ifEntry.0.3, enter the following value for the Subtree Mask parameter

ff:bf

8. In the View Type field, enter one of the following view types:

Included

Enter this value to permit the user to see the subtree specified above.

Excluded

Enter this value to not permit the user to see the subtree specified above.

9. In the Storage Type field, enter a storage type for this table entry:

Volatile

Select this storage type if you do not want the ability to save an entry in the View Table. After making changes to a View Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

NonVolatile

Select this storage type if you want the ability to save an entry in the View Table. After making changes to a View Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesyn recommends this storage type.

Note

The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 View Table entry takes effect immediately.

10. Click **Apply** to update the SNMPv3 View Table.
11. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting a View Table Entry

To delete an entry in the SNMPv3 View Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 92 on page 218.

3. In the SNMPv3 section, click the button next to **Configure View Table** and then click **Configure**.

The SNMPv3 View Table tab is shown in Figure 96 on page 229.

4. Click the button next to the View Table entry that you want to delete and then click **Remove**.

A warning message is displayed.

5. Click **OK**.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Modifying a View Table Entry

To modify an entry in the SNMPv3 View Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 92 on page 218.

3. In the SNMPv3 section, click the button next to Configure View Table and then click **Configure** at the bottom of the tab.

The SNMPv3 View Table tab is shown in Figure 96 on page 229.

4. Click the button next to the SNMPv3 View Table entry that you want to change and then click **Modify**.

The Modify SNMPv3 View page is shown in Figure 98.

The screenshot shows a web-based configuration interface for modifying an SNMPv3 view. The title bar is yellow and contains the text 'Modify SNMPv3 View'. The main content area is white and contains several labeled fields:

- View Name**: mgmt
- Subtree OID**: 1.3.6.1.2
- Subtree Mask**: An empty text input field.
- View Type**: A dropdown menu currently set to 'Included'.
- Storage Type**: A dropdown menu currently set to 'NonVolatile'.
- Row Status**: Active

At the bottom of the form are two blue buttons: 'Apply' and 'Cancel'.

Figure 98. Modify SNMPv3 View Page

5. In the Subtree Mask field, enter a subtree mask in hexadecimal format.

This is an optional parameter that is used to further refine the value of the Subtree OID parameter.

The Subtree OID parameter defines a MIB View and the Subtree Mask parameter further restricts a user's view to a specific the column and row of the MIB View. The value of the Subnet Mask parameter is dependent on the subtree you select. For example, if you configure the View Subtree parameter as MIB ifEntry.0.3, it has the following value:

1.3.6.1.2.1.2.2.1.0.3

To restrict the user's view to the third row (all columns) of the MIB ifEntry.0.3, enter the following value for the Subtree Mask parameter

ff:bf

6. In the View Type field, enter one of the following view types:

Included

Enter this value to permit the View Name to see the subtree specified above.

Excluded

Enter this value to not permit the View Name to see the subtree specified above.

7. In the Storage Type field, enter a storage type for this table entry:

Volatile

Select this storage type if you do not want the ability to save an entry in the Target Parameters Table. After making changes to an Target Parameters Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

NonVolatile

Select this storage type if you want the ability to save an entry in the View Table. After making changes to a View Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesyn recommends this storage type.

Note

The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 View Table entry takes effect immediately.

8. Click **Apply**.
9. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Configuring the SNMPv3 Access Table

You can create, delete, and modify an SNMPv3 Access Table entry. See the following procedures:

- “Creating an Access Table” on page 234
- “Deleting an Access Table Entry” on page 237
- “Modifying an Access Table Entry” on page 238

For information about the SNMPv3 Access Table, see Chapter 20, “SNMPv3” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Creating an Access Table

To create an entry in the SNMPv3 Access Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 92 on page 218.

3. In the SNMPv3 section, click the button next to **Configure Access Table** and then click **Configure** at the bottom of the tab.

The SNMPv3 Access Table tab is shown in Figure 99.

The screenshot shows the Configuration System interface. At the top, there is a yellow header with the text "Configuration" and "System Name: Marketing, MAC Addr: 00:30:84:AB:EF:CD". Below this, there are several tabs: "Server-based Authentication", "Secure Shell", "SNMP", and "Enhanced Stacking". The "SNMP" tab is selected. On the left side, there is a vertical menu with buttons for "Home", "System", "Layer 1", "Layer 2", "Mgmt. Security", "Mgmt. Protocols", "Network Security", "Services", "Multicast", "Utilities", "Help", and "Logout". The main content area displays the "SNMPv3 Access Table" configuration for a group named "testengineering". The configuration details are as follows:

SNMPv3 Access Table		Total Entries: 6. Page 2 of 6	
Group Name	testengineering	Security Model	v3
Context Prefix		Security Level	AuthPriv
Read View	internet	Context Match	Exact
Write View	private	Storage Type	NonVolatile
Notify View	internet	Row Status	Active

At the bottom of the configuration area, there are buttons for "Refresh", "Add", "Remove", "Modify", "Previous", and "Next". A "Back" button is located at the bottom center of the page.

Figure 99. SNMPv3 Access Table Tab (Configuration)

4. To create an SNMPv3 Access Table entry, click **Add**.

The Add New SNMPv3 Access page is shown in Figure 100.

Figure 100. Add New SNMPv3 Access Page

5. In the Group Name field, enter a descriptive name of the group.

The Group Name can consist of up to 32 alphanumeric characters.

You are not required to enter a unique value here because the SNMPv3 Access Table entry is indexed with the Group Name, Security Model, and Security Level parameter values. However, a unique group name makes it easier for you to tell the groups apart.

There are four default values for this field that are reserved for SNMPv1 and SNMPv2c implementations:

- defaultV1GroupReadOnly
- defaultV1GroupReadWrite
- defaultV2cGroupReadOnly
- defaultV2cGroupReadWrite

Note

The Context Prefix field is a read only field. The Context Prefix field is always set to null.

6. In the Read View Name field, enter a value that you configured with the View Name parameter in the SNMPv3 View Table.

This parameter allows the users assigned to this Group Name to view the information specified by the View Table entry. This value does not need to be unique.

7. In the Write View Name field, enter a value that you configured with the View Name parameter in the SNMPv3 View Table.

This parameter allows the users assigned to this Security Group to write, or modify, the information in the specified View Table. This value does not need to be unique.

8. In the Notify View Name field, enter a value that you configured with the View Name parameter in the SNMPv3 View Table.

This parameter allows the users assigned to this Group Name to send traps permitted in the specified View. This value does not need to be unique.

9. In the Security Model field, enter an SNMP protocol.

Select one of the following SNMP protocols as the Security Model for this Group Name.

v1

Select this value to associate the Group Name with the SNMPv1 protocol.

v2c

Select this value to associate the Group Name with the SNMPv2c protocol.

v3

Select this value to associate the Group Name with the SNMPv3 protocol.

10. In the Security Level field, enter a security level.

Select one of the following security levels:

No Authentication/Privacy

This option represents neither an authentication nor privacy protocol. Select this security level if you do not want to authenticate SNMP entities and you do not want to encrypt messages using a privacy protocol. This option provides the least security.

Note

If you have selected SNMPv1 or SNMPv2c, N-NoAuthNoPriv is the only security level you can select.

Authentication

This option permits an authentication protocol, but not a privacy

protocol. Select this security level if you want to authenticate SNMP users, but you do not want to encrypt messages using a privacy protocol. You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

Privacy

This option represents authentication and the privacy protocol. Select this security level to allow authentication and encryption. This level provides the greatest level of security. You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

Note

The Context Match field is a read only field. The Context Match field is always set to Exact.

11. In the Storage Type field, select one of the following storage types for this table entry:

Volatile

Select this storage type if you do not want the ability to save an entry in the Access Table. After making changes to an Access Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

NonVolatile

Select this storage type if you want the ability to save an entry in the Access Table. After making changes to an Access Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesyn recommends this storage type.

Note

The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 Access Table entry will take effect immediately.

12. Click **Apply**.
13. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting an Access Table Entry

To delete an entry in the SNMPv3 Access Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 92 on page 218.

3. In the SNMPv3 section, click the button next to **Configure Access Table** and then click **Configure** at the bottom of the tab.

The SNMPv3 Access Table tab is shown in Figure 99 on page 234.

4. Click **Next** or **Previous** to display the Access Table entry that you want to delete.

5. Click **Remove**.

A warning message is displayed. Click OK to remove the Access Table entry.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Modifying an Access Table Entry

To modify an entry in the SNMPv3 Access Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 92 on page 218.

3. In the SNMPv3 section, click the button next to **Configure Access Table** and then click **Configure** at the bottom of the tab.

The SNMPv3 Access Table tab is shown in Figure 99 on page 234.

4. Click **Next** or **Previous** to display the Access Table entry that you want to change.

5. Click **Modify**.

The Modify SNMPv3 Access page is shown in Figure 101.

Group Name	: testengineering
Context Prefix	:
Read View	: internet
Write View	: private
Notify View	: internet
Security Model	: v3
Security Level	: AuthPriv
Context Match	: Exact
Storage Type	: NonVolatile
Row Status	: Active

Figure 101. Modify SNMPv3 Access Page

Note

The Context Prefix field is a read-only field. The Context Prefix field is always set to null.

- In the Read View Name field, enter a value that you configured with the View Name parameter in the View Table.

This parameter allows the users assigned to this Group Name to view the information specified by the View Table entry. This value does not need to be unique.

- In the Write View Name field, enter a value that you configured with the View Name parameter in the View Table.

This parameter allows the users assigned to this Security Group to write, or modify, the information in the specified View Table. This value does not need to be unique.

- In the Notify View Name field, enter a value that you configured with the View Name parameter in the View Table.

This parameter allows the users assigned to this Group Name to send traps permitted in the specified View. This value does not need to be unique.

Note

The Context Match field is a read only field. The Context Match field is always set to Exact.

9. In the Storage Type field, select one of the following storage types for this table entry:

Volatile

Select this storage type if you do not want the ability to save an entry in the Access Table. After making changes to an Access Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

NonVolatile

Select this storage type if you want the ability to save an entry in the Access Table. After making changes to an Access Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesyn recommends this storage type.

Note

The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the Access Table entry takes effect immediately.

10. Click **Apply** to update the SNMPv3 Access Table.
11. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Configuring the SNMPv3 SecurityToGroup Table

You can create, delete, and modify an SNMPv3 SecurityToGroup Table entry. See the following procedures:

- “Creating a SecurityToGroup Table Entry” on page 241
- “Deleting a SecurityToGroup Table Entry” on page 244
- “Modifying a SecurityToGroup Table Entry” on page 244

For reference information about the SNMPv3 SecuritytoGroup Table, see Chapter 20, “SNMPv3” in the *AT-S63 Management Software Menus Interface User's Guide*.

Creating a SecurityToGroup Table Entry

To create an entry in the SNMPv3 SecurityToGroup Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 92 on page 218.

3. In the SNMPv3 section, click the button next to **Configure SecurityToGroup Table** and then click **Configure** at the bottom of the tab.

The SNMPv3 SecurityToGroup Table tab is shown in Figure 102.

The screenshot shows the Configuration page for a device (AT-9424T/SP). The main heading is "Configuration" with system information: System Name: Marketing, MAC Addr: 00:30:84:AB:EF:CD. The navigation menu on the left includes: Home, System, Layer 1, Layer 2, Mgmt. Security, Mgmt. Protocols, Network Security, Services, Multicast, Utilities, Help, and Logout. The main content area has tabs for Server-based Authentication, Secure Shell, SNMP, and Enhanced Stacking. The "SNMPv3 SecurityToGroup Table" tab is active, showing a table with 19 total entries (Page 5 of 5). The table has columns for Security Model, Security Name, Group Name, Storage Type, and Row Status. Below the table are buttons for Refresh, Add, Remove, Modify, Previous, and Back.

	Security Model	Security Name	Group Name	Storage Type	Row Status
<input checked="" type="radio"/>	v3	jenny	swengineering	NonVolatile	Active
<input type="radio"/>	v3	chitra	testengineering	NonVolatile	Active
<input type="radio"/>	v3	debashis	swengineering	NonVolatile	Active

Figure 102. SNMPv3 SecurityToGroup Table Tab (Configuration)

- To create an SNMPv3 SecurityToGroup Table entry, click **Add**.

The Add New SNMPv3 SecurityToGroup page is shown in Figure 103.

The screenshot shows the "Add New SNMPv3 SecurityToGroup" page. The form contains the following fields and values:

- Security Model: v3 (dropdown)
- Security Name: chitra (text input)
- Group Name: testengineering (text input)
- Storage Type: NonVolatile (dropdown)
- Row Status: Active (text input)

Buttons for "Apply" and "Cancel" are located at the bottom of the form.

Figure 103. Add New SNMPv3 SecurityToGroup Page

- In the Security Model field, select the SNMP protocol that was configured for this User Name.

Choose from the following:

v1

Select this value to associate the Group Name with the SNMPv1 protocol.

v2c

Select this value to associate the Group Name with the SNMPv2c protocol.

v3

Select this value to associate the Group Name with the SNMPv3 protocol.

6. In the Security Name field, enter the User Name that you want to associate with a group.

Enter a User Name that you configured in “Creating a User Table Entry” on page 220.

7. In the Group Name field, enter a Group Name that you configured in the Access Table.

See “Creating an Access Table” on page 234.

There are four default values for this field that are reserved for SNMPv1 and SNMPv2c implementations:

- defaultV1GroupReadOnly
- defaultV1GroupReadWrite
- defaultV2cGroupReadOnly
- defaultV2cGroupReadWrite

8. In the Storage Type field, select one of the following storage types for this table entry:

Volatile

Select this storage type if you do not want the ability to save an entry in the SecurityToGroup Table. After making changes to a SecurityToGroup Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

NonVolatile

Select this storage type if you want the ability to save an entry in the SecurityToGroup Table. After making changes to a SecurityToGroup Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesyn recommends this storage type.

Note

The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 SecurityToGroup Table entry takes effect immediately.

9. Click **Apply**.

10. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting a SecurityToGroup Table Entry

To delete an entry SNMPv3 SecurityToGroup Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 92 on page 218.

3. In the SNMPv3 section, click the button next to **Configure SecurityToGroup Table**, and then click **Configure** at the bottom of the tab.

The SNMPv3 SecurityToGroup Table tab is shown in Figure 102 on page 242.

4. Click the button next to the SecurityToGroup Table entry that you want to delete and then click **Remove**.

A warning message is displayed.

5. Click **OK**.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Modifying a SecurityToGroup Table Entry

To modify an entry SNMPv3 SecurityToGroup Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 92 on page 218.

3. In the SNMPv3 section, click the button next to **Configure SecurityToGroup Table** and then click **Configure** at the bottom of the tab.

The SNMPv3 SecurityToGroup Table tab is shown in Figure 102 on page 242.

- Click the button next to the SecurityToGroup Table entry that you want to change, and then click **Modify**.

The Modify SNMPv3 SecurityToGroup page is shown in Figure 104.

Figure 104. Modify SNMPv3 SecurityToGroup Page

- In the Group Name field, enter a Group Name that you configured in the SNMPv3 Access Table.

See “Creating an Access Table” on page 234.

There are four default values for this field that are reserved for SNMPv1 and SNMPv2c implementations:

- defaultV1GroupReadOnly
- defaultV1GroupReadWrite
- defaultV2cGroupReadOnly
- defaultV2cGroupReadWrite

- In the Storage Type field, select one of the following storage types for this table entry:

Volatile

Select this storage type if you do not want the ability to save an entry in the SecurityToGroup Table. After making changes to a SecurityToGroup Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

NonVolatile

Select this storage type if you want the ability to save an entry in the SecurityToGroup Table. After making changes to a SecurityToGroup Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesyn recommends this storage type.

Note

The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 SecurityToGroup Table entry takes effect immediately.

7. Click **Apply** to update the SNMPv3 SecurityToGroup Table.
8. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Configuring the SNMPv3 Notify Table

You can create, delete, and modify an SNMPv3 Notify Table entry. See the following procedures:

- “Creating a Notify Table Entry” on page 247
- “Deleting a Notify Table Entry” on page 249
- “Modifying a Notify Table Entry” on page 250

For reference information about the SNMPv3 Notify Table, see Chapter 20, “SNMPv3” in the *AT-S63 Management Software Menus Interface User's Guide*.

Creating a Notify Table Entry

To create an entry in the SNMPv3 Notify Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 92 on page 218.

3. In the SNMPv3 section, click the button next to **Configure Notify Table**, and then click **Configure** at the bottom of the tab.

The SNMPv3 Notify Table tab is shown in Figure 105.

AT-9424T/SP

Configuration

System Name: Marketing
MAC Addr: 00:30:84:AB:EF:CD

Server-based Authentication | Secure Shell | **SNMP** | Enhanced Stacking

Home | System | Layer 1 | Layer 2 | Mgmt. Security | Mgmt. Protocols | Network Security | Services | Multicast | Utilities | Help | Logout

SNMPv3 Notify Table

Total Entries: 16. Page 4 of 4

	Notify Name	Notify Tag	Notify Type	Storage Type	Row Status
<input checked="" type="radio"/>	swenginformat	swenginformatag	Inform	NonVolatile	Active
<input type="radio"/>	swengtrap	swengtag	Trap	NonVolatile	Active
<input type="radio"/>	testenginformat	testenginformatag	Inform	NonVolatile	Active
<input type="radio"/>	testengtrap	testengtag	Trap	NonVolatile	Active

Refresh | Add | Remove | Modify | Previous

Back

Figure 105. SNMPv3 Notify Table Tab (Configuration)

- Click **Add**.

The Add New SNMPv3 Notify page is shown in Figure 106.

Add New SNMPv3 Notify

Notify Name :

Notify Tag :

Notify Type : ▼

Storage Type : ▼

Row Status : Active

Apply | Cancel

Figure 106. Add New SNMPv3 Notify Page

- In the Notify Name field, enter the name associated with this trap message.

Enter a descriptive name of up to 32 alphanumeric characters. For example, you might want to define a trap message for hardware engineering and enter a value of “hardwareengineeringtrap” for the Notify Name.

- In the Notify Tag field, enter a description name of the Notify Tag.

Enter a name of up to 32 alphanumeric characters.

7. In the Notify Type field, enter one of the following message types:

Trap

Indicates this notify table is used to send traps. With this message type, the switch does not expect a response from the host.

Inform

Indicates this notify table is used to send inform messages. With this message type, the switch expects a response from the host.

8. In the Storage Type field, select one of the following storage types for this table entry:

Volatile

Select this storage type if you do not want the ability to save an entry in the Notify Table. After making changes to a Notify Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

NonVolatile

Select this storage type if you want the ability to save an entry in the Notify Table. After making changes to a Notify Table entry with a NonVolatile storage type, the **Save Config** option is not displayed on the Configuration menu.

The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 Notify Table entry takes effect immediately.

9. Click **Apply** to update the SNMPv3 Notify Table.
10. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting a Notify Table Entry

To delete an entry in the SNMPv3 Notify Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 92 on page 218.

3. In the SNMPv3 section, click the button next to **Configure Notify Table**, and then click **Configure** at the bottom of the tab.

The SNMPv3 Notify Table tab is shown in Figure 105 on page 248.

4. Click the button next to the Notify Table entry that you want to delete, and then click **Remove**.

A warning message is displayed.

5. Click **OK**.
6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Modifying a Notify Table Entry

To modify an entry in the SNMPv3 Notify Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 92 on page 218.

3. In the SNMPv3 section, click the button next to Configure Notify Table, and then click **Configure** at the bottom of the tab.

The SNMPv3 Notify Table tab is shown in Figure 105 on page 248.

4. Click the button next to the table entry that you want to change and then click **Modify**.

The Modify SNMPv3 Notify page is shown in Figure 107.

Notify Name	: swenginformat
Notify Tag	: <input type="text" value="swenginformatag"/>
Notify Type	: <input type="text" value="Inform"/>
Storage Type	: <input type="text" value="NonVolatile"/>
Row Status	: Active

Figure 107. Modify SNMPv3 Notify Page

5. In the Notify Tag field, enter a description name of the Notify Tag.

Enter a name of up to 32 alphanumeric characters.

6. In the Notify Type field, enter one of the following message types:

Trap

Indicates this notify table is used to send traps. With this message type, the switch does not expect a response from the host.

Inform

Indicates this notify table is used to send inform messages. With this message type, the switch expects a response from the host.

7. In the Storage Type field, select one of the following storage types for this table entry:

Volatile

Select this storage type if you do not want the ability to save an entry in the Notify Table. After making changes to an Notify Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

NonVolatile

Select this storage type if you want the ability to save an entry in the Notify Table. After making changes to an Notify Table entry with a NonVolatile storage type, the **Save Config** option is not displayed on the Configuration menu.

The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 Notify Table entry takes effect immediately.

8. Click **Apply** to update the SNMPv3 Notify Table.
9. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Configuring the SNMPv3 Target Address Table

You can create, delete, and modify an SNMPv3 Target Address Table entry. See the following procedures:

- “Creating a Target Address Table Entry” on page 252
- “Deleting a Target Address Table Entry” on page 255
- “Modifying Target Address Table Entry” on page 256

For reference information about the SNMPv3 Target Address Table, see Chapter 20, “SNMPv3” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Creating a Target Address Table Entry

To create an entry in the SNMPv3 Target Address Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 92 on page 218.

3. In the SNMPv3 section, click the button next to **Configure Target Address Table**, and then click **Configure** at the bottom of the tab.

The SNMPv3 Target Address Table tab is shown in Figure 108.

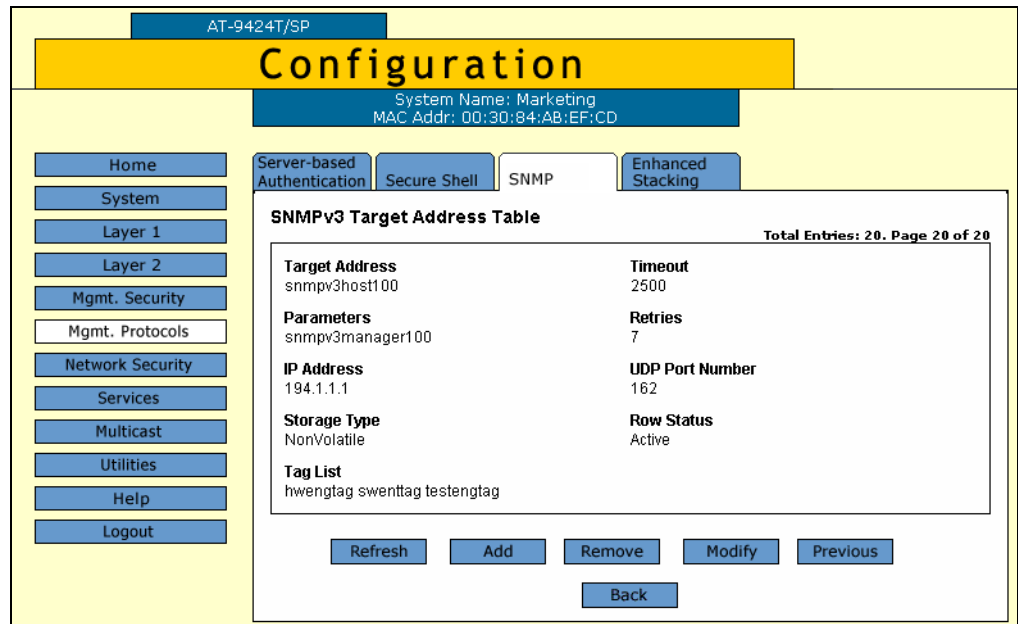


Figure 108. SNMPv3 Target Address Table Tab (Configuration)

4. Click **Add**.

The Add New SNMPv3 Target Address page is shown in Figure 109.

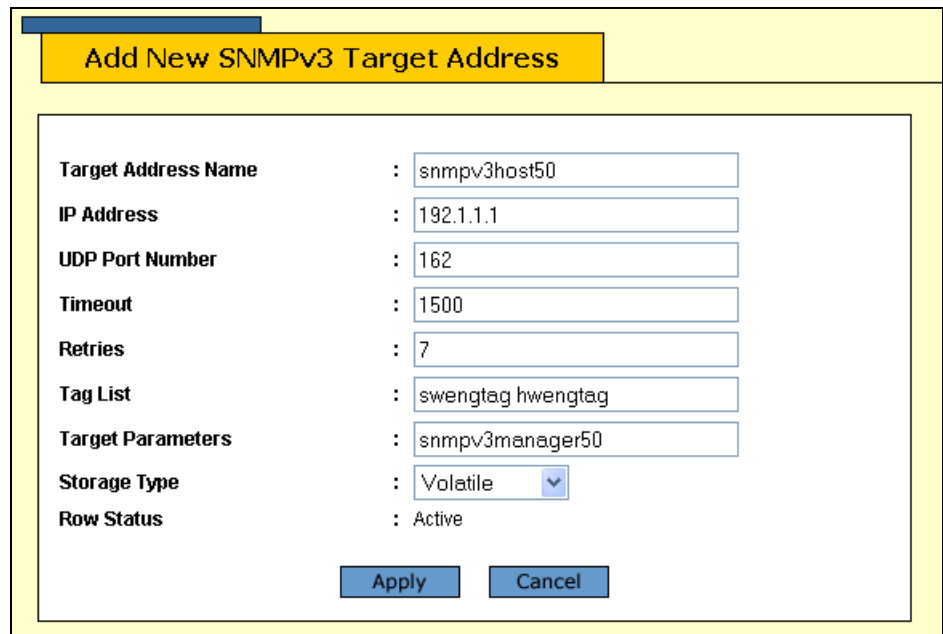


Figure 109. Add New SNMPv3 Target Address Page

5. In the Target Address Name field, enter the name of the SNMP manager, or host, that manages the SNMP activity on your switch.

You can enter a name of up to 32 alphanumeric characters.

6. In the IP Address field, enter the IP address of the host.

Use the following format for an IP address:
XXX.XXX.XXX.XXX

7. In the UDP Port Number field, enter a UDP port number.

You can enter a UDP port in the range of 0 to 65,535. The default UDP port is 162.

8. In the Timeout field, enter a timeout value in milliseconds.

When an Inform message is generated, it requires a response from the switch. The timeout value determines how long the switch considers the Inform message an active message. This parameter applies to Inform messages only. The range is from 0 to 2,147,483,647 milliseconds. The default value is 1500 milliseconds.

9. In the Retries field, enter the number of times the switch retries, or resends, an Inform message.

When an Inform message is generated, it requires a response from the switch. This parameter determines how many times the switch resends an Inform message. The Retries parameter applies to Inform messages only. The range is 0 to 255 retries. The default is 3 retries.

10. In the Tag List field, enter a list of tags that you configured in a SNMPv3 Notify Table with the Notify Tag parameter.

See “Creating a Notify Table Entry” on page 247. Enter a Tag List of up to 256 alphanumeric characters. Use a space to separate entries, for example:

```
hwengtag swengtag testengtag
```

11. In the Target Parameters field, enter a Target Parameters name.

This name can consist of up to 32 alphanumeric characters. The value configured here must match the value configured with the Target Parameters Name parameter in the SNMPv3 Target Parameters Table.

12. In the Storage Type field, enter one of the following storage types for this table entry:

Volatile

Select this storage type if you do not want the ability to save an entry in the Target Address Table. After making changes to a Target Address Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

NonVolatile

Select this storage type if you want the ability to save an entry in the Target Address Table. After making changes to a Target Address Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesyn recommends this storage type.

Note

The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 Target Address Table entry takes effect immediately.

13. Click **Apply** to update the SNMPv3 Target Address Table.
14. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting a Target Address Table Entry

To delete an entry in the SNMPv3 Target Address Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 92 on page 218.

3. In the SNMPv3 section, click the button next to **Configure Target Address Table** and then click **Configure** at the bottom of the tab.

The SNMPv3 Target Address Table tab is shown in Figure 108 on page 253.

4. Click **Next** or **Previous** to display the SNMPv3 Target Address Table entry that you want to delete.
5. Click **Remove**.

A warning message is displayed.

6. Click **OK**.

7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Modifying Target Address Table Entry

To modify an entry in the SNMPv3 Target Address Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 92 on page 218.

3. In the SNMPv3 section, click the button next to **Configure Target Address Table** and then click **Configure** at the bottom of the tab.

The SNMPv3 Target Address Table tab is shown in Figure 108 on page 253.

4. Click **Next** or **Previous** to display the Target Address Table entry that you want to change.

5. Click **Modify**.

The Modify SNMPv3 Target Address page is shown Figure 110.

Modify SNMPv3 Target Address	
Target Address Name	: snmpv3host50
IP Address	: <input type="text" value="192.1.1.1"/>
UDP Port Number	: <input type="text" value="162"/>
Timeout	: <input type="text" value="1500"/>
Retries	: <input type="text" value="7"/>
Tag List	: <input type="text" value="swengtag hwengtag"/>
Target Parameters	: <input type="text" value="snmpv3manager50"/>
Storage Type	: <input type="text" value="Volatile"/>
Row Status	: Active
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Figure 110. Modify SNMPv3 Target Address Page

6. In the IP Address field, enter the IP address of the host.

Use the following format for an IP address:
XXX.XXX.XXX.XXX

7. In the UDP Port Number field, enter a UDP port number.

You can enter a UDP port in the range of 0 to 65,535. The default UDP port is 162.

8. In the Timeout field, enter a timeout value in milliseconds.

When an Inform message is generated, it requires a response from the switch. The timeout value determines how long the switch considers the Inform message an active message. This parameter applies to Inform messages only. The range is from 0 to 2,147,483,647 milliseconds. The default value is 1500 milliseconds.

9. In the Retries field, enter the number of times the switch retries, or resends, an Inform message.

When an Inform message is generated, it requires a response from the switch. This parameter determines how many times the switch resends an Inform message. The Retries parameter applies to Inform messages only. The range is 0 to 255 retries. The default is 3 retries.

10. In the Tag List field, enter a list of tags that you configured with the Notify Tag parameter in a Notify Table entry.

See "Creating a Notify Table Entry" on page 247. Enter a Tag List of up to 256-alphanumeric characters. Use a space to separate entries, for example:

```
hwengtag swengtag testengtag
```

11. In the Target Parameters field, enter a Target Parameters name.

This name can consist of up to 32 alphanumeric characters. The value configured here must match the value configured with the Target Parameters Name parameter in the Target Parameters Table.

12. In the Storage Type field, enter one of the following storage types for this table entry:

Volatile

Select this storage type if you do not want the ability to save an entry in the Target Address Table. After making changes to a Target Address Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

NonVolatile

Select this storage type if you want the ability to save an entry in the Target Address Table. After making changes to an Target Address Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesyn recommends this storage type.

13. Click **Apply** to update the SNMPv3 Target Address Table.
14. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Configuring the SNMPv3 Target Parameters Table

You can create, delete, and modify an SNMPv3 Target Parameters Table entry. See the following procedures:

- “Creating a Target Address Table Entry” on page 252
- “Deleting a Target Address Table Entry” on page 255
- “Modifying Target Address Table Entry” on page 256

For reference information about the SNMPv3 Target Parameters Table, see Chapter 20, “SNMPv3” in the *AT-S63 Management Software Menus Interface User's Guide*.

Creating a Target Parameters Table Entry

To create an entry in the SNMPv3 Target Parameters Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 92 on page 218.

3. In the SNMPv3 section, click the button next to **Configure Target Parameters Table** and then click **Configure** at the bottom of the tab.

The SNMPv3 Target Parameters Table tab is shown in Figure 111.

AT-9424T/SP

Configuration

System Name: Marketing
MAC Addr: 00:30:84:AB:EF:CD

Server-based Authentication | Secure Shell | **SNMP** | Enhanced Stacking

SNMPv3 Target Parameters Table

Total Entries: 3, Page 1 of 1

	Params Name	Message Processing Model	Security Model	Security Name	Security Level	Storage Type	Row Status
<input checked="" type="radio"/>	snmpv3manager120	v3	v3	hoa	AuthNoPriv	NonVolatile	Active
<input type="radio"/>	snmpv3manager220	v3	v3	luke	AuthPriv	NonVolatile	Active
<input type="radio"/>	snmpv3manager330	v3	v3	chitra	AuthPriv	NonVolatile	Active

Figure 111. SNMPv3 Target Parameters Table Tab (Configuration)

- Click **Add**.

The Add New SNMPv3 Target Parameter page is shown in Figure 112.

The screenshot shows a web form titled "Add New SNMPv3 Target Parameter". The form fields are as follows:

- Target Parameters Name**: Text input field containing "snmpv3manager50".
- Message Processing Model**: Dropdown menu with "v3" selected.
- Security Model**: Dropdown menu with "v3" selected.
- Security Name**: Text input field containing "debashi".
- Security Level**: Dropdown menu with "Privacy" selected.
- Storage Type**: Dropdown menu with "Volatile" selected.
- Row Status**: Text input field containing "Active".

At the bottom of the form are two buttons: "Apply" and "Cancel".

