

AT-S60 Management Software

AT-S60



User's Guide

AT-8400 SERIES SWITCH

VERSION 2.1.0



PN 613-50400-00 Rev C

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 is a registered trademark 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.

Table of Contents

List of Figures	15
Preface	21
How This Guide is Organized	22
Document Conventions	24
Where to Find Web-based Guides	25
Contacting Allied Telesyn	26
Online Support	26
Email and Telephone Support	26
Returning Products	26
Sales or Corporate Information	26
Management Software Updates	26
Chapter 1	
AT-S60 Overview	27
Overview	28
Local Management Session	29
Telnet Management Session	30
Web Browser Management Session	31
SNMP Management Session	32
Management Access Levels	33
Specifying Ports	34
Specifying Time and Date	35
Section I	
Basic Features	36
Chapter 2	
Starting a Local or Telnet Management Session	38
Local Management Session	39
Starting a Local Management Session	40
Enhanced Stacking	42
Quitting from a Local Session	42
Telnet Management Session	43
Starting a Telnet Management Session	44
Quitting from a Telnet Management Interface	44

Chapter 3

Basic Switch Parameters	45
Assigning an IP Address to a Switch	46
How Do You Assign an IP Address?	47
Configuring an IP Address and Switch Name	48
Displaying and Clearing Line Card Information	51
Displaying Line Card Information	51
Displaying Line Card Statistics	53
Clearing Line Card Statistics	54
Displaying and Clearing System Information	55
Displaying System Information	55
Clearing System Statistics	56
Activating the BootP and DHCP Services	57
Setting the System Time	59
Rebooting a Switch	63
Configuring the AT-S60 Software Security Features	64
Configuring the Management Passwords	65
Configuring Management Access	66
Displaying the AT-S60 Hardware and Software Information	68
Displaying System Hardware Information	68
Displaying System Software Information	69
Pinging a Remote System	71
Returning the AT-S60 Software to the Factory Default Values	72
Configuring the Console Startup Mode	74

Chapter 4

Enhanced Stacking	75
Enhanced Stacking Overview	76
Guidelines	76
Example	78
Setting a Switch's Enhanced Stacking Status	79
Configuring Enhanced Stacking	80
Selecting a Switch in an Enhanced Stack	81
Returning to the Master Switch	83

Chapter 5

SNMPv1 and SNMPv2c Configuration	84
SNMP Overview	85
Configuring the SNMPv1 and SNMPv2c Protocols	86
Enabling the SNMP Protocol	86
Configuring SNMPv1 and SNMPv2c Communities	88
Deleting an SNMPv1 and SNMPv2 Community	91
Modifying SNMPv1 and SNMPv2 Community Attributes	92
Displaying an SNMPv1 and SNMPv2c Community	100

Chapter 6

Port Parameters	101
Displaying Port Status	102
Configuring Port Parameters	106
Displaying Port Statistics	112

Chapter 7

MAC Address Table	115
MAC Address Overview	116
Displaying MAC Addresses	118
Adding Static Unicast and Multicast MAC Addresses	122

Deleting MAC Addresses	124
Changing the Aging Time	126
Chapter 8	
Port Trunking	127
Port Trunking Overview	128
Port Trunking Guidelines	129
Before Creating Port Trunks	131
Load Distribution Methods	131
Creating a Port Trunk	132
Deleting a Port Trunk	134
Modifying a Port Trunk	135
Changing the Name of the Port Trunk	137
Adding Ports to an Existing Port Trunk	137
Deleting Ports from a Port Trunk	139
Replacing Ports in a Trunk	140
Clearing Ports in a Port Trunk	141
Chapter 9	
Port Mirroring	142
Port Mirroring Overview	143
Creating a Port Mirror	144
Modifying a Source Port Mirror	146
Deleting a Destination Port Mirror	148
Enabling a Destination Port Mirror	149
Disabling a Destination Port Mirror	150
Section II	
Advanced Features	151
Chapter 10	
File System Configuration	152
File System Configuration Overview	153
File Naming Conventions	154
Setting, Creating, Editing, and Displaying System Configuration Files	156
Setting a System Configuration File	156
Creating a System Configuration File	158
Editing a System Configuration File	159
Displaying System Configuration Files	159
Copying and Renaming System Files	162
Deleting System Files	163
Displaying System Files	165
Chapter 11	
File Downloads and Uploads	167
Overview	168
Obtaining Management Software Updates	171
Downloading Files	172
Downloading an Image File Using Xmodem or TFTP	173
Downloading a File Using Xmodem or TFTP	180
Uploading Files	187
Uploading an Image File Using Xmodem or TFTP	188
Uploading a File Using Xmodem or TFTP	194
Downloading the AT-S60 Image Switch to Switch	201

Chapter 12

Event Log	203
Event Log Overview	204
Configuring the Event Log	205
Displaying Events	207
Software Modules	210
Saving the Event Log	212
Configuring the Save Option	212
Clearing the Event Log	213

Chapter 13

Class of Service (CoS)	214
Class of Service Overview	215
Configuring CoS	217

Chapter 14

IGMP Snooping	218
IGMP Snooping Overview	219
Configuring IGMP Snooping	221
Displaying a List of Host Nodes	224
Displaying a List of Multicast Routers	226

Chapter 15

STP and RSTP	228
STP and RSTP Overview	229
Bridge Priority and the Root Bridge	230
Mixed STP and RSTP Networks	237
Spanning Tree and VLANs	237
Enabling or Disabling STP and RSTP	240
Configuring STP	242
Configuring STP Bridge Settings	242
Configuring STP Port Parameters	245
Displaying STP Port Settings	247
Configuring RSTP	248
Configuring RSTP Bridge Settings	248
Configuring RSTP Port Parameters	252
Displaying RSTP Port Configuration and Port State	254

Chapter 16

Multiple Spanning Tree Protocol (MSTP)	257
MSTP Overview	258
Multiple Spanning Tree Instance (MSTI)	259
VLAN and MSTI Associations	263
Multiple Spanning Tree Regions	263
Summary of Guidelines	268
Configuring MSTP	274
Enabling or Disabling MSTP	274
Configuring MSTP Bridge Settings	277
Configuring the CIST Priority	279
Creating, Deleting, and Modifying MSTI IDs	280
Associating VLANs to MSTI IDs	283
Configuring MSTP Port Settings	288
Displaying MSTP Port Settings and Status	290

Section III

SNMPv3 Protocol 292

Chapter 17

SNMPv3 Configuration	293
SNMPv3 Overview	294
SNMPv3 Authentication Protocols	295
SNMPv3 Privacy Protocol	296
SNMPv3 MIB Views	296
SNMPv3 Storage Types	297
SNMPv3 Message Notification	297
SNMPv3 Tables	298
SNMPv3 Configuration Example	303
Configuring the SNMPv3 Protocol	304
Configuring the SNMPv3 User Table	305
Creating an SNMPv3 User Table Entry	305
Deleting an SNMPv3 User Table Entry	309
Modifying an SNMPv3 User Table Entry	310
Configuring the SNMPv3 View Table	315
Creating an SNMPv3 View Table Entry	315
Deleting an SNMPv3 View Table Entry	318
Modifying an SNMPv3 View Table Entry	319
Configuring the SNMPv3 Access Table	324
Creating an SNMPv3 Access Table Entry	324
Deleting an SNMPv3 Access Table Entry	329
Modifying an SNMPv3 Access Table Entry	330
Configuring the SNMPv3 SecurityToGroup Table	340
Creating an SNMPv3 SecurityToGroup Table Entry	340
Deleting an SNMPv3 SecurityToGroup Table Entry	343
Modifying an SNMPv3 SecurityToGroup Table Entry	344
Configuring the SNMPv3 Notify Table	348
Creating an SNMPv3 Notify Table Entry	348
Deleting an SNMPv3 Notify Table Entry	350
Modifying an SNMPv3 Notify Table Entry	351
Configuring the SNMPv3 Target Address Table	355
Creating an SNMPv3 Target Address Table Entry	356
Deleting an SNMPv3 Target Address Table Entry	358
Modifying an SNMPv3 Target Address Table Entry	359
Configuring the SNMPv3 Target Parameters Table	368
Creating an SNMPv3 Target Parameters Table Entry	369
Deleting an SNMPv3 Target Parameters Table Entry	372
Modifying an SNMPv3 Target Parameters Table Entry	373
Configuring the SNMPv3 Community Table	381
Creating an SNMPv3 Community Table Entry	382
Deleting an SNMPv3 Community Table Entry	385
Modifying an SNMPv3 Community Table Entry	386
Displaying SNMPv3 Table Menus	391
Displaying the Display SNMPv3 User Table Menu	391
Displaying the Display SNMPv3 View Table Menu	393
Displaying the Display SNMPv3 Access Table Menu	394
Displaying the Display SNMPv3 SecurityToGroup Table Menu	395
Displaying the Display SNMPv3 Notify Table Menu	396
Displaying the Display SNMPv3 Target Address Table Menu	397

Displaying the Display SNMPv3 Target Parameters Table Menu	398
Displaying the Display SNMPv3 Community Table Menu	399
Section IV	
VLANs	400
Chapter 18	
Tagged and Port-based Virtual LANs	401
VLAN Overview	402
Port-based VLAN Overview	404
General Rules for Creating a Port-based VLAN	406
Drawbacks of Port-based VLANs	406
Port-Based Examples	408
Tagged VLAN Overview	412
General Rules for Creating a Tagged VLAN	414
Tagged VLAN Example	415
Basic VLAN Mode Overview	417
Displaying VLANs	418
Creating a Port-based or Tagged VLAN	421
Example of Creating a Port-Based VLAN	425
Example of Creating a Tagged VLAN	426
Modifying a VLAN	427
Deleting a VLAN	431
Setting a Switch's VLAN Mode	432
Specifying a Management VLAN	433
Chapter 19	
Multiple VLAN Modes	435
Multiple VLAN Mode Overview	436
802.1Q- Compliant Multiple VLANs Mode	437
Non-802.1Q Compliant Multiple VLANs	438
Multiple VLAN Modes and the Management VLAN	439
Selecting a VLAN Mode	440
Changing the Uplink Port	442
Displaying VLAN Information	443
Chapter 20	
GARP VLAN Registration Protocol	444
GARP VLAN Registration Protocol (GVRP) Overview	445
Guidelines	447
GVRP and Network Security	448
GVRP-inactive Intermediate Switches	448
Generic Attribute Registration Protocol (GARP) Overview	449
Configuring GVRP	453
Enabling or Disabling GVRP on a Port	455
Displaying GVRP Parameters and Statistics	458
GVRP Counters	459
GVRP Database	463
GIP Connected Ports Ring	464
GVRP State Machine	465

Section V

Security Features 468

Chapter 21

Port Security	469
Port Security Overview	470
Automatic	470
Limited	470
Secured	471
Locked	471
Security Violations and Intrusion Actions	472
Configuring Port Security	473

Chapter 22

Web Server	477
Web Server Overview	478
Protocols Supported	478
Configuring the Web Server for Security Features	479
Configuring SSL Certificates	481
Configuring Self-Signed Certificates	481
Configuring CA Certificates	482

Chapter 23

Encryption	484
Encryption Overview	485
Data Encryption	486
Symmetrical Encryption	486
Asymmetrical (Public Key) Encryption	487
Data Authentication	489
Key Exchange Algorithms	490
Configuring Keys for Encryption	491
Configuring a Distinguished Name and Keys	491
Modifying and Deleting Keys	495
Exporting Keys	497
Importing Keys	498

Chapter 24

Public Key Infrastructure (PKI)	501
Public Key Infrastructure Overview	502
Public Keys	502
Message Encryption	503
Digital Signatures	503
Certificates	503
Elements of a Public Key Infrastructure	504
Certificate Validation	505
Certificate Revocation Lists (CRLs)	506
PKI Implementation	507
PKI Standards	507
Certificate Retrieval and Storage	507
Configuring Certificates	508
Creating Certificates	508
Adding Certificates to the Database	513
Deleting and Modifying Certificates	515
Viewing Certificates	518
Generating Enrollment Requests	521

Chapter 25

Secure Sockets Layer (SSL)523
 Secure Sockets Layer Overview524
 SSL Encryption 525
 User Verification 525
 Authentication 526
 Support for SSL 526
 SSL and Enhanced Stacking 527
 Configuring SSL528

Chapter 26

Secure Shell (SSH)529
 SSH Overview530
 Support for SSH 530
 SSH Server 531
 SSH Clients 532
 SSH and Enhanced Stacking 532
 SSH Overall Configuration534
 Configuring SSH535
 Displaying SSH Information538

Chapter 27

TACACS+ and RADIUS Protocols540
 TACACS+ and RADIUS Overview541
 Enabling TACACS+ or RADIUS544
 Configuring TACACS+545
 Configuring RADIUS547

Chapter 28

802.1x Port-based Network Access Control549
 802.1x Port-based Access Network Control Overview550
 Authentication Process 551
 Port Roles 552
 Authentication Server555
 RADIUS Accounting 556
 Enabling and Disabling Port-based Access Control557
 Setting the Port Access Role559
 Configuring Authenticator Parameters561
 Configuring Supplicant Parameters565
 Configuring RADIUS Accounting568
 Displaying Port-based Access Control Status571
 Displaying Port Access Status 571
 Displaying Authenticator Ports 573
 Displaying Supplicant Ports 574

Section VI

Web Browser Management576

Chapter 29

Starting a Web Browser Management Session578
 Starting a Web Browser Management Session579
 Browser Tools 581
 Quitting a Web Browser Management Session 581

Chapter 30

Basic Switch Parameters	582
Configuring an IP Address and Switch Name	583
Setting the System Time	588
Setting Up SNTP	590
Activating the BOOTP and DHCP Services	591
Displaying System Information	592
Configuring SNMPv1 and SNMPv2c Protocols	595
Creating an SNMPv1 and SNMPv2c Community	595
Modifying an SNMPv1 and SNMPv2c Community	599
Deleting an SNMPv1 and SNMPv2c Community	601
Displaying the SNMPv1 and SNMPv2c Communities	601
Resetting a Switch	604
Pinging a Remote System	605
Returning the AT-S60 Software to the Factory Default Values	606

Chapter 31

File Downloads and Uploads	608
Downloading a File	609
Uploading a File	612

Chapter 32

Enhanced Stacking	614
Overview	615
Setting a Switch's Enhanced Stacking Status	616
Selecting a Switch in an Enhanced Stack	617

Chapter 33

Port Parameters	620
Configuring Port Parameters	621
Displaying Port Status and Statistics	626
Displaying Port Status	626
Displaying Port Statistics	630

Chapter 34

MAC Address Table	633
Displaying the MAC Address Table	634
Adding Static Unicast and Multicast MAC Addresses	637
Deleting MAC Addresses	639
Changing the Aging Time	640

Chapter 35

Port Trunking	641
Creating or Deleting a Port Trunk	642
Creating a Port Trunk	642
Deleting a Port Trunk	644
Modifying a Port Trunk	645
Displaying the Port Trunks	647

Chapter 36

Port Mirroring	648
Creating or Deleting a Port Mirror	649
Creating a Port Mirror	649
Deleting a Port Mirror	651
Modifying a Port Mirror	652
Displaying the Port Mirror List	654

Chapter 37

Event Log	655
Enabling or Disabling the Event Log	656
Displaying Events	658
Saving the Event Log	660
Clearing the Event Log	661

Chapter 38

IGMP Snooping	662
Configuring IGMP Snooping	663
Displaying a List of Host Nodes and Multicast Routers	666

Chapter 39

STP, RSTP, and MSTP	669
Enabling STP, RSTP, or MSTP	670
Configuring and Modifying STP	672
Configuring and Modifying RSTP	676
Configuring and Modifying MSTP	681
Configuring MSTP Parameters	681
Configuring the CIST Priority	684
Creating, Deleting, or Modifying MSTI IDs	685
Adding, Removing, or Modifying VLAN Associations to MSTIs	687
Configuring MSTP Port Parameters	689
Displaying STP, RSTP, or MSTP Settings	691

Chapter 40

SNMPv3 Protocol	694
Configuring the SNMPv3 Protocol	695
Enabling the SNMP Protocol	696
Configuring the SNMPv3 User Table	698
Creating a User Table Entry	698
Deleting a User Table Entry	701
Modifying a User Table Entry	702
Configuring the SNMPv3 View Table	705
Creating a View Table Entry	705
Deleting a View Table Entry	707
Modifying a View Table Entry	708
Configuring the SNMPv3 Access Table	710
Creating an Access Table	710
Deleting an Access Table Entry	714
Modifying an Access Table Entry	714
Configuring the SNMPv3 SecurityToGroup Table	717
Creating a SecurityToGroup Table Entry	717
Deleting a SecurityToGroup Table Entry	719
Modifying a SecurityToGroup Table Entry	720
Configuring the SNMPv3 Notify Table	722
Creating a Notify Table Entry	722
Deleting a Notify Table Entry	724
Modifying a Notify Table Entry	724
Configuring the SNMPv3 Target Address Table	727
Creating a Target Address Table Entry	727
Deleting a Target Address Table Entry	730
Modifying Target Address Table Entry	730
Configuring the SNMPv3 Target Parameters Table	733
Creating a Target Parameters Table Entry	733
Deleting a Target Parameters Table Entry	736

Modifying a Target Parameters Table Entry	737
Configuring the SNMPv3 Community Table	740
Creating an SNMPv3 Community Table Entry	740
Deleting an SNMPv3 Community Table Entry	743
Modifying an SNMPv3 Community Table Entry	743
Displaying SNMPv3 Tables	746
Displaying User Table Entries	747
Displaying View Table Entries	748
Displaying Access Table Entries	749
Displaying SecurityToGroup Table Entries	750
Displaying Notify Table Entries	751
Displaying Target Address Table Entries	752
Displaying Target Parameters Table Entries	753
Displaying SNMPv3 Community Table Entries	754
Chapter 41	
Port-based VLANs	755
Creating a Port Based VLAN	756
Modifying a Port-Based VLAN	760
Deleting a VLAN	762
Displaying VLANs	763
Setting the Switch's VLAN Mode	765
Chapter 42	
GARP VLAN Registration Protocol	766
Configuring GVRP	767
Resetting GVRP to the Defaults	769
Modifying the GVRP Port Configuration	770
Displaying the GVRP Settings	771
Displaying GVRP Port Configuration	771
Displaying the GVRP Counters	773
Displaying GVRP Database	776
Displaying GIP Connected Ports Ring	778
Displaying GVRP State Machine	779
Chapter 43	
Port Security	783
Displaying the Port Security Level	784
Chapter 44	
Web Server Security	787
Displaying the Encryption Keys	788
Displaying the PKI Settings	790
Displaying the SSL Settings	794
Chapter 45	
TACACS+ and RADIUS Protocols	796
Enabling TACACS+ or RADIUS	797
Configuring TACACS+	799
Configuring RADIUS	801
Displaying the TACACS+ Settings	803
Displaying the RADIUS Settings	805
Chapter 46	
802.1x Port-based Network Access Control	806
Configuring Port Access	807

Enabling Port-Based Access Control	807
Configuring RADIUS Accounting	809
Setting the Port Role	810
Configuring an Authenticator Port	811
Configuring a Supplicant Port	814
Displaying 802.1x Port-Based Access Control Information	816