Figure 112. Add New SNMPv3 Target Parameters Page

- In the Target Parameters Name field, enter a name of the SNMP manager or host.

Enter a value of up to 32 alphanumeric characters.

Note

Enter a value for the Message Processing Model parameter only if you select SNMPv1 or SNMPv2c as the Security Model. If you select the SNMPv3 protocol as the Security Model, then the Message Processing Model is automatically assigned to SNMPv3.

- In the Message Processing Model field, enter a Security Model that is used to process messages.

Select one of the following SNMP protocols:

v1

Select this value to process messages with the SNMPv1 protocol.

v2c

Select this value to process messages with the SNMPv2c protocol.

v3

Select this value to process messages with the SNMPv3 protocol.

- In the Security Model field, select one of the following SNMP protocols as the Security Model for this Security Name, or User Name.

v1

Select this value to associate the Security Name, or User Name, with the SNMPv1 protocol.

v2c

Select this value to associate the Security Name, or User Name, with the SNMPv2c protocol.

v3

Select this value to associate the Security Name, or User Name, with the SNMPv3 protocol.

8. In the Security Name field, enter a User Name that you previously configured with the SNMPv3 User Table.

See "Creating a User Table Entry" on page 220.

9. In the Security Level field, select one of the following Security Levels:

Note

The value you configure for the Security Level must match the value configured for the User Name in the User Table Menu. See "Creating a User Table Entry" on page 220.

No Authentication/Privacy

This option represents neither an authentication nor privacy protocol. Select this security level if you do not want to authenticate SNMP entities and you do not want to encrypt messages using a privacy protocol. This security level provides the least security.

Note

If you have selected SNMPv1 or SNMPv2c as the Security Model, you must select No Authentication/Privacy as the Security Level.

Authentication

This option represents authentication, but no privacy protocol. Select this security level if you want to authenticate SNMP users, but you do not want to encrypt messages using a privacy protocol. You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

Privacy

This option represents authentication and the privacy protocol. Select this security level to allow authentication and encryption. This level provides the greatest level of security. You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

- In the Storage Type parameter, select one of the following storage types for this table entry:

Volatile

Select this storage type if you do not want the ability to save an entry in the Target Parameters Table. After making changes to a Target Parameters Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

NonVolatile

Select this storage type if you want the ability to save an entry in the Target Parameters Table. After making changes to a Target Parameters Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesyn recommends this storage type.

Note

The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 Target Parameters Table entry takes effect immediately.

- Click **Apply** to update the SNMPv3 Target Parameters Table.
- From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting a Target Parameters Table Entry

To delete an entry in the SNMPv3 Target Parameters Table, perform the following procedure:

- From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

- Select the **SNMP** tab.

The SNMP tab is shown in Figure 92 on page 218.

- In the SNMPv3 section, click the button next to **Configure Target Parameters Table** and then click **Configure** at the bottom of the tab.

The SNMPv3 Target Parameters Table tab is shown in Figure 111 on page 259.

- Click the button next to the Target Parameters Table entry that you want to delete and then click **Remove**.

A warning message is displayed.

5. Click **OK**.
6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Modifying a Target Parameters Table Entry

To modify an entry in the SNMPv3 Target Parameters Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 92 on page 218.

3. In the SNMPv3 section, click the button next to **Configure Target Parameters Table** and then click **Configure** at the bottom of the tab.

The SNMPv3 Target Parameters Table tab is shown in Figure 111 on page 259.

4. Click the button next to the Target Parameters Table entry that you want to change, and then click **Modify**.

The Modify SNMPv3 Target Parameter page is shown in Figure 113 on page 263.

Modify SNMPv3 Target Parameter	
Target Parameters Name	: snmpv3manager100
Message Processing Model	: v3
Security Model	: v3
Security Name	: chitra
Security Level	: Privacy
Storage Type	: NonVolatile
Row Status	: Active
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Figure 113. Modify SNMPv3 Target Parameter Page

Note

Enter a value for the Message Processing Model field only if you select SNMPv1 or SNMPv2c as the Security Model. If you select the SNMPv3 protocol as the Security Model, then the switch automatically assigns the Message Processing Model to SNMPv3.

5. In the Message Processing Model field, enter a Security Model that is used to process messages.

Select one of the following SNMP protocols:

v1

Select this value to process messages with the SNMPv1 protocol.

v2c

Select this value to process messages with the SNMPv2c protocol.

v3

Select this value to process messages with the SNMPv3 protocol.

6. In the Security Model field, select one of the following SNMP protocols as the Security Model for this Security Name, or User Name.

v1

Select this value to associate the Security Name, or User Name, with the SNMPv1 protocol.

v2c

Select this value to associate the Security Name, or User Name, with the SNMPv2c protocol.

v3

Select this value to associate the Security Name, or User Name, with the SNMPv3 protocol.

7. In the Security Name field, enter a User Name that you previously configured with the SNMPv3 User Table.

See “Creating a User Table Entry” on page 220.

8. In the Security Level field, select one of the following Security Levels:

Note

The value you configure for the Security Level must match the value configured for the User Name in the SNMPv3 User Table Menu. See “Creating a User Table Entry” on page 220.

No Authentication/Privacy

This option represents neither an authentication nor privacy protocol.

Select this security level if you do not want to authenticate SNMP entities and you do not want to encrypt messages using a privacy protocol. This security level provides the least security.

Note

If you have selected SNMPv1 or SNMPv2c as the Security Model, you must select No Authentication/Privacy as the Security Level.

Authentication

This option represents authentication, but no privacy protocol. Select this security level if you want to authenticate SNMP users, but you do not want to encrypt messages using a privacy protocol. You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

Privacy

This option represents authentication and the privacy protocol. Select this security level to allow authentication and encryption. This level provides the greatest level of security. You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

9. In the Storage Type parameter, select one of the following storage types for this table entry:

Volatile

Select this storage type if you do not want the ability to save an entry in the Target Parameters Table. After making changes to an Target Parameters Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

NonVolatile

Select this storage type if you want the ability to save an entry in the Target Parameters Table. After making changes to an Target Parameters Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesyn recommends this storage type.

Note

The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 Target Parameters Table entry will take effect immediately.

10. Click **Apply** to update the SNMPv3 Target Parameters Table.
11. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Configuring the SNMPv3 Community Table

You can create, delete, and modify an SNMPv3 Community Table entry. See the following procedures:

- “Creating an SNMPv3 Community Table Entry” on page 266
- “Deleting an SNMPv3 Community Table Entry” on page 269
- “Modifying an SNMPv3 Community Table Entry” on page 269

For reference information about the SNMPv3 Community Table, see Chapter 20, “SNMPv3” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Note

Use the SNMPv3 Community Table only if you are configuring the SNMPv3 protocol with an SNMPv1 or an SNMPv2c implementation. Allied Telesyn does not recommend this configuration.

Creating an SNMPv3 Community Table Entry

To create an entry in the SNMPv3 Community Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 92 on page 218.

3. In the SNMPv3 section, click the button next to **Configure Community Table** and then click **Configure** at the bottom of the tab.

The SNMPv3 Community Table tab is shown in Figure 114.

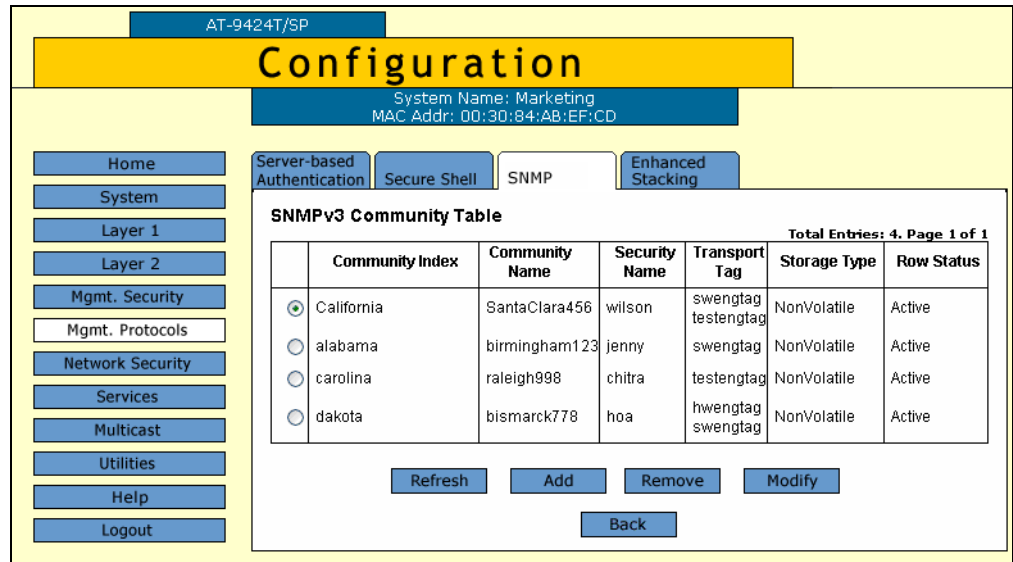


Figure 114. SNMPv3 Community Table Tab (Configuration)

4. Click **Add**.

The Add New SNMPv3 Community page is shown in Figure 115.

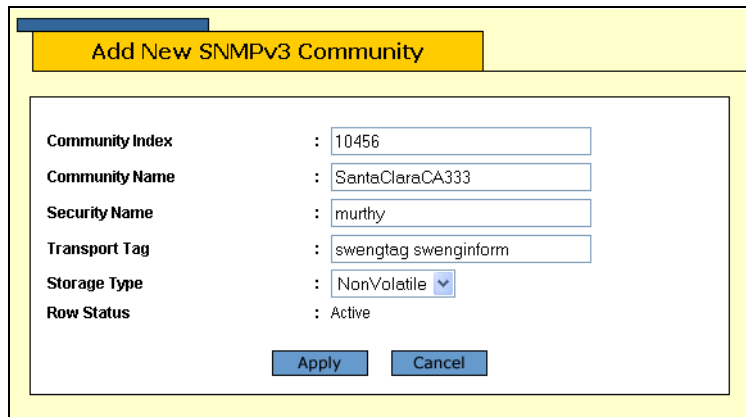


Figure 115. Add New SNMPv3 Community Page

5. In the Community Index field, enter a numerical value for this Community.

This parameter is used to index the other parameters in an SNMPv3 Community Table entry. Enter a value of up to 32- alphanumeric characters.

6. In the Community Name field, enter a Community Name of up to 64-alphanumeric characters.

The value of the Community Name parameter acts as a password for the SNMPv3 Community Table entry. This parameter is case sensitive.

Note

Allied Telesyn recommends that you select SNMP Community Names carefully to ensure these names are known only to authorized personnel.

7. In the Security Name field, enter a name of an SNMPv1 and SNMPv2c user.

This name must be unique. Enter a value of up to 32 alphanumeric characters.

Note

Do not use a value configured with the User Name parameter in the SNMPv3 User Table.

8. In the Transport Tag field, enter a name of up to 32 alphanumeric characters.

The Transport Tag parameter links an SNMPv3 Community Table entry with an SNMPv3 Target Address Table entry. Add the value you configure for the Transport Tag parameter to the Tag List parameter in the Target Address Table as desired. See “Creating a Target Address Table Entry” on page 252.

9. In the Storage Type field, select one of the following storage types for this table entry:

Volatile

Select this storage type if you do not want the ability to save an entry in the SNMPv3 Community Table. After making changes to an SNMPv3 Community Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

NonVolatile

Select this storage type if you want the ability to save an entry in the SNMPv3 Community Table. After making changes to an SNMPv3 Community Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesyn recommends this storage type.

Note

The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 Community Table entry takes effect immediately.

10. Click **Apply**.
11. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting an SNMPv3 Community Table Entry

To delete an entry in the SNMPv3 Community Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 92 on page 218.

3. In the SNMPv3 section, click the button next to **Configure Community Table** and then click **Configure** at the bottom of the tab.

The SNMPv3 Community Table tab is shown in Figure 114 on page 267.

4. Click the button next to the SNMPv3 Community Table entry that you want to delete and then click **Remove**.

A warning message is displayed.

5. Click **OK**.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Modifying an SNMPv3 Community Table Entry

To modify an entry in the SNMPv3 Community Table, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 92 on page 218.

3. In the SNMPv3 section, click the button next to **Configure Community Table**, and then click **Configure** at the bottom of the tab.

The SNMPv3 Community Table tab is shown in Figure 114 on page 267.

4. Click the button next to the SNMPv3 Community Table entry that you want to change and then click **Modify**.

The Modify SNMPv3 Community page is shown in Figure 116.

Modify SNMPv3 Community	
Community Index	: alabama
Community Name	: <input type="text" value="birmingham123"/>
Security Name	: <input type="text" value="jenny"/>
Transport Tag	: <input type="text" value="swengtag"/>
Storage Type	: <input type="text" value="NonVolatile"/>
Row Status	: Active
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Figure 116. Modify SNMPv3 Community Page

5. In the Community Name field, enter a Community Name of up to 64-alphanumeric characters.

The value of the Community Name parameter acts as a password for the SNMPv3 Community Table entry. This parameter is case sensitive.

Note

Allied Telesyn recommends that you select SNMP Community Names carefully to ensure these names are known only to authorized personnel.

6. In the Security Name field, enter a name of an SNMPv1 and SNMPv2c user.

This name must be unique. Enter a value of up to 32 alphanumeric characters.

Note

Do not use a value configured with the User Name parameter in the SNMPv3 User Table.

7. In the Transport Tag field, enter a name of up to 32 alphanumeric characters.

The Transport Tag parameter links an SNMPv3 Community Table entry with an SNMPv3 Target Address Table entry. Add the value you configure for the Transport Tag parameter to the Tag List parameter in the Target Address Table as desired. See “Creating a Target Address Table Entry” on page 252.

8. In the Storage Type field, select one of the following storage types for this table entry:

Volatile

Select this storage type if you do not want the ability to save an entry in the SNMPv3 Community Table. After making changes to an SNMPv3 Community Table entry with a Volatile storage type, the **Save Config** option is not displayed on the Configuration menu.

NonVolatile

Select this storage type if you want the ability to save an entry in the SNMPv3 Community Table. After making changes to an SNMPv3 Community Table entry with a NonVolatile storage type, the **Save Config** option is displayed on the Configuration menu. Allied Telesyn recommends this storage type.

Note

The Row Status parameter is a read-only field in the web browser interface. The Active value indicates the SNMPv3 Community Table entry takes effect immediately.

9. Click **Apply** to update the SNMPv3 Community Table.
10. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying SNMPv3 Tables

This section contains procedures to display the SNMPv3 Tables. The following procedures are provided:

- “Displaying User Table Entries,” next
- “Displaying View Table Entries” on page 274
- “Displaying Access Table Entries” on page 275
- “Displaying SecurityToGroup Table Entries” on page 276
- “Displaying Notify Table Entries” on page 277
- “Displaying Target Address Table Entries” on page 278
- “Displaying Target Parameters Table Entries” on page 279
- “Displaying SNMPv3 Community Table Entries” on page 280

Displaying User Table Entries

To display entries in the SNMPv3 User Table, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select **Mgmt. Protocols**.

The Mgmt. Protocols page is displayed with the Server-based Authentication tab displayed by default, as shown in Figure 22 on page 76.

3. Select the **SNMP** tab.

The SNMP tab is shown in Figure 117.

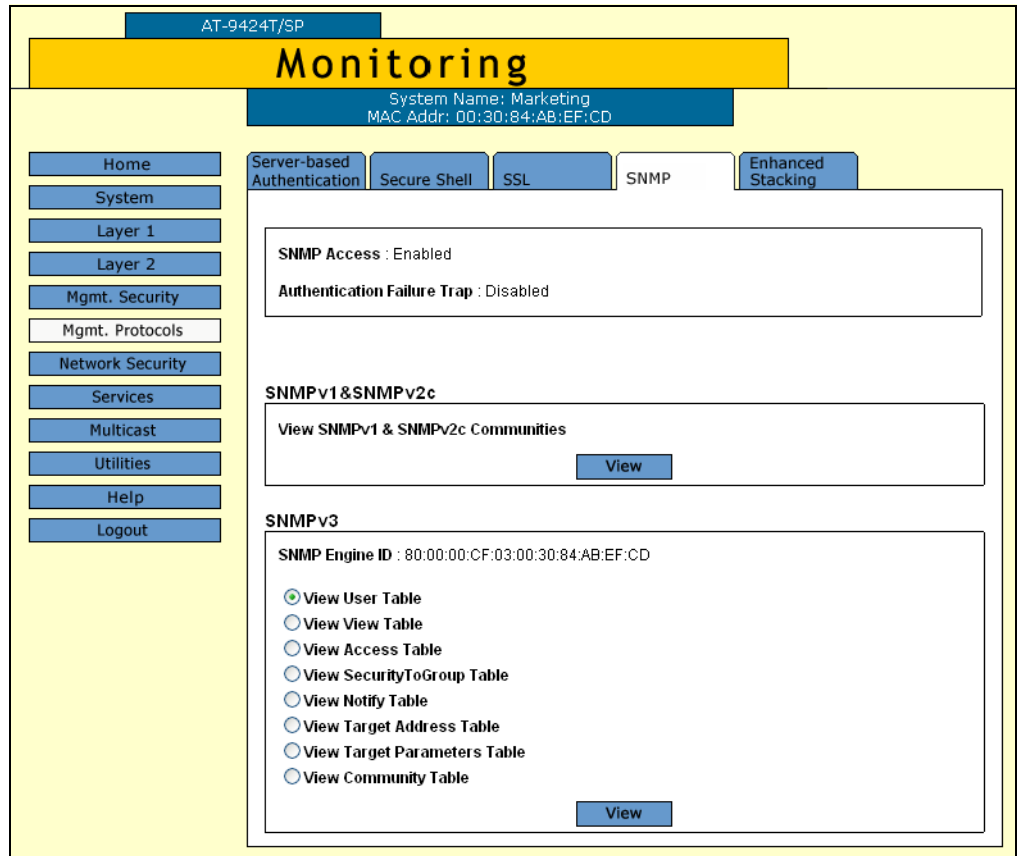


Figure 117. SNMP Tab (Monitoring)

- In the SNMPv3 section, click the button next to View User Table and then click **View** at the bottom of the tab.

The SNMPv3 User Table tab is shown in Figure 118.

The screenshot shows a web interface for a device (AT-9424T/SP) with a 'Monitoring' header. Below the header, system information is displayed: 'System Name: Marketing' and 'MAC Addr: 00:30:84:AB:EF:CD'. A navigation menu on the left lists various system functions. The main content area shows the 'SNMPv3 User Table' tab selected, displaying a table with two entries. Below the table are 'Refresh' and 'Back' buttons.

SNMPv3 User Table						Total Entries: 2. Page 1 of 1
	User Name	Authentication Protocol	Privacy Protocol	Storage Type	Row Status	
	blaze	SHA	DES	NonVolatile	Active	
	summer	MD5	DES	NonVolatile	Active	

Figure 118. SNMPv3 User Table Tab (Monitoring)

Displaying View Table Entries

To display entries in the SNMPv3 View Table, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 117 on page 273.

3. In the SNMPv3 section, click the button next to **View View Table** and then click **View** at the bottom of the tab.

The SNMPv3 View Table tab is shown in Figure 119.

The screenshot shows the 'Monitoring' section of the web browser interface. At the top, there is a yellow header with 'Monitoring' in large black text. Below the header, the system name 'Marketing' and MAC address '00:30:84:AB:EF:CD' are displayed. A navigation menu on the left includes buttons for Home, System, Layer 1, Layer 2, Mgmt. Security, Mgmt. Protocols, Network Security, Services, Multicast, Utilities, Help, and Logout. The main content area is titled 'SNMPv3 View Table' and contains a table with the following data:

Total Entries: 6. Page 1 of 2						
	View Name	SubTree OID	SubTree Mask	View Type	Storage Type	Row Status
<input checked="" type="radio"/>	mgmt	1.3.6.1.2		Excluded	NonVolatile	Active
<input type="radio"/>	private	1.3.6.1.4	ff:ff	Included	Volatile	Active
<input type="radio"/>	internet	1.3.6.1		Included	NonVolatile	Active
<input type="radio"/>	directory	1.3.6.1.1		Included	NonVolatile	Active
<input type="radio"/>	experimental	1.3.6.1.3		Excluded	NonVolatile	Active

Below the table are buttons for Refresh, Add, Remove, Modify, Next, and Back.

Figure 119. SNMPv3 View Table Tab (Monitoring)

Displaying Access Table Entries

To display entries in the SNMPv3 Access Table, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 117 on page 273.

3. In the SNMPv3 section, click the button next to **View Access Table** and then click **View** at the bottom of the tab.

The SNMPv3 Access Table tab is shown in Figure 120.

The screenshot shows the 'Monitoring' page for a device (AT-9424T/SP). The system name is 'Marketing' and the MAC address is '00:30:84:AB:EF:CD'. The 'SNMP' tab is selected. The 'SNMPv3 Access Table' section displays the following configuration for the 'techpubs' group:

SNMPv3 Access Table		Total Entries: 5, Page 1 of 5	
Group Name	techpubs	Security Model	v3
Context Prefix		Security Level	AuthPriv
Read View	internet1	Context Match	Exact
Write View	internet1	Storage Type	NonVolatile
Notify View	internet1	Row Status	Active

Navigation buttons include 'Refresh', 'Next', and 'Back'.

Figure 120. SNMPv3 Access Table Tab (Monitoring)

Displaying SecurityToGroup Table Entries

To display entries in the SNMPv3 SecurityToGroup Table, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 117 on page 273.

3. In the SNMPv3 section, click the button next to the **View SecurityToGroup Table** and then click **View** at the bottom of the tab.

The SNMPv3 SecurityToGroup Table tab is shown in Figure 121.

The screenshot shows a web browser interface for monitoring. At the top, there is a yellow banner with the word "Monitoring" in large black font. Below the banner, system information is displayed: "System Name: Marketing" and "MAC Addr: 00:30:84:AB:EF:CD". A navigation menu on the left side includes buttons for Home, System, Layer 1, Layer 2, Mgmt. Security, Mgmt. Protocols, Network Security, Services, Multicast, Utilities, Help, and Logout. The main content area has tabs for Server-based Authentication, Secure Shell, SSL, SNMP, and Enhanced Stacking. The SNMP tab is selected, and it displays the "SNMPv3 SecurityToGroup Table". The table has five columns: Security Model, Security Name, Group Name, Storage Type, and Row Status. There are five rows of data. Below the table are buttons for Refresh, Next, and Back. The text "Total Entries: 5. Page 1 of 2" is located at the top right of the table area.

Security Model	Security Name	Group Name	Storage Type	Row Status
v3	hoa	swengineering	NonVolatile	Active
v3	luke	testengineering	NonVolatile	Active
v3	jenny	swengineering	NonVolatile	Active
v3	chitra	testengineering	NonVolatile	Active
v3	debashis	swengineering	NonVolatile	Active

Figure 121. SNMPv3 SecurityToGroup Table Tab (Monitoring)

Displaying Notify Table Entries

To display entries in the SNMPv3 Notify Table, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 117 on page 273.

3. In the SNMPv3 section, click the button next to **View Notify Table** and then click **View** at the bottom of the tab.

The SNMPv3 Notify Table tab is shown in Figure 122.

The screenshot shows a web interface for monitoring. At the top, there is a yellow header with the word "Monitoring" in large black font. Below the header, system information is displayed: "System Name: Marketing" and "MAC Addr: 00:30:84:AB:EF:CD". A navigation menu on the left lists various system components like Home, System, Layer 1, Layer 2, Mgmt. Security, etc. In the center, there are several tabs: "Server-based Authentication", "Secure Shell", "SSL", "SNMP", and "Enhanced Stacking". The "SNMP" tab is selected, and it displays the "SNMPv3 Notify Table". The table has five columns: "Notify Name", "Notify Tag", "Notify Type", "Storage Type", and "Row Status". There is one entry in the table with the name "techpubsnotify", tag "tptag", type "Inform", storage type "NonVolatile", and status "Active". Below the table are "Refresh" and "Back" buttons.

Notify Name	Notify Tag	Notify Type	Storage Type	Row Status
techpubsnotify	tptag	Inform	NonVolatile	Active

Figure 122. SNMPv3 Notify Table Tab (Monitoring)

Displaying Target Address Table Entries

To display entries in the SNMPv3 Target Address Table, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. Select the **SNMP** Tab.

The SNMP tab is shown in Figure 117 on page 273.

3. In the SNMPv3 section, lick the button next to **View Target Address Table** and then click **View** at the bottom of the tab.

The SNMPv3 Target Address Table tab is shown in Figure 123.

The screenshot shows the web browser interface for the AT-S63 Management Software. The top navigation bar is yellow and contains the text 'Monitoring'. Below this, there is a blue bar with 'System Name: Marketing' and 'MAC Addr: 00:30:84:AB:EF:CD'. The left sidebar contains a list of navigation buttons: Home, System, Layer 1, Layer 2, Mgmt. Security, Mgmt. Protocols, Network Security, Services, Multicast, Utilities, Help, and Logout. The main content area is titled 'SNMPv3 Target Address Table' and shows the following details:

SNMPv3 Target Address Table		Total Entries: 2, Page 1 of 2	
Target Address	snmpv3host1	Timeout	1500
Parameters	snmpv3manager1	Retries	2
IP Address	187.1.1.1	UDP Port Number	162
Storage Type	NonVolatile	Row Status	Active
Tag List	testengtag swengtag		

At the bottom of the table, there are three buttons: 'Refresh', 'Next', and 'Back'.

Figure 123. SNMPv3 Target Address Table Tab (Monitoring)

Displaying Target Parameters Table Entries

To display entries in the SNMPv3 Target Parameters Table, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 117 on page 273.

3. In the SNMPv3 section, click the button next to the **View Target Parameters Table** and then click **View** at the bottom of the tab.

The SNMPv3 Target Parameters Table tab is shown in Figure 124.

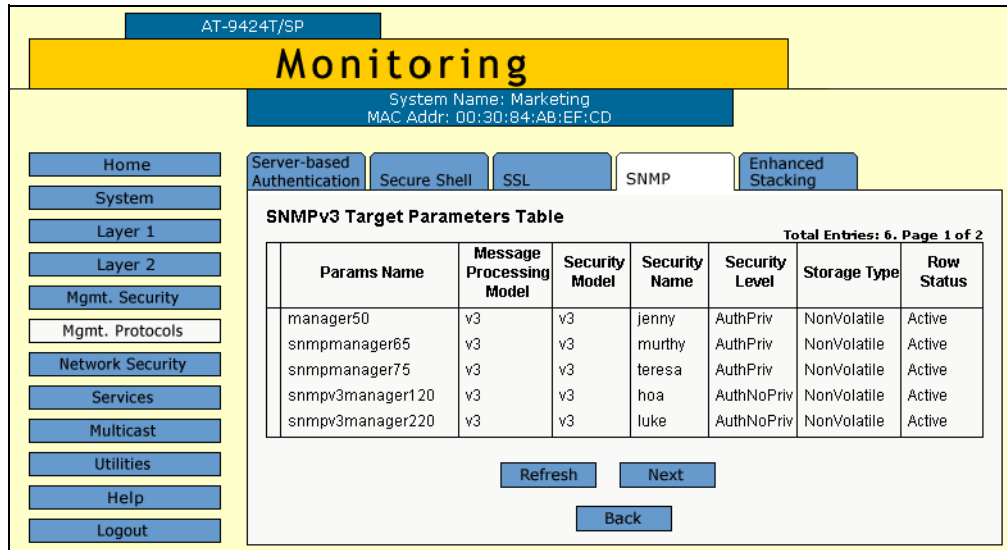


Figure 124. SNMPv3 Target Parameters Table Tab (Monitoring)

Displaying SNMPv3 Community Table Entries

To display entries in the SNMPv3 Community Table, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. Select the **SNMP** tab.

The SNMP tab is shown in Figure 117 on page 273.

3. In the SNMPv3 section, click the button next to **View Community Table** and then click **View** at the bottom of the tab.

The SNMPv3 Community Table tab is shown in Figure 125.

The screenshot shows a web browser interface for the AT-S63 Management Software. At the top, there is a header bar with the device ID 'AT-9424T/SP' and a large yellow 'Monitoring' title. Below the title, system information is displayed: 'System Name: Marketing' and 'MAC Addr: 00:30:84:00:00:00'. A navigation menu on the left includes links for Home, System, Layer 1, Layer 2, Mgmt. Security, Mgmt. Protocols, Network Security, Services, Multicast, Utilities, Help, and Logout. The main content area is titled 'SNMPv3 Community Table' and shows a table with 5 entries. The table has columns for Community Index, Community Name, Security Name, Transport Tag, Storage Type, and Row Status. Below the table are 'Refresh', 'Next', and 'Back' buttons.

SNMPv3 Community Table						Total Entries: 5, Page 1 of 2
Community Index	Community Name	Security Name	Transport Tag	Storage Type	Row Status	
10456	SantaClara5	tomas	testengtag testenginform	NonVolatile	Active	
10555	SanJose78	ross	testenginform	NonVolatile	Active	
10650	Sunnyvale45	nelmid	swengtag swenginform	NonVolatile	Active	
10675	Fremont7	loan	hwengtag hwenginform	NonVolatile	Active	
10725	Campbell98	frankk	testengtag testenginform	NonVolatile	Active	

Figure 125. SNMPv3 Community Table Tab (Monitoring)

Section IV

Spanning Tree Protocols

The chapters in this section provide information and procedures for the spanning tree protocols. The chapters include:

- ❑ Chapter 19, “STP and RSTP” on page 285
- ❑ Chapter 20, “MSTP” on page 303

Chapter 19

STP and RSTP

This chapter explains how to configure the STP and RSTP parameters on an AT-9400 Series switch. The sections in the chapter include:

- ❑ “Enabling or Disabling a Spanning Tree Protocol” on page 286
- ❑ “Configuring STP” on page 288
- ❑ “Configuring RSTP” on page 296

Note

For background information on spanning tree, refer to Chapter 21, “STP and RSTP,” in the *AT-S63 Management Software Menu Interface User’s Guide*.

Multiple Spanning Tree Protocol (MSTP) is described in Chapter 20, “MSTP” on page 303.

Enabling or Disabling a Spanning Tree Protocol

To enable or disable spanning tree on the switch, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 126.

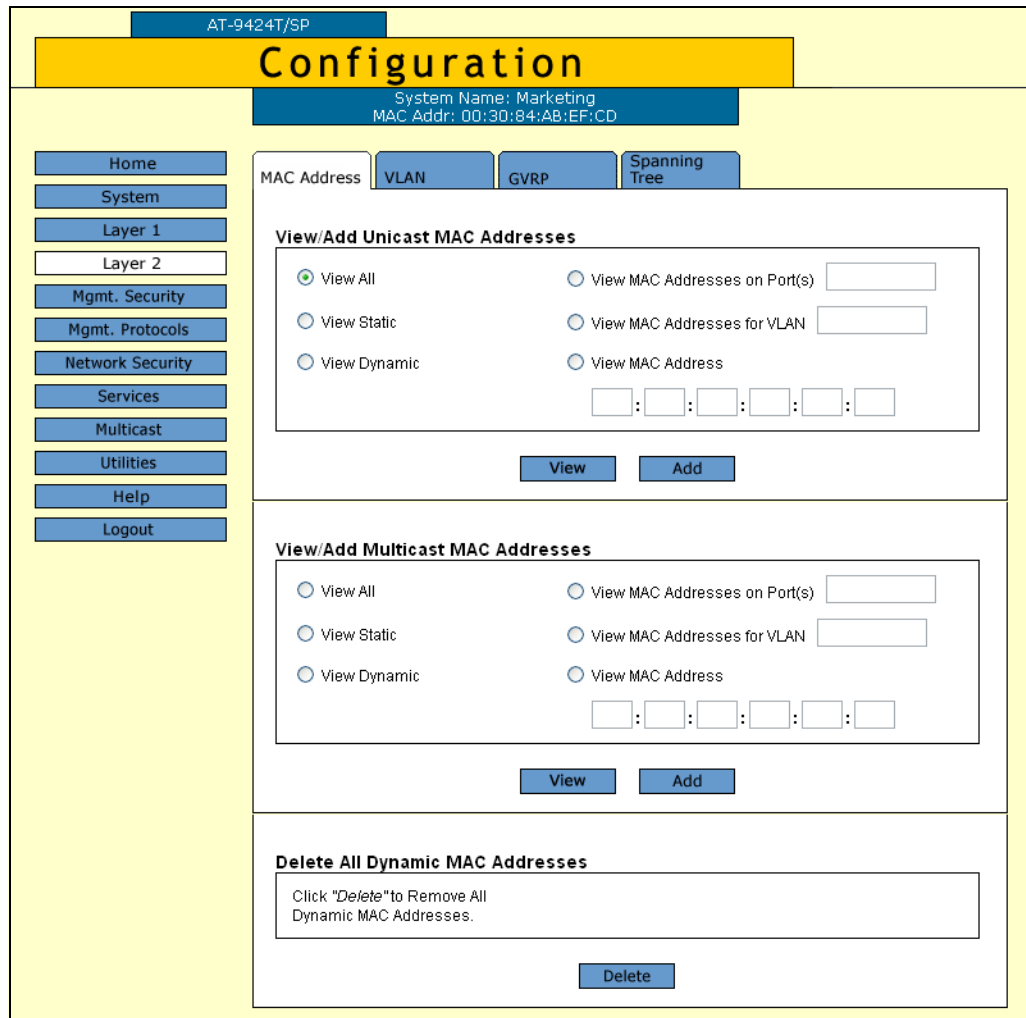


Figure 126. MAC Address Tab (Configuration)

3. Select the **Spanning Tree** tab.

The Spanning Tree tab is shown in Figure 127.

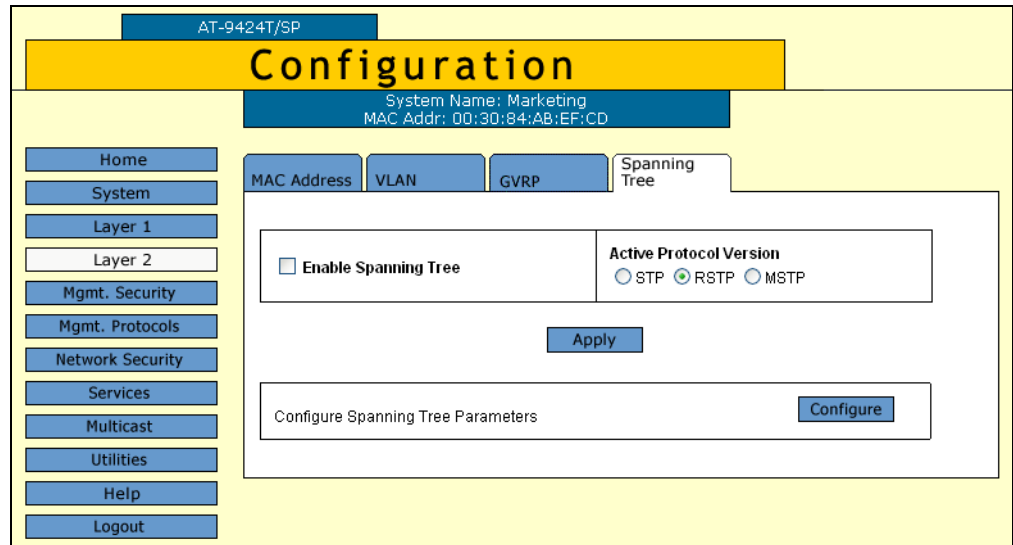


Figure 127. Spanning Tree Tab (Configuration)

4. To enable or disable spanning tree, click the **Enable Spanning Tree** check box. A check indicates that the feature is enabled while no check indicates that the feature is disabled. The default is disabled.
5. To select a spanning tree version, for the Active Protocol Version parameter click **STP**, **RSTP**, or **MSTP**. The default is RSTP.

Note

Only one spanning tree protocol can be active on the switch at a time.

6. Click **Apply**.
7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)
8. If you activated STP, go to “Configuring STP” on page 288. If you activated RSTP go to Step “Configuring RSTP” on page 296. If you activated MSTP, go to Chapter 15, “MSTP” on page 179.

Configuring STP



Caution

The bridge provides default STP parameters that are adequate for most networks. Changing them without prior experience and an understanding of how STP works might have a negative effect on your network. You should consult the IEEE 802.1d standard before changing any of the STP parameters.

To configure STP, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab shown by default, as shown in Figure 23 on page 91.

3. Select the **Spanning Tree** tab.

The Spanning Tree tab is shown in Figure 127 on page 287.

4. Click **Configure**.

The Configure STP Parameters tab is shown in Figure 128.

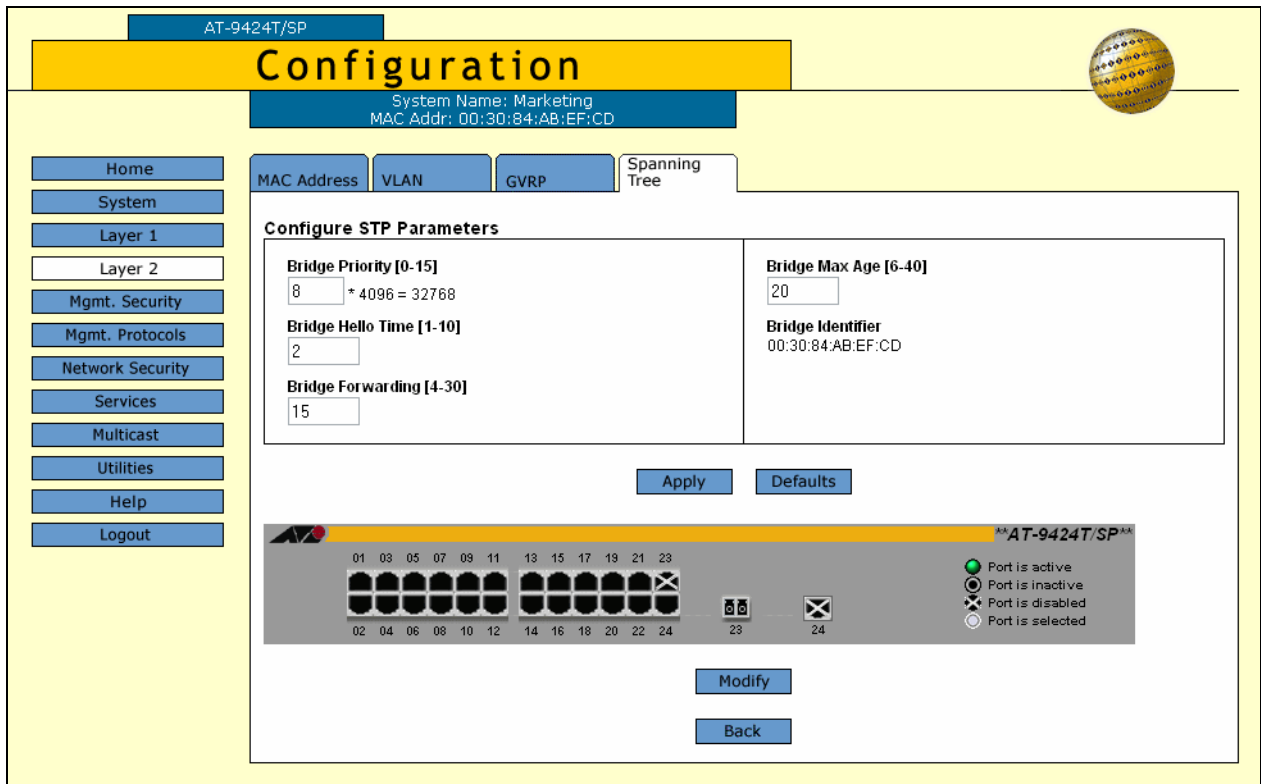


Figure 128. Configure STP Parameters Tab (Configuration)

Note

The Defaults button returns all STP settings to the default settings.

- Configure the following parameters as necessary.

Bridge Priority

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. When a root bridge goes off-line, the bridge with the next priority number automatically takes over as the root bridge. This parameter can be from 0 (zero) to 61,440 in increments of

4096, with 0 being the highest priority. For a list of the increments, refer to Table 6.

Table 6. 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

Bridge Hello Time

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.

Bridge Forwarding Delay

The waiting period in seconds 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.

Bridge Max Age

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 value 20, all bridges delete current configuration messages after 20 seconds. This parameter can be from 6 to 40 seconds.

In selecting a value for maximum age, the following rules must be observed:

MaxAge must be greater than $(2 \times (\text{HelloTime} + 1))$

MaxAge must be less than $(2 \times (\text{ForwardingDelay} - 1))$

Note

The aging time for BPDUs is different from the aging time used by the MAC address table.

Bridge Identifier

The MAC address of the bridge. The bridge identifier is used as a tie breaker in the selection of the root bridge when two or more bridges have the same bridge priority value. This value cannot be changed.

6. After you have made the desired changes, click **Apply**.
7. To configure a port's STP settings, click on the port in the switch image and click **Modify**. You can select more than one port at a time.

The STP Settings - Port(s) page is shown in Figure 129.

Figure 129. STP Settings - Port(s) Page

8. Configure the following parameters as necessary.

Port 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. The default value is 8 (priority value 128). For a list of the increments, refer to Table 7.

Table 7. 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

Table 7. Port Priority Value Increments (Continued)

Increment	Bridge Priority	Increment	Bridge Priority
6	96	14	224
7	112	15	240

Port Cost

The spanning tree algorithm uses the cost parameter to decide which port provides the lowest cost path to the root bridge for that LAN. The range is 0 to 65,535. The default setting is Auto-detect, which sets port cost depending on the speed of the port. If you select Auto-Detect, the management software assigns a value of 100 if the port is operating at 10 Mbps, 10 for 100 Mbps, and 4 for one gigabit.

9. After you have configured the parameters, click **Apply**.
10. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Note

A change to the port priority parameter takes effect immediately. A change to the port cost value requires you to reset the switch. A new port cost value is not implemented until the unit is reset.

Displaying the STP Settings

To display the STP settings, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 130.

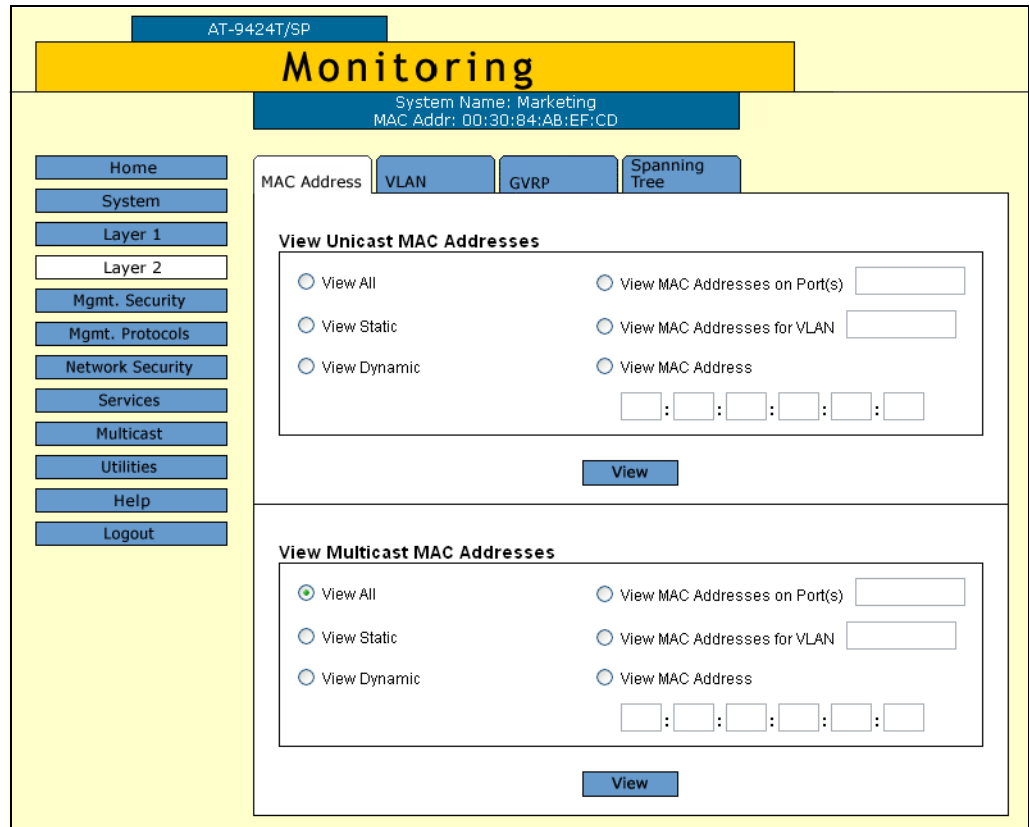


Figure 130. MAC Address Tab (Monitoring)

3. Select the **Spanning Tree** tab.

The Spanning Tree tabs is shown in Figure 131.

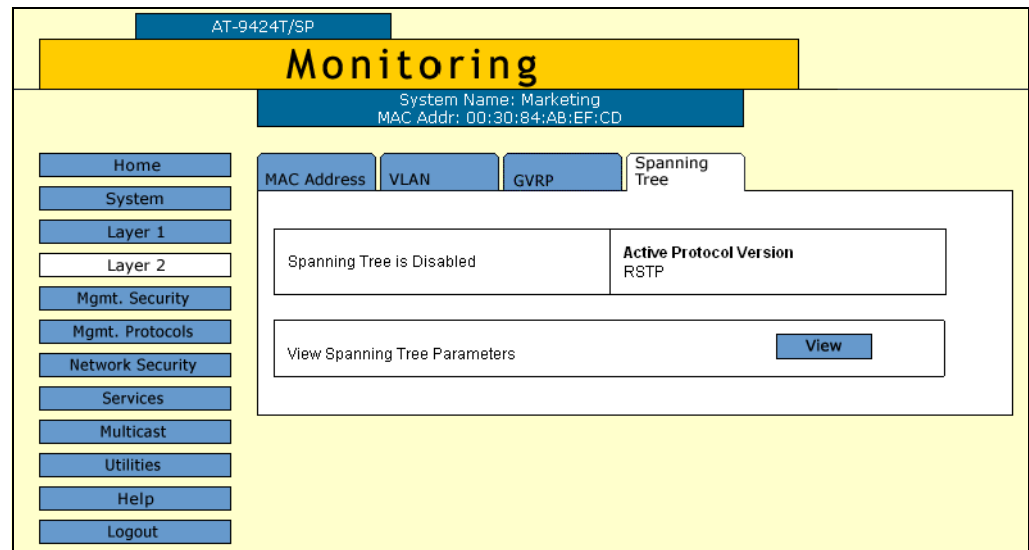


Figure 131. Spanning Tree Tab (Monitoring)

4. Click **View**.

The Monitor STP Parameters tab is shown in Figure 132.

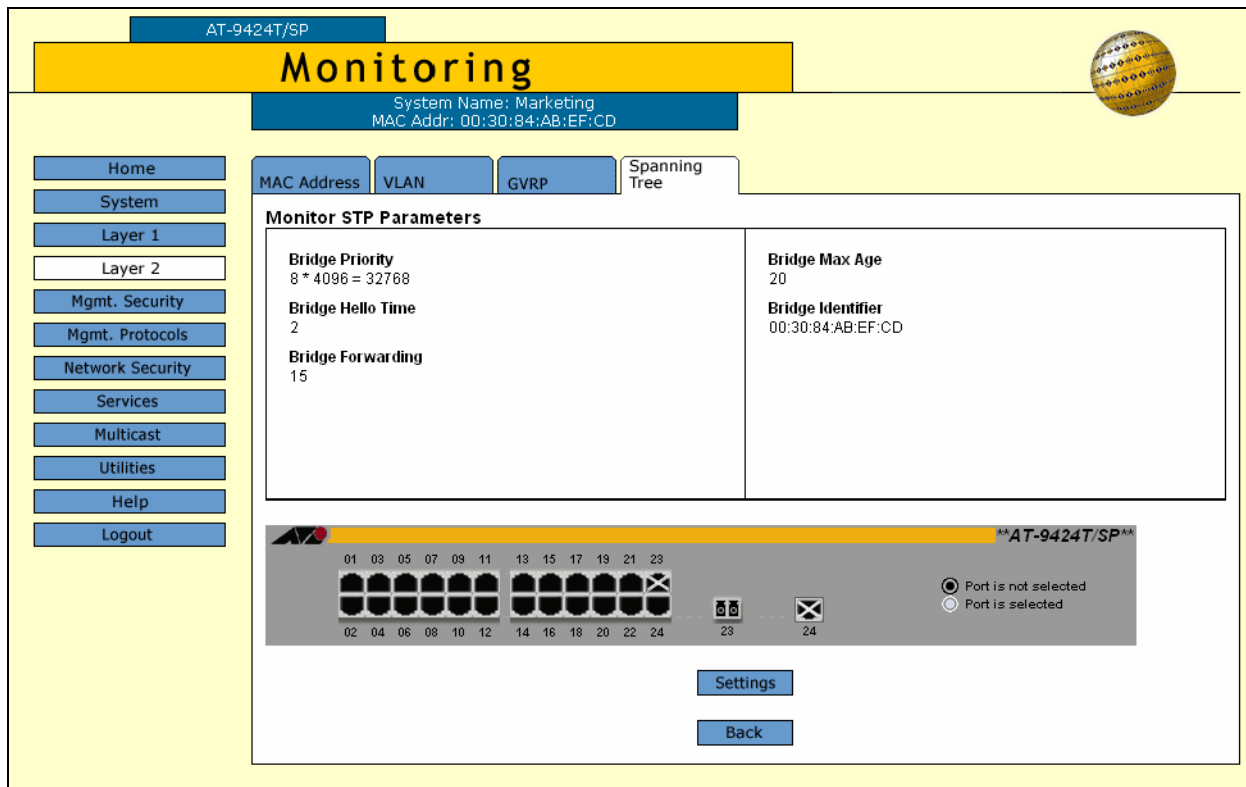


Figure 132. Monitor STP Parameters Tab (Monitoring)

5. To view port settings, click a port in the switch and click **Status** or **Settings**.

The STP Settings page is shown in Figure 133.

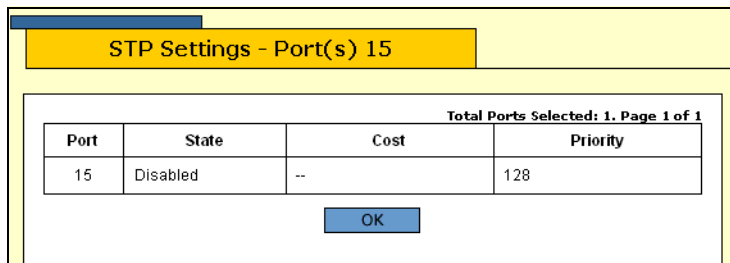


Figure 133. STP Settings Page

The STP Settings page displays a table that contains the following columns of information:

- Port**
Port number.

State

Current state of the port. The possible states are Enabled or Disabled.

Cost

Port cost of the port. The default is Auto-Update.

Priority

The number used as a tie-breaker when two or more ports have equal costs to the root bridge.

6. Click **OK** to close the page.

Resetting STP to the Default Settings

To reset STP to the factory default settings, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab shown by default, as shown in Figure 23 on page 91.

3. Select the **Spanning Tree** tab.

The Spanning Tree tab is shown in Figure 127 on page 287.

4. Click **Configure**.

The Configure STP Parameters tab is shown in Figure 128 on page 289.

5. Click **Defaults**.

The STP defaults are shown in "STP, RSTP, and MSTP Default Settings" on page 367.

Configuring RSTP



Caution

The bridge provides default RSTP parameters that are adequate for most networks. Changing them without prior experience and an understanding of how RSTP works might have a negative effect on your network. You should consult the IEEE 802.1w standard before changing any of the RSTP parameters.

To configure RSTP, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab shown by default, as shown in Figure 23 on page 91.

3. Select the **Spanning Tree** tab.

The Spanning Tree tab is shown in Figure 127 on page 287.

4. Click **Configure**.

The Configure RSTP Bridge Parameters tab is shown in Figure 134.

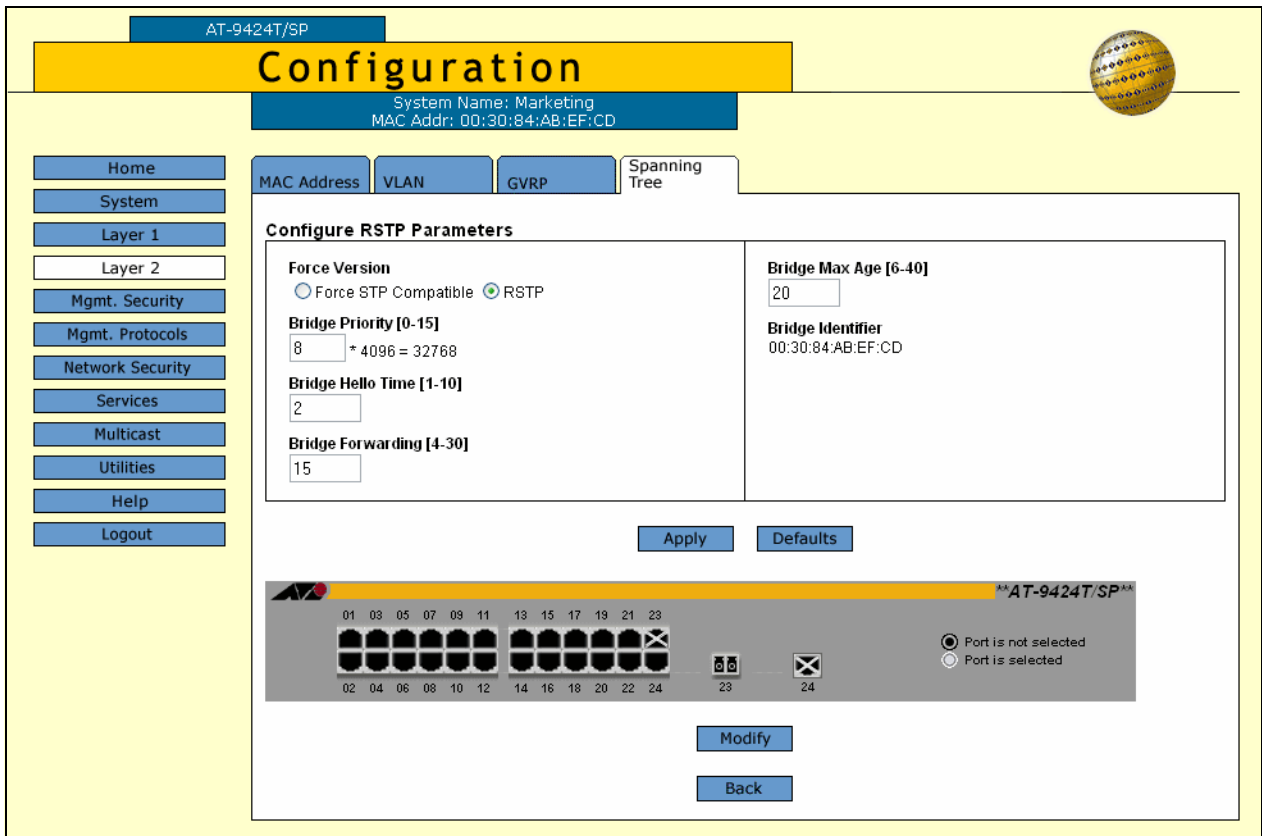


Figure 134. Configure RSTP Parameters Tab (Configuration)

- Configure the following parameters as necessary.

Force Version

This selection determines whether the bridge operates with RSTP or in an STP-compatible mode. If you select RSTP, the bridge operates all ports in RSTP, except for those ports that receive STP BPDU packets. If you select Force STP Compatible, the bridge operates in RSTP, using the RSTP parameter settings, but it sends only STP BPDU packets out the ports.

Bridge Priority

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. When a root bridge goes off-line, the bridge with the next priority number automatically takes over as the root bridge. This parameter can be from 0 (zero) to 61,440 in increments of 4096, with 0 being the highest priority. For a list of the increments, refer to Table 6 on page 290.

Bridge Hello Time

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.

Bridge Forwarding

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, possibly resulting in a network loop. The range is 4 to 30 seconds. The default is 15 seconds. This setting applies only to ports running in the STP-compatible mode.

Bridge Max Age

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. This parameter can be from 6 to 40 seconds. The default is 20 seconds.

In selecting a value for maximum age, the following must be observed:

MaxAge must be greater than $(2 \times (\text{HelloTime} + 1))$.

MaxAge must be less than $(2 \times (\text{ForwardingDelay} - 1))$

Bridge Identifier

The MAC address of the bridge. The bridge identifier is used as a tie breaker in the selection of the root bridge when two or more bridges have the same bridge priority value. This value cannot be changed.

6. After you have made your changes, click **Apply**.
7. To configure RSTP port settings, click on the port in the switch image and click **Modify**. You can select more than one port at a time.

The RSTP Settings - Port(s) page is shown in Figure 135.

Figure 135. RSTP Settings - Port(s) Page

8. Configure the following parameters as necessary.

Port 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. The default value is 8 (priority value 128). For a list of the increments, refer to Table 7 on page 291.

Port Cost

The spanning tree algorithm uses the cost parameter to decide which port provides the lowest cost path to the root bridge for that LAN. The range is 0 to 20,000,000. The default setting is Automatic detect, which sets port cost depending on the speed of the port. Default values are 2,000,000 for 10 Mbps ports, 200,000 for a 100 Mbps ports, and 20,000 for one gigabit ports.

Point-to-Point

This parameter defines whether the port is functioning as a point-to-point port. The possible settings are Yes, No, and Auto-Detect. For an explanation of this parameter, refer to “Point-to-Point and Edge Ports” in Chapter 16, “STP and RSTP” in the *AT-S63 Management Software Menus Interface User's Guide*.

Edge Port

This parameter defines whether the port is functioning as an edge port. The possible settings are Yes and No. For an explanation of this parameter, refer to “Point-to-Point and Edge Ports” in Chapter 16, “STP and RSTP” in the *AT-S63 Management Software Menus Interface User's Guide*.

9. After you have configured the parameters, click **Apply**.

10. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Note

All changes to a port's RSTP settings, with the exception of port cost, are activated immediately. A change to the port cost value requires you to reset the switch. A new port cost value is not implemented until the unit is reset.

Resetting RSTP to the Default Settings

To reset RSTP to the default settings, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select **Layer 2**.

The Layer 2 page is displayed with the MAC Address tab shown by default, as shown in Figure 23 on page 91.

3. Select the **Spanning Tree** tab.

The Spanning Tree tab is shown in Figure 127 on page 287.

4. Click **Configure**.

The Configure RSTP Bridge Parameters tab is shown in Figure 134 on page 297.

5. Click **Defaults**.

The RSTP defaults are shown in "STP, RSTP, and MSTP Default Settings" on page 367.

Displaying RSTP Settings

To display RSTP parameter settings, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Layer 2** option.

3. The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 130 on page 293.

4. Select the **Spanning Tree** tab.

The Spanning Tree tabs is shown in Figure 131 on page 293.

This tab displays information on whether spanning tree is enable or disabled and which protocol version, STP or RSTP, is active.

5. Click **View**.

The Monitor RSTP Parameters tab is shown in Figure 136.

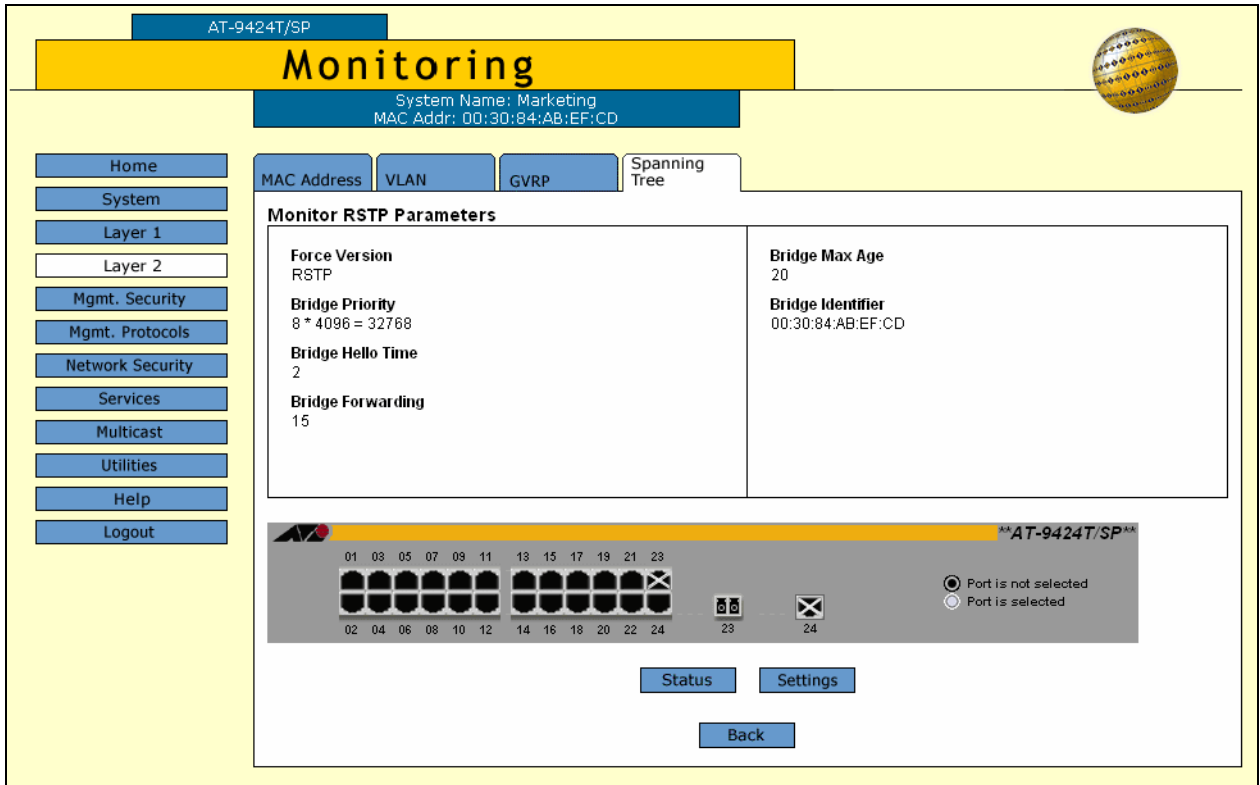


Figure 136. Monitor RSTP Parameters Tab (Monitoring)

6. To view port settings, click a port in the switch and click **Status** or **Settings**.

The RSTP Settings page is shown in Figure 137.

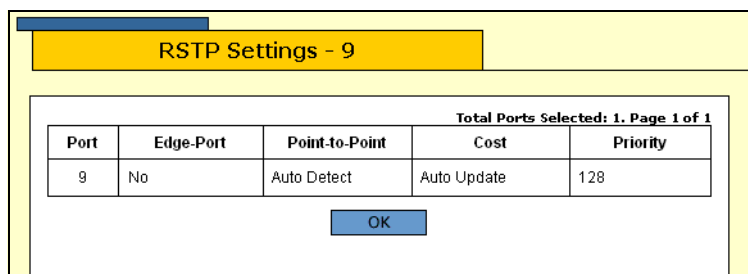


Figure 137. RSTP Settings Page

The RSTP Settings page displays a table that contains the following columns of information:

Port

The port number.

Edge-Port

Whether or not the port is operating as an edge port. The possible settings are Yes and No.

Point-to-Point

Whether or not the port is functioning as a point-to-point port. The possible settings are Yes, No, and Auto Detect.

Cost

Port cost of the port. The default is Auto Update.

Priority

The number used as a tie-breaker when two or more ports have equal costs to the root bridge.

7. Click **OK** to close the page.

Chapter 20

MSTP

This chapter explains how to configure MSTP parameters on an AT-9400 Series switch using a web browser management session. It contains the following procedures:

- ❑ “Enabling MSTP” on page 304
- ❑ “Configuring MSTP” on page 306
- ❑ “Creating, Deleting, or Modifying MSTI IDs” on page 310
- ❑ “Adding, Removing, or Modifying VLAN Associations to MSTIs” on page 314
- ❑ “Configuring MSTP Port Parameters” on page 317
- ❑ “Displaying the MSTP Port Configuration” on page 319
- ❑ “Displaying the MSTP Port Status” on page 322
- ❑ “Displaying the MSTP Port Status” on page 322
- ❑ “Resetting MSTP to the Default Settings” on page 324

Note

For background information on MSTP, refer to Chapter 22, “MSTP,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Enabling MSTP

The AT-9400 Series switch can support the three spanning tree protocols STP, RSTP, and MSTP. However, only one spanning tree protocol can be active on the switch at a time. So before you can enable a spanning tree protocol, you must first select it as the active spanning tree protocol. After you select it, you can then enable or disable it.

To select MSTP as the active spanning tree protocol and to enable or disable it, perform the following procedure:

Note

Changing the active spanning tree protocol resets the switch.

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab shown by default, as shown in Figure 126 on page 286.

3. Select the **Spanning Tree** tab.

The Spanning Tree tab is shown in Figure 138.