Appendix A

AT-S60 Default Settings	820
Basic Switch Default Settings	821
File Menu Default Setting	821
Management Access Default Settings	821
Management Interface Default Settings	821
RS-232 Port Default Settings	822
SNTP Default Settings	822
Switch Administration Default Settings	823
System Software Default Settings	823
Enhanced Stacking Default Setting	824
Event Log Settings	825
IGMP Snooping Default Settings	826
PKI Default Settings	827
Port Configuration Default Settings	828
Port Security Default Settings	829
Server-Based Authentication Default Settings	830
Server-Based Authentication Default Settings	830
RADIUS Default Settings	830
TACACS+ Client Default Settings	830
SNMP Default Settings	831
SSH Default Settings	832
SSL Default Settings	833
STP, RSTP, and MSTP Default Settings	834
Spanning Tree Switch Settings	834
STP Default Settings	834
RSTP Default Settings	835
MSTP Default Settings	835
VLAN Default Settings	837
VLAN Default Settings	837
GARP and GVRP Default Settings	837
Web Server Default Settings	838
802.1x Port-Based Network Access Control Default Settings	839

Appendix B

SNMPv3 Configuration Examples	840
SNMPv3 Configuration Examples	841
SNMPv3 Manager Configuration	841
SNMPv3 Operator Configuration	842
SNMPv3 Worksheet	843
Index	846

List of Figures

Figure 1: Main Menu	35
Figure 2: Connecting a Terminal or PC to the RS-232 Terminal Port	40
Figure 3: AT-S60 Main Menu	41
Figure 4: Administration Menu	48
Figure 5: System Menu	51
Figure 6: Display Line Card Menu	52
Figure 7: Display Line Card Information Menu	52
Figure 8: Display Line Card Statistics Menu	53
Figure 9: Display System Menu	55
Figure 10: Display System Statistics Menu	56
Figure 11: Configure System Menu	59
Figure 12: Configure System Software Menu	60
Figure 13: Configure System Time Menu	60
Figure 14: Passwords Menu	65
Figure 15: Display System Hardware Information Menu	68
Figure 16: Display System Fan A Information Menu	69
Figure 17: Display System Software Information Menu	70
Figure 18: Enhanced Stacking Example	78
Figure 19: Enhanced Stacking Menu	80
Figure 20: Stacking Services Menu	81
Figure 21: Updated Stacking Services Menu	82
Figure 22: Configure SNMP Menu	87
Figure 23: Configure SNMPv1 & SNMPv2c Community Menu	89
Figure 24: Modify SNMPv1 & SNMPv2c Community Menu	93
Figure 25: Display SNMPv1 & SNMPv2c Community Menu	100
Figure 26: Port Menu	102
Figure 27: Port Status Menu	102
Figure 28: Port Configuration Menu	106
Figure 29: Port Statistics Menu	112
Figure 30: Display Port Statistics Menu	113
Figure 31: MAC Address Tables Menu	118
Figure 32: Display MAC Addresses Menu	118
Figure 33: Show All MAC Addresses Menu	119
Figure 34: Configure MAC Addresses Menu	122
Figure 35: Port Trunk Example with 1000 Mbps Ports	128
Figure 36: Port Trunk Example with 10/100 Mbps Ports	129
Figure 37: Trunk Configuration Menu	132

Figure 38: Modify Trunk Menu	136
Figure 39: Port Mirroring Menu	144
Figure 40: Modify Mirror Menu	146
Figure 41: File Menu	157
Figure 42: View Configuration File Menu (page 1)	160
Figure 43: View Configuration File Menu (page 2)	161
Figure 44: Display File(s) Menu	166
Figure 45: Downloads & Uploads Menu	169
Figure 46: Downloads & Uploads Menu	173
Figure 47: Transfer Menu	175
Figure 48: Send File Window	175
Figure 49: XModem File Send Window	176
Figure 50: Downloads & Uploads Menu	181
Figure 51: Transfer Menu	182
Figure 52: Send File Window	183
Figure 53: XModem File Send Window	184
Figure 54: Downloads & Uploads Menu	188
Figure 55: Transfer Menu	190
Figure 56: Receive File Window	190
Figure 57: Receive Filename Window	191
Figure 58: Xmodem File Receive Window	191
Figure 59: Downloads & Uploads Menu	194
Figure 60: Transfer Menu	197
Figure 61: Receive File Window	197
Figure 62: Receive Filename Window	197
Figure 63: Xmodem File Receive Window	198
Figure 64: Event Log Menu	205
Figure 65: Event Log Example	209
Figure 66: Configure IGMP Snooping Menu	221
Figure 67: Configure Multicast Router Ports Menu	223
Figure 68: View Multicast Hosts List Menu	224
Figure 69: View Multicast Routers List Menu	226
Figure 70: Point-to-Point Ports	235
Figure 71: Edge Port	236
Figure 72: Point-to-Point and Edge Point	237
Figure 73: VLAN Fragmentation	238
Figure 74: Spanning Tree Menu	240
Figure 75: STP Menu	243
Figure 76: STP Port Parameters Menu	245
Figure 77: Configure STP Port Settings Menu	246
Figure 78: Display STP Port Configuration Menu	247
Figure 79: RSTP Menu	249
Figure 80: RSTP Port Parameters Menu	252
Figure 81: Configure RSTP Port Settings Menu	253
Figure 82: Display RSTP Port Configuration Menu	255
Figure 83: Display RSTP Port State	256
Figure 84: VLAN Fragmentation with STP or RSTP	260
Figure 85: MSTP Example of Two Spanning Tree Instances	261
Figure 86: Multiple VLANs in a MSTI	262
Figure 87: Multiple Spanning Tree Region	265
Figure 88: CIST and VLAN Guideline - Example 1	270
Figure 89: CIST and VLAN Guideline - Example 2	271
Figure 90: Spanning Regions - Example 1	272
Figure 91: Spanning Tree Menu	275
Figure 92: MSTP Menu	277

Figure 93: CIST Menu	279
Figure 94: MSTI Menu	281
Figure 95: VLAN-MSTI Association Menu	285
Figure 96: MSTP Port Parameters Menu	288
Figure 97: Configure MSTP Port Settings Menu	289
Figure 98: MIB Tree	296
Figure 99: SNMPv3 User Configuration Process	299
Figure 100: SNMPv3 Message Notification Process	300
Figure 101: Configure SNMPv3 Table Menu	306
Figure 102: Configure SNMPv3 User Table Menu	307
Figure 103: Modify SNMPv3 User Table Menu	311
Figure 104: Configure SNMPv3 View Table Menu	316
Figure 105: Modify SNMPv3 View Table Menu	320
Figure 106: Configure SNMPv3 Access Table Menu	325
Figure 107: Modify SNMPv3 Access Table Menu	332
Figure 108: Configure SNMPv3 SecurityToGroup Table Menu	341
Figure 109: Modify SNMPv3 SecurityToGroup Table Menu	345
Figure 110: Configure SNMPv3 Notify Table Menu	349
Figure 111: Modify SNMPv3 Notify Table Menu	352
Figure 112: Configure SNMPv3 Target Address Table Menu	356
Figure 113: Modify SNMPv3 Target Address Table Menu	360
Figure 114: Configure SNMPv3 Target Parameters Table Menu	369
Figure 115: Modify SNMPv3 Target Parameters Table Menu	375
Figure 116: Configure SNMPv3 Community Table Menu	383
Figure 117: Modify SNMPv3 Community Table Menu	387
Figure 118: Display SNMPv3 Table Menu	392
Figure 119: Display SNMPv3 User Table Menu	392
Figure 120: Display SNMPv3 View Table Menu	393
Figure 121: Display SNMPv3 Access Table Menu	394
Figure 122: Display SNMPv3 SecurityToGroup Table Menu	395
Figure 123: Display SNMPv3 Notify Table Menu	396
Figure 124: Display SNMPv3 Target Address Table Menu	397
Figure 125: Display SNMPv3 Target Parameters Table Menu	398
Figure 126: Display SNMPv3 Community Table Menu	399
Figure 127: Port-based VLAN - Example 1	408
Figure 128: Port-based VLAN - Example 2	410
Figure 129: Example of a Tagged VLAN	415
Figure 130: VLAN Menu	418
Figure 131: Display VLAN Menu	418
Figure 132: Display Port Based VLAN Menu	419
Figure 133: Configure VLAN Menu	421
Figure 134: Configure Port Based VLAN Menu	422
Figure 135: Modify Port Based VLAN Menu	427
Figure 136: Display Port Based VLAN Menu	443
Figure 137: GVRP Example	446
Figure 138: GARP Architecture	450
Figure 139: GID Architecture	451
Figure 140: GARP-GVRP Menu	453
Figure 141: GVRP Port Parameters Menu	455
Figure 142: Configure GVRP Port Settings Menu	456
Figure 143: Display GVRP Port Configuration Menu	456
Figure 144: Other GARP Port Parameters Menu	458
Figure 145: GVRP Counters Menu (page 1)	459
Figure 146: GVRP Counters Menu (page 2)	460
Figure 147: GVRP Database Menu	463

Figure 148: GIP Connected Ports Ring Menu 464

Figure 149: GVRP State Machine Menu (page 1) 465

Figure 150: Display GVRP State Machine Menu (page 2) 465

Figure 151: Security Menu 473

Figure 152: Local Port Security Menu 473

Figure 153: Configure Port Security Menu 474

Figure 154: Configure Port Security Menu 475

Figure 155: Web Server Configuration Menu 479

Figure 156: Keys/Certificate Configuration Menu 492

Figure 157: Key Management Menu 493

Figure 158: Create Key Menu 494

Figure 159: Export Key to File Menu 497

Figure 160: Import Key From File Menu 499

Figure 161: Public Key Infrastructure (PKI) Configuration Menu 509

Figure 162: X509 Certificate Management Menu 510

Figure 163: Create Self-Signed Certificate Menu 511

Figure 164: Add Certificate Menu 514

Figure 165: Modify Certificate Menu 516

Figure 166: View Certificate Details Menu (page 1) 519

Figure 167: View Certificate Details Menu (page 2) 519

Figure 168: Generate Enrollment Request Menu 521

Figure 169: Secure Socket Layer (SSL) Menu 528

Figure 170: SSH Remote Management of a Slave Switch 533

Figure 171: Secure Shell (SSH) Menu 536

Figure 172: Show Server Information Menu 538

Figure 173: Authentication Menu 544

Figure 174: TACACS+ Client Configuration Menu 545

Figure 175: RADIUS Client Configuration Menu 547

Figure 176: RADIUS Server Configuration Menu 548

Figure 177: Example of Authenticator Role 553

Figure 178: Example of the Supplicant Role 554

Figure 179: Authentication Messaging Exchange 555

Figure 180: Port Access Control Menu 557

Figure 181: Configure Port Access Role Menu 560

Figure 182: Configure Authenticator Menu 562

Figure 183: Configure Authenticator Port Access Parameters Menu 563

Figure 184: Configure Supplicant Menu 566

Figure 185: Configure Supplicant Port Access Parameters Menu 566

Figure 186: Radius Accounting Menu 568

Figure 187: Display Port Access Status Menu 572

Figure 188: Display Authentication Port Access Parameters 574

Figure 189: Display Supplicant Port Access Parameters Menu 575

Figure 190: Entering a Switch’s IP Address in the URL Field 580

Figure 191: Home Page 580

Figure 192: Configuration System Page, General Tab 584

Figure 193: Configuration System Page, System Time Tab 588

Figure 194: Monitoring System Page, General Tab 592

Figure 195: Configuration System Page, SNMP Tab 596

Figure 196: SNMPv1 & SNMPv2c Communities Page 597

Figure 197: Add New SNMPv1 & SNMPv2c Community Page 598

Figure 198: Modify SNMPv1 & SNMPv2c Community Page 600

Figure 199: SNMP Monitoring Tab 602

Figure 200: Monitoring, SNMPv1 & SNMPv2c Communities Page 603

Figure 201: Monitoring System Page, Ping Client Tab 605

Figure 202: Configuration System Page, System Maintenance Tab 606

Figure 203: System Maintenance Tab	610
Figure 204: Configuration Layer 2 Page, Enhanced Stacking Tab	616
Figure 205: Enhanced Stacking Page	618
Figure 206: AT-S39 Home Page	619
Figure 207: Configuration Layer 1 Page, Port Settings Tab	621
Figure 208: Port Configuration Page	622
Figure 209: Monitoring Layer 1 Page, Port Settings Tab	626
Figure 210: Port Status Page	627
Figure 211: Port Statistics Page	631
Figure 212: Configuration Layer 2 Page, MAC Address Tab	634
Figure 213: MAC Address Table Page	635
Figure 214: Add MAC Address Page	637
Figure 215: Configuration Layer 1 Page, Port Trunking Tab	642
Figure 216: Add New Trunk Page	643
Figure 217: Modify Trunk Page	646
Figure 218: Monitoring Layer 1 Page, Port Trunking Tab	647
Figure 219: Configuration Layer 1 Page, Port Mirroring Tab	649
Figure 220: Add New Mirror Page	650
Figure 221: Modify Mirror Page	652
Figure 222: Monitoring Layer 1 Page, Port Mirroring Tab	654
Figure 223: Event Log Tab	656
Figure 224: Event Log Example	659
Figure 225: Configuration System Page, IGMP Tab	663
Figure 226: Monitoring System Page, IGMP Tab	666
Figure 227: View Multicast Hosts List Page	667
Figure 228: View Multicast Routers List Page	668
Figure 229: View (Static) Multicast Routers List Page	668
Figure 230: Configuration Layer 2 Page, Spanning Tree Tab	670
Figure 231: Expanded STP Spanning Tree Tab	673
Figure 232: STP Settings Page	675
Figure 233: Expanded RSTP Spanning Tree Tab	677
Figure 234: RSTP Settings Page	679
Figure 235: Expanded MSTP Spanning Tree Tab	682
Figure 236: Add New MSTI Page	685
Figure 237: Modify MSTI Page	686
Figure 238: MSTP Port Settings Page	689
Figure 239: Monitoring Layer 2 Page, Spanning Tree Tab	691
Figure 240: Monitoring Layer 2 Page, Spanning Tree Tab	692
Figure 241: STP Settings Page	693
Figure 242: Configuration System Page, SNMP Tab	696
Figure 243: SNMPv3 User Table Page	699
Figure 244: Add New SNMPv3 User Page	699
Figure 245: Modify SNMPv3 User Page	702
Figure 246: SNMPv3 View Table Page	705
Figure 247: Add New SNMPv3 View Page	706
Figure 248: Modify SNMPv3 View Page	708
Figure 249: SNMPv3 Access Table Page	710
Figure 250: Add New SNMPv3 Access Page	711
Figure 251: Modify SNMPv3 Access Page	715
Figure 252: SNMPv3 SecurityToGroup Table Page	717
Figure 253: Add New SNMPv3 SecurityToGroup Page	718
Figure 254: Modify SNMPv3 SecurityToGroup Page	720
Figure 255: SNMPv3 Notify Table Page	722
Figure 256: Add New SNMPv3 Notify Page	723
Figure 257: Modify SNMPv3 Notify Page	725

Figure 258: SNMPv3 Target Address Table Page 728

Figure 259: Add New SNMPv3 Target Address Table Page 728

Figure 260: Modify SNMPv3 Target Address Table Page 731

Figure 261: SNMPv3 Target Parameters Table Page 733

Figure 262: Add New SNMPv3 Target Parameters Table Page 734

Figure 263: Modify SNMPv3 Target Parameters Table Page 737

Figure 264: SNMPv3 Community Table Page 741

Figure 265: Add New SNMPv3 Community Table Page 741

Figure 266: Modify SNMPv3 Community Table Page 744

Figure 267: Monitoring, SNMPv3 User Table Page 747

Figure 268: Monitoring, SNMPv3 View Table Page 748

Figure 269: Monitoring, SNMPv3 Access Table Page 749

Figure 270: Monitoring, SNMPv3 SecurityToGroup Table Page 750

Figure 271: Monitoring, SNMPv3 Notify Table Page 751

Figure 272: Monitoring, SNMPv3 Target Address Table Page 752

Figure 273: Monitoring, SNMPv3 Target Parameters Table Page 753

Figure 274: Monitoring, SNMPv3 Community Table Page 754

Figure 275: Configuration Layer 2 Page, VLAN Tab 756

Figure 276: Port-Based VLANs Page 757

Figure 277: Add New VLAN Page 757

Figure 278: Modify VLAN Page 761

Figure 279: Monitoring Layer 2 Page, VLAN Tab 763

Figure 280: Monitoring, Port-Based VLANs Page 764

Figure 281: Configuration Layer 2 Page, GVRP Tab 767

Figure 282: GVRP Port Configuration Page 770

Figure 283: Monitoring Layer 2 Page, GVRP Tab 772

Figure 284: GVRP Port Configuration Page 773

Figure 285: GVRP Counters Page 774

Figure 286: GVRP Database Page 777

Figure 287: GVRP GIP Connected Ports Ring Page 778

Figure 288: GVRP State Machine Page 780

Figure 289: Monitoring Layer 2 Page, Port Security Tab 784

Figure 290: Security for Ports Page 785

Figure 291: Monitoring Security Page, Keys Tab 788

Figure 292: Monitoring Security Page, PKI Tab 791

Figure 293: Certificate Page 792

Figure 294: Monitoring Security Page, SSL Tab 794

Figure 295: Configuration System Page, Server-based Authentication Tab 797

Figure 296: TACACS+ Client Configuration Page 799

Figure 297: RADIUS Client Configuration Page 801

Figure 298: Monitoring System Page, Server-based Authentication Tab 803

Figure 299: TACACS+ Client Configuration Page 804

Figure 300: RADIUS Client Configuration Page 805

Figure 301: 802.1x Port Access Tab 808

Figure 302: Port Role Configuration Page 811

Figure 303: Authenticator Parameters Page 812

Figure 304: Supplicant Parameters Page 814

Figure 305: Monitoring, 802.1x Port Access Tab 816

Figure 306: Port Access Port Status Page 817

Figure 307: Authenticator Port Parameters Page 818

Figure 308: Supplicant Port Parameters Page 818

Preface

This guide contains instructions on how to configure an AT-8400 Series Switch using the AT-S60 management software. The Preface contains the following sections:

- ❑ How This Guide is Organized on page 22
- ❑ Document Conventions on page 24
- ❑ Where to Find Web-based Guides on page 25
- ❑ Contacting Allied Telesyn on page 26

Note

Within this manual, the AT-8400 Series Switch is often abbreviated as switch.

How This Guide is Organized

This manual is divided into the following six sections:

- ❑ Section I: Basic Features
- ❑ Section II: Advanced Features
- ❑ Section III: SNMPv3 Protocol
- ❑ Section IV: VLANs
- ❑ Section VI: Security Features
- ❑ Section VII: Web Browser Management

See the description of each section below.

Overview

The Overview chapter reviews the different ways that you can access the AT-S60 management software on a switch. In addition, it describes how to specify ports.

Section I: Basic Features

This section explains how to manage a switch from a local or a Telnet management session. The chapters in this section discuss basic features such as port configuration, MAC address configuration, and port trunking as well as many other features.

Section II: Advanced Features

The chapters in this section explain how to use advanced features such as file system configuration, file downloads and uploads, and the Event log to manage a switch from a local or Telnet management session.

Section III: SNMPv3

There is one chapter in this section that provides a description of the AT-S60 software implementation of the SNMPv3 protocol. In addition, it provides procedures that allow you to create and modify SNMPv3 users from a local or Telnet management session.