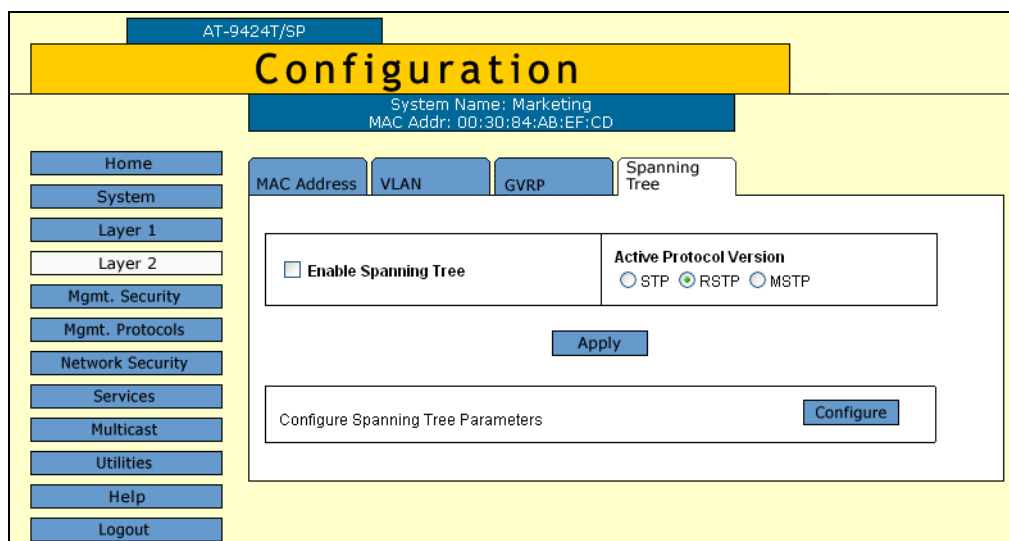


Figure 138. Spanning Tree Tab (Configuration)

Note

If you do not want to change the active spanning tree protocol and just want to enable or disable it, go to Step 5.

4. To change the active spanning tree protocol on the switch, click **STP**, **RSTP**, or **MSTP** in the Active Protocol Version section of the tab. The default is RSTP.

Note

Only one spanning tree protocol can be active on the switch at a time.

5. To enable or disable the active spanning tree protocol on the switch, click the **Enable Spanning Tree** check box. A check indicates that the spanning tree is enabled while no check indicates that spanning tree is disabled. The default is disabled.
6. Click **Apply**.

Note

If you changed the active spanning tree protocol, the switch resets and your management session is ended. To continue managing the switch, you must restart your management session after the switch is finished reloading the AT-S63 management software.

7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)
8. If you activated STP, go to “Configuring STP” on page 164. If you activated RSTP go to “Configuring RSTP” on page 172. If you activated MSTP, go to “Configuring MSTP” on page 306.

Configuring MSTP

This section contains the following procedures:

- ❑ “Configuring MSTP Parameters,” next
- ❑ “Configuring the CIST Priority” on page 309
- ❑ “Creating, Deleting, or Modifying MSTI IDs” on page 310
- ❑ “Adding, Removing, or Modifying VLAN Associations to MSTIs” on page 314
- ❑ “Configuring MSTP Port Parameters” on page 317

Note

MSTP must be selected as the active spanning tree protocol on the switch before you can configure it. For instructions on selecting the active spanning tree, refer to “Enabling MSTP” on page 304.

Note

When MSTP is enabled, the GVRP tab is not shown on the Configuration or Monitoring Layer 2 page.

Configuring MSTP Parameters

To configure MSTP parameters, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 23 on page 91.

3. Select the **Spanning Tree** tab.

The Spanning Tree tab is shown in Figure 51 on page 162.

4. Click **Configure**.

The expanded MSTP Spanning Tree tab is shown in Figure 139.

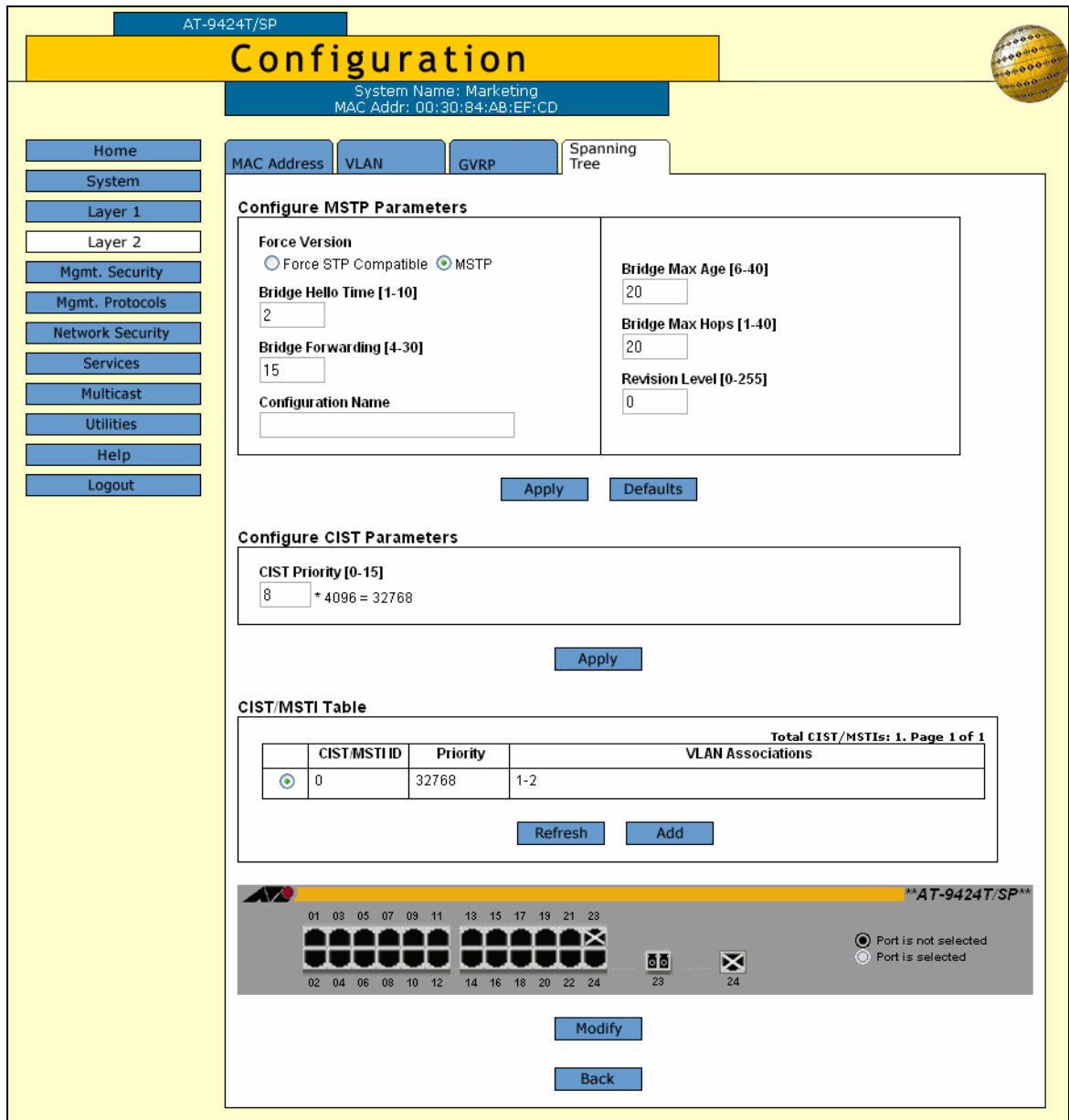


Figure 139. Configure MSTP Parameters Tab (Configuration)

Note

This procedure explains the Configure MSTP Parameters section of the page. The CIST/MSTI Table is explained in “Adding, Removing, or Modifying VLAN Associations to MSTIs” on page 314. The graphic image of the switch is described in “Configuring MSTP Port Parameters” on page 317.

Configure the following parameters as necessary.

Force Version

This selection determines whether the bridge operates with MSTP or in an STP-compatible mode. If you select MSTP, the bridge operates all ports in MSTP, except those ports that receive STP or RSTP BPDU packets. If you select Force STP Compatible, the bridge uses its MSTP parameter settings, but sends only STP BPDU packets from the ports. The default is MSTP.

Bridge Hello Time

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. This value is active only if the bridge is selected as the root bridge of the network.

Bridge Forwarding

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 of the links may have adapted to the change, possibly resulting in a network loop. The range is from 4 to 30 seconds. The default is 15 seconds. This setting applies only to ports running in the STP-compatible mode.

Configuration Name

The name of the MSTP region. The range is 0 (zero) to 32 alphanumeric characters in length. The name, which is case sensitive, must be the same on all bridges in a region. Examples of a configuration name include Sales Region and Production Region.

Bridge Max Age

The length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge. This parameter applies only if the bridged network contains an STP or RSTP single-instance spanning tree. Otherwise, the bridges use the Max Hop counter to delete BPDUs.

All bridges in a single-instance 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 of 20, all bridges delete current configuration messages after 20 seconds. The range of this parameter is from 6 to 40 seconds. The default is 20 seconds.

In selecting a value for maximum age, the following must be observed:

MaxAge must be greater than $(2 \times (\text{HelloTime} + 1))$

MaxAge must be less than $(2 \times (\text{ForwardingDelay} - 1))$

Bridge Max Hops

MSTP regions use this parameter to discard BPDUs. The Max Hop counter in a BPDU is decremented every time the BPDU crosses an MSTP region boundary. After the counter reaches zero, the BPDU is deleted.

Revision Level

The revision level of an MSTP region. This is an arbitrary number that you assign to a region. The revision level must be the same on all bridges in a region. Different regions can have the same revision level without conflict. The range is 0 (zero) to 255.

5. Click **Apply**.
6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Or, proceed to the next procedure to configure the CIST priority.

Configuring the CIST Priority

To configure the CIST priority, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 23 on page 91.

3. Select the **Spanning Tree** tab.

The Spanning Tree tab is shown in Figure 51 on page 162.

4. Click **Configure**.

The expanded MSTP Spanning Tree tab is shown in Figure 139 on page 307.

5. In the Configure CIST Parameters section, set the **CIST Priority**, the priority number for the bridge.

This number is used to determine the root bridge of the bridged network. This number is analogous to the RSTP bridge priority value. The bridge in the network with the lowest priority number is selected as the root bridge. If two or more bridges have the same bridge or CIST priority values, the bridge with the numerically lowest MAC address becomes the root bridge.

6. Click **Apply**.
7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Creating, Deleting, or Modifying MSTI IDs

To create, delete, or modify MSTI IDs, perform one of the following procedures.

Creating an MSTI ID

To create an MSTI ID, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 23 on page 91.

3. Select the **Spanning Tree** tab.

The Spanning Tree tab is shown in Figure 51 on page 162.

4. Click **Configure**.

The expanded MSTP Spanning Tree tab is shown in Figure 139 on page 307.

5. In the CIST/MSTI Table section of the tab, click **Add**.

The Add New MSTI page is shown in Figure 140.

Figure 140. Add New MSTI Page

6. In the MSTI ID field, enter a new MSTI ID. The range is 1 to 15.

7. In the Priority field, enter an MSTI Priority value. This parameter is used in selecting a regional root for the MSTI. The range is 0 (zero) to 61,440 in increments of 4,096, with 0 being the highest priority. This parameter is used in selecting a regional root for the MSTI. For a list of the increments, refer to Table 5, "Bridge Priority Value Increments" on page 166. The default is 0.
8. Click **Apply**.
9. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)
10. Repeat this procedure to create more MSTI IDs.

Deleting an MSTI ID

To delete an MSTI ID, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 23 on page 91.

3. Select the **Spanning Tree** tab.

The Spanning Tree tab is shown in Figure 51 on page 162.

4. Click **Configure**.

The expanded MSTP Spanning Tree tab is shown in Figure 139 on page 307.

5. In the CIST/MSTI Table section of the tab, click the button next to the MSTI ID you want to delete. You can select only one MSTI ID at a time.
6. Click **Remove**.
7. A confirmation prompt is displayed.
8. Click **OK** to delete the MSTI or **Cancel** to cancel the procedure:
9. If you select OK, the MSTI is deleted and VLANs associated with it are returned to CIST, which has an ID of 0.

Modifying an MSTI ID

To modify an MSTI ID, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

- From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 23 on page 91.

- Select the **Spanning Tree** tab.

The Spanning Tree tab is shown in Figure 51 on page 162.

- Click **Configure**.

The expanded MSTP Spanning Tree tab is shown in Figure 139 on page 307.

- In the CIST/MSTI Table section of the tab, click the button next to the MSTI ID you want to modify. You can select only one MSTI ID at a time. You cannot modify CIST.

- Click **Modify**.

The Modify MSTI page is shown in Figure 141.

The screenshot shows a web-based configuration interface for modifying an MSTI. The title bar at the top is yellow and contains the text 'Modify MSTI'. Below the title bar is a white rectangular area containing the configuration fields. The first field is 'MSTI ID' with a value of '2'. The second field is 'Priority' with a value of '7' and a calculation '* 4096 = 28672'. The third field is 'VLAN List' with a value of '3'. At the bottom of the white area are two blue buttons: 'Apply' and 'Cancel'.

Figure 141. Modify MSTI Page

- In the Priority field, enter a new MSTI Priority value. This parameter is used in selecting a regional root for the MSTI. The range is 0 (zero) to 61,440 in increments of 4,096, with 0 being the highest priority. For a list of the increments, refer to Table 5, “Bridge Priority Value Increments” on page 166. The default is 0.
- Click **Apply**.
- From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

10. Repeat this procedure to modify more MSTI IDs.

Adding, Removing, or Modifying VLAN Associations to MSTIs

This section explains how to add or remove VLANs associated to MSTI IDs.

Adding a VLAN Association

To add a VLAN association, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 23 on page 91.

3. Select the **Spanning Tree** tab.

The Spanning Tree tab is shown in Figure 51 on page 162.

4. Click **Configure**.

The expanded MSTP Spanning Tree tab is shown in Figure 139 on page 307.

5. In the CIST/MSTI Table section of the tab, the VLAN Associations field, enter the VIDs of the VLANs to be associated with this MSTI. You can specify more than one VID at a time (for example, 2,4,7).

6. Click **Apply**.

7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Or, proceed to the next procedure to configure the CIST priority.

Removing a VLAN Association

To remove a VLAN association, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 23 on page 91.

3. Select the **Spanning Tree** tab.

The Spanning Tree tab is shown in Figure 51 on page 162.

4. Click **Configure**.

The expanded MSTP Spanning Tree tab is shown in Figure 139 on page 307.

5. In the CIST/MSTI Table section of the tab, the VLAN Associations field, remove the VIDs of the VLANS that you no longer want to be associated with this MSTI. You can specify more than one VID at a time (for example, 2,4,7).
6. Click Apply.
7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Or, proceed to the next procedure to configure the CIST priority.

Modifying a VLAN Association

To modify a VLAN association, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 23 on page 91.

3. Select the **Spanning Tree** tab.

The Spanning Tree tab is shown in Figure 51 on page 162.

4. Click **Configure**.

The expanded MSTP Spanning Tree tab is shown in Figure 139 on page 307.

5. In the CIST/MSTI Table section of the tab, the VLAN Associations field, modify the VIDs of the VLANS that you no longer want to be associated with this MSTI. You can specify more than one VID at a time (e.g., 2,4,7).
6. Click Apply.

7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Configuring MSTP Port Parameters

To configure MSTP port parameters, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 23 on page 91.

3. Select the **Spanning Tree** tab.

The Spanning Tree tab is shown in Figure 138 on page 304.

4. Click **Configure**.

The expanded MSTP Spanning Tree tab is shown in Figure 139 on page 307.

5. In the diagram of the switch at the bottom of the MSTP Spanning Tree Expanded page, click the ports you want to configure. You can select more than one port at a time.

6. Click **Modify**.

The MSTP Settings - Port(s) page is shown in Figure 142.

Figure 142. MSTP Settings - Port(s) Page

7. Configure the following parameters as necessary.

Port Priority

This parameter is used as a tie breaker when two or more ports are

determined to have equal costs to the regional root bridge. The range is 0 to 240 in increments of 16. The default value is 8 (priority value is 128). For a list of the increments, refer to Table 6, “Port Priority Value Increments” on page 167.

Port Internal Path Cost

The port cost of the port if the port is connected to a bridge which is part of the same MSTP region. The range is 0 to 200,000,000. The default setting is Auto-detect, which sets port cost depending on the speed of the port. Default values are 2,000,000 for 10 Mbps ports, 200,000 for a 100 Mbps ports, and 20,000 for one gigabit ports.

Edge Port

This parameter defines whether the port is functioning as an edge port. The possible settings are Yes and No. For an explanation of this parameter, refer to “Point-to-Point and Edge Ports” in Chapter 16, “STP and RSTP” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Point-to-Point

This parameter defines whether the port is functioning as a point-to-point port. The possible settings are Yes, No, and Auto-Detect. For an explanation of this parameter, refer to “Point-to-Point and Edge Ports” in Chapter 21, “STP and RSTP” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Port External Path Cost

The port cost of the port if the port is connected to a bridge which is a member of another MSTP region or is running STP or RSTP. The range is 0 to 200,000,000. The default setting is 200,000.

8. After configuring the parameters, click **Apply**.
9. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)
10. Repeat this procedure to configure MSTP parameters for other switch ports.

Displaying the MSTP Port Configuration

To display the MSTP port configuration, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 126 on page 286.

3. Select the **Spanning Tree** tab.

The Spanning Tree tab is shown in Figure 127 on page 287.

This tab displays information on whether spanning tree is enable or disabled and which protocol version, STP, RSTP, or MSTP is active.

4. Click **View**.

The MSTP Parameters tab is shown in Figure 143.

The screenshot shows a network management interface with a yellow header 'Monitoring' and a sub-header 'AT-9424T/SP'. Below the header, system information is displayed: 'System Name: Marketing' and 'MAC Addr: 00:30:84:AB:EF:CD'. A navigation menu on the left includes options like Home, System, Layer 1, Layer 2, Mgmt. Security, Mgmt. Protocols, Network Security, Services, Multicast, Utilities, Help, and Logout. The main content area is divided into several sections:

- MAC Address**, **VLAN**, **GVRP**, and **Spanning Tree** tabs.
- Monitor MSTP Parameters** section with a table:

Force Version MSTP	Bridge Max Age 20
Bridge Hello Time 2	Bridge Max Hops 20
Bridge Forwarding 15	Revision Level 0
Configuration Name	
- Monitor CIST Parameters** section with a table:

CIST Priority 8 * 4096 = 32768	
--	--
- CIST/MSTI Table** section with a table:

CIST/MSTI ID	Priority	VLAN Associations
0	32768	1-2

 Total CIST/MSTIs: 1. Page 1 of 1. A 'Refresh' button is located below the table.
- A port selection interface showing a grid of ports (01-24) with a legend:
 - Port is not selected
 - Port is selected
 Port 15 is selected. Below the grid, there is a text input '0 CIST[0]MSTI[1-15]' and buttons for 'Status', 'Settings', and 'Back'.

Figure 143. Monitor MSTP Parameters Tab (Monitoring)

- Click a port in the switch and click **Settings**. You can select more than one port.

The MSTP Settings - Port (s) page is shown in Figure 144.

The screenshot shows the 'MSTP Settings - Port(s) 15' page. It features a table with the following data:

Port	Edge-Port	Point-to-Point	External Cost	Internal Cost	Priority
15	Yes	Auto Detect	200000	Auto Update	128

Total Ports Selected: 1. Page 1 of 1. An 'OK' button is located below the table.

Figure 144. MSTP Settings - Port(s) Page

The MSTP Settings page displays a table that contains the following columns of information:

Port

The port number.

Edge-Port

Whether or not the port is functioning as an edge port. The possible settings are Yes and No.

Point-to-Point

Whether or not the port is functioning as a point-to-point port. The possible settings are Yes, No, and Auto-Detect.

External Cost

The port cost of the port if the port is connected to a bridge which is a member of another MSTP region or is running STP or RSTP.

Internal Cost

The port cost of the port if the port is connected to a bridge which is part of the same MSTP region. The possible settings are:

Auto-detect - Port cost is automatically set depending on the speed of the port.

Default values - 2,000,000 for 10 Mbps ports, 200,000 for a 100 Mbps ports, and 20,000 for one gigabit ports.

Priority

This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the regional root bridge.

6. Click **OK** to close the page.

Displaying the MSTP Port Status

To display MSTP port status, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Layer 2** option.

The Monitoring Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 25 on page 95.

3. Select the **Spanning Tree** tab.

The Monitoring Spanning Tree tab for the active protocol, MSTP, is shown in Figure 143

4. Click a port in the switch and click **Status**. You can select more than one port.

The MSTP Port Status - Port(s) page is shown in Figure 145.

Total Ports Selected: 1. Page 1 of 1						
Port	State	CISTMSTIID	Role	P2P	Version	Port Cost
17	Disabled	0	---	---	---	---

OK

Figure 145. MSTP Port Status - Port(s) Page

The MSTP Port Status page displays a table that contains the following columns of information:

Port

The port number.

State

The MSTP state of the port. The possible states are:

Discarding - The port is discarding received packets and is not submitting forwarded packets for transmission.

Learning - The port is enabled for receiving, but not forwarding packets.

Forwarding - Normal operation.

Disabled - The port has not established a link with its end node.

Role

The MSTP role of the port. The possible roles are:

Root - The port that is connected to the root switch, directly or through other switches, with the least path cost.

Alternate - The port offers an alternate path in the direction of 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 on the designated switch for a LAN that has the least cost path to the root switch. This port connects the LAN to the root switch.

Master - Similar to the root port. When the port is a boundary port, the MSTI port roles follow the CIST port roles. The MSTI port role is called "master" when the CIST role is "root."

P2P

Whether or not the port is functioning as a point-to-point port. The possible settings are Yes, No, and Auto-Detect.

Version

Whether the port is operating in MSTP mode or STP-compatible mode.

Internal Port Cost

The port cost when the port is connected to a bridge in the same MSTP region.

5. Click **OK** to close the page.

Resetting MSTP to the Default Settings

To reset MSTP to the factory default settings, perform the following procedure:

1. From the home page, select **Configuration**.

The Configuration System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 23 on page 91.

3. Select the **Spanning Tree** tab.

The Spanning Tree tab is shown in Figure 138 on page 304.

4. Click **Configure**.

The expanded MSTP Spanning Tree tab is shown in Figure 139 on page 307.

5. Click **Defaults**.

The MSTP defaults are shown in “STP, RSTP, and MSTP Default Settings” on page 367.

Section V

Virtual LANs

The chapters in this section provide information and procedures for basic switch setup using the AT-S63 management software. The chapters include:

- ❑ Chapter 21, “Virtual LANs” on page 327
- ❑ Chapter 22, “Protected Ports VLANs” on page 341
- ❑ Chapter 23, “GARP VLAN Registration Protocol (GVRP)” on page 355

Chapter 21

Virtual LANs

This chapter explains how to create, modify, and delete port-based and tagged VLANs. This chapter also explains how to select a multiple VLAN mode.

This chapter contains the following sections:

- ❑ “Creating a New Port-Based or Tagged VLAN” on page 328
- ❑ “Modifying a VLAN” on page 332
- ❑ “Deleting a VLAN” on page 334
- ❑ “Selecting a VLAN Mode” on page 335
- ❑ “Displaying VLANs” on page 337
- ❑ “Specifying a Management VLAN” on page 339

Note

For background information on port-based and tagged VLANs, as well as management VLANs, refer to Chapter 23, “Port-based and Tagged VLANs,” in the *AT-S63 Management Software Menus Interface User’s Guide*. For more information about the multiple VLAN modes, refer to Chapter 25, “Multiple VLANs,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Creating a New Port-Based or Tagged VLAN

To create a new port-based or tagged VLAN, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 126 on page 286.

3. Select the **VLAN** tab.

The VLAN tab is shown in Figure 146.

AT-9424T/SP

Configuration

System Name: Marketing
MAC Addr: 00:30:84:AB:EF:CD

MAC Address | **VLAN** | GVRP | Spanning Tree

VLAN Configuration

VLAN Mode: User Configured
Uplink Port:
Mgmt. VLAN ID: 1

Apply

Total VLANs: 2. Page 1 of 1

VLAN List

VLAN ID	(Client) Name	Uplink Port	Type	Protocol	Tagged(T)/Untagged(U) Ports
1	Default_VLAN	NA	Port Based	None	U: 1-24
2	test	NA	Port Based	None	U: T: 5-6

Refresh | Modify | Add | Remove

Figure 146. VLAN Tab (Configuration)

Note

The Modify and Remove buttons are not shown in the tab if the only VLAN on the switch is the Default_VLAN.

The VLAN Mode and Uplink Port options are explained in “Selecting a VLAN Mode” on page 335. The Mgmt. VLAN ID option is explained in “Specifying a Management VLAN” on page 339.

The tab displays an existing VLANs on the switch.

- To add a new VLAN, click **Add**.

The Add New VLAN page is shown in Figure 147.

Figure 147. Add New VLAN Page

- Configure the following parameters as necessary.

VID

Enter a VID value for the new VLAN. The range of the VID value is 2 to 4096. The default is the next available VID number on the switch.

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, then the VID value for the VLAN should be the same on each switch. For example, if you are creating a VLAN called Sales that spans three switches, you should assign the Sales VLAN on each switch the same VID value.

Note

A VLAN must have a VID.

It is important to note that the switch is only aware of the VIDs of the VLANs that exist on the device, and not those that might already be in use in the network. For example, if you add a new AT-9400 Series switch to a network that already contains VLANs that use VIDs 2 through 24, the AT-S63 management software still uses VID 2 as the

default value when you create the first VLAN on the new switch, even though that VID number is already being used by another VLAN on the network. To prevent inadvertently using the same VID for two different VLANs, you should keep a list of all your network VLANs and their VID values.

Name

Specify a name for the new VLAN.

The name can be from one to fifteen alphanumeric characters in length. The name should reflect the function of the nodes that are part of the VLAN (for example, Sales or Accounting). The name cannot contain spaces or special characters, such as asterisks (*) or exclamation points (!).

If the VLAN is unique in your network, then the name should be unique as well. If the VLAN is part of a larger VLAN that spans multiple switches, then the name for the VLAN should be the same on each switch where nodes of the VLAN are connected.

Note




A VLAN must be assigned a name.

Type

Specify the VLAN type, either Port Based or Protected. Protected VLANs are described in

6. To select the ports for the VLAN, click on the appropriate ports in the switch image.

Clicking repeatedly on a port toggles the port through the following possible settings:

-  Untagged port
-  Tagged port
-  Port is not a member of the VLAN

Note

When a transceiver is inserted into an uplink slot and a link is established, that slot becomes a primary uplink port and the corresponding backup port, 23R or 24R, automatically transitions to redundant uplink status. Any VLAN settings remain intact when the backup port makes the transition to a redundant uplink state.

7. Click **Apply**.

Note

Any untagged ports that you assign to the new VLAN are automatically removed from their current untagged VLAN assignment.

The new user-configured VLAN is now ready for network operations.

8. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Modifying a VLAN

This procedure explains how to add or remove ports from a VLAN. When modifying a VLAN, note the following:

- ❑ You cannot change the VID of a VLAN.
- ❑ You cannot change the name of a VLAN from a web browser management session, but you can from a local or Telnet session.
- ❑ You cannot modify VLANs when the switch is operating in one of the multiple VLAN modes.

To modify a VLAN, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 23 on page 91.

3. Select the **VLAN** tab.

The VLAN tab is shown in Figure 146 on page 328.




4. Click the button next to the name of the VLAN you want to modify.

5. Click **Modify**.

The Modify VLAN page for the VLAN is displayed.

6. To add or remove ports from the VLAN, click on the appropriate ports in the switch image.

Clicking repeatedly on a port toggles the port through the following possible settings:

-  Untagged port
-  Tagged port
-  Port is not a member of the VLAN

7. Click **Apply**.

Note

Untagged ports that are added to a VLAN are automatically removed from their current untagged VLAN assignment. Untagged ports that are removed from a VLAN are returned to the Default_VLAN.

Removing an untagged port from the Default_VLAN without assigning it to another VLAN leaves the port as an untagged member of no VLAN.

The modified VLAN is now ready for network operations.

8. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting a VLAN

To delete a port-based or tagged VLAN from the switch, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 23 on page 91.

3. Select the **VLAN** tab.

The VLAN tab is shown in Figure 146 on page 328.

4. Click the button next to the name of the VLAN you want to delete. (You cannot delete the Default_VLAN.)

5. Click **Remove**.

A confirmation prompt is displayed.

6. Click **OK** to delete the VLAN or **Cancel** to cancel the procedure:

If you click OK, the VLAN is deleted from the switch. The untagged ports in the VLAN are returned to the Default_VLAN as untagged ports.

7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Selecting a VLAN Mode

The AT-S63 management software features three VLAN modes:

- Port-based and tagged VLAN Mode (default mode)
- IEEE 802.1Q-compliant Multiple VLAN Mode
- Non-IEEE 802.1Q compliant Multiple VLAN Mode

For background information on port-based and tagged VLANs, refer to Chapter 23, "Port-based and Tagged VLANs," in the *AT-S63 Management Software Menus Interface User's Guide*. For information on the multiple VLAN modes, refer to Chapter 25, "Multiple VLANs," in the *AT-S63 Management Software Menus Interface User's Guide*.

Note

Any port-based or tagged VLANs that you may have created are not retained when you change the VLAN mode from the user configured mode to a multiple VLAN mode and, at some point, reset the switch. The user configured VLAN information is lost and you must recreate the information if you later return the switch to the user configured VLAN mode.

To select a VLAN mode for the switch, perform the procedure below:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 23 on page 91.

3. Select the **VLAN** tab.

The VLAN tab is shown in Figure 146 on page 328.

4. In the VLAN Mode section, select a VLAN mode. Only one mode can be active on the switch at a time. The modes are:

User Configured - Port-based and tagged VLAN Mode

Multiple - Non-IEEE 802.1Q-compliant Multiple VLAN Mode

Multiple 802.1Q - IEEE 802.1Q-compliant Multiple VLAN Mode

5. If you select one of the multiple VLAN modes, specify an uplink port in the Uplink Port field. This port functions as the uplink port for the VLANs. The default is port 1.

6. Click **Apply**.

The new mode is automatically activated on the switch.

7. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying VLANs

To display the current VLANs on a switch, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Layer 2** option.
3. The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 126 on page 286.
4. Select the **VLAN** tab.

The VLAN tab is shown in Figure 148.

AT-9424T/SP

Monitoring

System Name: Marketing
MAC Addr: 00:30:84:AB:EF:CD

Home System Layer 1 Layer 2 Mgmt. Security Mgmt. Protocols Network Security Services Multicast Utilities Help Logout

MAC Address **VLAN** GVRP Spanning Tree

VLAN Configuration

VLAN Mode User Configured	Mgmt. VLAN ID 1
Uplink Port Not Applicable	

VLAN List Total VLANs: 2. Page 1 of 1

	VLAN ID	(Client) Name	Uplink Port	Type	Protocol	Tagged(T)/Untagged(U) Ports
<input checked="" type="radio"/>	1	Default_VLAN	NA	Port Based	None	U: 1-24
<input type="radio"/>	2	test	NA NA	Port Based	None	U: T: 5-6

Refresh View

Figure 148. VLAN Tab (Monitoring)

The upper part of the tab displays the following information:

Mode

The VLAN mode. The possible settings are:

User Configured - This mode supports port-based and tagged VLANs.

Multiple 802.1Q - The IEEE 802.1Q-compliant multiple VLAN mode.

Multiple - The non-IEEE 802.1Q-compliant multiple VLAN mode.

Management VLAN ID

VLAN ID of the management VLAN.

The lower part of the tab displays a table that contains the following columns of information:

VLAN ID

The VID number assigned to the VLAN.

(Client) Name

The name of the VLAN. If the switch is operating in one of the multiple VLAN modes, the names of the VLANs start with “Client,” with the exception of the VLAN containing the uplink port, which starts with “Uplink.”

Uplink Port

This column is applicable only when the switch is operating in one of the two multiple VLAN modes. The column lists the port that is functioning as the uplink port for all the other ports on the switch.

VLAN Type

The VLAN type. The possible settings are:

Port Based - The VLAN is a port-based or tagged VLAN.

GARP - The VLAN was automatically created by GARP.

Protocol

The protocol associated with this VLAN. The possible settings are:

Blank - The VLAN is a port-based or tagged VLAN.

GARP - The VLAN is a dynamic GVRP VLAN or the port is a dynamic GVRP port of a static VLAN.

Tagged(T)/Untagged(U) Port

Lists the ports of the VLAN. Tagged ports are designated with a “T” and untagged ports with a “U.”

Specifying a Management VLAN

The management VLAN is the VLAN through which an AT-9400 Series switch expects to receive management packets. This VLAN is important if you are managing a switch remotely or using the enhanced stacking feature of the switch. For more details about specifying a management VLAN, see Chapter 23, "Port-based and Tagged VLANs," in the *AT-S63 Management Software Menus Interface User's Guide*.

Note

You cannot specify a management VLAN when the switch is operating in a multiple VLAN mode.

To specify the management VLAN, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 23 on page 91.

3. Select the **VLAN** tab.

The VLAN tab is shown in Figure 146 on page 328.