Section IV: Security Features

This section describes how to configure tagged and port-based VLANs, Multiple VLAN modes, and the GARP VLAN Registration Protocol (GVRP) from a local or Telnet management session.

Section V: Security Features

The chapters in this section describe how to configure the authentication and advanced security features. The authentication features, 802.1x Port Based Access Control as well as TACACS+ and RADIUS protocols appear in both the AT-S60 version 2.0.0 NE and 2.0.0 software. The Encryption Services, Public Key Infrastructure (PKI), Secure Socket Layer (SSL), and Secure Shell (SSH) features **only** appear in the AT-S60 version 2.0.0 software. The Web Server chapter contains features that appear in both versions of the software as well as features that only appear in the AT-S60 version 2.0.0 software.



Caution

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

Section IV: Web Browser Management

The chapters in this section explain how to manage a switch using a web browser, such as Microsoft Internet Explorer or Netscape Navigator, from a workstation on your network.

Document Conventions

This document uses the following conventions:



Warning

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



Caution

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

Where to Find Web-based Guides

The installation and user guides for all Allied Telesyn products are available in Portable Document Format (PDF) from on our web site at www.alliedtelesyn.com. You can view the documents on-line 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

AT-S60 Overview

This chapter describes the AT-S60 software functions, the types of sessions you can use to access the software, and the management access levels. This chapter contains the following sections:

- ❑ Overview on page 28
- ❑ Local Management Session on page 29
- ❑ Telnet Management Session on page 30
- ❑ Web Browser Management Session on page 31
- ❑ SNMP Management Session on page 32
- ❑ Management Access Levels on page 33
- ❑ Specifying Ports on page 34
- ❑ Specifying Time and Date on page 35

Overview

The AT-S60 management software is intended for the AT-8400 Series switch. The software is used to monitor and adjust a switch's operating parameters. Functions that you can perform with the software include:

- Enable and disable ports
- Configure port parameters, such as port speed and duplex mode
- Create virtual LANs (VLANs)
- Create port trunks and port mirrors
- Assign an Internet Protocol (IP) address and subnet mask
- Activate and configure the Spanning Tree Protocol (STP)
- Configure port security

The AT-S60 management software comes pre-installed on the AT-8401 management card with default settings for all operating parameters. If the default settings are adequate for your network, you can use the switch as an unmanaged switch simply by connecting the unit to your network (as explained in the hardware installation guide) and powering on the device.

Note

The default settings for the management software can be found in Appendix A, AT-S60 Default Settings on page 820.

To actively manage a switch, by changing or adjusting the operating parameters, you must access the switch's AT-S60 management software. The AT-S60 software has a menu interface that makes it very easy to use and a web interface for managing a switch with a web browser. In addition, you can use a command line interface to manage the switch, as explained in the *AT-S60 Management Software Command Line Interface User's Guide (PN 613-50401-00)*.

There are four different ways that you can access the management software on an AT-8400 switch. The methods are referred to as management sessions in this guide. They are:

- Local Management Session
- Telnet Management Session
- Web Browser Management Session
- SNMP Management Session

The following sections in this chapter briefly describe each type of management session. In addition, the following sections are provided:

- ❑ Management Access Levels on page 33
- ❑ Specifying Ports on page 34
- ❑ Specifying Time and Date on page 35

Local Management Session

To establish a local management session with an AT-8400 switch, connect a terminal (or a PC) with a terminal emulator program to the RS-232 Terminal port on the switch. This type of management session 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.

Once the session is started, a menu is displayed from which you can make selections to configure and monitor the switch. You can configure all of a switch's operating parameters from a local management session. The first time you assign an IP address to a switch, you must use a local connection.

Note

For instructions on starting a local management session, refer to Starting a Local Management Session on page 40.

Telnet Management Session

Any management workstation on your network that has the Telnet application protocol can be used to manage an AT-8400 switch. In this guide, this type of management session is referred to as a remote management session because you do not have to be in the same wiring closet as the switch you are managing. Instead, you can manage the switch from any workstation on the network that has the application protocol.

To establish a remote management session, you need to assign an Internet Protocol (IP) address to a switch. To establish a Telnet management session with a switch on a subnet, there must be at least one AT-8400 switch with an assigned IP address. Only one switch in a subnet needs to have an IP address. Once you have established a Telnet management session, you can use the enhanced stacking feature of the AT-S60 software to access all AT-8400 switches and all Allied Telesyn International switches with Enhanced Stacking capability.

Note

For further information on enhanced stacking, refer to Enhanced Stacking Overview on page 76.

Note

For instructions on how to start a Telnet management session, refer to Starting a Telnet Management Session on page 44.

A Telnet management session gives you complete access to all of a switch's operating parameters. You can perform nearly all the same functions from a Telnet management session as you can from a local management session. There are two configuration changes that can only be done with a local connection. The first time you assign an IP address to a switch, you must use a local connection. In addition, you must use a local connection to perform downloads using an xmodem connections.

Web Browser Management Session

You can also use a web browser to manage a switch. Using a web browser management session is also referred to as remote management, just like a Telnet management session. You can manage a switch from any workstation on your network that has a web browser.

Note

For instructions on starting this type of management session, refer to Starting a Web Browser Management Session on page 579.

SNMP Management Session

Another way to remotely manage the switch is with an SNMP management program. AT-S60 software supports the SNMPv1, SNMPv2c, and SNMPv3 protocols. You need to be very familiar with Management Information Base (MIB) objects to configure SNMP management.

The AT-S60 software supports the following MIBs:

- SNMP MIB-II (RFC 1213)
- Bridge MIB (RFC 1493)
- SNMPv3 (RFC 2571-6)
- User-based Security Model (USM) for SNMPv3 (RFC 2574)
- Interface Group MIB (RFC 2863)
- Ethernet MIB (RFC 1643)
- Remote Network MIB (RFC 1757)
- Allied Telesyn managed switch MIB

You must download the Allied Telesyn managed switch MIB files (atiChassisSwitch.mib and atiStackinginfo.mib) from the Allied Telesyn web site and compile the file with your SNMP program. For instructions on how to compile the MIB file with your SNMP program, refer to your SNMP management documentation.

For information about how to configure SNMP communities using a local or Telnet management session, see Chapter 5, SNMPv1 and SNMPv2c Configuration on page 84 and Chapter 17, SNMPv3 Configuration on page 293.

Note

SNMP management can use the enhanced stacking feature through the private MIB (atiStackinginfo.mib). See Chapter 5: Enhanced Stacking on page 75.

Management Access Levels

There are two levels of management access on an AT-8400 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. As an Operator, you cannot change any values.

To log in, you enter a login id of Manager or Operator and the appropriate password when you start an AT-S60 management session. For Manager access, enter the following at the prompts:

```
Login: manager  
password: friend
```

For Operator access, enter the following at the prompts:

```
Login: operator  
password: operator
```

The password is case-sensitive for both Manager and Operator access.

There are a total of 14 login sessions available using the local, Telnet, and web browser management sessions. However, you can have only one Manager session on the switch regardless of how you or others are accessing the switch. There are additional limitations for the different types of management sessions. The local and Telnet sessions allow a total of 10 active sessions. While a web browser management session, allows four active login sessions.

Specifying Ports

Many of the commands and parameters, in this manual involve specifying the port(s) on the switch. Port numbers are specified in the following format:

```
slot.port
```

Slot is the number of the slot in the switch that contains the line card. There are twelve line card slots in the AT-8400 chassis. Port is the port number on the line card. For example, to indicate port 4 on the line card in Slot 8, enter:

```
8.4
```

In many commands, you can specify a list of ports. You can list ports on the same line card individually, as a range, or both. The following example refers to Ports 1, 3, and 5 through 8 on the line card in Slot 3:

```
3.1,3,5-8
```

Some commands can be performed on ports on different line cards. The following example refers to Ports 1 and 4 on the line card in Slot 4 and Ports 6 through 8 on the line card in Slot 11:

```
4.1,4,11.6-8
```

Specifying Time and Date

The Simple Network Time Protocol (SNTP) feature places the time and date on the local and telnet interfaces. The time and date appear in the upper right hand corner of the menu. See Figure 1.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
                          High School Switch 142
User: Manager                                00:14:33 15-Feb-2004
                          Main Menu
1 - Port Menu
2 - VLAN Menu
3 - Spanning Tree Menu
4 - Administration Menu
5 - System Menu
6 - Security Menu
7 - MAC Address Tables
8 - Enhanced Stacking
9 - File Menu
C - Command Line Interface
Q - Quit
Enter your selection?
```

Figure 1 Main Menu

When you access remote switches using the enhanced stacking feature, the time and date set by the local switch appears. It is possible for a local switch and a remote switch to display different time stamps. For example, if you are using a switch in one time zone it displays the local time. If you access a remote switch which is located in a different time zone, the time on that switch reflects local time.

For information about how to configure the time and date, see Setting the System Time on page 59.

Section I

Basic Features

The chapters in Section I explain how to manage an AT-8400 switch from a local or Telnet management session. It includes the following chapters.

- ❑ Chapter 2: Starting a Local or Telnet Management Session on page 38
- ❑ Chapter 3: Basic Switch Parameters on page 45
- ❑ Chapter 4: Enhanced Stacking on page 75
- ❑ Chapter 5: SNMPv1 and SNMPv2c Configuration on page 84
- ❑ Chapter 6: Port Parameters on page 101
- ❑ Chapter 7: MAC Address Table on page 115
- ❑ Chapter 8: Port Trunking on page 127
- ❑ Chapter 9: Port Mirroring on page 142

Chapter 2

Starting a Local or Telnet Management Session

This chapter contains the procedure for starting a local or Telnet management session on an AT-8400 Series switch. It contains the following sections:

- ❑ Local Management Session on page 39
- ❑ Telnet Management Session on page 43

Local Management Session

To establish a local management session using the AT-S60 management software, connect an RS-232 straight-through cable to the RS-232 terminal port on the AT-8400 chassis. Connect the other end of the cable to a terminal or a PC with a terminal emulator program.

A local management session is so named because you must be physically close to the switch, usually within a few meters, to start this type of management session. A local management session requires you to connect a terminal directly to the switch. Typically, this means that you are in the wiring closet where the switch is located.

A switch does not need an IP address to be managed from a local management session. You can start a local management session at any time on any AT-8400 switch in your network. Running a local management session does not interfere with the flow of Ethernet traffic through the unit.

Starting a local management session on a switch that has been configured as a Master switch of an enhanced stack allows you to manage all the switches in the subnet from the same local management session. You do not have to start a separate local management session for each switch. This can simplify network management.

There are a total of 14 login sessions available using the local, Telnet, and web browser management sessions. However, you can have only one Manager session on the switch regardless of how you or others are accessing the switch. There are additional limitations for the different types of management sessions. The local and Telnet sessions allow a total of 10 active sessions. While a web browser management session, allows four active login sessions.

Note

For information on enhanced stacking, refer to Enhanced Stacking Overview on page 76.

Starting a Local Management Session

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

1. Connect one end of a straight-through RS-232 cable with a DB-9 connector to the RS-232 terminal port. See Figure 2.

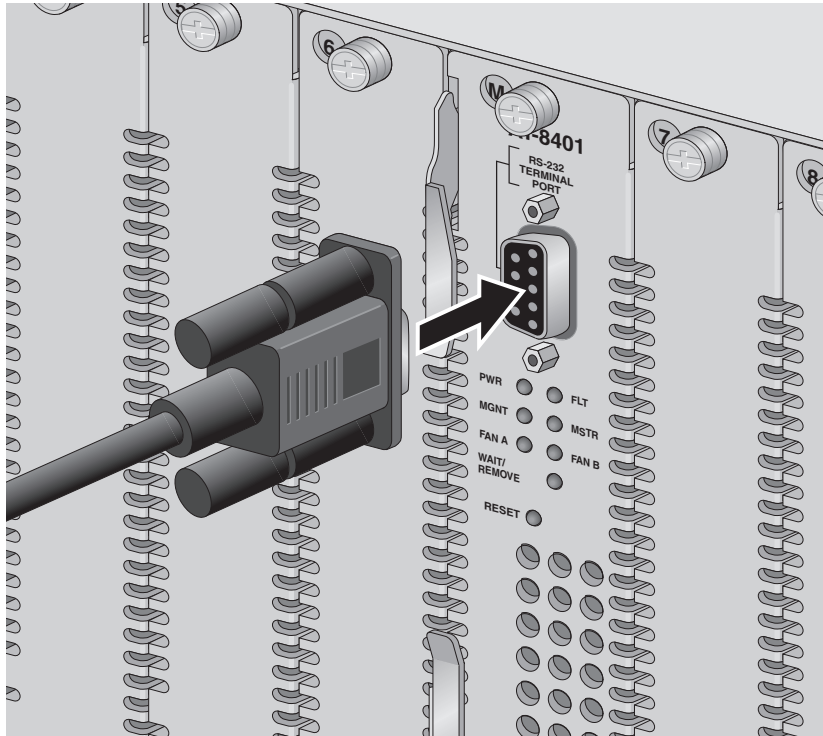


Figure 2 Connecting a Terminal or PC to the RS-232 Terminal Port

2. Connect the other end of the cable to an RS-232 port on a terminal or PC with a terminal emulator program.
3. Configure the terminal or terminal emulator program as follows:
 - Baud rate: 9600 bps (default)
 - Data bits: 8
 - Parity: None
 - Stop bits: 1
 - Flow control: None

Note

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

4. Press the Return key twice.
5. You are prompted to input a login id and password.

When prompted for the user name and password, enter one of the following options.

- For Manager access, type **manager** as the login id. The default password is "friend." Then press Return.
- For Operator access, type **operator** as the login id. The default password is "operator." Then press Return.

Note

The user names cannot be changed. The passwords are case sensitive. For instructions on how to change a password, refer to Configuring the Management Passwords on page 65. For information on the two access levels, refer to Management Access Levels on page 33.

The Main Menu is shown in Figure 3.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
High School Switch 142

User: Manager                                00:14:33 15-Jan-2004

Main Menu

1 - Port Menu
2 - VLAN Menu
3 - Spanning Tree Menu
4 - Administration Menu
5 - System Menu
6 - Security Menu
7 - MAC Address Tables
8 - Enhanced Stacking
9 - File Menu

C - Command Line Interface
E - Event Log
Q - Quit

Enter your selection?

```

Figure 3 AT-S60 Main Menu

To select a menu item, type the corresponding letter or number.

Pressing the Esc key or typing the letter **R** returns you to the previous menu.

Please note the following:

- ❑ The Command Line Interface selection in the Main Menu is not described in this manual. For instructions on this option, refer to the *AT-S60 Management Software Command Line Interface User's Guide (PN 613-50401-00)*.
- ❑ If a pound sign (#) or dollar sign (\$) is displayed instead of the Main Menu, the local interface has been configured for a command line prompt when a management session is started. The pound sign means that you logged in as the Manager and the dollar sign means you logged in as an Operator. To display the Main Menu, type **menu** and press Return.
- ❑ During boot up, the switch displays the following message:
Press any key to stop image loading and go to Boot Prompt. This message is for manufacturing purposes only. If you do inadvertently display the boot prompt (=>), type **boot** and press Return to start the switch's software.

Enhanced Stacking

When you start a management session on an AT-8400 (or an Allied Telesyn switch that supports Enhanced Stacking) that has been designated as the Master switch of an enhanced stack, you can manage all the switches in the same subnet from one management session. This can save you time because you do not have to start a separate local management session each time you want to manage each switch in your network. It can also save you from having to go to the individual wiring closets where the switches are located.

For information on enhanced stacking and how to manage different switches from the same management session, refer to **Chapter 2**, Enhanced Stacking on page 75.

Quitting from a Local Session

To quit a local session, return to the Main Menu and type **Q** for Quit.

Allied Telesyn recommends that you exit from a management session when you are finished managing a switch. This can prevent unauthorized individuals from making changes to a switch's configuration should you leave your management station unattended.

Note

The AT-S60 management software automatically ends a management session if it does not detect any activity from the local management station after the specified period of time. The default value of the local timeout is 10 minutes. To change this setting, refer to Configuring the AT-S60 Software Security Features on page 64.

Telnet Management Session

You can use the Telnet application protocol from a workstation on your network to manage an AT-8400 switch. This type of management is referred to as remote management because you can be physically far from the switch when you start the session. (In contrast to a local management session, which requires that you connect a terminal directly to the switch.) Any workstation on your network that has the Telnet application protocol can be used to manage the switch.

In terms of functionality, there are almost no differences between managing a switch locally through the RS-232 Terminal Port and remotely with the Telnet application protocol. You see the same menu selections and have nearly the same management capabilities. However, there are two configuration changes that can only be done with a local connection. The first time you assign an IP address to a switch, you must use a local connection. In addition, you must use a local connection to perform downloads with a xmodem connection.

Starting a Telnet management session requires that there be at least one AT-8400 Series switch on your network that has an IP address. The switch with the IP address is referred to as the master switch. Once you have started a Telnet management session on the master switch, you have management access to all the other AT-8400 Series switches as well as all the Allied Telesyn switches that reside in the same subnet.

There are a total of 14 login sessions available using the local, Telnet, and web browser management sessions. However, you can have only one Manager session on the switch regardless of how you or others are accessing the switch. There are additional limitations for the different types of management sessions. The local and Telnet sessions allow a total of 10 active sessions. While a web browser management session, allows four active login sessions.

Note

For background information on enhanced stacking, refer to Enhanced Stacking Overview on page 76.

Starting a Telnet Management Session

To start a Telnet management interface, specify the IP address of the Master switch of the stack in the Telnet application protocol.

When prompted for the user name and password, enter one of the following options.

- For Manager access, type **manager** as the user name. The default password is "friend."
- For Operator access, type **operator** as the user name. The default password is "operator."

Note

The user names cannot be changed. The passwords are case sensitive. For instructions on how to change a password, refer to Configuring the Management Passwords on page 65. For information on the two access levels, refer to Management Access Levels on page 33.

The Main Menu of a Telnet management interface is the same menu that you see in a local management interface, shown in Figure 3 on page 41. Nearly all the functions from a local management interface are available to you from a Telnet management interface.

The menus also function in the same manner. To make a selection, type its corresponding number or letter. To return to a previous menu, type **R** or press the Esc key.

Quitting from a Telnet Management Interface

To end a Telnet management interface, return to the Main Menu and type **Q** for Quit.

Note

The AT-S60 management software automatically ends a management session if it does not detect any activity from the remote management station after the specified period of time. The default for the Telnet timeout value is 10 minutes. To change this setting, refer to Configuring the AT-S60 Software Security Features on page 64.

Chapter 3

Basic Switch Parameters

This chapter contains a variety of information about basic switch parameters and procedures for using them with a local or Telnet management session.

This chapter contains the following sections:

- Assigning an IP Address to a Switch on page 46
- Configuring an IP Address and Switch Name on page 48
- Displaying and Clearing Line Card Information on page 51
- Displaying and Clearing System Information on page 55
- Activating the BootP and DHCP Services on page 57
- Setting the System Time on page 59
- Rebooting a Switch on page 63
- Configuring the AT-S60 Software Security Features on page 64
- Displaying the AT-S60 Hardware and Software Information on page 68
- Pinging a Remote System on page 71
- Returning the AT-S60 Software to the Factory Default Values on page 72
- Configuring the Console Startup Mode on page 74

Assigning an IP Address to a Switch

When building or expanding your network, you need to decide which managed switches need unique IP addresses. The rule used to be that a managed switch needed an IP address if you wanted to manage it remotely, such as with the Telnet application protocol. However, if a network contained a lot of managed switches, assigning each one an IP address was often cumbersome and time consuming. Also, it was often difficult keeping track of all the IP addresses.