4. For the Mgmt. VLAN ID parameter, enter the VID of the VLAN on the switch that you want to function as the management VLAN. The VLAN must already exist on the switch. The default is 1, which is the VID of the Default_VLAN.

5. Click **Apply**.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Chapter 22

Protected Ports VLANs

This chapter explains how to create, modify, and delete protected ports VLANs and contains the following sections:

- ❑ “Creating a New Protected Ports VLAN” on page 342
- ❑ “Modifying a Protected Ports VLAN” on page 347
- ❑ “Deleting a Protected Ports VLAN” on page 351
- ❑ “Displaying a Protected Ports VLAN” on page 352

Note

For background information on protected ports VLANs, refer to Chapter 26, “Protected Ports VLANs” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Creating a New Protected Ports VLAN

To create a new protected ports VLAN, perform the procedure below:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 126 on page 286.

3. Select the **VLAN** tab.

The VLAN tab is shown in Figure 146 on page 328.

Note

The Modify and Remove buttons are not included in the tab if the only VLAN on the switch is the Default_VLAN.

This tab displays the VLANs in a table that contains the following columns of information:

VLAN ID

The VID number assigned to the VLAN.

(Client) Name

The name of the VLAN.

Uplink Port

This column is applicable only when the switch is operating in one of the two multiple VLAN modes. The column lists the port that is functioning as the uplink port for the other ports on the switch.

Type

This column contains “Port Based” for both port-based and tagged VLANs, “GVRP Dynamic” for VLANs created by GVRP, and “Protected” for protected ports VLANs.

Protocol

Not used.

Tagged(T)/Untagged(U) Port

Lists the ports of the VLAN. Tagged ports are designated with a “T” and untagged ports with a “U.”

4. To create a new protected ports VLAN, click **Add**.

The Add New VLAN page is shown in Figure 149.

Figure 149. Add New VLAN Page

5. Select the **VID** field and enter a VID value for the new VLAN. The range of the VID value is 2 to 4096. The default is the next available VID number on the switch.

The switch is only aware of the VIDs of the VLANs that exist on the device, and not those that might already be in use in the network. For example, if you add a new AT-8500 Series switch to a network that already contains VLANs that use VIDs 2 through 24, the AT-S62 software will still use VID 2 as the default value when you create the first VLAN on the new switch, even though that VID number is already being used by another VLAN on the network. To prevent inadvertently using the same VID for two different VLANs, you should keep a list of all your network VLANs and their VID values.

Note

A VLAN must have a VID.

6. Select the **Name** field and enter a name for the new VLAN.




The name can be from one to fifteen alphanumeric characters in length. The name should reflect the function of the nodes that will be a part of the VLAN (for example, Sales or Accounting). The name cannot contain spaces or special characters, such as asterisks (*) or exclamation points (!).

Note

A VLAN must be assigned a name.

7. Select **Protected** as the Type.
8. Select the ports for the protected ports VLAN by clicking the ports in the switch image. (Designating group membership of the ports is performed later in the procedure.)

Clicking repeatedly on a port toggles the port through the following possible settings:

-  Untagged port
-  Tagged port
-  Port is not a member of the VLAN

9. Click **Apply**.

Note

Any untagged ports you assign to the new VLAN are automatically removed from their current untagged VLAN assignment.

The Add New Protected VLAN page is shown in Figure 150.

Add New Protected VLAN

Protected VLAN Details

VID 2	Name another test
Type Protected	Protocol None
Untagged Ports None	Tagged Ports None
Uplink Ports <input type="text"/>	

Apply

VLAN Groups

Group Number	Port List
--	--

Remove

Group Number <input type="text"/> [1-256]	Available Tagged Ports None
Available Untagged Ports None	

Add

Back **Refresh** **Apply** **Close**

Figure 150. Add New Protected VLAN Page

- Use the Uplinks Port menu to select an uplink port for the groups of this protected ports VLAN.

The menu lists all of the ports you selected as members of this VLAN. You can select more than one uplink port. To select multiple ports, hold down the Ctrl key when selecting the ports.

- Click **Apply**.
- In the Group Number field, enter a group number for one of the groups you want to create in the VLAN. Each group on the switch must be given a unique group number. The range is 1 to 256.
- In the Available Untagged Port and Available Tagged Ports lists, select the port you want to be in the group. You can assign more than one port to group. To select multiple ports from a list, use <Ctrl>+click.
- Click **Add**.

The switch creates the group and adds it to the VLAN Groups section of the window.

15. Repeat steps 12 and 13 to create the other groups for the VLAN.

16. After you have assigned all of the ports in the VLAN to a group, click the **Apply** button at the bottom of the window.

The management software will not allow you to create the VLAN until all of the ports have been assigned to a group.

The new protected ports VLAN is now ready for network operations.

17. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Modifying a Protected Ports VLAN

This procedure explains how to change the uplink port of a protected ports VLAN and how to add or remove ports from a VLAN. When modifying a protected ports VLAN, note the following:

- ❑ You cannot change the VID of a protected port VLAN.
- ❑ You cannot change the name of a VLAN from a web browser management session; but you can from a local or Telnet session.
- ❑ If you are adding untagged ports, the ports must be untagged members of the Default_VLAN or a port-based or tagged VLAN. They cannot be members of another protected ports VLAN.
- ❑ An untagged port removed from a VLAN is automatically returned to the Default_VLAN.
- ❑ A port that is already an untagged member of a protected ports VLAN cannot be made an untagged member of another protected ports VLAN until it is first removed from its current VLAN assignment and returned to the Default_VLAN.
- ❑ Changing the uplink port of a protected ports VLAN will require recreating all the VLAN's groups. If you need to change the uplink port, Allied Telesyn recommends that you write down on paper the VLAN's current configuration (i.e., port to group assignments). This information will make it easier for you to recreate the current configuration, with whatever modifications you want to make, when you perform the procedure. To display a VLAN's configuration, refer to "Displaying a Protected Ports VLAN" on page 352.

To modify a protected ports VLAN, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 126 on page 286.

3. Select the **VLAN** tab.

The VLAN tab is shown in Figure 146 on page 328.




4. Click the button next to the name of the protected ports VLAN you want to modify.

5. Click **Modify**.

The Modify VLAN window for the VLAN is displayed.

6. To add or remove ports from the VLAN, click on the appropriate ports in the switch image.

Clicking repeatedly on a port toggles the port through the following possible settings:

-  Untagged port
-  Tagged port
-  Port is not a member of the VLAN

7. After making the necessary changes, click **Apply**.

Note

Untagged ports that are added to a VLAN are automatically removed from their current untagged VLAN assignment. Untagged ports that are removed from a VLAN are returned to the Default_VLAN.

Removing an untagged port from the Default_VLAN without assigning it to another VLAN will leave the port as an untagged member of no VLAN.

The Modify Protected VLAN page is shown in Figure 151.

Protected VLAN Details

VID 2	Name Bldg_2_Floor_1st
Type Protected	Protocol None
Untagged Ports 1-6,9-12	Tagged Ports None
Uplink Ports 1	

Apply

VLAN Groups

	Group Number	Port List
<input checked="" type="radio"/>	1	2
<input type="radio"/>	2	3-4
<input type="radio"/>	3	5
<input type="radio"/>	5	6,9
<input type="radio"/>	7	10-11
<input type="radio"/>	8	12

Remove

Group Number
 [1-256]

Available Untagged Ports
None

Available Tagged Ports
None

Add

Back Refresh Apply Close

Figure 151. Modify Protected VLAN Page

8. To change the uplink port, do the following:

Note

Changing the uplink port will delete all the groups.

- a. Use the Uplinks Port menu to select a new uplink port for the groups of this protected ports VLAN. The menu lists all of the ports you selected as members of this VLAN. You can select more than one uplink port. To select multiple ports, hold down the Ctrl key when selecting the ports.
- b. When the confirmation prompt is displayed, click **OK**.
- c. Click **Apply**.

- d. Recreate the groups.
9. To delete a group, do the following:
 - a. Click the circle next to the group number and click **Remove**. The ports of the deleted group are now listed in the Available Untagged Ports and Available Untagged Ports lists.
 - b. Assign the ports to another group or use the ports to create a new group. All the ports in a protected ports VLAN must belong to a group.
 10. To modify an existing group, such as to add or remove ports, you must first delete the group and then recreate it with the desired changes.

Note

To completely remove a port from a protected ports VLAN, you must deselect the port in the graphical image of the switch in step 6, then delete its group, and finally recreate the group without the port.

11. To create a new group, do the following:
 - a. In the Group Number field, enter a group number for the new group. Each group on the switch must be given a unique group number. The range is 1 to 256.
 - b. In the Available Untagged Port and Available Tagged Ports lists, select the port to be in the group. You can assign more than one port to group. To select multiple ports from a list, hold down the Ctrl key when selecting the ports.
 - c. Click **Add**. The switch creates the group and adds it to the VLAN Groups section of the window.
12. After you have made the necessary changes and assigned all of the ports to a group, click **Apply** at the bottom of the window.

VLAN changes are immediately implemented on the switch.
13. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting a Protected Ports VLAN

To delete a protected ports VLAN from the switch, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 126 on page 286.

3. Select the **VLAN** tab.

The VLAN tab is shown in Figure 146 on page 328.

4. Click the button next to the name of the protected ports VLAN you want to delete. You cannot delete the Default_VLAN.

5. Click **Remove**.

A confirmation prompt is displayed.

6. Click **OK** to delete the VLAN or **Cancel** to cancel the procedure.

If you click OK, the VLAN is deleted from the switch. All ports in the VLAN are returned to the Default_VLAN as untagged ports.

7. To permanently save the change, select the **Save Config** menu selection.

Displaying a Protected Ports VLAN

To display the details of a protected port VLAN, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Layer 2** option.
3. The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 126 on page 286.
4. Select the **VLAN** tab.

The VLAN tab is shown in Figure 148 on page 337.

5. Click the circle next to the protected ports VLAN you want to view and click **View**.

The View Protected VLAN page is shown in Figure 152.

Protected VLAN Groups	
Group Number	Port List
22	15-21

Figure 152. View Protected VLAN Page

The VLAN Details section displays the following information.

VID

The VLAN ID.

Type

The VLAN type which is always Protected.

Untagged Ports

The untagged ports that are members of the VLAN.

Uplink Ports

The uplink port(s) for this group of ports.

Name

The VLAN name.

Protocol

Not use.

Tagged Ports

The tagged ports that are members of the VLAN.

The Protected VLAN Groups section displays the following information:

Group Number

The number assigned to the group.

Port List

The ports that are members of this group.

6. Click **Clear** to close the page.

Chapter 23

GARP VLAN Registration Protocol (GVRP)

This chapter contains instructions on how to configure GARP VLAN Registration Protocol (GVRP). This chapter contains the following procedures:

- ❑ “Configuring GVRP” on page 356
- ❑ “Enabling or Disabling GVRP on a Port” on page 358
- ❑ “Displaying the GVRP Configuration” on page 359
- ❑ “Displaying the GVRP Port Configuration” on page 361
- ❑ “Displaying the GVRP Database” on page 362
- ❑ “Displaying the GVRP State Machine” on page 363
- ❑ “Displaying the GVRP Counters” on page 366
- ❑ “Displaying the GIP Connected Ports Ring” on page 369

Note

For background information on GVRP, refer to Chapter 24, “GARP VLAN Registration Protocol,” in the *AT-S63 Management Software Menu Interface User’s Guide*.

Configuring GVRP

To configure GVRP, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab shown by default, as shown in Figure 126 on page 286.

3. Select the **GVRP** tab.

The GVRP tab is shown in Figure 153.

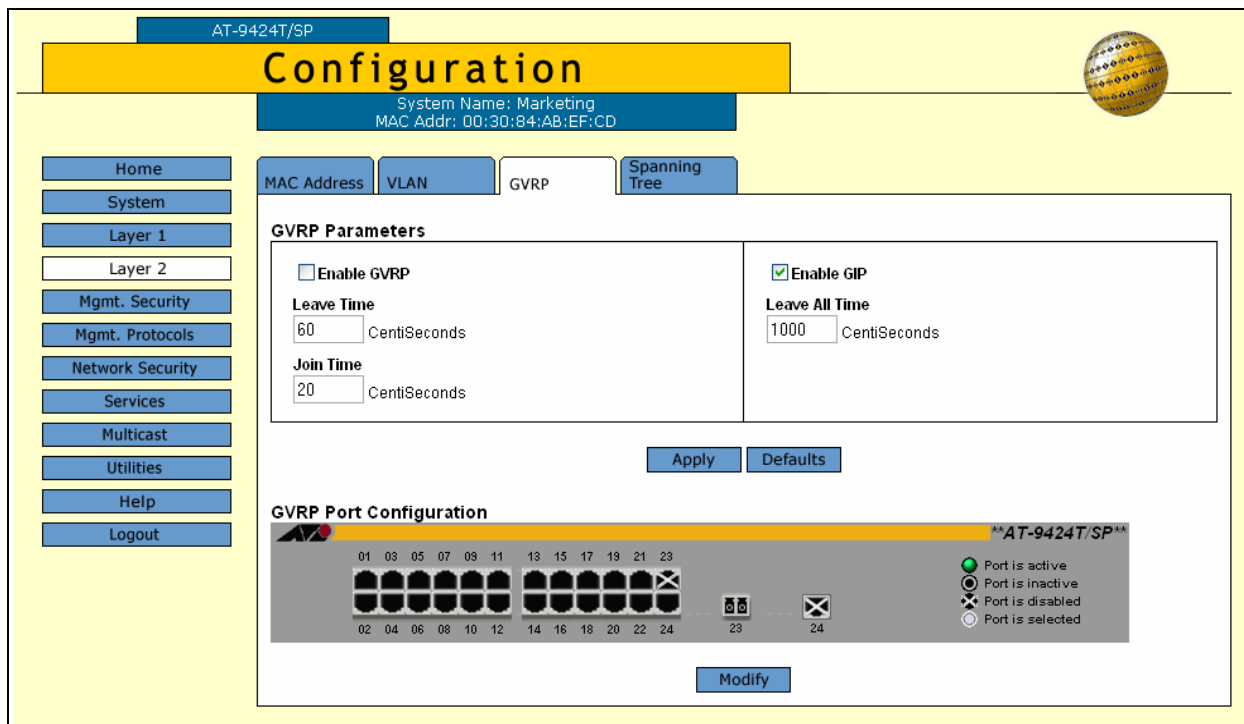


Figure 153. GVRP Tab (Configuration)

4. In the GVRP Parameters section, configure the following parameters as necessary.

Enable GVRP

Click to enable or disable GVRP.

Leave Time

Use this parameter to specify the leave time. The range is 30 to 80 centiseconds and the default is 60 centiseconds.

Join Time

Use this parameter to specify the join time. The range is 10 to 60 centiseconds and the default is 20 centiseconds.

Enable GIP

Click to enable GIP, which is required to propagate VLAN information among the ports of the switch.

Leave All Time

The range is 500 to 300 centiseconds and the default is 1000 centiseconds.

5. Click **Apply**.

Configuration changes are immediately activated on the switch.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Enabling or Disabling GVRP on a Port

To enable or disable GVRP on a port, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 23 on page 91.

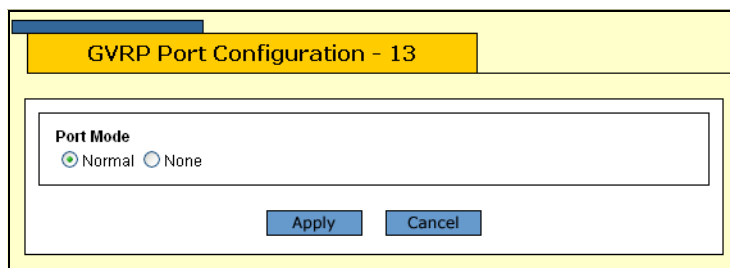
3. Select the **GVRP** tab.

The GVRP tab is shown in Figure 153 on page 356.

4. In the GVRP Port Configuration section, click the ports that you want to configure.

5. Click **Modify**.

The GVRP Port Configuration page is shown in Figure 154.



The screenshot shows a web interface for configuring GVRP on a port. The title bar reads "GVRP Port Configuration - 13". The main content area is titled "Port Mode" and contains two radio buttons: "Normal" (which is selected) and "None". Below the radio buttons are two buttons: "Apply" and "Cancel".

Figure 154. GVRP Port Configuration Page

6. Click **Normal** to have the port propagate GVRP information, or **None** to prevent processing GVRP information and transmitting PDUs.
7. Click **Apply** to save the change, or **Cancel** to cancel.

Displaying the GVRP Configuration

To display the GVRP configuration, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 126 on page 286.

3. Select the **GVRP** tab.

The GVRP tab is shown in Figure 155.

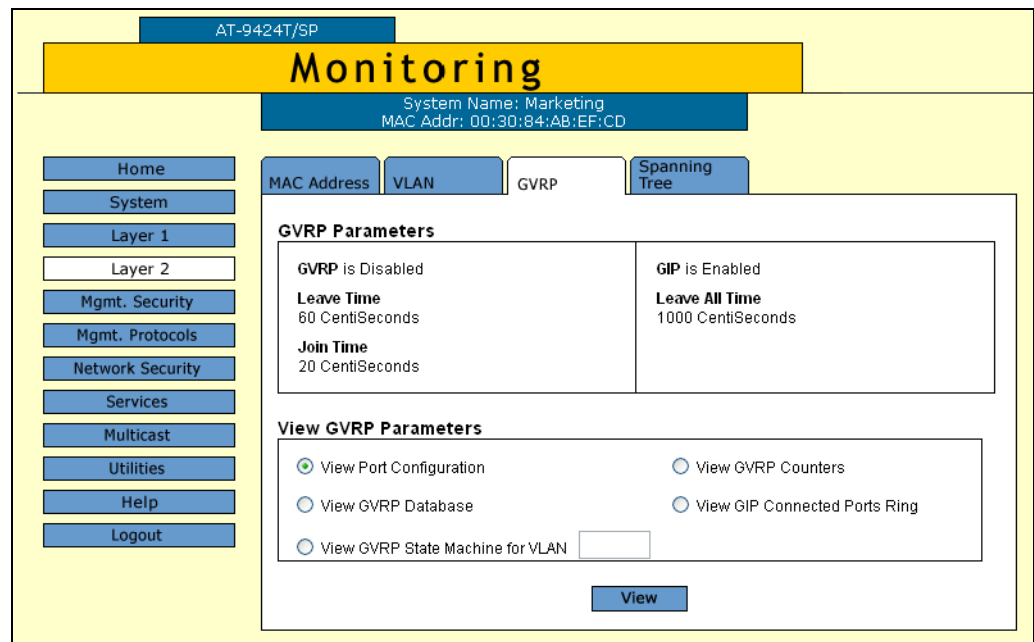


Figure 155. GVRP Tab (Monitoring)

The GVRP Parameters section provides the following information:

GVRP

The GVRP status, Enabled or Disabled.

Leave Time

The range is 30 to 80 centiseconds and the default is 60 centiseconds.

Join Time

The range is 10 to 60 centiseconds and the default is 20 centiseconds.

GIP

The GIP status, Enabled or Disabled.

Leave All Time

The range is 500 to 300 centiseconds and the default is 1000 centiseconds.

Displaying the GVRP Port Configuration

To display the GVRP port configuration, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 126 on page 286.

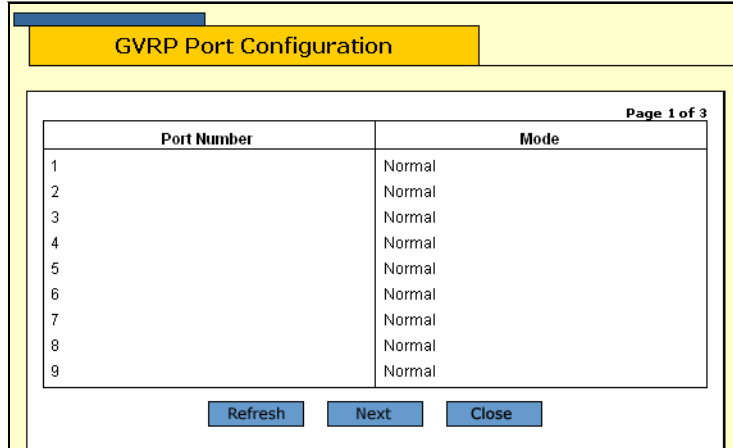
3. Select the **GVRP** tab.

The GVRP tab is shown in Figure 155 on page 359.

4. In the View GVRP Parameters section, click **View Port Configuration**.

5. Click **View**.

The GVRP Port Configuration page is shown in Figure 156.



GVRP Port Configuration	
Port Number	Mode
1	Normal
2	Normal
3	Normal
4	Normal
5	Normal
6	Normal
7	Normal
8	Normal
9	Normal

Page 1 of 3

Refresh Next Close

Figure 156. GVRP Port Configuration Page

The GVRP Port Configuration page provides the following information:

Port Number

The port number.

Mode

The port mode, either Normal or None.

Displaying the GVRP Database

To display the GVRP database, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 126 on page 286.

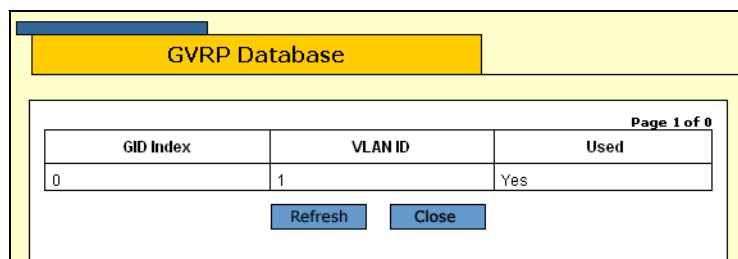
3. Select the **GVRP** tab.

The GVRP tab is shown in Figure 155 on page 359.

4. In the View GVRP Parameters section, click **View GVRP Database**.

5. Click **View**.

The GVRP Database page is shown in Figure 157.



GVRP Database		
GID Index	VLAN ID	Used
0	1	Yes

Page 1 of 0

Refresh Close

Figure 157. GVRP Database Page

The GVRP Database page provides the following information:

GID Index

The value of the GID index corresponding to the attribute.

VLAN ID

The value of the attribute.

Used

Whether the GID index is currently being used by any port in the GARP application.

Displaying the GVRP State Machine

To display the GVRP state machine, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 126 on page 286.

3. Select the **GVRP** tab.

The GVRP tab is shown in Figure 155 on page 359.

4. In the View GVRP Parameters section, click **View GVRP State Machine for VLAN** and enter the VLAN number in the box.

5. Click **View**.

The GVRP State Machine for VLAN page is shown in Figure 158.

Port	App.	Reg.	Port	App.	Reg.	Port	App.	Reg.	Port	App.	Reg.
1	Aa	Fix	2	Aa	Fix	3	Aa	Fix	4	Aa	Fix
5	Aa	Fix	6	Aa	Fix	7	Aa	Fix	8	Aa	Fix
9	Aa	Fix	10	Aa	Fix	11	Aa	Fix	12	Aa	Fix
13	Aa	Fix	14	Aa	Fix	15	Aa	Fix	16	Aa	Fix
17	Aa	Fix	18	Aa	Fix	19	Aa	Fix	20	Aa	Fix
21	Aa	Fix	22	Aa	Fix	23	Aa	Fix	24	Aa	Fix

Figure 158. GVRP State Machine for VLAN Page

The GVRP State Machine for VLAN page provides the information shown in Table 8.

Table 8. GVRP State Machine Parameters

Parameter	Meaning
Port	Port number on the switch; this port belongs to the GARP application. If the GARP application has no ports, "No ports have been assigned" is displayed.

Table 8. GVRP State Machine Parameters (Continued)

Parameter	Meaning	
App	Applicant state machine for the GID index on that particular port. One of:	
	<i>Normal Participant Management state:</i>	
	"Vo"	Very Anxious Observer
	"Ao"	Anxious Observer
	"Qo"	Quiet Observer
	"Lo"	Leaving Observer
	"Vp"	Very Anxious Passive Member
	"Ap"	Anxious Passive Member
	"Qp"	Quiet Passive Member
	"Va"	Very Anxious Active Member
	"Aa"	Anxious Active Member
	"Qa"	Quiet Active Member
	"La"	Leaving Active Member
App (Continued)	<i>Non-Participant Management state:</i>	
	"Von"	Very Anxious Observer
	"Aon"	Anxious Observer
	"Qon"	Quiet Observer
	"Lon"	Leaving Observer
	"Vpn"	Very Anxious Passive Member
	"Apn"	Anxious Passive Member
	"Qpn"	Quiet Passive Member
	"Van"	Very Anxious Active Member
	"Aan"	Anxious Active Member
	"Qan"	Quiet Active Member
	"Lan"	Leaving Active Member
	The initialized state for the Applicant is Vo.	

Table 8. GVRP State Machine Parameters (Continued)

Parameter	Meaning	
Reg	Registrar state machine for the GID index on that particular port. One of:	
	"Mt"	Empty
	"Lv3"	Leaving substate 3 (final Leaving substate)
	"Lv2"	Leaving substate 2
	"Lv1"	Leaving substate 1
	"Lv"	Leaving substate (initial Leaving substate)
	"In"	In
	"Fix"	Registration Fixed
	"For"	Registration Forbidden
	The initialized state for the Registrar is Mt.	

Displaying the GVRP Counters

To display the GVRP counters, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 126 on page 286.

3. Select the **GVRP** tab.

The GVRP tab is shown in Figure 155 on page 359.

4. In the View GVRP Parameters section, click **View GVRP Counters**.

5. Click **View**.

The GVRP Counters page is shown in Figure 159.

GVRP Counters			
Receive		Transmit	
Total GARP Packets	0	Total GARP Packets	0
Invalid GARP Packets	0		
Discarded			
GARP Disabled	0	GARP Disabled	24
Port Not Listening	0	Port Not Sending	0
Invalid Port	0		
Invalid Protocol	0		
Invalid Format	0		
Database Full	0		
GARP Messages			
LeaveAll	0	LeaveAll	0
JoinEmpty	0	JoinEmpty	0
JoinIn	0	JoinIn	0
LeaveEmpty	0	LeaveEmpty	0
LeaveIn	0	LeaveIn	0
Empty	0	Empty	0
Bad Message	0		
Bad Attribute	0		

Figure 159. GVRP Counters Page

The GVRP Counters page provides the information shown in Table 9.

Table 9. GVRP Counters

Parameter	Meaning
Receive: Total GARP Packets	Total number of GARP PDUs received by this GARP application.
Transmit: Total GARP Packets	Total number of GARP PDUs transmitted by this GARP application.
Receive: Invalid GARP Packets	Number of invalid GARP PDUs received by this GARP application.
Receive Discarded: GARP Disabled	Number of received GARP PDUs discarded because the GARP application was disabled.
Transmit Discarded: GARP Disabled	Number of GARP PDUs discarded because the GARP application was disabled. This counter is incremented when ports are added to or deleted from the GARP application arising from port movements in the underlying VLAN or STP.
Receive Discarded: Port Not Listening	Number of GARP PDUs discarded because the port that received the PDUs was not listening, that is, MODE=NONE was set on the port.
Transmit Discarded: Port Not Sending	Number of GARP PDUs discarded because the port that the PDUs were to be transmitted on was not sending, that is, MODE=NONE was set on the port.
Receive Discarded: Invalid Port	Number of GARP PDUs discarded because the port that received the PDU does not belong to the GARP application.
Receive Discarded: Invalid Protocol	Number of GARP PDUs discarded because the GARP PDU contained an invalid protocol.
Receive Discarded: Invalid Format	Number of GARP PDUs discarded because the format of the GARP PDU was not recognized.
Receive Discarded: Database Full	Number of GARP PDUs discarded because the database for the GARP application was full, that is, the maximum number of attributes for the GARP application is in use.
Receive GARP Messages: LeaveAll	Number of GARP LeaveAll messages received by the GARP application.
Transmit: GARP Messages: LeaveAll	Number of GARP LeaveAll messages transmitted by the GARP application.

Table 9. GVRP Counters (Continued)

Parameter	Meaning
Receive GARP Messages: JoinEmpty	Total number of GARP JoinEmpty messages received for all attributes in the GARP application.
Transmit GARP Messages: JoinEmpty	Total number of GARP JoinEmpty messages transmitted for all attributes in the GARP application.
Receive GARP Messages: JoinIn	Total number of GARP JoinIn messages received for all attributes in the GARP application.
Transmit GARP Messages: JoinIn	Total number of GARP JoinIn messages transmitted for all attributes in the GARP application.
Receive GARP Messages: LeaveEmpty	Total number of GARP LeaveEmpty messages received for all attributes in the GARP application.
Transmit GARP Messages: LeaveEmpty	Total number of GARP LeaveEmpty messages transmitted for all attributes in the GARP application.
Receive GARP Messages: LeaveIn	Total number of GARP LeaveIn messages received for all attributes in the GARP application.
Transmit GARP Messages: LeaveIn	Total number of GARP LeaveIn messages transmitted for all attributes in the GARP application.
Receive GARP Messages: Empty	Total number of GARP Empty messages received for all attributes in the GARP application.
Transmit GARP Messages: Empty	Total number of GARP Empty messages transmitted for all attributes in the GARP application.
Receive GARP Messages: Bad Message	Number of GARP messages that had an invalid Attribute Type value, an invalid Attribute Length value or an invalid Attribute Event value.
Receive GARP Messages: Bad Attribute	Number of GARP messages that had an invalid Attribute Value value.

Displaying the GIP Connected Ports Ring

To display the GIP connected ports ring, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 126 on page 286.

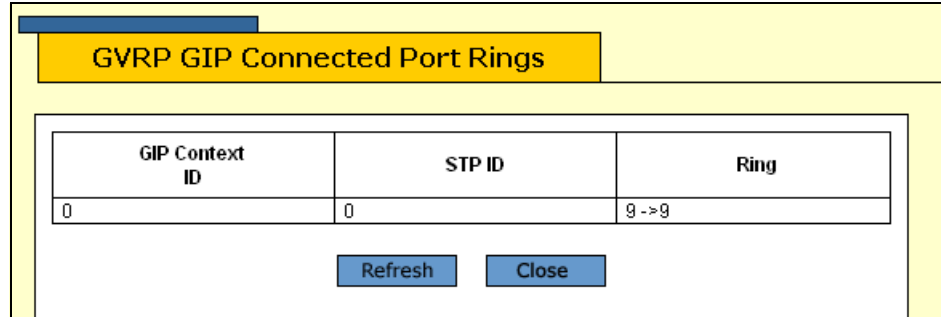
3. Select the **GVRP** tab.

The GVRP tab is shown in Figure 155 on page 359.

4. In the View GVRP Parameters section, click **View GIP Connected Ports Ring**.

5. Click **View**.

The GIP Connected Ports Ring page is shown in Figure 160.



GIP Context ID	STP ID	Ring
0	0	g->g

Refresh Close

Figure 160. GIP Connected Ports Ring Page

The GIP Connected Ports Ring page displays a table that contains the following columns of information:

GIP Context ID

A number assigned to the instance for the GIP context.

STP ID

Present if the GARP application is GVRP; identifies the spanning tree instance associated with the GIP context.

Ring

The ring of connected ports. Only ports presently in the spanning tree Forwarding state are eligible for membership in the GIP connected

ring. If no ports exist in the GIP connected ring, “No ports are connected” is displayed. If the GARP application has no ports, “No ports have been assigned” is displayed.

Section VI

Port Security

The chapters in this section provide information and procedures for basic switch setup using the AT-S63 management software. The chapters include:

- ❑ Chapter 23, “Port Security” on page 373
- ❑ Chapter 24, “802.1x Port-based Network Access Control” on page 379
- ❑ Chapter 25, “MAC Address Table” on page 397

Chapter 23

Port Security

This chapter explains how to display the MAC address security levels on the ports on the switch. It contains the following sections:

- “Configuring Port Security” on page 374
- “Displaying the Port Security Level” on page 376

Note

For background information on port security, refer to Chapter 27, “Port Security,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Configuring Port Security

To configure security for the ports, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Network Security** option.

The Network Security page opens with the Port Security tab selected by default, as shown in Figure 161.