The enhanced stacking feature of the AT-8400 switch simplifies when to assign an IP address. With enhanced stacking, you need assign an IP address to only one AT-8400 or other Allied Telesyn switch that supports enhanced stacking, for each subnet in your network. The switch with the IP address is referred to as the Master switch of the subnetwork. All switches in the same subnet share the IP address.

Starting a local or remote management session on the Master switch automatically gives you complete management access to all the other switches in the same subnet.

This feature has two primary benefits. First, it helps reduce the number of IP addresses you have to assign to your network devices. Second, it allows you to configure multiple switches through the same local or remote management session.

If your network consists of multiple subnets, you must assign a unique IP address to at least one switch in each subnet. The switch with the IP address is the Master switch of that subnet.

Note

For further information on enhanced stacking, refer to Enhanced Stacking Overview on page 76.

When you assign a switch an IP address, you must also assign it a subnet mask. The switch uses the subnet mask to determine which portion of an IP address represents the network address and which portion represents the node address.

You must also assign the switch a gateway address if there is a router between the switch and the remote management workstation. This gateway address is the IP address of the router through which the switch and management station communicate.

If you do not plan to remotely manage any of the AT-8400 switches in your network, then you do not need to assign an IP address to any of them. The switches operate fine without an IP address and you are still able to manage them completely using the local management interface.

How Do You Assign an IP Address?

Once you have decided which, if any, switches on your network need an IP address, you have to access the AT-S60 software on the switches and assign the address or addresses. There are actually two ways in which you can assign a switch an IP address.

The first method is to assign the IP configuration information manually. This method is explained in the next procedure, *Configuring an IP Address and Switch Name* on page 48. Initially, assigning an IP address to a switch can only be done through a local management session.

The second method is to activate the BOOTP and DHCP services on the switch and have the switch automatically download its IP configuration information from a BOOTP or DHCP server on your network. This procedure is explained in *Activating the BootP and DHCP Services* on page 57.

Configuring an IP Address and Switch Name

The procedure in this section explains how to manually assign an IP address, subnet mask, and gateway address to the switch using a local or Telnet management session. Initially, it must be done from the local management interface. (If you want the switch to obtain its IP configuration from a DHCP or BOOTP server on your network, go to the procedure Activating the BootP and DHCP Services on page 57.)

In addition, this procedure explains how to assign a name to the switch, along with other optional information, such as the name of the administrator responsible for maintaining the unit and the location of the switch.

To manually set a switch's IP address, perform the following procedure:

1. From the Main Menu, type **4** to select Administration Menu.

The Administration Menu is shown in Figure 4.

```
Allied Telesyn AT-8400 Series - AT-S60 V2.1.0
Engineering Switch 142

User: Manager                                00:14:33 15-Jan-2004

Administration Menu

1 - IP Address ..... 0.0.0.0
2 - Subnet Mask ..... 0.0.0.0
3 - Default Gateway ..... 0.0.0.0
4 - System Name .....
5 - Administrator .....
6 - Comments .....
7 - Set Password .....
8 - BOOTP/DHCP ..... Disabled
9 - Set Console Baud Rate .... 9600 bps

B - Reboot the switch
D - Downloads & Uploads
P - Ping a remote system

R - Return to Previous Menu

Enter your selection?
```

Figure 4 Administration Menu

2. Change the parameters as desired.

The parameters in the Administrative Menu are described below:

1 - IP Address

This parameter specifies the IP address of the switch. You must specify an IP address if you intend to remotely manage the switch using a web browser, a Telnet utility, or an SNMP management program, or if you want a switch to function as the Master switch of an enhanced stack.

2 - 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.

3 - 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.

4 - System Name

This parameter specifies a name for the switch (for example, Sales Ethernet switch). This parameter is optional.

Note

Allied Telesyn International recommends that you assign each switch a name because names help you identify the various switches when you manage them. In addition, switch names help you avoid performing a configuration procedure on the wrong switch.

5 - Administrator

This parameter specifies the name of the network administrator responsible for managing the switch. This parameter is optional.

6 - Comments

This parameter specifies additional information about the Fast Ethernet switch, such as its location (for example, 4th Floor - wiring closet 402B). This parameter is optional.

7 - Set Password

This parameter is used to change the Manager and Operator's login passwords. For instructions, refer to *Configuring the Management Passwords* on page 65.

8 - BOOTP/DHCP

This selection activates and deactivates the BOOTP and DHCP services on the switch. For information on this selection, refer to **Activating the BootP and DHCP Services** on page 57.

9 - Set Console Baud Rate

This selection allows you set the baud rate of the serial port on the AT-8401 management card. The range is 2400 to 115,200 bps. This menu selection is only available from a local management session. The default is 9600 bps.

B - Reboot the switch

This selection allows you to reboot the switch without affecting the saved configuration on the switch.

D - Downloads & Uploads

For information on this selection, refer to Chapter 11, File Downloads and Uploads on page 167.

R - Ping a Remote System

For information on this selection, refer to Pinging a Remote System on page 71.

3. After you have set the parameters, type **R** to return to the Main Menu. Then type **S** to select Save Configuration Changes.

Always be sure to save your changes. Unsaved changes are lost if you reset or power cycle the switch.

Changes to any of the parameters on this menu, including the IP address, subnet mask, or gateway address, are immediately activated on a switch.



Caution

Every time you save your changes on the switch, a message advising you to refrain from resetting the device for 15 seconds is displayed. This message applies only if you actually intend to reset or power cycle the device, a task that does not need to be performed for most management procedures. The warning is there in the rare circumstance where you do intend to reset the device after making a change. The switch may take up to 15 seconds to save the change to flash. Resetting the switch too soon might cause the change to be lost.

Displaying and Clearing Line Card Information

This section describes how to display line cards installed in an AT-8400 switch. The following procedures are provided:

- Displaying Line Card Information on page 51
- Displaying Line Card Statistics on page 53
- Clearing Line Card Statistics on page 54

Displaying Line Card Information

Use this procedure to display the line cards and the AT-8401 management card, installed in your AT-8400 chassis. Naturally, this procedure is very useful if your chassis is in a remote location and you need to know what cards are installed in the chassis.

To display the current line card configuration, perform the following procedure:

1. From the Main Menu, type **5** to select System Menu.

The System Menu is shown in Figure 5.

```

Allied Telesyn AT-8400 Series - AT-S60 V2.1.0
Engineering Switch 14
User: Manager                                00:14:33 15-Jan-2004
System Menu

1 - Configure System
2 - Display System
3 - Display Line Card

R - Return to Previous Menu

Enter your selection?

```

Figure 5 System Menu

2. From the System Menu, type **3** to select Display Line Card.

The Display Line Card Menu is shown in Figure 6.

```

Allied Telesyn AT-8400 Series - AT-S60 V2.1.0
Engineering Switch 14
User: Manager                                00:14:33 15-Jan-2004
Display Line Card

1 - Display Line Card Information
2 - Display Line Card Statistics
3 - Clear Line Card Statistics

R - Return to Previous Menu

Enter your selection?
    
```

Figure 6 Display Line Card Menu

- From the Display Line Card Menu, type **1** to select Display Line Card Information.

The Display Line Card Information Menu is shown in Figure 7.

```

Allied Telesyn AT-8400 Series - AT-S60 V2.1.0
Engineering Switch 14
User: Manager                                00:14:33 15-Jan-2004
Display Line Card Information

Line Card   Serial Number      Model Name      Temperature      Threshold
              (C Degree)         (C Degree)
=====
SCP          A00501S03040001G   AT-8401         36                80
1            S05525A023600007   AT-8411         36                80
2            S05525A023600001   AT-8411         36                80
3            S05525A023600102   AT-8411         36                80
4            S05525A023600011   AT-8414/ST      36                80
7            S05525A023600019   AT-8414/SC      36                80
8            S05525A023600001   AT-8413         36                80
9            S05525A023600201   AT-8413         36                80

U - Update Display
R - Return to Previous Menu

Enter your selection?
    
```

Figure 7 Display Line Card Information Menu

The SCP entry represents the AT-8401 management card which is installed in slot M of the chassis.

- Select **U** - Update the Display to update the display after you have installed or removed line cards from your chassis.

Displaying Line Card Statistics

To display the current line card statistics, perform the following procedure:

1. From the Main Menu, type **5** to select System Menu.
The System Menu is displayed in Figure 5 on page 51.
2. From the System Menu, type **3** to select Display Line Card.
The Line Card Menu is displayed in Figure 6 on page 52.
3. From the Line Card Menu, type **2** to select Display Line Card Statistics.
The following prompt appears:

```
Enter line card-list:
```

4. Type the slot number of the line card in the chassis. Then press Return.
To enter a list of line cards, separate the line card numbers with a comma. For example, to list statistics for line cards 4, 6, and 9, enter:

```
4,6,9
```

The Display Line Card Statistics Menu is shown in Figure 8.

```

Allied Telesyn AT-8400 Series - AT-S60 V2.1.0
Engineering Switch 14

User: Manager                                00:14:33 15-Jan-2004
Display Line Card Statistics

Line Card 4

Bytes Received ..... 983409801           Bytes Sent ..... 965734443
Frames Received ..... 815423             Frames Sent ..... 691396
Broadcast Frames Received.... 107774     Broadcast Frames Sent .. 1853
Multicast Frames Received .... 11429     Multicast Frames Sent .. 0
Total Bytes Received ..... 983511361     Jabber ..... 0
Total Frames Received ..... 815518       CRC Error ..... 0
Frames 64 Bytes ..... 110509             Fragments ..... 0
Frames 65-127 Bytes ..... 15192         Collision ..... 23
Frames 128-255 Bytes..... 1928          Late Collision ..... 0
Frames 256-511 Bytes ..... 442          Dropped Frames ..... 0
Frames 512-1023 Bytes ..... 157796     UnderSize Frames ..... 0
Frames >1024 Bytes ..... 1221024       OverSize Frames ..... 0

N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 8 Display Line Card Statistics Menu

5. To update the menu with the latest statistics, type **U**.

Clearing Line Card Statistics

To clear the current line card statistics, perform the following procedure:

1. From the Main Menu, type **5** to select System Menu.
The System Menu is shown in Figure 5 on page 51.
2. From the System Menu, type **3** to select Display Line Card.
The Display Line Card Menu is shown in Figure 6 on page 52.
3. Type **3** to select Clear Line Card Statistics.
The following prompt is displayed:
Enter Line card-list:
4. Type the slot number of the line card in the chassis. Then press Return.
To enter a list of line cards, separate the line card numbers with a comma. For example, to clear statistics on line cards 4, 6, and 9, enter:
4,6,9
The line card statistics are cleared.

Displaying and Clearing System Information

This section describes how to display and clear the system information for an AT-8400 switch. See the following procedures:

- Displaying System Information on page 55
- Clearing System Statistics on page 56

Displaying System Information

To display the system information, perform the following procedure.

1. From the Main Menu, type **5** to select System Menu.
The System Menu is shown in Figure 5 on page 51.
2. From the System Menu, type **2** to select Display System.
The Display System Menu is shown in Figure 9.

```

Allied Telesyn AT-8400 Series - AT-S60 V2.1.0
Engineering Switch 14
User: Manager                                00:14:33 15-Jan-2004
Display System

1 - Display System Software Information
2 - Display System Hardware Information
3 - Display System Statistics
4 - Clear System Statistics

R - Return to Previous Menu

Enter your selection?

```

Figure 9 Display System Menu

3. From the Display System Menu, type **3** to select Display System Statistics.

The Display System Statistics Menu is shown in Figure 10.

```
Allied Telesyn AT-8400 Series - AT-S60 V2.1.0
Engineering Switch 14

User: Manager                                00:14:33 15-Jan-2004

Display System Statistics

Bytes Received.....41631    Bytes Sent.....1037
Frames Received.....499     Frames Sent.....11
Broadcast Frames Received..351  Broadcast Frames Sent..1
Multicast Frames Received..136  Multicast Frames Sent..0
Total Bytes Received.....41631  Jabber.....0
Total Frames Received.....499   CRC Error.....0
Frames 64 Bytes.....324       Fragments.....0
Frames 64-127 Bytes.....161    Collision.....0
Frames 128-255 Bytes.....11    Late Collision.....0
Frames 256-511 Bytes.....14    Dropped Frames.....0
Frames 512-1023 Bytes.....0    UnderSize Frames.....0
Frames > 1024 Bytes.....0     OverSize Frames.....0

U - Update Display
R - Return to Previous Menu

Enter your selection?
```

Figure 10 Display System Statistics Menu

Clearing System Statistics

To clear the system statistics, perform the following procedure:

1. From the Main Menu, type **5** to select System Menu.
The System Menu is shown in Figure 5 on page 51.
2. From the System Menu, type **2** to select Display System.
The Display System Menu is shown in Figure 9 on page 55.
3. From the Display System Menu, type **4** to select Clear System Statistics.
The system statistics are reset or cleared.

Activating the BootP and DHCP Services

The BootP and DHCP application protocols were developed to simplify network management. They are used to automatically assign IP configuration information—such as an IP address, subnet mask, and a default gateway address—to the devices on your network.

An AT-8400 switch supports these protocols and can obtain its IP configuration information from a BootP or DHCP server on your network. If you activate this feature, the switch seeks its IP address and other IP configuration information from a BootP or DHCP server on your network whenever you reset or power cycle the switch.

Naturally, for this to work there must be a BootP or DHCP server residing on your network and you must configure the service by entering in the switch's MAC address. The MAC address is located on a sticker on the power supply cover (on the front of the chassis).

BootP and DHCP services typically allow you to specify how the IP address is assigned to the switch. The choices are static and dynamic. If you choose static, the server always assigns the same IP address to the switch when the switch is reset or powered ON. This is the preferred configuration. Because the BootP and DHCP services always assigns the same IP address to a switch, you know which IP address to use when you need to remotely manage a particular switch.

If you specify the IP address as dynamic, the server assigns the switch any unused IP address. As a result, a switch might have a different IP address each time you reset or power cycle the device, making it difficult for you to remotely manage the unit.

Note

By default, the BootP and DHCP option is disabled on the switch.

To activate or deactivate the BootP and DHCP protocols on the switch, perform the following procedure:

1. From the Main Menu, type **4** to select Administration Menu.
The Administration Menu is displayed in Figure 4 on page 48.
2. From the Administration Menu, type **8** to select BOOTP/DHCP.
The following prompt is displayed:
`BOOTP/DHCP (E-Enabled, D-Disabled):`
3. Type **E** to enable BOOTP and DHCP services on the switch or **D** to disable the services. Then press Return. The default is disabled.

Note

If you activate BOOTP/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.

4. After making changes, type **R** to return to the Main Menu. Then type **S** to select Save Configuration Changes.

Setting the System Time

To set system time on the switch, configure the Simple Network Time Protocol (SNTP). This feature allows you to synchronize computer clocks on the Internet by specifying the difference between local time and Universal Coordinated Time (UTC). You can either set the system time manually every time you boot the switch or you can set the system time with an SNTP server.

SNTP is a reduced version of the Network Time Protocol (NTP). However, it is important to note that SNTP servers and clients are interoperable with NTP servers and clients.

Note

If SNTP is disabled, or you have not configured an SNTP server, the system time defaults to midnight of January 1, 1970.

Use the following procedure to configure the system date and time for your switch.

1. From the Main Menu, type **5** to select System Menu.
The System Menu is shown in Figure 5 on page 51.
2. From the System Menu, type **1** to select Configure System.
The Configure System Menu is shown in Figure 11.

```

Allied Telesyn AT-8400 Series - AT-S60 V2.1.0
Engineering Switch 142

User: Manager                                00:14:33 15-Jan-2004

                                Configure System

1 - Configure System Software
2 - Configure System Hardware

R - Return to Previous Menu

Enter your selection?

```

Figure 11 Configure System Menu

3. From the Configure System Menu, type **1** - Configure System Software.

The Configure System Software Menu is displayed in Figure 12.

```
Allied Telesyn AT-8400 Series - AT-S60 V2.1.0
Engineering Switch 142

User: Manager                                00:14:33 15-Jan-2004

Configure System Software

1 - Switch Mode ..... Tagged
2 - Console Disconnect Timer Interval ..... 10 minute(s)
3 - MAC address aging time ..... 300 second(s)
4 - Console Startup Mode ..... Menu
5 - Telnet Server ..... Enabled

6 - Configure Web Server
7 - Configure IGMP Snooping
8 - Configure SNMP
9 - Configure System Time

D - Reset to Factory Defaults
R - Return to Previous Menu

Enter your selection?
```

Figure 12 Configure System Software Menu

- 4. From the Configure System Software Menu, type **9** - Configure System Time.

The Configure System Time Menu is shown in Figure 13.