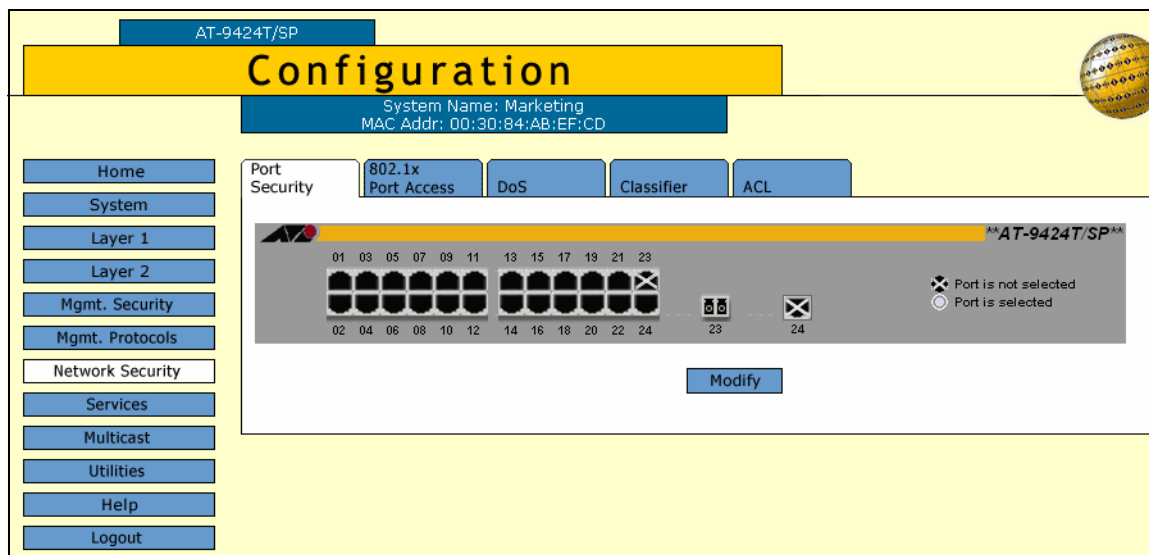


Figure 161. Port Security Tab (Configuration)

3. In the graphical image of the switch, click the ports you want to configure and click **Modify**.

The Security for Ports page is shown in Figure 164.

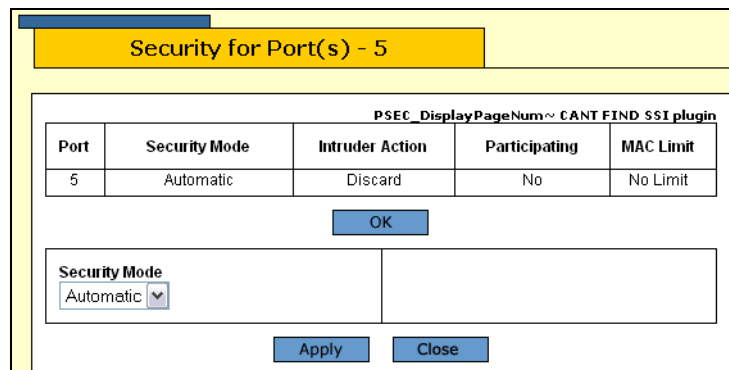


Figure 162. Security for Ports Page (Configuration)

4. Configure the following parameter as desired:

Security Mode

The options are:

Automatic - Port security is automatically disabled. This is the default.

Limited - Specifies a number of MAC addresses the port can learn.

Secured - The port forwards frames using only static MAC addresses.

Locked - The port immediately stops learning new dynamic MAC addresses.

5. Click **Apply**.
6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying the Port Security Level

To display the MAC address security level of a port, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select **Network Security**.

The Network Security page is displayed with the Port Security tab selected by default, as shown in Figure 163.

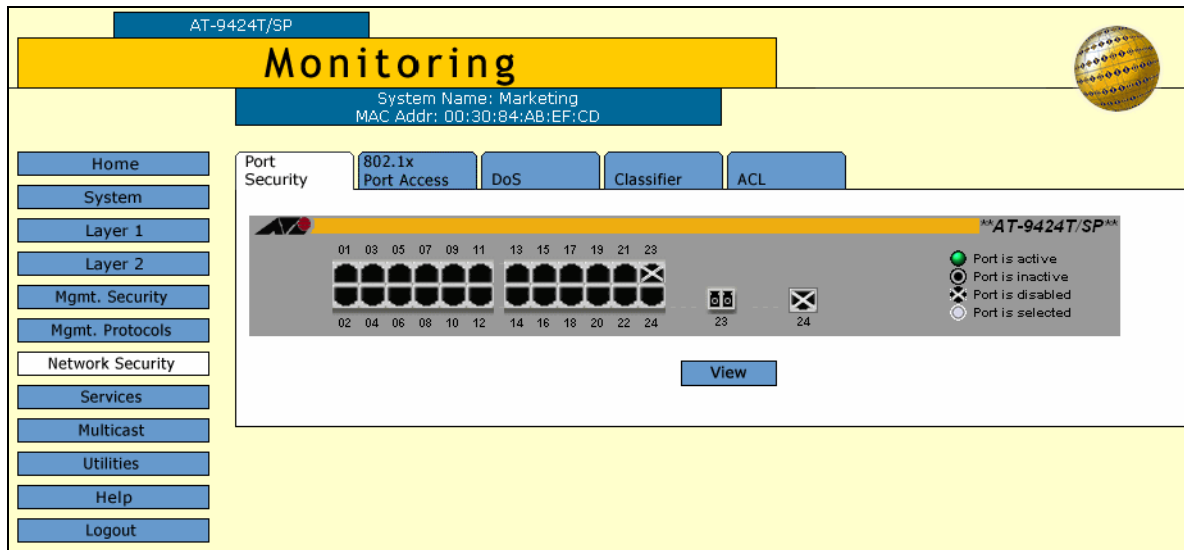


Figure 163. Port Security Tab (Monitoring)

3. Click the port whose port security level you want to view. A selected port turns white. You can select more than one port at a time.
4. Click **View**.

The Security for Port(s) page is shown in Figure 164.

Total Ports Selected: 3. Page 1 of 1				
Port	Security Mode	Intruder Action	Participating	MAC Limit
2	Limited	Send Trap Only	Yes	10
3	Limited	Send Trap Only	Yes	10
4	Limited	Send Trap Only	Yes	10

OK

Figure 164. Security for Port(s) Page

The Security for Ports page displays a table that contains the following columns of information:

Port

The number of the port.

Security Mode

The active security mode on the port. The possible settings are Automatic, Limited, Secured, and Locked.

Intruder Action

The column specifies the action taken by the switch if a port receives an invalid packet. The possible settings are:

No Action (Discard) - The port discards invalid packets. This is the default.

Trap - The port discards invalid packets and sends a trap.

Trap/Disable - The port discards invalid packets, sends a trap, and disables the port.

Participating

This column applies only when the intrusion action for a port is set to trap or disable. This option does not apply when intrusion action is set to No Action (discard). If this option is set to No when intrusion action is set to trap or disable, the port discards invalid packets, but it does not send a trap or disable the port.

MAC Limit

This column specifies the maximum number of dynamic MAC addresses the port learns. It only applies when a port is operating in the Limited security mode.

Chapter 24

802.1x Port-based Network Access Control

This chapter contains instructions on how to configure the 802.1x Port-based Network Access Control feature on the switch. The chapter contains the following sections:

- ❑ “Setting Port Roles” on page 380
- ❑ “Enabling or Disabling 802.1x Port-based Network Access Control” on page 382
- ❑ “Configuring Authenticator Port Parameters” on page 383
- ❑ “Configuring Supplicant Port Parameters” on page 386
- ❑ “Displaying the Port-based Network Access Control Parameters” on page 388
- ❑ “RADIUS Accounting” on page 393

Note

For background information on port-based network access control, refer to Chapter 28, “802.1x Port-based Network Access Control,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Setting Port Roles

To set port roles for port-based network access control, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Network Security** option.

The Network Security page opens with the Port Security tab selected by default, as shown in Figure 161 on page 374.

3. Select the **802.1x Port Access** tab.

The 802.1x Port Access tab is shown in Figure 165.

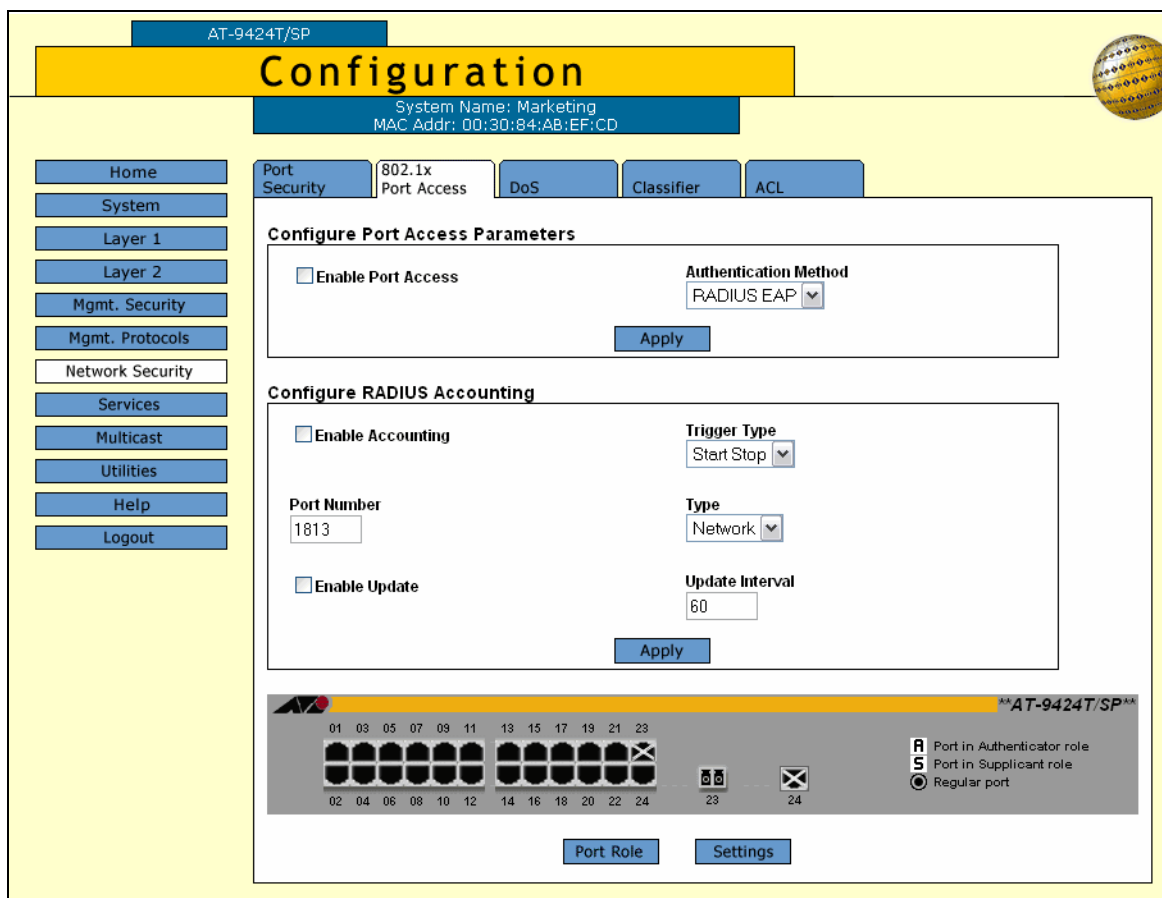


Figure 165. 802.1x Port Access Tab (Configuration)

The graphical image of the switch shows which ports have already been assigned port roles. An “A” indicates that a port is functioning as

an authenticator while an “S” indicates the port is functioning as a supplicant. A black port has not been assigned a port role and is not participating in port-based access control. This is the default setting for a port.

4. To set a port's role, click on the port. The selected port turns white. You can select more than one port at a time.
5. Click **Port Role**.

The Port Role Configuration page is shown in Figure 166.

Figure 166. Port Role Configuration Page

6. Select the desired role for the port. The possible settings are:

None

The port is not to participate in port-based access control. This is the default setting.

Authenticator

The port is to function as an authenticator. This is the appropriate setting if the port is connected to a supplicant.

Supplicant

The port is to function as a supplicant. This is the appropriate setting if the port is connected to an authenticator. A port can have only one port role at a time.

7. Click **Apply**.

To enable or disable port-based access control, go to “Enabling or Disabling 802.1x Port-based Network Access Control” on page 382. Then, to configure authenticator port settings, go to “Configuring Authenticator Port Parameters” on page 383. To configure supplicant port settings, go to “Configuring Supplicant Port Parameters” on page 386.

Enabling or Disabling 802.1x Port-based Network Access Control

To enable or disable 802.1x Port-based Network Access Control, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Network Security** option.

The Network Security page opens with the Port Security tab selected by default, as shown in Figure 161 on page 374.

3. Select the **802.1x Port Access** tab.

The 802.1x Port Access tab is shown in Figure 165 on page 380.

4. Click the **Enable Port Access** check box. A check in the box means that the feature is activated on the switch. No check means that the feature is disabled.

5. Click **Apply**.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Configuring Authenticator Port Parameters

To configure authenticator port parameters, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Network Security** option.

The Network Security page opens with the Port Security tab selected by default, as shown in Figure 161 on page 374.

3. Select the **802.1x Port Access** tab.

The 802.1x Port Access tab is shown in Figure 165 on page 380.

4. Click the authenticator port that you want to configure. You can select more than one authenticator port at a time. The selected port turns white.

Note

A port must already be configured as an authenticator before you can configure its settings. For instructions on how to set the role of a port, refer to “Setting Port Roles” on page 380.

5. Click **Settings**.

The Authenticator Parameters page is shown in Figure 167.

Authenticator Parameters - 1	
Port Control Auto	Piggyback Mode Disabled
Tx Period 30	Quiet Period 60
Reauth Enabled Enabled	Control Direction Both
Reauth Period 3600	Max Requests 2
Supplicant Timeout 30	Server Timeout 30
<input type="button" value="Apply"/> <input type="button" value="Close"/>	

Figure 167. Authenticator Parameters Page

6. Configure the following parameters as necessary:

Port Control

The possible settings are:

Force-authorized - Disables IEEE 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. This is the default setting

Force-unauthorized - Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface

Auto - Enables 802.1x port-based authentication and causes the port to begin 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 or the port receives an EAPOL-Start packet from a supplicant. 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 using the client's MAC address.

TX Period

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.

Reauth Enabled

Specifies if reauthentication should occur according to the reauthentication period. The options are Enabled or Disabled.

Reauth Period

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.

Supplicant Timeout

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.

Piggyback Mode

Opens up the port after authentication to all other unauthenticated devices and closes the port when reauthentication takes place. The options are Enabled or Disabled.

Quiet Period

Sets the number of seconds that the port 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.

Control Direction

Specifies how the port handles 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 the client logs on by providing a username and password combination. In the unauthorized state, the port only accepts EAP packets from the client. All other ingress packets that the port might receive from the client, including multicast and broadcast traffic, is discarded until the supplicant has logged in. The options are:

Ingress - A port, when in the unauthorized state, discards all ingress broadcast and multicast packets from the client, but forwards all egress broadcast and multicast traffic to the same client.

Both - A port, when in the unauthorized state, does not forward ingress or egress broadcast and multicast packets from or to the same client until the client logs in. This is the default.

Max Requests

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 default value for this parameter is 2 retransmissions. The range is 1 to 10 retransmissions.

Server Timeout

Sets the timer used by the switch to determine authentication server timeout conditions. The default value for this parameter is 10 seconds. The range is 1 to 60 seconds.

7. Click **Apply**.
8. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Configuring Supplicant Port Parameters

To configure supplicant port parameters, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Network Security** option.

The Network Security page opens with the Port Security tab selected by default, as shown in Figure 161 on page 374.

3. Select the **802.1x Port Access** tab.

The 802.1x Port Access tab is shown in Figure 165 on page 380.

4. Click the supplicant port that you want to configure. You can select more than one supplicant port at a time. The selected port turns white.

Note

A port must already be designated as a supplicant before you can configure its settings. For instructions on how to set the role of a port, refer to “Setting Port Roles” on page 380.

5. Click **Settings**.

The Supplicant Parameters page is shown in Figure 167.

Supplicant Parameters - 20	
Auth Period <input type="text" value="30"/>	Held Period <input type="text" value="60"/>
Max Start <input type="text" value="3"/>	Start Period <input type="text" value="30"/>
User Name <input type="text"/>	User Password <input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Close"/>	

Figure 168. Supplicant Parameters Page

6. Configure the following parameters as needed:

Auth Period

Specifies the period of time in seconds that the supplicant waits for a reply from the authenticator after sending an EAP-Response frame. The range is 1 to 60 seconds. The default is 30 seconds.

Held Period

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 seconds. The default value is 60 seconds.

Max Start

Specifies the maximum number of times the supplicant sends EAPOL-Start frames before assuming that there is no authenticator present. The range is 1 to 10. The default is 3.

Start Period

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.

User Name

Specifies the username for the switch port. 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.

User 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.

7. Click **Apply**.
8. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying the Port-based Network Access Control Parameters

You can display information about the port-based network access control status and settings of the ports on the switch. This section contains the following procedures:

- ❑ "Displaying the Port Status" (next)
- ❑ "Displaying the Port Settings" on page 389

Displaying the Port Status

To display the port-based network access control port status, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select **Network Security**.

The Network Security page is displayed with the Port Security tab selected by default, as shown in Figure 163 on page 376.

3. Select the **802.1x Port Access** tab.

The 802.1x Port Access tab is shown in Figure 169.

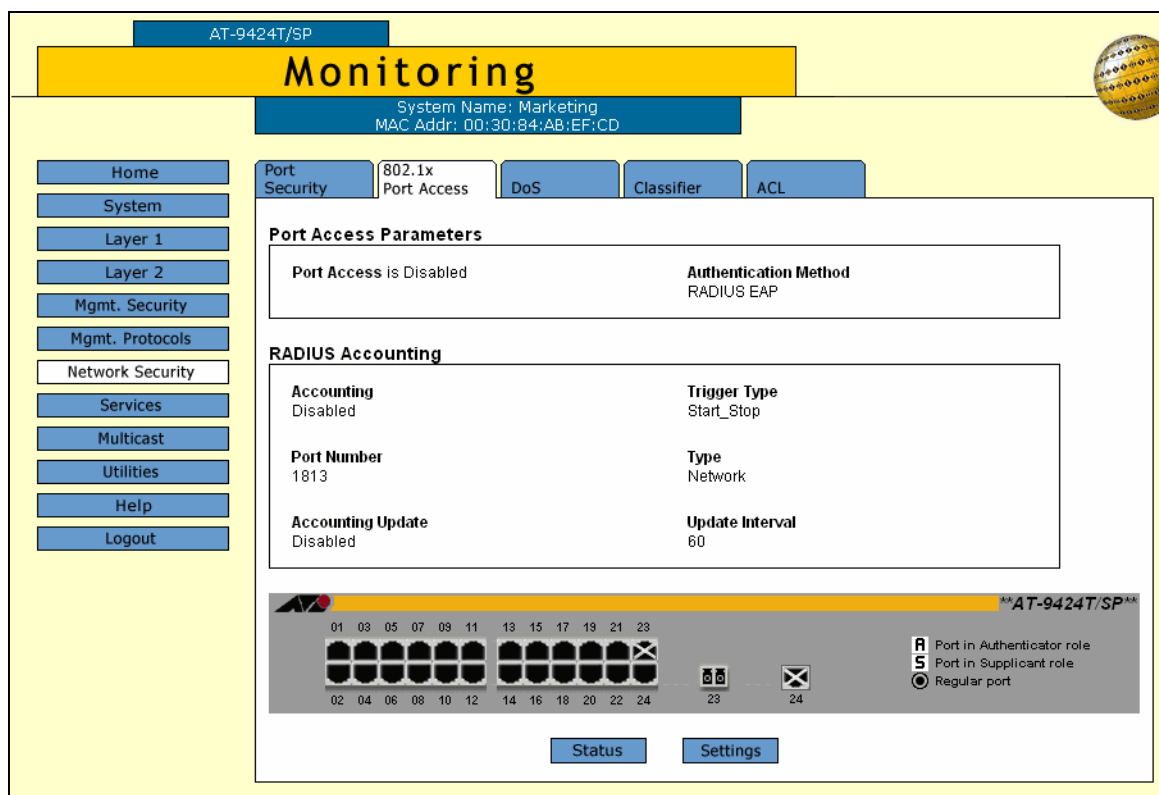


Figure 169. 802.1x Port Access Tab (Monitoring)

- To see the status of the port, click the port and click **Status**. You can select more than one port at a time.

The Port Access Port Status page is shown in Figure 170.

Port Access Port Status - 8			
Total Ports = 1. Page 1 of 1			
Port	Port Role	Status	Additional Info.
8	Authenticator	-----	-----

OK

Figure 170. Port Access Port Status Page

The Port Access Port Status page displays a table that contains the following columns of information:

Port

The port number.

Port Role

The port role: None, Authenticator, or Supplicant.

Status

The options include: Initialize, Disconnected, and so forth.

Additional Info.

More information about the port including the MAC address.

Displaying the Port Settings

To display the port-based network access control port settings, perform the following procedure:

- From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

- From the Monitoring menu, select **Network Security**.

The Network Security page is displayed with the Port Security tab selected by default, as shown in Figure 58 on page 160.

- Select the **802.1x Port Access** tab.

The 802.1x Port Access tab is shown in Figure 169 on page 389.

4. To review the port access settings, click OK to close the Port Access Port Status page and return to the 802.1x Port Access tab
5. To see the port settings, click the port and click **Settings**. You can select more than one port at a time.

Note

To view the settings of multiple ports, you must select ports that have the same port role (authenticator or supplicant).

For authenticator port(s), the Authenticator Port Parameters page is displayed, as shown in Figure 171.

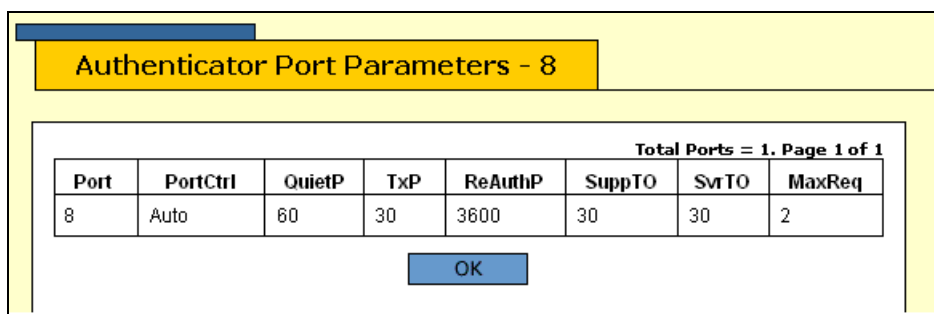


Figure 171. Authenticator Port Parameters Page

The Authenticator Port Parameters page displays a table that contains the following columns of information:

Port

The port number.

PortCtrl

The port control setting. The possible settings are:

Force-authorized - 802.1x port-based authentication is disabled.

Force-unauthorized - The port is in an unauthorized state, ignoring attempts by the client to authenticate.

Auto - 802.1x port-based authentication is enabled.

QuietP

The number of seconds the port remains in a quiet state following a failed authentication exchange with the client.

TxP

The number of seconds that the switch waits for a response to an EAP Request packet/identity packet from the client before retransmitting the request.

ReAuthP

The frequency of the periodic reauthentication of the client.

SuppTO

The switch-to-client retransmission time for the EAP Request packet.

MaxReq

The maximum number of times that the switch retransmits an EAP Request packet to the client before it times out the authentication session.

For supplicant port(s), the Supplicant Port Parameters Page is displayed, as shown in Figure 172.

Supplicant Port Parameters - 11

Total Ports = 1. Page 1 of 1

Port	AuthPeriod	HeldPeriod	MaxStart	StartPeriod	User Name	User Password
11	30	60	3	30		

Figure 172. Supplicant Port Parameters Page

The Supplicant Port Parameters page displays a table that contains the following columns of information:

Port

The port number.

AuthPeriod

The period of time in seconds that the supplicant waits for a reply from the authenticator.

HeldPeriod

The amount of time the supplicant is to refrain from trying to recontact the authenticator in the event that the end user provides an invalid user name and/or password.

MaxStart

The maximum number of times the supplicant sends EAPoL-Start packets before assuming that there is no authenticator present.

StartPeriod

The time period between successive attempts by the supplicant to establish contact with an authenticator when there is no reply.

User Name

The user name for the port.

User Password

The password for the port.

RADIUS Accounting

The AT-S63 management software supports RADIUS accounting for 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. For background information on this feature, refer to Chapter 28, "802.1x Port-based Network Access Control" in the *AT-S63 Management Software Menus Interface User's Guide*. This feature is disabled by default on the switch.

Configuring RADIUS Accounting

To configure RADIUS accounting, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Network Security** option.

The Network Security page opens with the Port Security tab selected by default, as shown in Figure 161 on page 374.

3. Select the **802.1x Port Access** tab.

The 802.1x Port Access tab is shown in Figure 165 on page 380

4. In the Configure RADIUS Accounting section, configure the following parameters as necessary.

Enable Accounting

This parameter activates or deactivates RADIUS accounting on the switch. Select Enabled to activate the feature or Disabled to deactivate it. The default is Disabled.

Trigger Type

This parameter specifies the action that causes the switch to send accounting information to the RADIUS server. The possible settings are:

Start_Stop - The switch sends accounting information whenever a client logs on or logs off the network. This is the default.

Stop - The switch sends accounting information only when a client logs off.

Port Number

Specifies the UDP port for RADIUS accounting. The default is port 1813.

Type

This parameter specifies the type of RADIUS accounting. The default is Network. You cannot change this value.

Enable Update

This parameter controls whether the switch is to send interim accounting updates to the RADIUS server. A check in the box indicates that updating is enabled. No check in the box means that updating is disabled.

Update Interval

Specifies the intervals at which the switch sends interim accounting updates to the RADIUS server. The range is 30 to 300 seconds. The default is 60 seconds.

5. Click **Apply**.
6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying the RADIUS Accounting Settings

To display the RADIUS accounting settings, perform the following procedure:

1. From the home page, select **Monitoring**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Monitoring menu, select the **Network Security** option.

The Network Security page is displayed with the Port Security tab selected by default, as shown in Figure 163 on page 376.

3. Select the **802.1x Port Access** tab.

The 802.1x Port Access tab is shown in Figure 173.

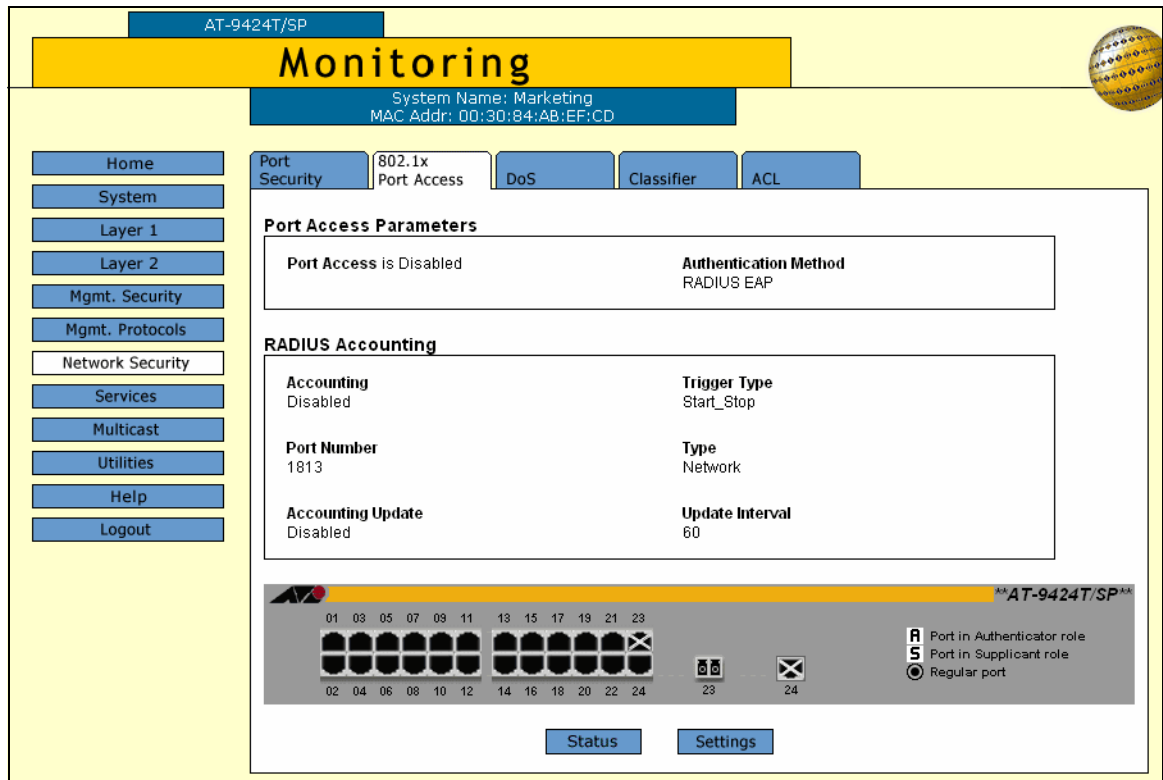


Figure 173. 802.1x Port Access Tab (Monitoring)

The RADIUS Accounting section provides the following information:

Accounting

The status of RADIUS accounting, either Enabled or Disabled.

Trigger Type

The action that causes the switch to send accounting information to the RADIUS server. The possible settings are:

Start_Stop - The switch sends accounting information whenever a client logs on or logs off the network. This is the default.

Stop - The switch sends accounting information only when a client logs off.

Port Number

The UDP port for RADIUS accounting.

Type

The type of RADIUS accounting. The default is Network.

Accounting Update

Whether or not the switch sends interim accounting updates to the RADIUS server. The options are Enabled or Disabled.

Update Interval

The intervals, in seconds, at which the switch sends interim accounting updates to the RADIUS server.

The graphical image of the switch and the Status and Settings buttons refer to the 802.1x Port-based Network Access Control settings, described in “Displaying the Port-based Network Access Control Parameters” on page 388.

Chapter 25

MAC Address Table

This chapter contains instructions on how to add and view the dynamic and static addresses in the MAC address table of the switch. This chapter contains the following procedure:

- ❑ “Adding Static Unicast and Multicast MAC Addresses” on page 398
- ❑ “Deleting Unicast and Multicast MAC Addresses” on page 400
- ❑ “Deleting All Dynamic MAC Addresses” on page 401
- ❑ “Displaying the MAC Address Tables” on page 402
- ❑ “Changing the Aging Time” on page 405

Note

For background information on MAC address tables, refer to Chapter 29, “MAC Address Table,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Adding Static Unicast and Multicast MAC Addresses

This section contains the procedure for assigning a static unicast or multicast address to a port on the switch. You can assign up to 255 static MAC addresses per port.

To add a static address to the MAC address table, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab selected by default, as shown in Figure 174.

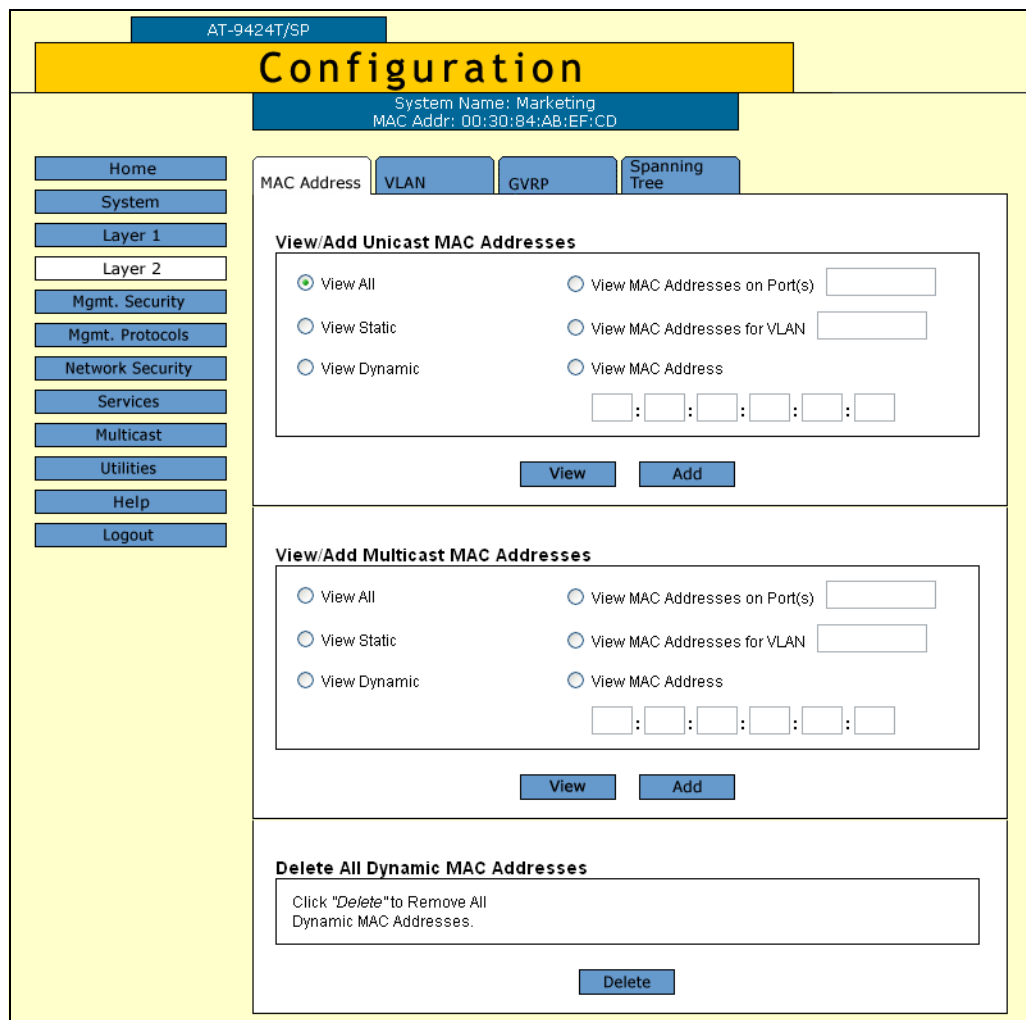


Figure 174. MAC Address Tab (Configuration)

- To add a static unicast address, in the View/Add Unicast MAC Addresses section, click **Add**. To add a static multicast address, in the View/Add Multicast MAC Addresses section, click **Add**.

The Add MAC Address page is shown in Figure 175.

Figure 175. Add MAC Address Page

- Configure the following parameters as necessary.

MAC Address

The new static unicast or multicast MAC address.

Port Number

The number of the port on the switch where you want to assign the static address. If you are adding a static unicast address, you can enter only one port.

If you are entering a static multicast address, you must specify the port when the multicast application is located as well as the ports where the host nodes are connected. Assigning the address only to the port where the multicast application is located results in the failure of the multicast packets to be properly forwarded to the host nodes. You can specify the ports individually (e.g., 1,4,5), as a range (e.g., 11-14) or both (e.g., 15-17,22,24).

VLAN ID

The VLAN ID where the port is a member.

- Click **Apply**.
- Repeat this procedure to add other static addresses to the switch.
- From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting Unicast and Multicast MAC Addresses

To delete a static or dynamic unicast or multicast MAC address from the switch, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page opens with the MAC Address tab selected by default, as shown in Figure 174 on page 398.

3. Display the MAC addresses on the switch by selecting one of the options.

For detailed instructions, refer to “Displaying the MAC Address Tables” on page 402.

4. Click the button next to the MAC address that you want to delete from the switch.

5. Click **Remove**.

Note

You cannot delete a switch’s MAC address, an STP BPDU MAC address, or a broadcast address.

6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Deleting All Dynamic MAC Addresses

To delete all the dynamic MAC addresses, unicast or multicast, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Layer 2** option.

The Layer 2 page opens with the MAC Address tab selected by default, as shown in Figure 174 on page 398.

3. In the Delete All Dynamic MAC Addresses section, click **Delete**.

4. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying the MAC Address Tables

To view the MAC address table, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Layer 2** option.

The Layer 2 page is displayed with the MAC Address tab displayed by default, as shown in Figure 176.

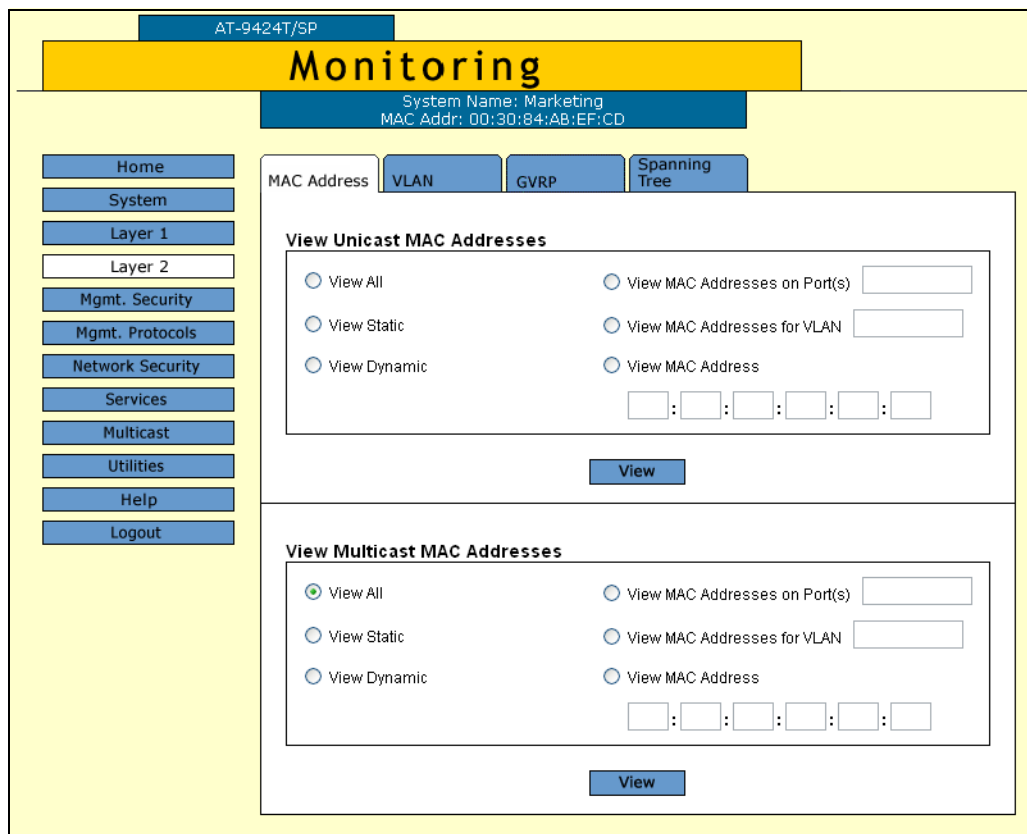


Figure 176. MAC Address Tab (Monitoring)

The tab contains two sections. The View Unicast MAC Addresses section displays unicast addresses. The View Multicast MAC Addresses section displays multicast addresses. The options function the same in both sections, and are described below. You can select only one option at a time.

View All

Displays all dynamic addresses learned on the ports of the switch and all static addresses that have been assigned to the ports.

View Static

Displays just the static addresses assigned to the ports on the switch.

View Dynamic

Displays only the dynamic addresses learned on the ports on the switch.

View MAC Addresses on Port

Displays the dynamic and static MAC addresses of a particular port. You can specify more than one port at a time.

View MAC Addresses for VLAN

Displays the static and dynamic addresses learned on the tagged and untagged ports of a specific VLAN. You specify the VLAN by entering the VLAN ID number. You can specify only one VLAN at a time.

View MAC Address

Displays the port number on which a MAC address was assigned or learned.

In some situations, you might want to know on which port a particular MAC address was learned. You could display the MAC address table and scroll through the list looking for the MAC address. But if the switch is part of a large network, finding the address could prove difficult.

The View MAC Address option allows you to specify the MAC address and let the AT-S63 management software automatically locate the port on the switch where the device is connected.

3. After you select an option, click **View**.

Figure 177 shows an example of viewing all unicast MAC addresses.

Total MAC Addresses: 117. Page 1 of 12

VLAN ID	MAC ADDRESS	PORT(s)	TYPE
1	00:00:CD:01:6B:5D	5	Dynamic
1	00:00:CD:0D:40:CC	5	Dynamic
1	00:00:F4:A4:12:44	5	Dynamic
1	00:00:F4:DD:29:31	5	Dynamic
1	00:02:2D:7B:AA:EA	5	Dynamic
1	00:02:2D:7C:AF:F9	5	Dynamic
1	00:02:55:B1:1E:98	5	Dynamic
1	00:02:DD:32:3D:1C	5	Dynamic
1	00:04:23:56:70:6B	5	Dynamic
1	00:04:23:80:B3:0E	5	Dynamic

Figure 177. View MAC Addresses Page

The View MAC Addresses page displays a table that contains the following columns of information:

VLAN ID

The ID number of the VLAN where the port is a member.

MAC Address

The static or dynamic unicast MAC address.

Port(s)

The port on which the address was learned or assigned. The MAC address with port “CPU” is the address of the switch.

Type

The type of the address: static or dynamic.

Changing the Aging Time

The switch uses the aging time to delete inactive dynamic MAC addresses from the MAC address table. When the switch 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, the switch deletes the address. This prevents the table from becoming full of addresses of nodes that are no longer active.

The default setting for the aging time is 300 seconds (5 minutes).

To configure the aging time, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. In the Configuration section, for the MAC Address Aging Time, enter a new value in seconds. The range is 8 to 512 seconds. The default is 300 seconds (5 minutes).
3. Click **Apply**.
4. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Section VII

Management Security

The chapters in this section provide information and procedures for basic switch setup using the AT-S63 management software. The chapters include:

- ❑ Chapter 26, “Encryption Keys, PKI, and SSL” on page 409
- ❑ Chapter 27, “Secure Shell (SSH)” on page 417
- ❑ Chapter 28, “TACACS+ and RADIUS” on page 423
- ❑ Chapter 29, “Management Access Control Lists” on page 433

Chapter 26

Encryption Keys, PKI, and SSL

This chapter explains how to view the encryption keys, PKI-based certificates, and SSL settings and includes the following sections:

- ❑ “Displaying the Encryption Keys” on page 410
- ❑ “Displaying the PKI Settings and Certificates” on page 412
- ❑ “Displaying the SSL Settings” on page 415

Note

To configure encryption keys, PKI, or SSL, you must use the AT-S63 menus or CLI interface.

For information about encryption keys, refer to Chapter 31, “Encryption Keys,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

For information about PKI and SSL, refer to Chapter 32, “PKI Certificates and SSL” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Displaying the Encryption Keys

To configure the encryption keys, you must use the AT-S63 menus or command line interface. For more information about encryption keys, refer to the *AT-S63 Management Software Menu Interface User's Guide*.

To display the encryption keys, perform the following procedure:

1. From the Home page, select **Monitoring**.

The System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Mgmt. Security** option.

The Mgmt. Security page is displayed with the Mgmt. ACL tab displayed by default, as shown in Figure 178.

AT-9424T/SP

Monitoring

System Name: Marketing
MAC Addr: 00:30:84:AB:EF:CD

Home
System
Layer 1
Layer 2
Mgmt. Security
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Help
Logout

Mgmt ACL | **Keys** | PKI

Mgmt. ACL(s) are **Enabled**

Browse Mgmt. ACL(s)

	IP Address	IP Mask	Protocol	Interface
🔍	149.35.8.31	255.255.255.0	TCP	ALL

Refresh

Figure 178. Mgmt. Security Tab (Monitoring)

3. Select the **Keys** tab.

The Keys tab is shown in Figure 179.

The screenshot shows the AT-S63 Management Software Web Browser Interface. At the top, there is a yellow banner with the word "Monitoring" in large black letters. Below the banner, a blue bar displays "System Name: Marketing" and "MAC Addr: 00:30:84:AB:EF:CD". On the left side, there is a vertical navigation menu with buttons for Home, System, Layer 1, Layer 2, Mgmt. Security, Mgmt. Protocols, Network Security, Services, Multicast, Utilities, Help, and Logout. In the center, there are three tabs: "Mgmt ACL", "Keys" (which is selected), and "PKI". Below the tabs, a table displays key information. The table has five columns: Key ID, Algorithm, Length, Digest, and Description. There is one row of data. Below the table is a "Refresh" button. In the top right corner of the table area, it says "Total Keys: 1. Page 1 of 1".

Key ID	Algorithm	Length	Digest	Description
243	RSA-Private	512	E8DD94FB	Local key

Figure 179. Keys Tab (Monitoring)

The Keys tab displays a table that contains the following columns of information:

ID

The identification number of the key.

Algorithm

The algorithm used in creating the encryption. This is always RSA - Private.

Length

The length of the key in bits.

Digest

The CRC32 value of the MD5 digest of the public key.

Description

The key's description.

You use these keys when you configure Secure Sockets Layer (SSL) or Secure Shell (SSH). To configure SSL you must use the AT-S63 menus or CLI interface. To configure SSH, refer to Chapter 27, "Secure Shell (SSH)" on page 417.

Displaying the PKI Settings and Certificates

You can view the current PKI settings and certificates on the switch. To configure the PKI settings and certificates, you must use the AT-S63 menus or command line interface. For more information about PKI, refer to the *AT-S63 Management Software Menus Interface User's Guide*.

To display the PKI settings and certificates, perform the following procedure:

1. From the Home page, select **Monitoring**.

The System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Mgmt. Security** option.

The Mgmt. Security page is displayed with the Mgmt. ACL tab displayed by default, as shown in Figure 178 on page 410.

3. Select the **PKI** tab.

The PKI tab is shown in Figure 180.

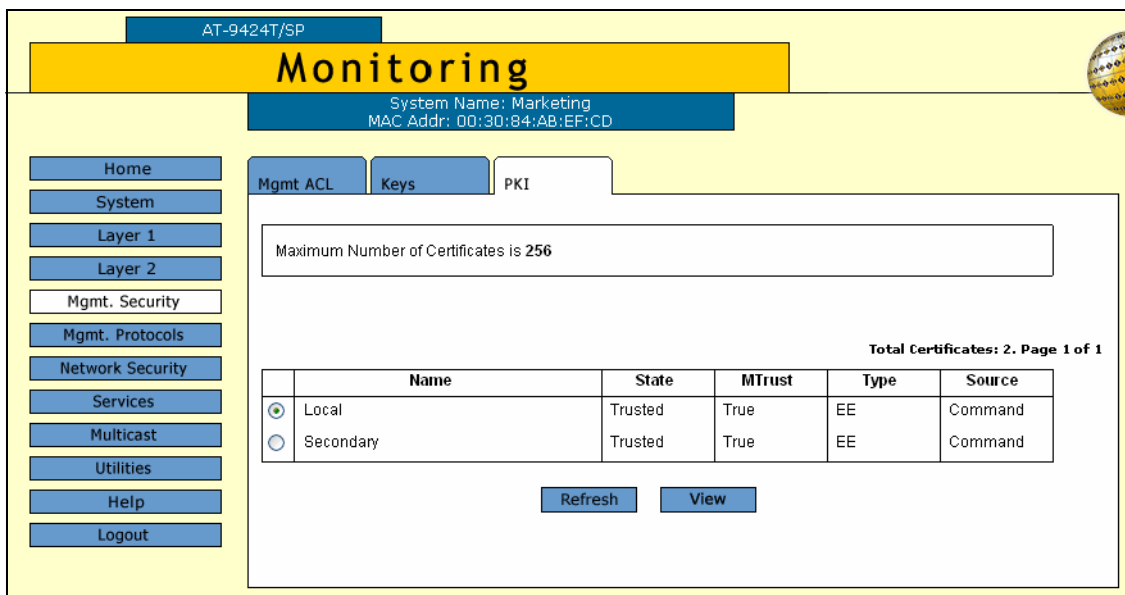


Figure 180. PKI Tab (Monitoring)

The upper section states the maximum number of certificates that can be configured on the switch.

The lower section displays a table that lists the currently configured certificates and contains the following columns of information:

Name

The certificate name.

State

The state of the certificate, one of the following:

Trusted - The certificate is from a trusted CA.

Untrusted - The certificate is from an untrusted CA.

MTrust (Manually Trusted)

The certificate has been manually verified that it is from a trusted or untrusted authority.

Type

The certificate type, one of the following:

EE - The certificate was issued by a CA.

CA - The certificate belongs to a CA.

Self - A self-signed certificate.

Source

The certificate was created on the switch.

- To view the details about a certificate, click the certificate and click **View**.

The X509 Certificate Details page is shown in Figure 181.

X509 Certificate Details	
Name	first
State	Trusted
Manually Trusted	True
Type	EE
Source	Command
Version	V3 (0X2)
Serial Number	0 (0X0)
Signature Algorithm	md5WithRSAEncryption
Public Key Algorithm	rsaEncryption
Not Valid Before	May 12 07:39:41 2004 GMT
Not Valid After	May 12 07:39:41 2006 GMT
Subject	CN=marketing
Issuer	CN=marketing
MD5 Fingerprint	6B:5C:A8:81:AA:17:AE:DB:E7:2B:3C:11:2F:90:92:D3
SHA1 Fingerprint	A5:0D:6B:89:E7:75:25:36:BE:72:34:BC:2A:87:33:8D:15:80:75:94

[Close](#)

Figure 181. X509 Certificate Details Page

The X509 Certificate Details page provides the following information about the certificate:

Name

The name of the certificate.

State

Whether the certificate is Trusted or Untrusted.

Manually Trusted

You verified the certificate is from a trusted or untrusted authority.

Type

The type of the certificate. The options are EE, SELF, and CA.

Source

The certificate was created on the switch.

Version

The version number of the AT-S63 management software.

Serial Number

The certificate's serial number.

Signature Algorithm

The signature algorithm of the certificate.

Public Key Algorithm

The public key algorithm.

Not Valid Before

The date the certificate became active.

Not Valid After

The date the certificate expires. Self-signed certificates are valid for two years.

Subject

The Subject distinguished name.

Issuer

The certificate issuer's distinguished name.

MD5 Fingerprint

The MD5 algorithm. This value provides a unique sequence for each certificate consisting of 16 bytes.

SHA1 Fingerprint

The Secure Hash Algorithm. This value provides a unique sequence for each certificate consisting of 20 bytes.

5. Click **Close** to close the page.

Displaying the SSL Settings

To configure the SSL settings, you must use the AT-S63 menus or command line interface. For information, refer to the *AT-S63 Management Software Menus Interface User's Guide* and the *AT-S63 Management Software Command Line Interface User's Guide*.

To display the SSL settings, perform the following procedure:

1. From the Home page, select **Monitoring**.

The System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Mgmt. Protocols** option.

The Mgmt. Protocols page is displayed with the Server-based Authentication tab selected by default, as shown in Figure 21 on page 75.

3. Select the **SSL** tab.

The SSL tab is shown in Figure 179.

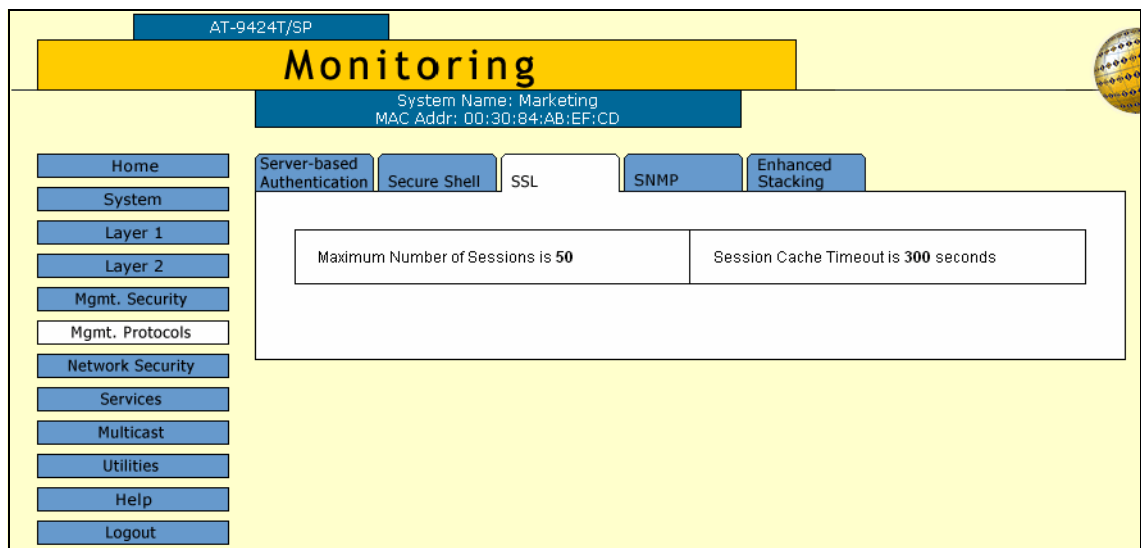


Figure 182. SSL Tab (Monitoring)

The SSL tab provides the following information:

Maximum Number of Sessions

The maximum number of SSL sessions allowed at one time.

Session Cache Timeout

The length of time before the session cache times out, in seconds.

Chapter 27

Secure Shell (SSH)

This chapter explains how to configure the Secure Shell (SSH) protocol and contains the following sections:

- “Configuring SSH” on page 418
- “Displaying the SSH Settings” on page 420

Note

For background information on SSH, refer to Chapter 33, “Secure Shell (SSH),” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Configuring SSH

To display the MAC address security level of a port, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Configuration menu, select the **Mgmt. Protocols** option.

The Mgmt. Protocols page is displayed with the Server-based Authentication tab selected by default, as shown in Figure 10 on page 54.

3. Select the **Secure Shell** tab.

The Secure Shell tab is shown in Figure 183.

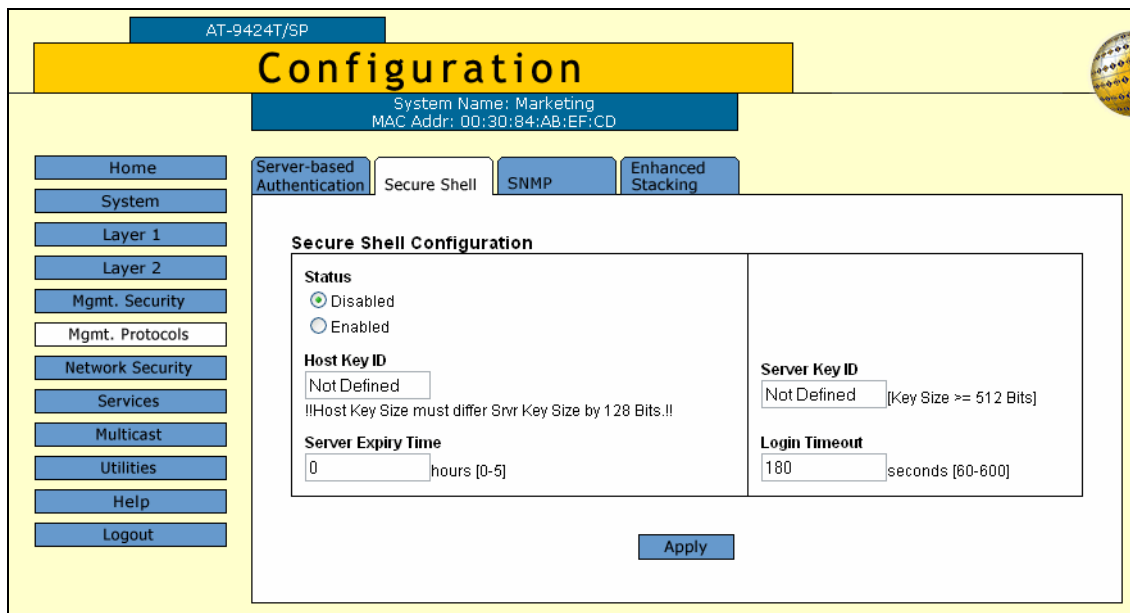


Figure 183. Secure Shell Tab (Configuration)

4. Configure the following parameters as necessary:

Key ID

Enter a host key ID. The default is Not Defined. Enter a value that you configured in the encryption menus using the AT-S63 menus interface.

Server Key ID

Enter a server key ID. The default is Not Defined. Enter a value that

you configured in the encryption menus using the AT-S63 menus interface.

Server Expiry Time

Set the time, in hours, for the server key to expire.

This timer determines how often the server key is regenerated. A server key is regenerated for security purposes. A server key is only valid for the time period configured in the Server Key Expiry (Expiration) Time timer. Allied Telesyn recommends that you set this field to 1. With this setting, a new key is generated every hour.

Login Timeout

Enter a number between 60 and 600. The default is 180.

This is the time it takes to release the SSH server from an incomplete SSH client connection. Enter a time in seconds. The default is 180 seconds (3 minutes). The range is 60 to 600 seconds.

Status

Enable the SSH server after you have finished the configuration and want to log on to the server. Or, click Disabled while you are configuring the protocol. SSH must be disabled while you are configuring the protocol. This is the default.

5. Click **Apply**.
6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying the SSH Settings

To view the Secure Shell settings, perform the following procedure:

1. From the Home page, select **Monitoring**.

The System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Configuration menu, select the **Mgmt. Protocols** option.

The Mgmt. Protocols page is displayed with the Server-based Authentication tab selected by default, as shown in Figure 21 on page 75.

3. Select the **Secure Shell** tab.

The Secure Shell tab is shown in Figure 184.

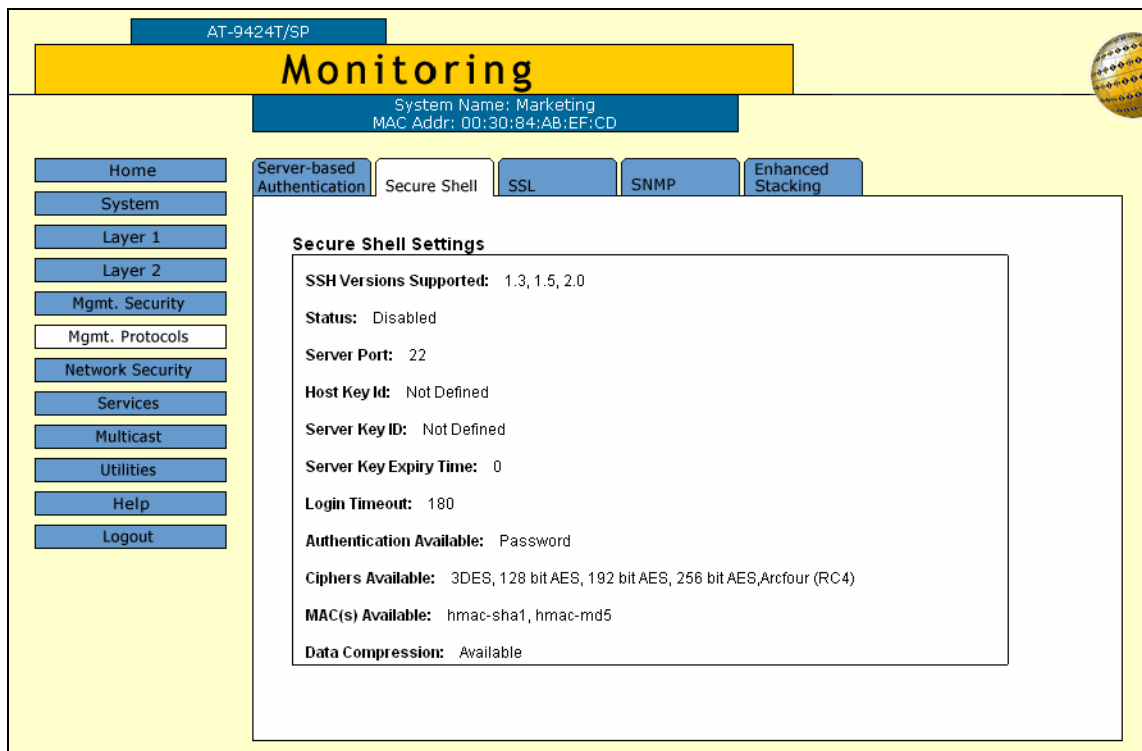


Figure 184. Secure Shell Tab (Monitoring)

The Secure Shell tab provides the following information:

SSH Versions Supported

The versions of SSH that the AT-S63 management software supports.

Status

Whether or not the SSH server is enabled or disabled.

Server Port

The well-known port for SSH. The default is port 22.

Host Key ID

The host key ID defined for SSH.

Server Key ID

Server key ID defined for SSH.

Server Key Expiry Time

Length of time, in hours, until the server key is regenerated. The default is 0 hours which means the server key is not regenerated.

Login Timeout

Time, in seconds, until a SSH server is released from an incomplete connection with a SSH client.

Authentication Available

Authentication method available. Currently, password authentication is the only supported method.

Ciphers Available

SSH ciphers that are available on the switch.

MAC(s) Available

Message Authorization Code (MAC) that is used to validate incoming SSH messages to the server. Two algorithms are supported.

Data Compression

Whether or not data compression is available on the switch. Data compression is useful for networks that have a slow throughput speed.

Chapter 28

TACACS+ and RADIUS

This chapter contains instructions on how to configure the authentication protocols. This chapter contains the following procedures:

- ❑ “Enabling or Disabling TACACS+ or RADIUS” on page 424
- ❑ “Configuring TACACS+” on page 425
- ❑ “Displaying the TACACS+ Settings” on page 427
- ❑ “Configuring RADIUS” on page 429
- ❑ “Displaying the RADIUS Settings” on page 431

Note

For background information on the authentication protocols, refer to Chapter 34, “TACACS+ and RADIUS,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Enabling or Disabling TACACS+ or RADIUS

To enable or disable the authentication protocols, perform the following procedure:

1. From the Home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Mgmt. Protocols** option.

The Mgmt. Protocols page is displayed with the Server-based Authentication tab selected by default, as shown in Figure 10 on page 54.

3. To select an authentication protocol, in the Authentication Method section of the tab, click either RADIUS or TACACS+. The default is TACACS+.

Note

The switch can support only one authentication protocol at a time. Additionally, you cannot select a different authenticator protocol when this feature is enabled.

4. To enable or disable the authentication feature on the switch, click the Enable Server-based Authentication check box. A check in the box indicates that this feature is enabled. No check indicate the feature is disabled. The default is disabled.
5. Click **Apply**.
6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

To configure TACACS+, go to "Configuring TACACS+", next. To configure RADIUS, go to "Configuring RADIUS" on page 429-.

Configuring TACACS+

To configure TACACS+, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40

2. Select the **Server-based Authentication** tab.

The Server-based Authentication tab is shown in Figure 18 on page 69.

3. In lower section of the Server-based Authentication tab, click TACACS+ Configuration and click **Configure**.

The TACACS+ Client Configuration page is shown in Figure 185.

Server #	IP Address	Encryption Key
1	0.0.0.0	
2	0.0.0.0	
3	0.0.0.0	

Figure 185. TACACS+ Client Configuration Page

4. Configure the following parameters as necessary.

Global Secret

If all of the TACACS+ servers have the same encryption secret, you can enter the key here. If the servers have different keys, you must specify each key when you specify a server's IP address.

Global Server Timeout

This parameter specifies the maximum amount of time the switch waits for a response from a TACACS+ server before assuming the server

cannot respond. If the timeout expires and the server has not responded, the switch queries the next TACACS+ server in the list. If there are no more servers, the switch defaults to the standard Manager and Operator accounts. The default is 30 seconds. The range is 1 to 30 seconds.

IP Address and Encryption Key

Use these fields to specify the IP addresses and encryption secrets of up to three network servers containing TACACS+ server software. You can leave an encryption field blank if you entered the server's secret in the Global Secret field.

5. Click **Apply**.
6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying the TACACS+ Settings

To display the TACACS+ settings on the switch, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. Select the **Mgmt. Protocols** option.

The Mgmt. Protocols tab is displayed with the Server-based Authentication tab selected by default, as shown in Figure 186.

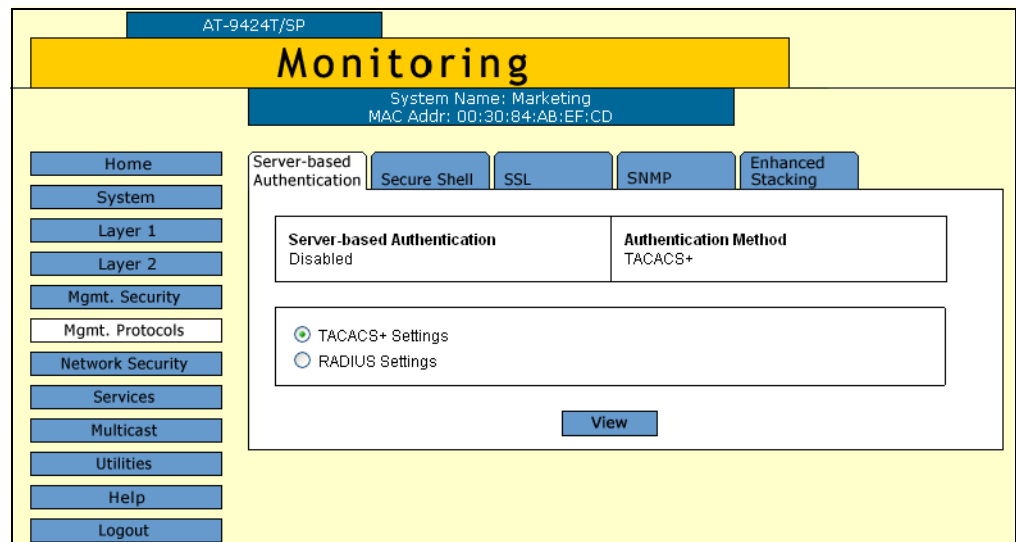


Figure 186. Server-Based Authentication Tab (Monitoring)

The upper part of the page shows if server-based authentication is enabled or disabled and the authentication method. The lower part of the page allows you to view either the settings for the current authentication method.

3. In the lower portion of the tab, click TACACS+ Settings.
4. Click **View**.

The TACACS+ client configuration page is shown in Figure 187.