```
Allied Telesyn AT-8400 Series - AT-S60 V2.1.0
High School Switch 142

User: Manager                                00:05:38 01-Jan-1970

Configure System Time

1 - System Time..... 00:05:38 on 01-Jan-1970
2 - SNTP Status ..... Disabled
3 - SNTP Server ..... 0.0.0.0
4 - UTC Offset ..... +0
5 - Daylight Savings Time (DST)... Enabled
6 - Poll Interval ..... 600 Seconds
7 - Last Delta ..... +0 Seconds

U - Update System Time
R - Return to Previous Menu

Enter your selection?
```

Figure 13 Configure System Time Menu

5. Type **1** - System Time to manually set the time and date for the switch. To set system time with an SNTP server, go to step 8.

The following prompt is displayed:

```
Enter new system time [hh:mm:ss] ->
```

6. Enter a new time for the system.

To specify time for the switch, use a 24-hour clock (or military time). Use the following format: hours, minutes, and seconds. Separate each unit of time with a colon. For example, enter 17:20:00 for 5:20 PM.

The following prompt is displayed:

```
Enter new system date [dd-mm-yyyy] ->
```

7. Enter a new date for the system.

Use two numbers to specify the day and month. Use four numbers to specify the year. Separate each value with a hyphen. For example, enter September 5, 2003 as 05-09-2003.

8. Type **2** - SNTP Status to enable or disable the SNTP client.

The following prompt is displayed:

```
SNTP Status (E-Enabled, D-Disabled) ->
```

9. Select one of the following and press Return:

Type **E** (for Enabled) to allow the switch to query a NTP or SNTP server at the specified polling interval for the current time and date. You configure the server in the SNTP Server field. You configure the time interval in the Poll field. If you enable the SNTP status field before you configure a SNTP server, this field has no effect until you configure the server.

Type **D** (for Disabled) to prevent the switch from querying a NTP or SNTP server.

10. Type **3** to select SNTP Server to configure the IP address of an SNTP server.

Note

If you have enabled DHCP on the switch, the switch attempts to retrieve the SNTP server IP address from the DHCP server automatically. The automatic determination of server IP occurs either at boot-up (start-up) or when you enable the DHCP option in the Administration Menu.

The following prompt is displayed:

```
Enter SNTP server IP address ->
```

11. Enter an IP address of your SNTP or NTP server.

Use the standard IP format: xxx.xxx.xxx.xxx

12. Type **4** - UTC Offset to specify a difference between the UTC and local time.

Note

If you have enabled DHCP, the switch automatically attempts to determine this value. In this case, you do not need to configure a value for the UTC Offset parameter.

The following prompt is displayed:

```
Enter UTC Offset [-12 to 12] -> 0
```

13. Enter a UTC Offset time.

The default is 0 hours. The range is -12 to +12 hours.

14. Type **5** - Daylight Savings Time (DST) to enable or disable the switch's ability to adjust its system time to daylight savings time.

The following prompt is displayed:

```
Adjust for Daylight Savings Time (E - Enabled, D - Disabled) ->
```

15. Select one of the following:

- Type **E** (for Enabled) to allow the switch to adjust system time to daylight savings time. This is the default value.
- Type **D** (for Disabled) to not allow the switch to adjust system time to daylight savings time.

16. Type **6** - Poll Interval to specify the time interval between two successive queries to the SNTP server.

The following prompt is displayed:

```
Enter interval to poll SNTP server [60 to 1200] ->
600
```

17. Enter the number of seconds the switch waits to poll the SNTP server.

The default is 600 seconds. The range is from 60 to 1200 seconds.

Note

The Last Delta field displays the last adjustment that was applied to system time due to a drift in the system clock between two successive queries to the SNTP server. This is a read only field.

18. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Rebooting a Switch

To reset a switch while preserving the switch configuration, perform the following procedure:

1. From the Main Menu, type **4** to select Administration Menu.
2. From the Administration, type **B** to select Reboot the switch.

The following prompt is displayed:

```
The switch is about to reboot. Do you want to
proceed? [Yes/No] ->
```

3. Type **Y** to reset the switch or **N** to cancel this procedure.

If you type **Y**, the following is displayed:

```
Rebooting the Switch...
```

```
.
```

```
.
```

```
.
```

```
Init Done!
```

4. Press the Return key.

The switch reloads its operating system, a task requiring a few minutes to complete.



Caution

The switch does not forward traffic during the brief period required to reload its operating software. Some data traffic may be lost.

Configuring the AT-S60 Software Security Features

The AT-S60 software has several security features that can help prevent unauthorized individuals from changing the parameter settings of an AT-8400 switch. The security features are:

- ❑ **Manager and Operator Passwords** - The management software has two standard, management login accounts: Manager and Operator. The Manager account allows you to configure all switch parameters, while the Operator account only allows you to view the parameter settings. The default login password for Manager access is "friend." The default password for Operator access is "operator." The passwords are case-sensitive. For instructions on how to change a password, refer to *Configuring the Management Passwords* on page 65.
- ❑ **Console Timeout** - This parameter causes the management software to automatically end a management session if it does not detect any activity from the local or remote management station after the specified period of time. This security feature can prevent unauthorized individuals from using your management station should you step away from your system while configuring a switch. The default for the console timeout value is 10 minutes. For instructions on how to set this security feature, refer to *Configuring Management Access* on page 66.
- ❑ **Web Access** - You can disable the web browser management feature to prevent individuals from managing the switch remotely using a web browser. For instructions on how to set this security feature, refer to *Configuring Management Access* on page 66.
- ❑ **Telnet Access** - You can disable the Telnet server to prevent individuals from managing the switch remotely using the Telnet application. For instructions on how to set this security feature, refer to *Configuring Management Access* on page 66.
- ❑ **SNMPv1 and SNMPv2c Access** - You can also disable the SNMPv1 and SNMPv2c management feature to prevent individuals from managing the switch remotely using a SNMP management program. For instructions on how to set this security feature, refer to *Chapter 5, SNMPv1 and SNMPv2c Configuration* on page 84.
- ❑ **SNMPv3 Access** - You can configure the authentication and privacy (encryption) features of the SNMPv3 protocol. For instructions on how to set this security feature, refer to *Chapter 17, SNMPv3 Configuration* on page 293.

Configuring the Management Passwords

There are two levels of management access on an AT-8400 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. As an Operator, you cannot change any values.

Log in as a Manager or an Operator by entering the appropriate login id and password when you start an AT-S60 management session. The default password for Manager access is "friend." The default password for Operator access is "operator." The passwords are case-sensitive.

To change the Manager or Operator password, perform the following procedure:

1. From the Main Menu, type **4** to select Administration.
2. From the Administration, type **7** to select Set Password.

The Passwords Menu is shown in Figure 14.

```

Allied Telesyn AT-8400 Series - AT-S60 V2.1.0
High School Switch 142
User: Manager                                00:14:33 15-Jan-2004
                                           Passwords Menu

1 - Set Manager Password
2 - Set Operator Password

R - Return to Previous Menu

Enter your selection?

```

Figure 14 Passwords Menu

3. To change the Manager password, type **1**.
Follow the prompts. The password can be from 0 to 20 alphanumeric characters. The passwords are case-sensitive.
4. To change the Operator password, type **2**.
Follow the prompts. The password can be from 0 to 20 alphanumeric characters. The passwords are case-sensitive.



Caution

Allied Telesyn recommends that you 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 do not accept special characters in passwords.

Note

You must assign different values to each password.

**Configuring
Management
Access**

This procedure configures the console timer. It also enables and disables Telnet access and SNMP access. To configure management access, perform the following procedure:

1. From the Main Menu, type **5** to select System Menu.
The System Menu is shown in Figure 5 on page 51.
2. From the System Menu, type **1** - Configure System.
The Configure System Menu is shown in Figure 11 on page 59.
3. From the Configure System Menu, type **1** - Configure System Software.
The Configure System Software Menu is shown in Figure 12 on page 60.
4. To configure the console timer, type **2** - Console Disconnect Timer Interval.

The following prompt is displayed:

```
Enter Console Disconnect Timer [1 to 60] -> 10
```

5. Enter a value of from 1 to 60 minutes. Then press Return.

The default is 10 minutes.

If you specify 2 minutes, the AT-S60 management software automatically ends a management session if it does not detect any activity from the local or remote management station after 2 minutes.

6. To enable or disable Telnet access, type **5** to select Telnet Server.

The following prompt is displayed:

```
Telnet Server Status (E-Enabled, D-Disabled) ->
```

7. Toggle between the following selections:
 - Type **E** (for Enabled) to enable the switch to access the Telnet server. This the default.
 - Type **D** (for Disabled) to not allow the switch to access the Telnet server.

Note

Disable Telnet access if you are using the SSH (Secure Shell) feature. (The SSH feature is not available on all versions of the AT-S60 management software.)

8. To configure SNMPv1 and SNMPv2 access, type **8** to select Configure SNMP.

The Configure SNMP Menu is displayed in Figure 22 on page 87. See Chapter 5, SNMPv1 and SNMPv2c Configuration on page 84 for details about how to configure SNMPv1 and SNMPv2.

If you disable SNMP access, no one can manage the switch remotely using an SNMP management program.

9. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Your changes are immediately activated on the switch.

Displaying the AT-S60 Hardware and Software Information

The procedures in this section display the following switch information:

- System hardware information
- System Software information
- Fan status
- AT-S60 version number
- Bootloader version number
- MAC address

Displaying System Hardware Information

To display the system power and fan information, do the following:

1. From the Main Menu, type **5** to select the System Menu.

The System Menu is shown in Figure 5 on page 51.

2. Select **2** - Display System.

The Display System Menu is shown in Figure 9 on page 55.

3. Select **2** - Display System Hardware Information.

The Display System Hardware Information Menu is shown in Figure 15.

You cannot change the information displayed in selections 1 through 3 in the Display System Hardware Information Menu. These fields are for display purposes only.

```

Allied Telesyn AT-8400 Series - AT-S60 V2.1.0
High School Switch 142
User: Manager                                00:14:33 15-Jan-2004
Display System Hardware Information

1 - System 3.3V Power..... 3.3V
2 - System 5V Power..... 5.1V
3 - System Temperature (Celsius) .... 27 C
4 - Display System Fan A Information
5 - Display System Fan B Information

R - Return to Previous Menu
Enter your selection?
```

Figure 15 Display System Hardware Information Menu

4. To display fan information, select **4** - Display System Fan A Information or select **5** - Display System Fan B Information.

The Display System Fan A Information Menu is shown in Figure 16 on page 69. The Display System Fan A Information Menu is identical to the Display System Fan B Information Menu.

You cannot change the information displayed in selections 1 through 6 in the Display System Fan A Information Menu. These fields are for display purposes only.

```

Allied Telesyn AT-8400 Series - AT-S60 V2.1.0
Engineering Switch 142

User: Manager                                00:14:33 15-Jan-2004

Display System Fan A Information

1 - Fan Status..... On
2 - Fan 3.3V Power..... 3.2V
3 - Fan 12V Power..... 11.8V
4 - Fan Temperature (Celsius)..... 28 C
5 - Fan 1 ..... 5625 RPM
6 - Fan 2 ..... 5625 RPM

R - Return to Previous Menu
Enter your selection?

```

Figure 16 Display System Fan A Information Menu

Displaying System Software Information

To display the system software information, perform the following procedure:

1. From the Main Menu, type **5** - System Menu.
The System Menu is displayed.
2. From the System Menu, type **2** - Display System.
The Display System Menu is displayed.
3. From the Display System Menu, type **1** - Display System Software Information.

The Display System Software Information Menu is displayed in Figure 9 on page 55.

You cannot change the information displayed in selections 1 through 6 in the Display System Software Information Menu. These fields are for display purposes only.

```
Allied Telesyn AT-8400 Series - AT-S60 V2.1.0
Engineering Switch 142
User: Manager                                00:14:33 15-Jun-2004
Display System Software Information
1 - Application Software Version ... AT-S60 v2.1.0
2 - Application Software Build Date. Dec 9 2004 12:25:59
3 - Bootloader Version ..... ATS60_LOADER v1.3.0
4 - Bootloader Build Date ..... Dec 29 2003 15:20:44
5 - MAC Address ..... 00.A0.D2.17.32.00
6 - System Up Time ..... 3 Days 2 Hours 1 Minutes 5 Seconds
R - Return to Previous Menu
Enter your selection?
```

Figure 17 Display System Software Information Menu

Pinging a Remote System

You can instruct the switch to ping a remote device 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 Main Menu, type **4** to select Administration Menu.

The Administration Menu is shown in Figure 4 on page 48.

2. From the Administration Menu, type **P** to select Ping a Remote System.

The following prompt is displayed:

```
Please enter an IP address ->
```

3. Enter the IP address of the end node you want the switch to ping in the following format: xxx.xxx.xxx.xxx.

The results of the ping command are displayed on the screen. To stop the ping, press any key.

Returning the AT-S60 Software to the Factory Default Values

The procedure in this section returns all AT-S60 software parameters to their default values. This procedure also deletes any VLANs that you have created on the switch.

Note

The AT-S60 software default values can be found in **Appendix A, AT-S60 Default Settings** on page 820.

To return the AT-S60 management software to its default settings, perform the following procedure:

1. From the Main Menu, type **5** to select the System Menu.
The System Menu is shown in Figure 5 on page 51.
2. From the System Menu, type **1** to select Configure System.
The Configure System Menu is shown in Figure 11 on page 59.
3. From the Configure System Menu, type **1** - Configure System Software.
The Configure System Software Menu is shown in Figure 12 on page 60.
4. Select **D** - Reset to Factory Defaults.
The following prompt is displayed:

```
Do you want to reset to Factory Defaults? [Yes/No] ->
```
5. Type **Y** for yes or **N** for no.
The following prompt is displayed:

```
Do you want to reset IP Configuration (Static/DHCP) [Yes/No] ->
```
6. Choose from one of the following selections:
 - Type **Y** (for yes) to configure all switch parameters with their default values including the IP address, subnet mask, and gateway address.
 - Type **N** (for no) to configure all switch parameters with their default values excluding the IP address, subnet mask, and gateway address. (If you activated BOOTP and DHCP, resetting the switch to its default settings disables BOOTP and DHCP.)

The following prompt is displayed:

```
Please reboot the switch for the Factory Defaults to take effect. Switch is about to reboot. Do you want to proceed? [Yes/No] ->
```


7. Type **Y** to reboot the switch.

The operating parameters are returned to their default values and the switch is reset.

The following message is displayed:

```
Rebooting the switch, please wait...
```

```
.  
.
.
```

```
Init Done!
```

8. Press any key to log in.



Caution

The switch does not forward traffic during the brief period required to reload its operating software. Some data traffic may be lost.

Configuring the Console Startup Mode

You can configure the AT-S60 software to display either the Main Menu or the command line interface prompt (#) when you start a local or Telnet management session. The default is the Main Menu.

To change the console startup mode, perform the following procedure:

1. From the Main Menu, type **5** to select the System Menu.
The System Menu is shown in Figure 5 on page 51.
2. From the System Menu, type **1** to select Configure System.
The Configure System Menu is shown in Figure 11 on page 59.
3. From the Configure System Menu, type **1** to select Configure System Software.
The Configure System Software Menu is shown in Figure 12 on page 60.
4. Type **4** to select Console Startup Mode to toggle between the following values.
 - Select **Menu** to start a management session with the Main Menu when you log in. Menu is the default.
 - Select **CLI** to start a management session with the Command Line Interface when you log in.
5. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Your changes to the console startup mode take effect the next time you start a management session.

Chapter 4

Enhanced Stacking

This chapter explains the enhanced stacking feature and provides procedures for using this feature with a local or Telnet management session. This chapter contains the following sections:

- ❑ Enhanced Stacking Overview on page 76
- ❑ Setting a Switch's Enhanced Stacking Status on page 79
- ❑ Selecting a Switch in an Enhanced Stack on page 81

Enhanced Stacking Overview

The enhanced stacking feature can make it easier for you to manage an AT-8400 switch and any other ATl switches in your network that feature enhanced stacking. It offers the following benefits:

- ❑ From one local or remote management session, you can manage up to 24 switches. This eliminates having to initiate a separate management session for each switch in your network. For example, with the AT-8400 switch as the master switch, you can manage AT-8000 Series switches that are configured with the AT-S39 software version 3.1 and above.
- ❑ You can assign an IP address to the master switch. In addition, you can manage slave switches without assigning them individual IP addresses. This feature reduces the number of IP addresses that you need to assign to your network devices for remote management.
- ❑ Remotely managing a new switch in your network is simplified. Once you connect a new switch to your network, you can begin to manage it immediately from any workstation in your network.

Guidelines

There are a few guidelines to keep in mind when implementing enhanced stacking for your network:

- ❑ Each subnet in your network constitutes an enhanced stack. You cannot have multiple enhanced stacks in a subnet.
- ❑ All switches within an enhanced stack must use the same management VLAN. For information on management VLANs, refer to Specifying a Management VLAN on page 433.
- ❑ Different enhanced stacks can use different management VLANs.
- ❑ Each subnet must have at least one master switch. Allied Telesyn recommends you assign two master switches to an enhanced stack.
- ❑ You must assign the master switch an IP address and a subnet mask to use enhanced stacking through the Telnet, Web, or SNMP interfaces.
- ❑ You must change the master switch's stacking status to Master.
- ❑ The enhanced stacking feature uses the IP address 172.16.16.16. Do not assign this address to any device on your subnet if you intend to use the enhanced stacking feature.

There are three basic steps to implementing this feature on your network:

1. Select a switch in your network to function as the master switch of the stack.

You can select an AT-8400 switch, or any other ATI switch that is capable of enhanced stacking, to act as the master switch of an enhanced stack. For networks that consist of more than one subnet, you must assign at least one master switch in each subnet.

Allied Telesyn recommends that you assign two master switches to each subnet. That way, if you remove one of the master switches from the network, such as for maintenance, you are able to remotely manage the switches in the subnet using the second master switch.

Note

Only switches connected to the management VLAN of the master switch can be discovered and managed through enhanced stacking. Switches that are not connected to the management VLAN are not discovered even if they are in the same subnet as the master switch.

2. You must assign the master switch an IP address and a subnet mask.

A master switch must have an IP address and subnet mask. The other switches in an enhanced stack, referred to as slave switches, do not need an IP address and a subnet mask.

If your enhanced stack has more than one master switch, you must assign a unique IP address to each master switch.

You can set an IP address manually or activate the BOOTP and DHCP services on a master switch and have the master switch obtain its IP information from a BOOTP or DHCP server on your network. Initially, assigning an IP address or activating the BOOTP and DHCP services can only be performed through a local management session.

Note

For instructions on how to set the IP address manually, refer to *Configuring an IP Address and Switch Name* on page 48. For instructions on activating the BOOTP and DHCP services, refer to *Activating the BootP and DHCP Services* on page 57.

3. You must change the enhanced stacking status of the master switch to Master.

This is explained in the procedure *Setting a Switch's Enhanced Stacking Status* on page 79.

Example For an example of the enhanced stacking feature, see Figure 18. This example shows a mixture of AT-8400 and AT-8000 Series switches. With this configuration, starting a local or remote management sessions on either AT-8400 Series master switch, provides management access to the AT-8000 Series switches as well.

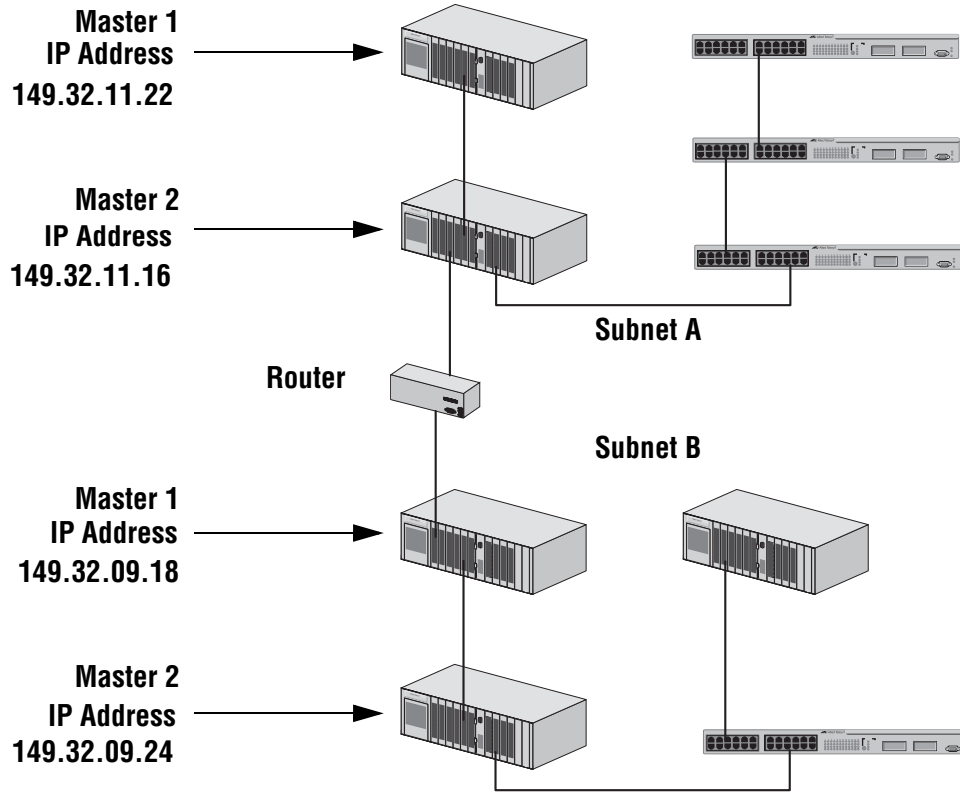


Figure 18 Enhanced Stacking Example

The example shown in Figure 18 consists of a network of two subnets interconnected by a router. Two switches in each subnet have been selected as the master switches of their respective subnets, and each has been assigned a unique IP address.

To manage the switches of a subnet, you start a local management session or a remote Telnet management session with one of the master switches in the subnet. Then, you have management access to all the AT-8400 switches in the same subnet.

Setting a Switch's Enhanced Stacking Status

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

- Master switch - A master switch of a stack can be used to manage all the other switches in a subnet. You can assign the master status to either an AT-8400, or any other ATI switch that features enhanced stacking, which can then be used to manage a mixture of AT-8400 and AT-8000 Series switches. Once you have established a local or remote management session with the master switch, you can access and manage all the 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 services on the switch.

- Slave switch - 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.

Note

You can use Telnet or the Web to manage a switch with an unavailable stacking status remotely. However, the switch must be directly connected to the AT-8400 and you must assign it a unique IP address.

Note

The default setting for a switch is Slave.

Configuring Enhanced Stacking

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

1. From the Main Menu, type **8** to select Enhanced Stacking.

The Enhanced Stacking menu is shown in Figure 19.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
High School Switch 142
User: Manager                                00:14:33 15-Jan-2004
Enhanced Stacking
1 - Switch State-(M)aster/(S)lave/(U)navailable.... Master
2 - Stacking Services

R - Return to Previous Menu

Enter your selection?

```

Figure 19 Enhanced Stacking Menu

The menu displays the current status of the switch at the end of selection "1 - Switch State." The default is Slave.

Note

The "2 - Stacking Services" selection in the menu is available only when you set the status to master. For information regarding using this selection, see *Selecting a Switch in an Enhanced Stack* on page 81

2. To change a switch's stacking status, type **1** to select Switch State.

The following prompt is displayed.

```
Enter new setup (M/S/U) ->
```

3. Type **M** to change the switch to a master switch, **S** to make it a slave switch, or **U** to make the switch unavailable. Press Return.
4. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

A change to the status is immediately activated on the switch.

Selecting a Switch in an Enhanced Stack

Before performing a procedure on a switch, check that you are accessing the correct switch. If you assigned system names to your switches, this is a simple check. The name of the switch you are currently managing is displayed at the top of every management menu. For example, in Figure 20, the name of the switch is Sales Switch 591.

When you start a management session on the Master switch of a subnet, you are, by default, addressing that particular switch. The management tasks that you perform effect only the master switch.

To manage a slave switch or another Master switch in the subnet, 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 Main Menu, type **8** to select Enhanced Stacking.
The Enhanced Stacking menu is shown in Figure 19 on page 80.
2. From the Enhanced Stacking menu, type **2** to select Stacking Services.
The Stacking Services menu is shown in Figure 20.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Sales Switch 591

User: Manager                                00:14:33 15-Jan-2004

Stacking Services

Num  MAC Address      Name      Switch  Software  Switch
-----
1 - Get/Refresh List of Switches
2 - Sort Switches in New Order
3 - Access Switch
4 - Download Image/Bootloader

R - Return to Previous Menu

Enter your selection?

```

Figure 20 Stacking Services Menu

3. Type **1** to select Get/Refresh List of Switches.

The Master switch polls the network for all slave and Master switches in the subnet and displays a list of the switches in the Stacking Services menu.

The updated Stacking Services menu is shown in Figure 21.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
High School Switch 142
User: Manager                                00:14:33 15-Jan-2004
Stacking Services
Num  MAC Address      Name      Switch  Software  Switch
-----
1    00:30:84:5b:a2:e0 Sales     Master  v1.1.4    AT-8400
2    00:30:84:52:03:80 Finance   Slave   v1.1.4    AT-8400
3    00:30:84:c7:6e:20 Production Slave    v3.1.0    AT-8026FC
1 - Get/Refresh List of Switches
2 - Sort Switches in New Order
3 - Access Switch
4 - Download Image/Boot Loader
R - Return to Previous Menu
Enter your selection?
```

Figure 21 Updated Stacking Services Menu

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.

By default, the switches are sorted in the menu by MAC address. You can sort the switches by name as well. This is accomplished with the selection **2** - Sort Switches in New Order.

4. To manage a different switch in an enhanced stack, type **3** to select Access Switch.

A prompt similar to the following is displayed:

```
Enter the switch number -> [1 to 24]
```

5. Type the number of the switch you want to manage. Press Return.

A login prompt is displayed.

6. Enter a username. The usernames are "manager" to view and change the switch settings and "operator" to just view the settings. Press Return.

A password prompt is displayed.

7. Enter the switch's password and press Return.

The default password for Manager access on an AT-8400 switch is "friend." The default password for Operator access is "operator." The passwords are case-sensitive.

The Main Menu of the selected switch is displayed. You now can manage the switch. Any management tasks you perform effect only the selected switch.

Note

Option 4 - Download Image/Boot Loader is explained in Chapter 11, File Downloads and Uploads on page 167.

Returning to the Master Switch

When you are finished managing a slave switch and want to manage another switch in the subnet, return to the Main Menu of the slave switch. Then type **S** to save your configuration changes and type **Q** for Quit. This returns you to the Stacking Services menu. Once you see that menu, 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, return to the master switch's Main Menu by typing **R** twice.

Chapter 5

SNMPv1 and SNMPv2c Configuration

This chapter provides a description of the AT-S60 implementation of the SNMPv1 and SNMPv2c protocols. In addition, it provides procedures that allow you to create, modify, and display SNMPv1 and SNMPv2c communities. The following sections are provided:

- ❑ SNMP Overview on page 85
- ❑ Configuring the SNMPv1 and SNMPv2c Protocols on page 86
- ❑ Displaying an SNMPv1 and SNMPv2c Community on page 100

Note

For information about the SNMPv3 protocol, see Chapter 6 “SNMPv3 Configuration.”

SNMP Overview

The SNMPv1 and SNMPv2c protocols allow you to create groups, called communities, and define IP addresses for SNMP managers. In addition, you can configure IP addresses for sending SNMP messages called traps. Using the SNMPv1 and SNMPv2c protocols, you can authenticate messages based on a password, called a community name, and manager IP addresses. Messages sent using the SNMPv1 and SNMPv2c protocols are plain text messages.

Over time, some security issues have developed with the SNMPv1 and SNMPv2c protocols. For example, it has become standard practice to use "public" and "private" as community names. As a result, Allied Telesyn International suggests using carefully selected community names.

There are two ways to configure the SNMPv1 and SNMPv2c protocols. You can use the SNMPv1 and SNMPv2c menus described in this chapter to configure these protocols or you can use SNMPv3 Table menus described in Chapter 17: SNMPv3 Configuration on page 293. Allied Telesyn International recommends you configure SNMPv1 and SNMPv2c with the SNMPv1 and SNMPv2c menu described in this chapter because the SNMPv3 Table menu require a much more extensive configuration.

For procedures to configure SNMPv1 and SNMPv2c menus, see Configuring the SNMPv1 and SNMPv2c Protocols on page 86.

Note

For the SNMP RFCs supported by this release of the AT-S60 software, see SNMP Management Session on page 32.

Configuring the SNMPv1 and SNMPv2c Protocols

This section describes how to configure the SNMPv1 and SNMPv2c protocols. In this section, these protocols are configured together. You can configure the SNMPv1 and SNMPv2c protocols independently using the SNMPv3 Tables. (See Configuring the SNMPv3 Community Table on page 381.) However, Allied Telesyn International recommends you configure the SNMPv1 and SNMPv2c protocols with the menus described in this chapter because the SNMPv3 menus require a much more extensive configuration.

The following procedures are provided:

- Enabling the SNMP Protocol on page 86
- Configuring SNMPv1 and SNMPv2c Communities on page 88
- Deleting an SNMPv1 and SNMPv2 Community on page 91
- Modifying SNMPv1 and SNMPv2 Community Attributes on page 92

Note

To display the SNMPv1 and SNMPv2 parameters see Displaying an SNMPv1 and SNMPv2c Community on page 100.

Enabling the SNMP Protocol

To activate the SNMP configuration, allowing the switch to communicate with a Network Manager System (NMS), you need to enable SNMP on your switch. In addition, enable the switch to send authentication failure traps.

Traps generated by the SNMP agent are forwarded to all trap receivers in all of the SNMPv1 and SNMPv2c communities. The SNMP community name and manager IP addresses are used to provide authentication. An incoming SNMP message is deemed authentic if it contains a valid community name and it originated from an IP address that is defined as a management station for that community.

When a community is disabled, the SNMP agent behaves as if the community does not exist. In addition, the switch generates authentication failure traps for messages directed to the disabled community.

The authentication failure trap may be generated as a result of the failure to authenticate an SNMP message. See the following procedure for instructions on how to enable or disable the generation of authentication failure traps.

To enable SNMPv1 and SNMPv2 as well as authentication trap messages, perform the following procedure.

1. From the Main Menu, type **5** to select System Menu.
The System Menu is shown in Figure 5 on page 51.
2. From the System Menu, type **1** to select Configure System.
The Configure System menu is shown Figure 11 on page 59.
3. From the Configure System menu, type **1** to select Configure System Software.
The Configure System Software menu is shown in Figure 12 on page 60.
4. From the Configure System Software menu, type **8** to select Configure SNMP.
The Configure SNMP menu is shown in Figure 22.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
High School Switch 142
User: Manager                                00:14:33 15-Jan-2004
                                Configure SNMP
1 - SNMP Status..... Disabled
2 - Authentication Failure Trap Status.... Disabled
3 - Configure SNMPv1 & SNMPv2c Community
4 - Display SNMPv1 & SNMPv2c Community
5 - Configure SNMPv3 Table
6 - Display SNMPv3 Table

R - Return to Previous Menu

Enter your selection?

```

Figure 22 Configure SNMP Menu

5. To enable or disable SNMPv1 and SNMPv2c management on your switch, type **1** to select SNMP Status.
Toggle between Enabled and Disabled by pressing **1** again.
6. To configure the switch to send authentication failure traps to trap receiver hosts, type **2** to select Authentication Failure Trap Status.
Choose one of the following options:
 - Enabled** - Sends authentication failure traps to IP addresses of configured trap receiver hosts.
 - Disabled** - Does not send authentication failure traps.

When this parameter is enabled, the switch sends authentication failure traps under two conditions:

- The SNMP management station attempts to access the switch using an incorrect or invalid community name.
- The IP address of this SNMP management station is not configured as an SNMP manager within the community.

Toggle between Enabled and Disabled by pressing **2** again.



Caution

You must configure a trap receiver IP address in order for trap message to be sent. See the following procedure.

7. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Configuring SNMPv1 and SNMPv2c Communities

Use this procedure to configure the SNMPv1 and SNMPv2c community strings for the switch and assign SNMP community names. You can assign up to eight IP addresses of management stations and up to eight IP addresses of trap receivers.

To configure SNMPv1 and SNMPv2c parameters, perform the following procedure.

1. From the Main Menu, type **5** to select System Menu.
The System Menu is shown in Figure 5 on page 51.
2. From the System Menu, type **1** to select Configure System.
The Configure System Menu is shown in Figure 11 on page 59.
3. From the Configure System Menu, type **1** to select Configure System Software.
The Configure System Software Menu is shown in Figure 12 on page 60.
4. From the Configure System Software Menu, type **8** to select Configure SNMP.
The Configure SNMP Menu is shown in Figure 22 on page 87.
5. To configure SNMPv1 and SNMPv2c parameters, type **3** to select Configure SNMPv1 & SNMPv2c Community.

The Configure SNMPv1 and SNMPv2c Community menu is shown in Figure 23.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
High School Switch 142

User: Manager                                00:14:33 15-Jan-2004

Configure SNMPv1 & SNMPv2c Community

Community Name  Access Mode  Status  OpenAcc  Manager IP Address  Trap Receiver IP
=====
ati777          Read|Write  Enabled  No       147.35.18.87        1.1.1.1
atipublic750   Read Only  Enabled  Yes      147.35.18.88        1.1.1.1

1 - Create SNMP Community
2 - Delete SNMP Community
3 - Modify SNMP Community

U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 23 Configure SNMPv1 & SNMPv2c Community Menu

- To configure SNMP parameters, type **1** to select Create SNMP Community.

The following prompt is displayed:

```
Enter SNMP Community Name:
```

- Enter an SNMP community name of up to 15 alphanumeric characters. This parameter is case sensitive.

Note

Community names act as passwords for the SNMP protocol. Allied Telesyn recommends that you select SNMP community names carefully to ensure these names are known only to authorized personnel.

The following prompt is displayed:

```
Enter Access Mode [R-Read Only, W-Read|Write]:
```

- Enter an access mode for the SNMP community.

Choose one of the following:

R - Enter R to permit read only access to the SNMP community.

W - Enter W to permit read-write access to the SNMP community.

The following prompt is displayed:

```
Enter Open Access Status [Y-Yes, N-No]:
```

9. Enter an open access status for the SNMP community.

Choose one of the following options:

Y - Enter Y to permit access to the SNMP community by any management station.

N - Enter N to permit access to the SNMP community by a management station configured within this community.

The following prompt is displayed:

```
Enter SNMP Manager IP Addr:
```

10. Enter an IP address of an SNMP management station to permit it to access the switch.

Use the following format for an IP address:

XXX.XXX.XXX.XXX

You can enter an IP address of an SNMP management station with the Open Access Status parameter set to Yes. In this case, the switch permits access to the SNMP community by any management station, including the one configured here. To limit access to the switch to only the IP address configured in this parameter, configure the Open Access parameter to No. With the Open Access parameter set to No, access to the switch is limited to the IP address configured with the SNMP Manager IP Addr parameter.

The following prompt is displayed:

```
Enter Trap Receiver IP Addr:
```

11. Enter an IP address to receive trap messages.

Use the following format for an IP address:

XXX.XXX.XXX.XXX

The Trap Receiver IP Address value is used when the switch generates a trap message and when the switch authenticates the SNMP Manager IP address.

Note

Within an SNMP community, Trap Receiver IP addresses are automatically added to an internal Manager IP address list. This information is not displayed.

12. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Deleting an SNMPv1 and SNMPv2 Community

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

1. From the Main Menu, type **5** to select System Menu.
The System Menu is shown in Figure 5 on page 51.
2. From the System Menu, type **1** to select Configure System.
The Configure System Menu is shown in Figure 11 on page 59.
3. From the Configure System Menu, type **1** to select Configure System Software.
The Configure System Software Menu is shown in Figure 12 on page 60.
4. From the Configure System Software Menu, type **8** to select Configure SNMP.
The Configure SNMP Menu is shown in Figure 22 on page 87.
5. To configure SNMPv1 and SNMPv2c parameters, type **3** to select Configure SNMPv1 & SNMPv2c Community
The Configure SNMPv1 & SNMPv2c Community Menu is shown in Figure 23 on page 89.
6. To remove an SNMPv1 and SNMPv2c community, type **2** to select Delete SNMP Community.
The following prompt is displayed:
Enter SNMP Community Name:
7. Enter an SNMP community name from the list at the top of the menu.
The following prompt is displayed:
Do you want to delete this Community? (Y/N):
[Yes/No]->
8. Choose from the following options:
Y - Select Y to delete the SNMP community.
N -Select N to retain the SNMP community.
9. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Modifying SNMPv1 and SNMPv2 Community Attributes

For each SNMPv1 and SNMPv2c community, you can modify several attributes. See the following procedures:

- Adding SNMP Manager and Trap Receiver IP Addresses on page 92
- Deleting Attributes from a Community on page 94
- Changing the Access Mode of a Community on page 95
- Changing the Community Status on page 97
- Changing the Community Open Access Mode on page 98

Adding SNMP Manager and Trap Receiver IP Addresses

To add IP addresses to the list of SNMP Manager and Trap Receivers, perform the following procedure:

1. From the Main Menu, type **5** to select System Menu.
The System Menu is shown in Figure 5 on page 51.
2. From the System Menu, type **1** to select Configure System.
The Configure System Menu is shown in Figure 11 on page 59.
3. From the Configure System Menu, type **1** to select Configure System Software.
The Configure System Software Menu is shown in Figure 12 on page 60.
4. From the Configure System Software Menu, type **8** to select Configure SNMP.
The Configure SNMP Menu is shown in Figure 22 on page 87.
5. To configure SNMPv1 and SNMPv2c parameters, type **3** to select Configure SNMPv1 & SNMPv2c Community.
The Configure SNMP Community Menu is shown in Figure 23 on page 89.
6. To modify SNMP community attributes, type **3** to select Modify SNMP Community.

The Modify SNMPv1 and SNMPv2c Community Menu is shown in Figure 24.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142

User: Manager                                00:14:33 15-Jan-2004

                          Modify SNMPv1 & SNMPv2c Community
Community Name      Access Mode  Status  OpenAcc  Manager IP Addr  Trap Receiver IP
=====
142alliedtelesyn   Read|Write  Enabled  No       147.35.18.85     1.1.1.1
                  2.2.2.2         2.2.2.2
sunnyvalepub23    Read Only   Enabled  No       147.35.18.86     158.12.18.1
                  158.12.18.20    158.10.10.16

1 - Add Attributes to Community
2 - Delete Attributes from Community
3 - Set Community Access Mode
4 - Set Community Status
5 - Set Community Open Access

U - Update Display
R - Return to Previous Menu

```

Figure 24 Modify SNMPv1 & SNMPv2c Community Menu

- To add SNMP manager and Trap Receiver IP addresses, type **1** to select Add Attributes to Community.

For each community, you can add up to eight IP addresses for SNMP Managers and up to eight Trap Receiver IP addresses.

The following prompt is displayed:

```
Enter SNMP Community Name:
```

- Enter an SNMP community name from the list at the top of the menu. SNMP community names are case sensitive.

The following prompt is displayed:

```
Enter SNMP Manager IP Addr:
```

- Enter an IP address to permit the SNMP manager to access the switch. Or, to skip this prompt, press Return.

Use the following format for an IP address:
XXX.XXX.XXX.XXX

The following prompt is displayed:

```
Enter Trap Receiver IP Addr:
```

- Enter an IP address to send trap messages. Or, to skip this prompt, press Return.

Use the following format for an IP address:
XXX.XXX.XXX.XXX

11. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Deleting Attributes from a Community

To delete an IP address from either the list of Manager IP addresses or the list of Trap Receiver IP addresses, perform the following procedure:

1. From the Main Menu, type **5** to select System Menu.
The System Menu is shown in Figure 5 on page 51.
2. From the System Menu, type **1** to select Configure System.
The Configure System Menu is shown in Figure 11 on page 59.
3. From the Configure System Menu, type **1** to select Configure System Software.
The Configure System Software Menu is shown in Figure 12 on page 60.
4. From the Configure System Software Menu, type **8** to select Configure SNMP.
The Configure SNMP Menu is shown in Figure 22 on page 87.
5. To configure SNMP parameters, type **3** to select Configure SNMPv1 & SNMPv2c Community.
The Configure SNMPv1 & SNMPv2c Community Menu is shown in Figure 23 on page 89.
6. To modify SNMP Community attributes, type **3** to select Modify SNMP Community.
The Modify SNMPv1 and SNMPv2c Community menu is shown in Figure 24 on page 93.
7. To delete an IP address from either the list of SNMP managers or the list of trap receivers, type **2** to select Delete Attributes from Community.
The following prompt is displayed:
Enter SNMP Community Name:
8. Enter a community name from the list at the top of the Modify SNMPv1 & SNMPv2c Community Menu.
SNMP community names are case sensitive.
The following prompt is displayed:
Enter SNMP Manager IP Addr:

9. Enter an IP address that you want to delete. Or, to skip this prompt, press Return.

Delete an IP address to deny an SNMP manager to access the switch. Use the following format for an IP address:

XXX.XXX.XXX.XXX

The following prompt is displayed.

```
Do you want to delete this SNMP Manager? (Y/N):
[Yes/No]->
```

10. Choose from the following options:

Y - Select Y to delete the IP address of this SNMP manager.