Server #	IP Address	Encryption Key
1	149.32.14.237	RC Corp.
2	149.32.14.248	RC Corp.
3	149.32.14.248	

Figure 187. TACACS+ Client Configuration Page

The upper portion of the page provides the following information:

Global Secret

The TACACS+ server encryption secret.

Global Server Timeout

The maximum amount of time the switch waits for a response from a TACACS+ server before assuming the server cannot respond.

The lower portion of the page displays a table that contains the following columns of information:

Server #

The server number, one of three.

IP Address

IP addresses of up a network server containing TACACS+ server software.

Encryption Key

Encryption key for the server. This parameter is blank if all the TACACS+ servers have the same encryption secret.

Configuring RADIUS

To configure RADIUS, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40

2. Select the **Server-based Authentication** tab.

The Server-based Authentication tab is shown in Figure 18 on page 69.

3. In lower section of the Server-based Authentication tab, click RADIUS Configuration and click **Configure**.

The RADIUS Client Configuration page is shown in Figure 185.

Server No.	IP Address	Port # [1-65535]	Encryption Key
1	0.0.0.0	1812	[Not Defined]
2	0.0.0.0	1812	[Not Defined]
3	0.0.0.0	1812	[Not Defined]

Figure 188. RADIUS Client Configuration Page

4. Configure the following parameters as necessary.

Global Encryption Key

If all of the TACACS+ servers have the same encryption secret, you can enter the key here. If the servers have different keys, you must specify each key when you specify a server's IP address.

Global Server Timeout

This parameter specifies the maximum amount of time the switch waits for a response from a TACACS+ server before assuming the server

cannot respond. If the timeout expires and the server has not responded, the switch queries the next TACACS+ server in the list. If there no more servers, the switch defaults to the standard Manager and Operator accounts. The default is 30 seconds. The range is 1 to 30 seconds.

IP Address, Port #, and Encryption Key

Use these fields to specify the IP address, UDP port number, and encryption key of each RADIUS server. You can specify up to a maximum of three servers. You can leave the encryption field blank if you entered the server's key in the Global Secret field.

5. Click **Apply**.
6. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying the RADIUS Settings

To display the RADIUS settings on the switch, perform the following procedure:

1. From the Home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. Select the **Mgmt. Protocols** option.

The Mgmt. Protocols tab is displayed with the Server-based Authentication tab selected by default, as shown in Figure 186 on page 427.

The upper part of the page shows if server-based authentication is enabled or disabled and the authentication method. The lower part of the page allows you to view either the settings for the current authentication method.

3. In the lower portion of the page, click **RADIUS Settings**.
4. Click **View**.

The RADIUS Client Configuration page is shown in Figure 187.

Server No.	IP Address	Port # [1-65535]	Encryption Key
1	149.11.11.11	1812	s24aa
2	149.22.22.22	1812	s45nnn
3	0.0.0.0	1812	[Not Defined]

Figure 189. RADIUS Client Configuration Page

The upper portion of the page displays the following information:

Global Encryption Key

The global encryption secret.

Global Server Timeout

The maximum amount of time the switch waits for a response from a RADIUS server before assuming the server cannot respond.

The lower portion of the page displays a table that contains the following columns of information:

Server #

The server number, one of three.

IP Address

IP address of the RADIUS server.

Port

Port of the RADIUS server.

Encryption Key

Encryption key for that server. This parameter is blank if all the RADIUS servers have the same encryption secret.

Chapter 29

Management Access Control Lists

A management access control list (ACL) allows you to restrict Telnet and web browser management access to the switch. The sections in this chapter include:

- ❑ “Configuring a Management ACL” on page 434
- ❑ “Deleting a Management ACL” on page 436
- ❑ “Displaying the Management Access Control Lists” on page 437

Note

For background information about management access control lists, refer to Chapter 35, “Management Access Control Lists,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Configuring a Management ACL

To configure a management ACL, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Mgmt. Security** option.

The Mgmt. Security page is displayed with the Mgmt. ACL tab selected by default, as shown in Figure 190.

AT-9424T/SP

Configuration

System Name: Marketing
MAC Addr: 00:30:84:AB:EF:CD

- Home
- System
- Layer 1
- Layer 2
- Mgmt. Security**
- Mgmt. Protocols
- Network Security
- Services
- Multicast
- Utilities
- Help
- Logout

Mgmt ACL

Configure Mgmt. ACL(s)

Disable Mgmt. ACLs Enable Mgmt. ACLs

Apply

IP Address	IP Mask	Protocol	Interface

Delete Refresh

Mgmt. ACL IP Address: 0 . 0 . 0 . 0

Mgmt. ACL IP Mask: 0 . 0 . 0 . 0

Protocol: TCP

Interface: TELNET

Add

Figure 190. Mgmt. ACL Tab (Configuration)

3. In the Configure Mgmt. ACL(s) section, click **Enable Mgmt. ACL(s)** to enable this feature, or **Disable Mgmt. ACL(s)** to disable it.
4. Click **Apply**.
5. In the lower section of the tab, configure the following parameters:

Mgmt. ACL IP Address

The IP address of a specific management station (for example, 149.11.11.11) or a subnet (for example, 149.11.11.0).

Protocol

Select the protocol from the list. The AT-S63 management software allows you to select UDP, but because management packets from

Telnet and web browser management sessions are TCP, you should specify TCP or ALL.

Mgmt. ACL IP Mask

A mask that indicates the parts of the IP address the switch should filter on.

Interface

The interface you want the management station to be able to use when managing the switch. The options are:

Telnet - Allows Telnet management packets.

Web - Allows web browser management packets.

All - Allows both Telnet and web browser management packets.

6. Click **Add.**

The management ACL is added to the table displayed in the middle section of the tab.

7. From the Configuration menu, select the **Save Config option to permanently save your changes. (This option is not displayed if there are no changes to save.)**

Deleting a Management ACL

To modify a management ACL, perform the following procedure:

1. From the home page, select **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 5 on page 40.

2. From the Configuration menu, select the **Mgmt. Security** option.

The Mgmt. Security page is displayed with the Mgmt. ACL tab selected by default, as shown in Figure 190 on page 434.

3. Select the management ACL you want to modify from the table in the middle section of the tab and click **Delete**.

The management ACL is deleted from the list. To see the new list, click **Refresh**.

4. From the Configuration menu, select the **Save Config** option to permanently save your changes. (This option is not displayed if there are no changes to save.)

Displaying the Management Access Control Lists

To display the currently configured management access control lists, perform the following procedure:

1. From the home page, select **Monitoring**.

The Monitoring System page is displayed with the General tab selected by default, as shown in Figure 6 on page 44.

2. From the Monitoring menu, select the **Mgmt. Security** option.

The Mgmt. Security page is displayed with the Mgmt. ACL tab selected by default, as shown in Figure 191.

AT-9424T/SP

Monitoring

System Name: Marketing
MAC Addr: 00:30:84:AB:EF:CD

Home
System
Layer 1
Layer 2
Mgmt. Security
Mgmt. Protocols
Network Security
Services
Multicast
Utilities
Help
Logout

Mgmt ACL | Keys | PKI

Mgmt. ACL(s) are Enabled

Browse Mgmt. ACL(s)

	IP Address	IP Mask	Protocol	Interf
▶	149.35.8.31	255.255.255.0	TCP	ALL

Refresh

Figure 191. Mgmt. ACL Tab (Monitoring)

The Mgmt. ACL tab contains two sections of information. The top section shows if management ACLs are enabled or disabled.

The bottom section displays a table that contains the following columns of information:

IP Address

The IP address of a specific management station.

IP Mask

A mask that indicates the parts of the IP address the switch should filter on.

Protocol

The protocol for the management packets.

Interface

The interface the management station uses when managing the switch.

Appendix A

AT-S63 Default Settings

This appendix lists the AT-S63 factory default settings. It contains the following sections in alphabetical order:

- ❑ “Basic Switch Default Settings” on page 440
- ❑ “Enhanced Stacking Default Setting” on page 443
- ❑ “SNMP Default Settings” on page 444
- ❑ “Port Configuration Default Settings” on page 445
- ❑ “Event Log Default Settings” on page 446
- ❑ “Quality of Service” on page 447
- ❑ “IGMP Snooping Default Settings” on page 448
- ❑ “Denial of Service Prevention Default Settings” on page 449
- ❑ “STP, RSTP, and MSTP Default Settings” on page 450
- ❑ “VLAN Default Settings” on page 452
- ❑ “GVRP Default Settings” on page 453
- ❑ “Port Security Default Settings” on page 454
- ❑ “802.1x Port-Based Network Access Control Default Settings” on page 455
- ❑ “Web Server Default Settings” on page 456
- ❑ “SSL Default Settings” on page 457
- ❑ “PKI Default Settings” on page 458
- ❑ “SSH Default Settings” on page 459
- ❑ “Server-Based Authentication Default Settings” on page 460
- ❑ “Management Access Control List Default Setting” on page 461

Basic Switch Default Settings

This section lists the default settings for basic switch parameters. The following topics are covered:

- “Boot Configuration File Default Setting” on page 440
- “Management Access Default Settings” on page 440
- “Management Interface Default Settings” on page 440
- “RJ-45 Serial Terminal Port Default Settings” on page 441
- “SNTP Default Settings” on page 441
- “Switch Administration Default Settings” on page 442
- “System Software Default Settings” on page 442

Boot Configuration File Default Setting

The following table lists the File menu default setting.

File Menu Setting	Default
Default Configuration File	boot.cfg

Management Access Default Settings

The following table lists the management access default settings.

Remote Management Access Setting	Default
Telnet	Enabled
SNMP	Disabled
TFTP	Enabled
Web Server	Enabled

Management Interface Default Settings

The following table lists the management interface default settings.

Management Interface Setting	Default
Manager Login Name	manager
Manager Password	friend
Operator Login Name	operator
Operator Password	operator
Console Disconnect Timer Interval	10 minutes

Note

Login names and passwords are case sensitive.

RJ-45 Serial Terminal Port Default Settings

The following table lists the RJ-45 serial terminal port default settings.

RJ-45 Serial Terminal Port Setting	Default
Data Bits	8
Stop Bits	1
Parity	None
Flow Control	None
Baud Rate	9600 bps

SNTP Default Settings

The following table lists the SNTP default settings.

SNTP Setting	Default
System Time	00:00:00 on January 1, 1970
SNTP Status	Disabled
SNTP Server	0.0.0.0
UTC Offset	+0
Daylight Savings Time (DST)	Enabled
Poll Interval	600 seconds

Switch Administration Default Settings

The following table describes the switch administration default settings.

Administration Setting	Default
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway Address	0.0.0.0
System Name	None
Administrator	None
Comments	None
BOOTP/DHCP	Disabled
MAC Address Aging Time	300 seconds

System Software Default Settings

The following table lists the system software default settings.

System Software Setting	Default
Console Startup Mode	CLI

Enhanced Stacking Default Setting

The following table lists the enhanced stacking default setting.

Enhanced Stacking Setting	Default
Switch State	Slave

SNMP Default Settings

The following table describes the SNMP default settings.

SNMP Communities Setting	Default
SNMP Status	Disabled
Authentication Failure Trap Status	Disabled
Community Name	public (Read only)
Community Name	private (Read Write)
Status (public)	Enabled
Status (private)	Enabled
Open Status (public)	Yes
Open Status (private)	Yes

Port Configuration Default Settings

The following table lists the port configuration default settings.

Port Configuration Setting	Default
Status	Enabled
Broadcast Filter	Disabled
Override Priority	No override
HOL Blocking	Disabled
Back Pressure	Disabled
Flow Control	Auto
Flow Control/Back Pressure Limit	7935
Speed	Auto-Negotiation
Duplex Mode	Auto-Negotiation
MDI/MDI-X	Auto-MDI/MDIX

Event Log Default Settings

The following table lists the event log default settings.

Event Log Setting	Default
Status	Enabled
Full Log Action	Wrap

Quality of Service

The following table lists the default mappings of IEEE 802.1p priority levels to egress port priority queues

IEEE 802.1p Priority Level	Port Priority Queue
0 or 1	Q0 (lowest)
2 or 3	Q1
4 or 5	Q2
6 or 7	Q3 (highest)

IGMP Snooping Default Settings

The following table lists the IGMP Snooping default settings.

IGMP Snooping Setting	Default
IGMP Snooping Status	Disabled
Multicast Host Topology	Single Host/ Port (Edge)
Host/Router Timeout Interval	260 seconds
Maximum Multicast Groups	64
Multicast Router Ports Mode	Auto Detect

Denial of Service Prevention Default Settings

The following table lists the default settings for the Denial of Service prevention feature.

Denial of Service Prevention Setting	Default
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Uplink Port	26
SYN Flood Defense	Disabled
Smurf Defense	Disabled
Land Defense	Disabled
Teardrop Defense	Disabled
Ping of Death Defense	Disabled
IP Options Defense	Disabled

STP, RSTP, and MSTP Default Settings

This section provides the spanning tree, STP RSTP, and MSTP, default settings.

Spanning Tree Switch Settings

The following table describes the Spanning Tree Protocol default settings for the switch.

STP Switch Setting	Default
Spanning Tree Status	Disabled
Active Protocol Version	RSTP

STP Default Settings

The following table describes the STP default settings.

STP Setting	Default
Bridge Priority	32768
Bridge Hello Time	2
Bridge Forwarding	15
Bridge Max Age	20
Port Cost	Automatic -Update
Port Priority	128

RSTP Default Settings

The following table describes the RSTP default settings.

RSTP Setting	Default
Force Version	RSTP
Bridge Priority	32768
Bridge Hello Time	2
Bridge Forwarding	15
Bridge Max Age	20
Edge Port	Yes
Point-to-Point	Auto Detect
Port Cost	Automatic Update
Port Priority	128

MSTP Default Settings

The following table lists the MSTP default settings..

MSTP Setting	Default
Status	Disabled
Force Version	MSTP
Bridge Hello Time	2
Bridge Forwarding Delay	15
Bridge Max Age	20
Maximum Hops	20
Configuration Name	null
Revision Level	0
CIST Priority	Increment 8 (32768)
Port Priority	Increment 8 (128)
Port Internal Path Cost	Auto Update
Port External Path Cost	Auto Detect
Point-to-Point	Auto Detect
Edge Port	Yes

VLAN Default Settings

This section provides VLAN default settings.

VLAN Setting	Default
Default VLAN Name	Default_VLAN (all ports)
Management VLAN ID	1 (Default_VLAN)
VLAN Mode	User Configured
Uplink Port	None

GVRP Default Settings

This section provides the default settings for GVRP.

GVRP Setting	Default
Status	Disabled
GIP Status	Enabled
Join Timer	20 centiseconds
Leave Timer	60 centiseconds
Leave All Timer	1000 centiseconds
Port Mode	Normal

Port Security Default Settings

The following table lists the port security default settings.

Port Security Setting	Default
Security Mode	Automatic (no security)
Intrusion Action	Discard
Participating	No
MAC Limit	No Limit

802.1x Port-Based Network Access Control Default Settings

The following table describes the 802.1x Port-based Network Access Control default settings.

802.1x Port-based Network Access Control Settings	Default
Port Access Control	Disabled
Authentication Method	RADIUS EAP
Port Role	None

The following table lists the default settings for RADIUS accounting.

RADIUS Accounting Settings	Default
Status	Disabled
Port	1813
Type	Network
Trigger Type	Start_Stop
Update Status	Disabled
Update Interval	60

Web Server Default Settings

The following table lists the web server default settings.

Web Server Configuration Setting	Default
Status	Enabled
Mode	HTTP
Port Number	80
SSL Key ID	None

SSL Default Settings

The following table lists the SSL default settings.

SSL Setting	Default
Maximum Number of Sessions	50
Session Cache Timeout	300 seconds

PKI Default Settings

The following table lists the PKI default settings, including the generate enrollment request settings.

PKI Setting	Default
Switch Distinguished Name	None
Maximum Number of Certificates	256
Request Name	None
Key Pair ID	0
Format	PEM
Type	PKCS10

SSH Default Settings

The following table lists the SSH default settings.

SSH Setting	Default
Status	Disabled
Host Key ID	Not Defined
Server Key ID	Not Defined
Server Key Expiry Time	0 hours
Login Timeout	180 seconds

Server-Based Authentication Default Settings

This section describes the server-based authentication, RADIUS, and TACACS+ client default settings.

Server-Based Authentication Default Settings

The following table describes the server-based authentication default settings.

Server-based Authentication Setting	Default
Server-based Authentication	Disabled
Active Authentication Method	TACACS+

RADIUS Default Settings

The following table lists the RADIUS configuration default settings.

RADIUS Configuration Setting	Default
Global Encryption Key	ATI
Global Server Timeout Period	30 seconds
RADIUS Server 1 Configuration	0.0.0.0
RADIUS Server 2 Configuration	0.0.0.0
RADIUS Server 3 Configuration	0.0.0.0
Auth Port	1812
Encryption Key	Not Defined

TACACS+ Client Default Settings

The following table lists the TACACS+ client configuration default settings.

TACACS+ Client Configuration Setting	Default
TAC Server 1	0.0.0.0
TAC Server 2	0.0.0.0
TAC Server 3	0.0.0.0
TAC Server Order	1 2 3
TAC Global Secret	None
TAC Timeout	30 seconds

Management Access Control List Default Setting

The following table lists the default setting for the Management Access Control List.

Management ACL Setting	Default
Status	Disabled

Index

Numerics

- 802.1x Port-based Network Access Control
 - access role, configuring 380
 - authenticator port, configuring 383
 - configuring 380
 - default settings 455
 - disabling 382
 - enabling 382
 - port parameters, displaying 389
 - port role, configuring 380
 - port status, displaying 388
 - supplicant port, configuring 386

A

- access control list (ACL), default setting 461
- administrator name
 - configuring 41
 - default setting 442
- aging time
 - changing 405
 - default setting 442
- app (applicant state machine) 364
- associations, VLANs to MSTI IDs 314
- AT-S63 software
 - default settings 439
 - resetting to factory defaults 51
- auth period 387
- authentication failure trap, default setting 444
- authentication protocols, enabling or disabling 424
- autonegotiation, configuring 80

B

- back pressure
 - configuring 83
 - default setting 445
- Boot Protocol (BootP)
 - activating 43
 - default setting 442
- bridge forwarding delay
 - default setting 450, 451
 - Multiple Spanning Tree Protocol (MSTP) 308
 - Rapid Spanning Tree Protocol (RSTP) 298
 - Spanning Tree Protocol (STP) 290
- bridge hello time
 - default setting 450
 - Multiple Spanning Tree Protocol (MSTP) 308
 - Rapid Spanning Tree Protocol (RSTP) 298
 - Spanning Tree Protocol (STP) 290
- bridge identifier

- Rapid Spanning Tree Protocol (RSTP) 298
- Spanning Tree Protocol (STP) 291
- bridge max age
 - default setting 450
 - Multiple Spanning Tree Protocol (MSTP) 308
 - Rapid Spanning Tree Protocol (RSTP) 298
 - Spanning Tree Protocol (STP) 290
- bridge priority
 - default setting 450
 - Rapid Spanning Tree Protocol (RSTP) 297
 - Spanning Tree Protocol (STP) 289
- bridge protocol data unit (BPDU) 298
- broadcast filter, default setting 445
- browser tools 36

C

- ciphers available parameter 421
- CIST priority parameter 309
- Class of Service (CoS)
 - configuring 192
 - mapping to egress queues 195
 - schedule, displaying 202
 - scheduling, configuring 198
 - settings, displaying 200
- Common and Internal Spanning Tree (CIST), configuring 309
- community name
 - SNMPv1 and SNMPv2c 57
 - SNMPv3 protocol 267, 270
- compact flash card, listing files on 118
- configuration file, default name 440
- console disconnect interval, default setting 440
- console startup mode, default setting 442
- CoS. *See* Class of Service (CoS)

D

- data compression parameter 421
- daylight savings time (DST), default setting 441
- default values, AT-S63 software 439
- Denial of Service (DoS) defense
 - configuring 164
 - default settings 449
 - enabling or disabling 166
 - mirror port 166
 - settings, displaying 167
- distinguished name, default setting 458
- DoS. *See* Denial of Service (DoS) Defense
- duplex mode
 - configuring 80

- default setting 445
- Dynamic Host Control Protocol (DHCP)
 - activating 43
 - default setting 442

E

- edge port
 - default setting 450, 451
 - Multiple Spanning Tree Protocol (MSTP) 318
- encryption keys, displaying 410
- enhanced stacking
 - changing switches 71
 - configuring 68
 - default switch setting 443
 - setting switch status 68
- event log
 - clearing 136
 - default settings 446
 - disabling 128, 136
 - displaying 130
 - enabling 128
 - saving to a file 136
 - severity codes 134
 - software module list 132

F

- factory defaults
 - list 439
 - resetting switch 51
- flash memory, displaying files in 116
- flow control
 - configuring 82
 - default setting 445
- flow group
 - configuring 170
 - deleting 173
 - displaying 173
 - modifying 172
- force version
 - default setting 450, 451
 - Multiple Spanning Tree Protocol (MSTP) 308
 - Rapid Spanning Tree Protocol (RSTP) 297

G

- GARP VLAN Registration Protocol (GVRP)
 - configuration, displaying 359
 - configuring 356
 - counters, displaying 366
 - database, displaying 362
 - default settings 453
 - disabling 358
 - enabling 358
 - GIP connected ports ring, displaying 369
 - GVRP state machine, displaying 363
 - port configuration, displaying 361
- gateway address
 - configuring 42
 - default setting 442
 - displaying 45

- global encryption key
 - configuring 429, 432
 - default setting 460
- global secret
 - configuring 425, 428
 - default setting 460
- global server timeout
 - configuring 425, 428
 - default setting 460
- GVRP. *See* GARP VLAN Registration Protocol (GVRP)

H

- hardware information 44
- held period 387
- hello time
 - default setting 450
 - Rapid Spanning Tree Protocol (RSTP) 298
 - Spanning Tree Protocol (STP) 290
- HOL blocking, default setting 445
- host key ID parameter 418
- host nodes, displaying 207
- host/router timeout interval
 - configuring 205, 208
 - default setting 448

I

- IGMP. *See* Internet Group Management Protocol (IGMP)
 - Snooping
- ingress packet threshold 83
- Internet Group Management Protocol (IGMP) snooping
 - configuring 204
 - default settings 448
 - disabling 204, 207
 - displaying 207
 - enabling 204, 207
- Internet Protocol (IP) address
 - configuring 42
 - default 442
- intrusion action (port)
 - configuring 377
 - default setting 454

L

- local management session, defined 24
- login timeout parameter 419

M

- MAC address aging time
 - changing 405
 - default setting 442
- MAC address table, displaying 402
- MAC addresses
 - adding 398
 - deleting dynamic 401
 - deleting multicast 400
 - displaying 402
- MAC limit, default setting 454
- MACs available parameter 421
- management access defaults 440

- management access levels 27, 46
- Management Information Base. *See* MIBs
- management interface defaults 440
- management VLAN ID
 - configuring 339
 - default setting 452
- management VLAN, specifying 339
- manager access 27, 46
- manager password
 - configuring 46
 - default setting 440
- master switch
 - assigning 68
 - defined 68
 - returning to 74
- max age
 - default setting 450
 - Rapid Spanning Tree Protocol (RSTP) 298
 - Spanning Tree Protocol (STP) 290
- max hops, Multiple Spanning Tree Protocol (MSTP) 308
- max requests 385
- max start 387
- maximum multicast groups
 - configuring 205
 - default setting 448
 - displaying 208
- maximum number of sessions, default setting 457
- MDI/MDIX mode 81
- MIBs, supported 25
- MSTI ID
 - creating 310
 - deleting 311
 - modifying 311
- MSTI ID association to a VLAN
 - adding 314
 - modifying 315
- MSTI. *See* Multiple Spanning Tree Instance (MSTI)
- MSTP. *See* Multiple Spanning Tree Protocol (MSTP)
- multicast groups, maximum
 - configuring 205
 - displaying 208
- multicast host topology
 - configuring 204
 - default setting 448
 - displaying 207
- multicast MAC address
 - adding 398
 - deleting 400
 - displaying 402
- multicast router ports
 - configuring 205, 208
 - default setting 448
- multicast routers, displaying 210
- Multiple Spanning Tree Instance (MSTI)
 - associating to VLANs 314
 - disassociating from VLANs 314
 - modifying association to VLANs 315
 - MSTI ID
 - creating 310

- deleting 311
 - modifying 311
 - removing a VLAN association 314
- Multiple Spanning Tree Protocol (MSTP)
 - associating VLANs to MSTI IDs 314
 - bridge forwarding delay 308
 - bridge hello time 308
 - bridge max age 308
 - bridge settings, configuring 306
 - configuration name 308
 - configuring 306
 - connecting to VLANs 314
 - default settings 451
 - disabling 304
 - edge port 318
 - enabling 304
 - force version 308
 - max hops 308
 - MSTI ID
 - creating 310
 - deleting 311
 - modifying 311
 - parameters, configuring 306
 - point-to-point port 318
 - port external path cost 318
 - port internal path cost 318
 - port parameters
 - configuring 317
 - displaying 319
 - port priority 317
 - port settings, displaying 322
 - port status, displaying 322
 - resetting to defaults 324

O

- operator access 27, 46
- operator password
 - configuring 46
 - default setting 440
- override priority, default setting 445

P

- password
 - changing 46
 - default 33
- pinging 49
- PKI certificates
 - displaying 412
 - maximum number of certificates, default setting 458
- PKI certificates, displaying 412
- PKI. *See* Public Key Infrastructure (PKI)
- point-to-point port
 - default setting 450
 - Multiple Spanning Tree Protocol (MSTP) 318
 - Rapid Spanning Tree Protocol (RSTP) 299
- policy
 - configuring 184
 - deleting 188
 - displaying 188

- modifying 186
 - poll interval, default setting 441
 - port
 - configuring parameters, basic 78
 - disabling 79
 - enabling 79
 - link status 86
 - resetting to defaults 92
 - statistics, displaying 89
 - status
 - default setting 445
 - displaying 85
 - port control
 - 802.1x port-based access control 384
 - force-authorized 384
 - force-unauthorized 384
 - port cost
 - default setting 450
 - Multiple Spanning Tree Protocol (MSTP) 318
 - Rapid Spanning Tree Protocol (RSTP) 299
 - Spanning Tree Protocol (STP) 292
 - port costdefault setting 451
 - port mirror
 - creating 104
 - deleting 109
 - disabling 108
 - displaying 110
 - modifying 107
 - port parameters, configuring
 - basic 78
 - Multiple Spanning Tree Protocol (MSTP) 306
 - Rapid Spanning Tree Protocol (RSTP) 296
 - Spanning Tree Protocol (STP) 288
 - port priority
 - default setting 450
 - Multiple Spanning Tree Protocol (MSTP) 317
 - Rapid Spanning Tree Protocol (RSTP) 299
 - Spanning Tree Protocol (STP) 291
 - port role, default setting 455
 - port security
 - default settings 454
 - displaying 376
 - intrusion action 377
 - port speed
 - configuring 80
 - default setting 445
 - port trunk
 - creating 94
 - deleting 99
 - displaying 100
 - modifying 97
 - port-based access control. *See* 802.1x Port-based Network Access Control
 - port-based VLAN
 - creating 328
 - deleting 334, 351
 - displaying 337, 352
 - modifying 332
 - protected ports VLAN
 - creating 342
 - deleting 351
 - displaying 352
 - modifying 347
 - Public Key Infrastructure (PKI)
 - default settings 458
 - settings, displaying 412
- Q**
- QoS. *See* Quality of Service (QoS)
 - Quality of Service (QoS)
 - default settings 447
 - See also* traffic class, flow group, and policy 169
 - quiet period, configuring 385
- R**
- RADIUS
 - configuring 429
 - default settings 460
 - disabling 424
 - displaying settings 431
 - enabling 424
 - server timeout 432
 - RADIUS accounting
 - configuring 393
 - settings, displaying 394
 - RADIUS server
 - encryption secret 430
 - encryption secret, configuring 426
 - IP address, configuring 430
 - Rapid Spanning Tree Protocol (RSTP)
 - bridge forwarding delay 298
 - bridge hello time 298
 - bridge identifier 298
 - bridge max age 298
 - bridge priority 297
 - bridge settings, configuring 296
 - default settings 450
 - disabling 286, 304
 - edge port, configuring 299
 - enabling 286, 304
 - force version 297
 - point-to-point port, configuring 299
 - port cost 299
 - port priority 299
 - port settings, displaying 300, 322
 - resetting to defaults 300
 - rate limit, setting 83
 - reauth period, configuring 384
 - reg (registrar state machine) parameter 365
 - remote management access defaults 440
 - remote management session, defined 25
 - RJ-45 serial terminal port, default settings 441
 - RSTP. *See* Rapid Spanning Tree Protocol (RSTP)
- S**
- Secure Shell (SSH) protocol
 - configuring 418
 - default settings 459

- displaying settings 420
- Secure Sockets Layer (SSL)
 - default settings 457
 - displaying settings 415
- server authentication UDP port
 - configuring 430
 - default setting 460
- server key ID parameter 418
- server timeout, configuring 385
- server-based authentication method, default setting 455, 460
- session cache timeout
 - configuring 415
 - default setting 457
- Simple Network Management Protocol. *See* SNMP
- Simple Network Time Protocol (SNTP), default setting 441
- slave switch
 - assigning 68
 - defined 68
- SNMP
 - default setting for remote management 440
 - default settings 444
- SNMP community string, default name 444
- SNMP management
 - default setting 444
 - disabling 54
 - enabling 54
 - session, starting 25
- SNMPv1 and SNMPv2c community
 - creating 56
 - deleting 62
 - displaying 63
 - modifying 59
- SNMPv3 Access Table entry
 - creating 234
 - deleting 237
 - displaying 275
 - modifying 238
- SNMPv3 community name, modifying 270
- SNMPv3 Community Table entry
 - creating 266
 - deleting 269
 - displaying 280
 - modifying 269
- SNMPv3 Notify Table entry
 - creating 247
 - deleting 249
 - displaying 277
 - modifying 250
- SNMPv3 SecurityToGroup Table entry
 - creating 241
 - deleting 244
 - displaying 276
 - modifying 244
- SNMPv3 Target Address Table entry
 - creating 252
 - deleting 255
 - displaying 278
 - modifying 256
- SNMPv3 Target Parameters Table entry
 - creating 259
 - deleting 262
 - displaying 279
 - modifying 263
- SNMPv3 User Table entry
 - creating 220
 - deleting 223
 - displaying 272
 - modifying 224
- SNMPv3 View Table entry
 - creating 228
 - deleting 231
 - displaying 274
 - modifying 231
- SNTP server, default setting 441
- software information 44
- Spanning Tree Protocol (RSTP)
 - parameters, displaying 292
- Spanning Tree Protocol (STP)
 - bridge forwarding delay 290
 - bridge hello time 290
 - bridge identifier 291
 - bridge max age 290
 - bridge parameters, configuring 288
 - bridge priority 289
 - default settings 450
 - disabling 286, 304
 - enabling 286, 304
 - parameters, displaying 292
 - port cost 292
 - port priority 291
 - port settings, displaying 322
 - resetting to defaults 295
- spanning tree, default setting 450
- SSH. *See* Secure Shell (SSH)
- SSL. *See* Secure Sockets Layer (SSL)
- static MAC address
 - adding 398
 - deleting 400
- static unicast MAC address, displaying 402
- STP ID 369
- STP. *See* Spanning Tree Protocol (STP)
- subnet mask
 - configuring 42
 - default setting 442
- supplicant port, start period 387
- supplicant timeout 384
- switch
 - hardware information 44
 - software information 44
 - switch name, configuring 40
 - switch state, default setting 443
 - switch, rebooting 48
 - system date, default setting 441
 - system file
 - downloading 122
 - uploading 125
 - system name

- configuring 41
- default setting 442
- system software default settings 442
- system time, default setting 441

- starting 32
- web server, default settings 456

T

TACACS+

- configuring 425
- default settings 460
- disabling 424
- displaying settings 427
- enabling 424
- server timeout
 - configuring 429
 - default setting 460

tagged VLAN

- creating 328
- deleting 334, 351
- displaying 337, 352
- modifying 332

Telnet, default setting for remote management 440

TFTP, default setting for remote management 440

traffic class

- configuring 176
- deleting 180
- displaying 180
- modifying 178

tx period, configuring 384

U

unavailable status, defined 68

uplink port

- configuring 336
- default setting 452

user name

- configuring 387
- default 33

user password, configuring 387

UTC offset, default setting 441

V

versions supported (SSH) parameter 420

virtual LAN (VLAN)

- associating to MSTI IDs 314
- creating 328
- default settings 452
- deleting 334, 351
- displaying 337, 352
- mode, selecting 335
- modifying 332

VLAN identifier (VID)

- configuring 342

VLAN name

- configuring 342

VLAN name, default setting 452

W

web browser management session

- quitting 38