N - Select N to retain the IP address of the SNMP manager.

The following prompt is displayed:

```
Enter the Trap Receiver IP address:
```

11. Enter the Trap Receiver IP address that you want to delete. Or, to skip this prompt, press Return.

Use the following format for an IP address:

XXX.XXX.XXX.XXX

The following prompt is displayed:

```
Do you want to delete this Trap Receiver? (Y/N):
[Yes/No]->
```

12. Choose from the following options:

Y - Select Y to delete the IP address of the Trap Receiver.

N - Select N to retain the IP address of the Trap Receiver.

13. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Changing the Access Mode of a Community

Use this procedure to change the access mode of an SNMPv1 and SNMPv2c community.

To enable or disable an SNMPv1 and SNMPv2c community, perform the following procedure:

1. From the Main Menu, type **5** to select System Menu.
The System Menu is shown in Figure 5 on page 51.
2. From the System Menu, type **1** to select Configure System.
The Configure System Menu is shown in Figure 11 on page 59.
3. From the Configure System Menu, type **1** to select Configure System Software.

The Configure System Software Menu is shown in Figure 12 on page 60.

4. From the Configure System Software Menu, type **8** to select Configure SNMP.

The Configure SNMP Menu is shown in Figure 22 on page 87.

5. To configure SNMP parameters, type **3** to select Configure SNMPv1 & SNMPv2c Community.

The Configure SNMP Community Menu is shown in Figure 23 on page 89.

6. To modify SNMPv1 & SNMPv2c Community attributes, type **3** to select Modify SNMP Community.

The Modify SNMPv1 & SNMPv2c Community Menu is shown in Figure 24 on page 93.

7. To change the access mode from read only to read/write or vice versa, type **3** to select Set Community Access Mode.

The following prompt is displayed:

```
Enter SNMP Community Name:
```

8. Enter a community name from the list at the top of the menu.
SNMP community names are case sensitive.

The following prompt is displayed:

```
Enter Access Mode [R-Read Only, W-Read/Write]:
```

9. Select an access mode for this community.

Choose from the following options:

- R** - Select R for Read Only access to this SNMP community name.
- W** - Select W to Read/Write access to this SNMP community name.

The following prompt is displayed:

```
Do you want to change this Community Access Mode?  
(Y/N): [Yes/No]->
```

10. Choose one of the following options:
 - Y** - Select Y to change the Community Access Mode.
 - N** - Select N to retain the current Community Access Mode.
11. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Changing the Community Status

You may want to change the status of a community to temporarily disable a community.

To change the community status from enabled to disabled, perform the following procedure:

1. From the Main Menu, type **5** to select System Menu.
The System Menu is shown in Figure 5 on page 51.
2. From the System Menu, type **1** to select Configure System.
The Configure System Menu is shown in Figure 11 on page 59.
3. From the Configure System Menu, type **1** to select Configure System Software.
The Configure System Software Menu is shown in Figure 12 on page 60.
4. From the Configure System Software Menu, type **8** to select Configure SNMP.
The Configure SNMP Menu is shown in Figure 22 on page 87.
5. To configure SNMPv1 and SNMPv2c parameters, type **3** to select Configure SNMPv1 & SNMPv2c Community.
The Configure SNMPv1 & SNMPv2c Community Menu is shown in Figure 23 on page 89.
6. To modify SNMP Community attributes, type **3** to select Modify SNMP Community.
The Modify SNMPv1 and SNMPv2c Community menu is shown in Figure 24 on page 93.
7. To enable or disable the current community, type **4** to select Set Community Status.
The following prompt is displayed:
Enter SNMP Community Name:
8. Enter a community name from the list at the top of the Modify SNMPv1 and SNMPv2c Community Menu.
SNMP community names are case sensitive.
The following prompt is displayed:
Enter Community Status [E-Enable, D-Disable]:
9. Enter the status of this community.
Choose one of the following selections:
E - Select E to enable the SNMP Community.

D - Select D to disable the SNMP Community.

The following prompt is displayed:

```
Do you want to change Community Status? (Y/N) :  
[Yes/No] ->
```

10. Choose one of the following selections:

Y - Select Y to change the Community Status.

N - Select N to retain the Community Status.

11. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Changing the Community Open Access Mode

To change the Community Open Access Mode, perform the following procedure.

1. From the Main Menu, type **5** to select System Menu.

The System Menu is shown in Figure 5 on page 51.

2. From the System Menu, type **1** to select Configure System.

The Configure System Menu is shown in Figure 11 on page 59.

3. From the Configure System Menu, type **1** to select Configure System Software.

The Configure System Software Menu is shown in Figure 12 on page 60.

4. From the Configure System Software Menu, type **8** to select Configure SNMP.

The Configure SNMP Menu is shown in Figure 22 on page 87.

5. To configure SNMPv1 and SNMPv2c parameters, type **3** to select Configure SNMPv1 & SNMPv2c Community.

The Configure SNMPv1 & SNMPv2c Community Menu is shown in Figure 23 on page 89.

6. To modify SNMP Community attributes, type **3** to select Modify SNMP Community.

The Modify SNMPv1 & SNMPv2c Community Menu is shown in Figure 24 on page 93.

7. To allow access to an SNMP community, type **5** to select Set Community Open Access.

The following prompt is displayed:

```
Enter SNMP Community Name:
```

8. Enter a community name from the list at the top of the Modify SNMPv1 & SNMPv2c Community Menu.

SNMP community names are case sensitive.

The following prompt is displayed:

```
Enter Open Access Status [Y-Yes, N-No]:
```

9. Enter the access status of this community.

Choose one of the following options:

Y - Select Y to allow access to this community by any management station.

N - Select N to allow access to this community by the management stations configured within this community.

The following prompt is displayed:

```
Do you want to change Open Access Status? (Y/N):  
[Yes/No]->
```

10. Choose one of the following options:

Y - Select Y to change the Open Access Status.

N - Select N to retain the Open Access Status.

11. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Displaying an SNMPv1 and SNMPv2c Community

Use the following procedure to display the attributes of an SNMPv1 and SNMPv2c communities.

1. From the Main Menu, type **5** to select System Menu.
The System Menu is shown in Figure 5 on page 51.
2. From the System Menu, type **1** to select Configure System.
The Configure System Menu is shown in Figure 11 on page 59.
3. From the Configure System Menu, type **1** to select Configure System Software.
The Configure System Software Menu is shown in Figure 12 on page 60.
4. From the Configure System Software Menu, type **8** to select Configure SNMP.
The Configure SNMP Menu is shown in Figure 22 on page 87.
5. To display the attributes of an SNMPv1 and SNMPv2c community, type **4** to select Display SNMPv1 & SNMPv2c Community.
The Display SNMPv1 & SNMPv2c Community Menu is shown in Figure 25.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
High School Switch 142

User: Manager                                00:14:33 15-Jan-2004

Display SNMPv1 & SNMPv2c Community
Community Name  Access Mode  Status  OpenAcc  Manager IP Addr  Trap Receiver IP
=====
Private125     Read|Write   Enabled No        147.41.11.30     147.45.16.70
               147.45.16.80     147.45.16.80
PublicATI78    Read Only   Enabled No        147.41.11.12     147.42.22.22
               147.44.16.86     147.45.16.88
               147.45.16.88     147.45.16.90
               147.45.16.90     147.45.16.90
HighSchool2    Read|Write   Enabled No        147.45.10.80     147.45.10.80

U - Update Display
R - Return to Previous Menu

Enter your selection?
    
```

Figure 25 Display SNMPv1 & SNMPv2c Community Menu

Note
 Within an SNMP community, Trap Receiver IP addresses are automatically added to an internal Manager IP address list. This information is not displayed.

Chapter 6

Port Parameters

The chapter contains procedures for viewing and changing the parameter settings for the individual ports on a switch with a local or Telnet management session. It contains the following procedures:

- ❑ [Displaying Port Status on page 102](#)
- ❑ [Configuring Port Parameters on page 106](#)
- ❑ [Displaying Port Statistics on page 112](#)

Displaying Port Status

This section provides a procedure to display the status of a port. To display port statistics, see Displaying Port Statistics on page 112.

To display the status of the ports on the switch, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.

The Port Menu is shown in Figure 26.

```

Allied Telesyn AT-8400 Series - AT-S60 V2.1.0
High School Switch 142

User: Manager                                00:14:33 15-Jan-2004

                                Port Menu

1 - Port Configuration
2 - Port Status
3 - Port Statistics
4 - Port Trunking
5 - Port Mirroring

R - Return to Previous Menu

Enter your selection?
    
```

Figure 26 Port Menu

2. From the Port Menu, type **2** to select Port Status.

The Port Status Menu is shown in Figure 27.

```

Allied Telesyn AT-8400 Series - AT-S60 V2.1.0
High School Switch 142

User: Manager                                00:14:33 15-Jan-2004

                                Port Status

Port  Media  Status  Link Neg  MDI/X Speed  Duplex PVID  Flow Ctl  STP  Pri
-----
1.1   FIBER  Enabled Up      Auto      MDI    0010   Half    0001  Disabled  Fwd  No
1.2   FIBER  Enabled Up      Auto      MDI    0100   Full    0001  Disabled  Fwd  No
1.3   FIBER  Enabled Up      Auto      MDI    0100   Full    0001  Disabled  Fwd  No
1.4   FIBER  Enabled Up      Auto      MDI    0100   Full    0001  Disabled  Fwd  No
2.1   GBIC   Enabled Up      Manual    MDI    1000   Full    0001  Auto      Fwd  No
3.1   TP     Enabled Up      Manual    MDIX   1000   Full    0001  Auto      Fwd  No
9.1   FIBER  Enabled Up      Auto      MDI    0100   Full    0001  Disabled  Fwd  No
9.2   FIBER  Enabled Up      Auto      MDI    0010   Half    0001  Disabled  Fwd  No

N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection?
    
```

Figure 27 Port Status Menu

The information in this menu is for viewing purposes only. The columns in the menu are described below:

Port

Indicates the port number in the following format:

slot number. port number

For more information, see *Specifying Ports* on page 34.

Media

Indicates the type of port. See the following:

- TP (for twisted pair) indicates one of the following:
 - An RJ-45 port on an AT-8411 line card.
 - An RJ-45 port on an AT-8413 line card when the Negotiation parameter on the Port Configuration Menu is set to Auto and the port is connected to another RJ-45 port. For more information about the Port Configuration Menu, see *Configuring Port Parameters* on page 106.
 - An RJ-45 port on an AT-8413 line card when the Negotiation parameter on the Port Configuration Menu is set to Manual and the Media Selection parameter on the Port Configuration Menu is set to TP. For more information about the Port Configuration Menu, see *Configuring Port Parameters* on page 106.
- Fiber indicates a fiber optic port on an AT-8412 or AT-8414 line card.
- GBIC (for GBIC port) indicates one of the following:
 - A GBIC port on an AT-8413 line card when Negotiation is set to Auto and the port is connected to another GBIC port.
 - A GBIC port on an AT-8413 line card when Negotiation is set to Manual and the Media Selection is set to GBIC.
- Auto indicates a port on an AT-8413 line card with Auto-negotiation enabled when the port is not connected to another port.

Status

Indicates the administrative status, enabled or disabled, of the port.

Enabled -Indicates the port is able to send and receive Ethernet frames. This is the default setting for all ports on the switch.

Disabled - Indicates the port has been manually disabled. The port is not able to send or receive Ethernet frames.

Link

The status of the link between the port and the end node connected to the port. Possible values are:

Up - Indicates that a valid link exists between the port and the end node.

Down - Indicates that the port and the end node have not established a valid link.

Note

The link status between the port and the end node can be displayed as "Up" even after it has been disabled in the Port Configuration menu. For more information on how to configure a port, refer to Configuring Port Parameters on page 106.

Neg

The status of Auto-Negotiation on the port. Possible values are:

Auto - Indicates that the port is using Auto-Negotiation to set operating speed and duplex mode.

Manual - Indicates that the operating speed and duplex mode have been set manually.

MDI/X

The operating configuration of the port. Possible values are Auto, MDI, MDI-X. The Auto value indicates that the port is automatically determining the appropriate MDI or MDI-X setting.

Speed

The operating speed of the port. Possible values are:

0010 - Indicates 10 Mbps.

0100 - Indicates 100 Mbps.

1000 - Indicates 1000 Mbps.

Duplex

The duplex mode of the port. Possible values are half-duplex and full-duplex.

PVID

The port VLAN identifier currently assigned to the port.

Flow Ctl

The flow control setting for the port. Possible values are:

Auto - Flow control is automatically activated on the port if the end node connected to the port uses flow control. If the end node does not use flow control, neither does the port.

Enabled - Flow control occurs on both frames entering and leaving the port.

Disabled - No flow control occurs on the port.

STP

The current operating status of the port. Possible values are:

Forwarding - The port is sending and receiving Ethernet frames. This is the normal state for a switch port.

Disabled - STP operations have been disabled on the port.

Blocking - This is the standby mode. The port does not participate in frame relay. The forwarding process discards received frames and does not submit forwarded frames for transmission.

Listening - The port is enabled for receiving frames only. The port is preparing to participate in frame relay.

Learning - The port is enabled for receiving frames only. The learning process can add new source address information to the forwarding database.

Pri

The priority assigned to frames that are received by the port.

Possible values are:

No - Indicates no override priority has been assigned to the port. Untagged frames are forwarded to the low priority queue. Tagged frames are forwarded to either the high or low queue, depending on the priority embedded in the frames.

Low - Indicates low priority has been assigned to the port. As a result, all tagged and untagged frames are sent to the low priority queue.

High - Indicates high priority has been assigned to the port. As a result, all tagged and untagged frames are sent to the high priority queue.

For more information, see Class of Service Overview on page 215.

Configuring Port Parameters

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

1. From the Main Menu, type **1** to select Port Menu.
The Port Menu is shown in Figure 26 on page 102.
2. From the Port Menu, type **1** to select Port Configuration.

The following prompt is displayed:

```
Enter port-list:
```

3. Enter the number of the port you want to configure and press Return.
See Specifying Ports on page 34.

The Port Configuration menu is shown in Figure 28.

```

Allied Telesyn AT-8400 Series - AT-S60 V2.1.0
High School Switch 142

User: Manager                                00:14:33 15-Jan-2004

                                Port Configuration

Configuring Port 1.3
0 - Port Name ..... Port_1.3
1 - Status ..... Enabled
2 - Broadcast Filter..... Disabled
3 - Override Priority.... No override
4 - HOL Blocking ..... Disabled
5 - Back Pressure ..... Disabled
6 - Flow Control ..... Auto
7 - Negotiation ..... Manual
8 - Speed ..... 1000
9 - Duplex ..... Full
A - MDI/MDIX ..... MDIX
B - Media Selection ..... TP

D - Set Default Port Configuration
R - Return to Previous Menu

Enter your selection?

```

Figure 28 Port Configuration Menu

Note

The sample Port Configuration Menu in the figure above is for a 10/100 Mbps twisted pair port.

4. Adjust the port parameters as desired. You adjust a parameter by typing its number. This toggles the parameter through its possible settings. The parameters are described below.

0 - Port Name

This parameter appears only if you are configuring a single port. You can use this selection to assign a name to a port. The name can be up to fifteen alphanumeric characters. Spaces are allowed.

1 - Status

You use this selection to change the administrative status of a port. When disabled, a port does not forward frames.

You might want to disable a port and prevent frames from being forwarded if a problem occurs with the node or cable connected to the port. Once the problem has been fixed, you can enable the port again to resume normal operation. You can also disable an unused port to secure it from unauthorized connections.

Press **1** to toggle between the following settings:

Enabled - The port is able to send and receive Ethernet frames. This is the default setting for all ports on the switch.

Disabled - The port is not able to send or receive Ethernet frames.

2 - Broadcast Filter

You use this selection to protect a port from a deluge of packets caused by a broadcast storm. Enabling the broadcast filter parameter on a port causes the port to drop broadcast frames.

Press **2** to toggle between the following settings:

Enabled - When a port receives a broadcast frame, the port drops the frame.

Disabled - The port does not watch for broadcast frames. Instead, it accepts broadcast frames. This is the default.

3 - Override Priority

You use this selection to determine frame priority. For information about override priority, see Class of Service Overview on page 215.

Press **3** to toggle between the following settings:

No override - Indicates that no override priority is assigned to incoming frames. Instead, the port forwards frames according to the priority embedded in the frame. This is the default.

Low Priority - Indicates low priority has been assigned to the port. All ingress tagged and untagged frames received on the port are forwarded to the egress port's low priority queue.

High Priority - Indicates high priority has been assigned to the port. All ingress tagged and untagged frames received on the port are forwarded to the egress port's high priority queue.

4 - HOL Blocking

You use this selection to prevent a frame from being forwarded to a blocking or blocked port. For example, a blocking or blocked port can be one that is receiving too many frames.

Press **4** to toggle between the following settings:

Enabled - Indicates HOL blocking is turned on. Frames sent from this port are not forwarded to a blocked port.

Disabled - Indicated HOL blocking is turned off. Frames sent from this port are not prevented from being forwarded to a blocked port. This is the default.

5 - Back Pressure

You can use this selection only if the port or ports you specified are operating at half-duplex mode. When you configure a port in this mode and it has a frame that is pending transmission, the port uses the JAM signal when its buffer is full to prevent the end node from sending any more frames.

Press **5** to toggle between the following settings:

Enabled - Indicates back pressure is activated on this port. When the port is receiving too many frames, the port sends a signal to the end node to stop sending information.

Disabled - Indicates back pressure is not activated on this port. When the port is receiving too many frames, the port does not send a signal to the end node to stop sending information. This is the default.

Note

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

6 - Flow Control

Flow control applies only to ports operating in full-duplex mode. The switch uses a special pause frame when its buffer is full to stop the end node from sending frames. The pause frame notifies the end node to stop transmitting for a specified period of time.

Press **6** to toggle between the following settings:

Auto - Indicates the port conforms to the flow control setting of the end node. For example, if flow control is active on the end node then flow control is active on this port. Also, if flow control is not active on the end node, then flow control is not active on this port. This is the default.

Disabled - Indicates that no flow control occurs on the port.

Enabled - Indicates that flow control occurs on the port.

7 - Negotiation

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

Press **7** to toggle between the following settings:

- Auto - Select Auto (for Auto-Negotiation) to set both speed and duplex mode for the port automatically.

Note

For the AT-8412/SC FX and AT-8412/MT FX line cards, the default setting of the Negotiation parameter is Manual. The default setting for ports on all the other line cards is Auto.

- Manual - Select Manual to set the speed and duplex for the port.

If you select Manual, four additional selections are displayed in the Port Configuration menu:

- 8** - Speed 0100
- 9** - Duplex Full
- A** - MDI/MDIX Crossover MDIX
- B** - Media Selection GBIC

You use the selections listed above to configure the port's speed, duplex mode, MDI/MDI/X, and media selection settings.

8 - Speed

You use this selection to configure the port speed. See Table 1 for port speed settings for each line card. Choose from the following options:

- 0010 - Indicates 10 Mbps.
- 0100 - Indicates 100 Mbps.
- 1000 - Indicates 1000 Mbps.

Table 1 Line Card Port-Speed Settings

Line Card	Port Speed
AT-8411 TX	10/100 Mbps
AT-8412/SC FX AT-8412/MT FX	100 Mbps

Table 1 Line Card Port-Speed Settings

Line Card	Port Speed
AT-8413 GB/T copper port	10/100/1000 Mbps
AT-8413 GB/T fiber port	1000 Mbps
AT-8414/ST AT-8414/SC	10 Mbps

9 - Duplex:

Use this selection to configure the duplex mode of the port.

See Table 2 for duplex settings for each line card. Choose from the following selections:

- Full - Indicates full-duplex mode.
- Half - Indicates half-duplex mode.

Table 2 Port-Duplex Settings on Line Cards

Line Card	Port Duplex
AT-8411 TX	Full and half
AT-8412/SC FX AT-8412/MTFX	Full only
AT-8413 GB/T copper port	Full only
AT-8413 GB/T fiber port	Full only
AT-8414/ST AT-8414/SC	Full and half

A - MDI/MDIX Crossover:

Use this selection to configure the Ethernet interface for the port.

Choose from the following settings:

- Type MDI to indicate the MDI setting.
- Type MDI/X to indicate the MDI-X setting.

Note

MDI/X applies only to copper ports, not fiber ports.

B - Media Selection

Use this parameter to select the media type on an AT-8413 line card. This parameter is only available when the Negotiation parameter is set to manual.

Choose from the following settings:

- Type GBIC (for GBIC port) to indicate only the GBIC port is available for connectivity.
- Type TP (for twisted pair) to indicate only the twisted pair port is available for connectivity.

D - Set Default Port Configuration

Use this selection to reset the port parameters to their default values. The port parameter defaults are illustrated in Figure 28 on page 106.

5. After setting the port parameters, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Configuration changes are immediately activated on a port.

Displaying Port Statistics

To display Ethernet port statistics, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
The Port Menu is shown in Figure 26 on page 102.
2. From the Port Menu, type **3** to select Port Statistics.
The Port Statistics menu is shown in Figure 29.

```
Allied Telesyn AT-8400 Series - AT-S60 V2.1.0
                          High School Switch 142
User: Manager              00:14:33 01-Jan-2004
                          Port Statistics

1 - Display Port Statistics
2 - Clear Port Statistics

R - Return to Previous Menu

Enter your selection?
```

Figure 29 Port Statistics Menu

3. Type **1** to select Display Port Statistics.
The following prompt is displayed:
Enter port-list:
4. Enter the port or ports whose statistics you want to display.
You can specify more than one port at a time. For information on entering ports, refer to Specifying Ports on page 34.

The Display Port Statistics Menu is shown in Figure 30.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
High School Switch 142
User: Manager                                00:14:33 15-Jan-2004
Display Port Statistics

Port 6.1

Bytes Received ..... 983409801           Bytes Sent ..... 965734443
Frames Received ..... 815423             Frames Sent ..... 691396
Broadcast Frames Received..... 107774    Broadcast Frames Sent .. 1853
Multicast Frames Received .... 11429     Multicast Frames Sent .. 0
Total Bytes Received ..... 983511361    Jabber ..... 0
Total Frames Received ..... 815518       CRC Error ..... 0
Frames 64 Bytes ..... 110509             Fragments ..... 0
Frames 65-127 Bytes ..... 15192          Collision ..... 23
Frames 128-255 Bytes..... 1928           Late Collision ..... 0
Frames 256-511 Bytes ..... 442           Dropped Frames ..... 0
Frames 512-1023 Bytes ..... 157796      UnderSize Frames ..... 0
Frames >1024 Bytes ..... 1221024         OverSize Frames ..... 0

N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 30 Display Port Statistics Menu

The information in this menu is for viewing purposes only. The statistics are defined below:

Bytes Received

Number of bytes received by the port.

Bytes Sent

Number of bytes transmitted from the port.

Frames Received

Number of frames received by the port.

Frames Sent

Number of frames transmitted from the port.

Broadcast Frames Received

Number of broadcast frames received by the port.

Broadcast Frames Sent

Number of broadcast frames transmitted from the port.

Multicast Frames Received

Number of multicast frames received by the port.

Multicast Frames Sent

Number of multicast frames transmitted from the port.

Total Bytes Received

Number of bytes received by the port.

Jabber

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

Total Frames Received

Number of frames received by the port.

CRC Error

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

Frames 64 Bytes

Frames 65 - 127 Bytes

Frames 128 - 255 Bytes

Frames 256 - 511 Bytes

Frames 512 - 1023 Bytes

Frames > 1024 Bytes

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

Fragments

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

Dropped Frames

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

Collisions

Number of collisions that have occurred on the port.

Late Collisions

Number of collisions that have occurred late in the transmission of a frame.

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.

5. If you want to clear the counters on the port and return them to "0", select option **2** - Clear Statistics from the Port Statistics menu.

Chapter 7

MAC Address Table

This chapter provides an overview of MAC addresses. In addition, it describes the procedures for viewing the static and dynamic MAC address table using a local or Telnet management session. This chapter contains the following sections:

- ❑ [MAC Address Overview on page 116](#)
- ❑ [Displaying MAC Addresses on page 118](#)
- ❑ [Adding Static Unicast and Multicast MAC Addresses on page 122](#)
- ❑ [Deleting MAC Addresses on page 124](#)
- ❑ [Changing the Aging Time on page 126](#)

MAC Address Overview

Every hardware device that you connect to your network has a unique MAC address associated with it. A MAC address is assigned to a device by the device's manufacturer. For example, every network interface card that you use to connect your computers to your network has a MAC address assigned to it by the adapter's manufacturer.

The AT-8400 Series switch has a MAC address table. The switch uses the table to store the MAC addresses of the network nodes connected to its ports, along with the port number on which each address was learned. The table can store up to 8,000 addresses.

The switch learns the MAC addresses of the end nodes by examining the source address of every packet received on a port. It adds the address and port on which the packet was received to the MAC table (if the address has not already been entered in the table). The result is a table that contains all the MAC addresses of the devices that are connected to the switch's ports, and the port number where each address was learned.

When the switch receives a packet, it also examines the destination address and, by referring to its MAC address table, determines the port where the destination node is connected. It then forwards the packet to the appropriate port and on to the end node. This increases network bandwidth by limiting each frame to the appropriate port when the intended end node is located, freeing the other switch ports for receiving and transmitting data.

If the switch receives a packet with a destination address that is not in the MAC address table, it floods the packet to all the ports on the switch. If the ports have been grouped into virtual LANs, the switch floods the packet only to those ports which belong to the same VLAN as the port on which the packet was received. This prevents packets from being forwarded onto inappropriate LAN segments and increases network security. When the destination node responds, the switch adds its MAC address and port number to the table.

If the switch receives a packet with a destination address that is on the same port on which the packet was received, it discards the packet without forwarding it on to any port. Since both the source node and the destination node for the packet are located on the same port on the switch, there is no reason for the switch to forward the packet. This too increases network performance by preventing frames from being forwarded unnecessarily to other network devices.

The type of MAC address described above is referred to as a *dynamic MAC address*. Dynamic MAC addresses are addresses that the switch learns by examining the source MAC addresses of the frames received on the ports.

Dynamic MAC addresses are not stored indefinitely in the MAC address table. The switch deletes a dynamic MAC address from the table if it does not receive any frames from the node over a specified period of time. The switch assumes that the node with that MAC address is no longer active and that its MAC address can be purged from the table. This prevents the MAC address table from becoming filled with addresses of nodes that are no longer active.

The period of time that the switch waits before purging an inactive dynamic MAC address is called the *aging time*. This value is adjustable on the AT-8400 Series switch. The default value is 300 seconds (5 minutes). For instructions on changing the aging timer, refer to Changing the Aging Time on page 126.

The MAC address table can also store *static MAC addresses*. A static MAC address, once entered in the table, remains in the table indefinitely and is never deleted, even when the end node is inactive.

You might need to enter static MAC addresses of end nodes the switch might not learn in its normal dynamic learning process. You could also enter a static MAC address so that the address remains permanently in the table, even when the end node is inactive.

Displaying MAC Addresses

The management software has menu selections for displaying all or parts of the MAC addresses table of the AT-8400 Series switch.

To display the MAC address table, perform the following procedure:

1. From the Main Menu, type **7** to select MAC Address Tables.

The MAC Address Tables Menu is shown in Figure 31.

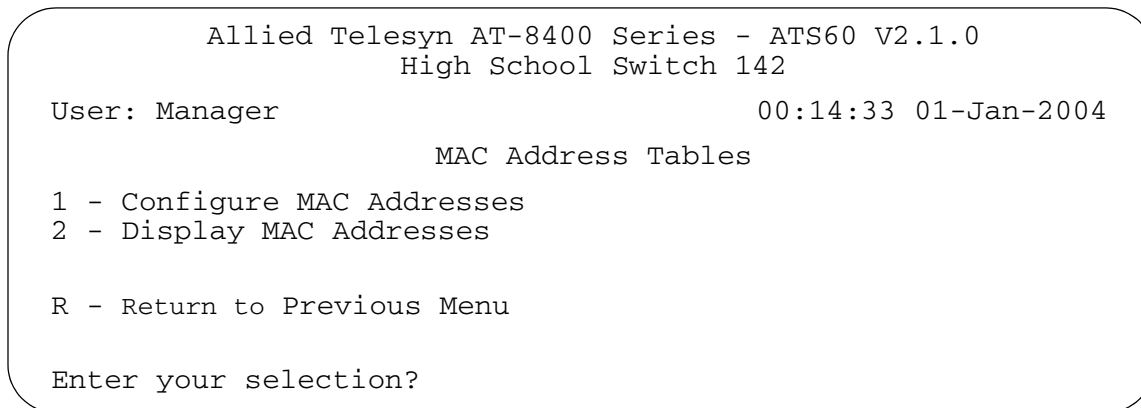


Figure 31 MAC Address Tables Menu

2. Type **2** to select Display MAC Addresses.

The Display MAC Addresses Menu is shown in Figure 32.

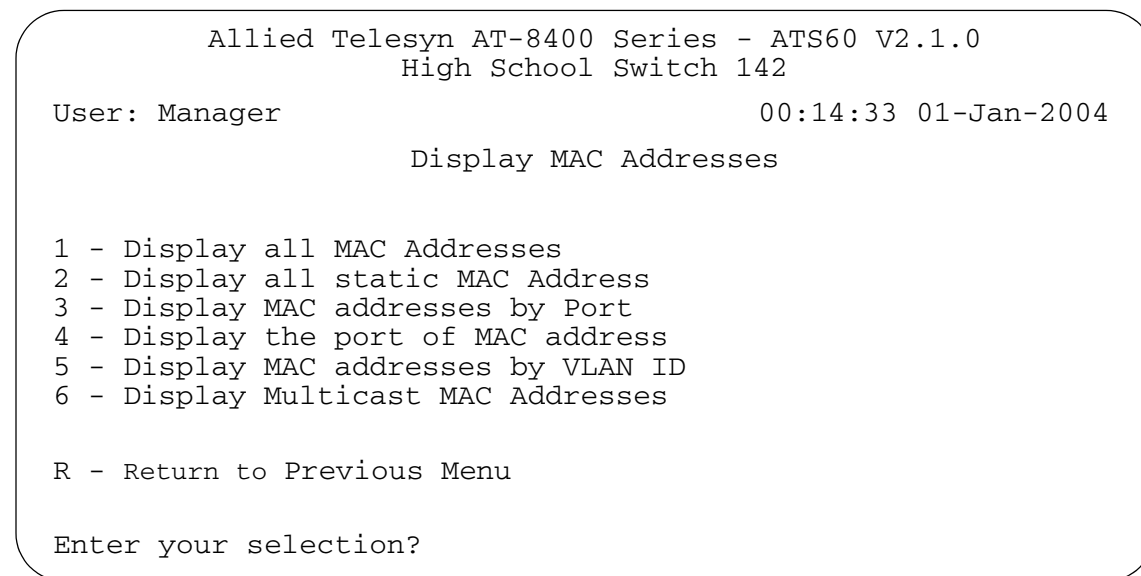


Figure 32 Display MAC Addresses Menu

3. Select the desired option. Each option is described below:

1 - Display All MAC Addresses

This option displays the Display All MAC Addresses menu. This menu lists all the switch's dynamic and static address, including multicast addresses. An example of the menu is shown in Figure 33.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
High School Switch 142

User: Manager                                00:14:33 01-Jan-2004

Display All MAC Addresses
Total Number of MAC Addresses: 212
VlanID    MAC                               Port    Type
-----
1          00:a0:d2:18:1a:c8    1.1     Dynamic
1          00:a0:c4:16:3b:80    1.2     Dynamic
1          00:a0:12:c2:10:c6    1.3     Dynamic
1          00:a0:c2:09:10:d8    1.4     Dynamic
1          00:a0:33:43:a1:87    1.5     Dynamic
1          00:a0:12:a7:14:68    1.6     Dynamic
1          00:a0:d2:22:15:10    1.7     Dynamic
1          00:a0:d4:18:a6:89    1.8     Dynamic

N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 33 Show All MAC Addresses Menu

The columns in the menu are defined in Table 3.

Table 3 Columns in the Display All MAC Addresses Menu

Column	Definition
VlanID	The VID of the port where the MAC address was learned.
MAC Address	The dynamic, static, or multicast MAC address.
Port	The port where the address was learned (dynamic) or assigned (static).
TYPE	The type of MAC address: dynamic, static, or multicast.

2 - Display All static MAC Addresses

This option displays only the static MAC addresses. The columns in the menu are the same as those in the Display All MAC Addresses Menu. For definitions of the columns, refer to Table 3 on page 119.

3 - Display MAC addresses by Port

You can use this option to view the MAC addresses that have been learned on a particular port. When you select this option, the following prompt is displayed:

```
Enter port-list:
```

Enter the ports. For information on entering ports, refer to Specifying Ports on page 34. The management software responds by listing only those addresses learned on the specified ports.

4 - Display the Port of MAC Address

In some situations, you might want to know which port learned a particular MAC address. You could display the entire MAC address table and scroll through the list looking for the MAC address. But if the switch is part of a large network, finding it could prove difficult.

Instead, you can use this option. When you select this option, the following prompt is displayed:

```
Please enter MAC address:
```

After you enter the MAC address and press Return, the following prompt is displayed:

```
Please enter a VLAN ID: [1 to 4094] ->
```

Enter a VLAN ID and press Return. Then the management software displays the number of the port where it learned the address.

5 - Display MAC Addresses by VLAN ID

This option is useful if you created VLANs on the switch and want to view the MAC addresses of the nodes of a particular VLAN. (This procedure is not of much value if the switch contains only the Default VLAN, in which case displaying the entire MAC address table, produces the same result.)

To use this option, you need to know the VID number of the VLAN whose MAC addresses you want to view. (To view VLAN VIDs, refer to Displaying VLANs on page 418.) When you select the option, the following prompt is displayed:

```
Please enter a VLAN ID: [1 to 4094] ->
```

After you have entered the VID and press Return, the management software displays all of the static and dynamic MAC address of the corresponding VLAN.

6 - Display Multicast MAC Addresses

This selection displays the multicast MAC addresses. For definitions of the columns, refer to Table 3 on page 119.

Adding Static Unicast and Multicast MAC Addresses

This section contains the procedure for adding static addresses to the switch. A MAC address added to the table with this procedure remains permanently in the table, even when the source end node is inactive. You can assign up to 255 static MAC addresses per port on the AT-8400 Series switch.

Note

When you add a static multicast address you must assign the address to all ports on the switch that belong to the multicast group. This includes the ports connected to the multicast application server and the host nodes. Failure to assign the address to all ports in the group prevents the multicast packets from reaching all appropriate nodes.

To add a static unicast or multicast address to the MAC address table, perform the following procedure:

1. From the Main Menu, type **7** to select MAC Address Tables.
The MAC Address Tables Menu is shown in Figure 31 on page 118.
2. From the MAC Address Tables menu, type **1** to select Configure MAC Addresses.

The Configure MAC Addresses menu is shown in Figure 34.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
High School Switch 142
User: Manager                                00:14:33 01-Jan-2004
Configure MAC Addresses
1 - Add static MAC Addresses
2 - Delete MAC Address
3 - Delete all dynamic MAC addresses
R - Return to Previous Menu
Enter your selection?
```

Figure 34 Configure MAC Addresses Menu

3. From the Configure MAC Addressed menu, type **1** to select Add Static MAC Addresses.

The following prompt is displayed:

```
Please enter MAC address ->
```

4. Enter the static MAC address in the following format:

```
XXXXXX XXXXXX
```

Once you have specified the MAC address, the following prompt is displayed:

```
Enter port-list:
```

5. Enter the number of the port on the switch where you want the address assigned.

The management software adds the address to the MAC address table.

6. Repeat this procedure starting with step 3 to enter additional static or multicast MAC addresses.
7. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Deleting MAC Addresses

This section contains the procedure for deleting static and dynamic unicast and multicast MAC addresses from the MAC address table and for purging the table of all dynamic addresses.

To delete MAC addresses from the table, perform the following procedure:

1. From the Main Menu, type **7** to select MAC Address Tables.
The MAC Address Tables menu is shown in Figure 31 on page 118.
2. From the MAC Address Tables menu, type **1** to select Configure MAC Addresses.

The Configure MAC Addresses menu is shown in Figure 34 on page 122.

3. To delete a MAC address from the table, do the following:
 - a. From the Configure MAC Addressed menu, type **2** to select Delete MAC Address.

The following prompt is displayed:

```
Please enter a MAC address ->
```

- b. Enter the MAC address you want deleted from the table in the following format:

```
XXXXXX XXXXXX
```

Note

You cannot delete the switch's MAC address.

The address is immediately deleted from the table.

- c. Repeat the procedure to delete additional MAC addresses.
 - d. Return to the Main Menu and type **S** to select Save Configuration Changes.
4. To delete all dynamic MAC addresses from the table, do the following:
 - a. From the Configure MAC Addressed menu, type **3** to select Delete All dynamic MAC Addresses.

The following prompt is displayed:

```
All learned MAC (non-static) addresses will be deleted.
```

```
Do you want to continue? [Yes/No] ->
```

- b. Type **Y** for yes to delete the dynamic MAC addresses or **N** for no to cancel the procedure.

If you type **Y** for yes, all dynamic MAC addresses are deleted from the MAC address table. The switch immediately begins to relearn the addresses and to add them to the table.

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 adjust the aging time, perform the following procedure:

1. From the Main Menu, type **5** to select the System Menu.
2. From the System Menu, type **1** to select Configure System.
The Configure System Menu is shown in Figure 11 on page 59.
3. From the Configure System menu, type **1** to select Configure System Software.

The Configure System Software menu is shown in Figure 12 on page 60.

4. From the Configure System Software menu, type **3** to select MAC Address Aging Time.

The following prompt is displayed:

```
Enter MAC address aging timer -> [8 to 512]
```

5. Enter a new value in seconds.
The new value is immediately activated on the switch.
6. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Chapter 8

Port Trunking

This chapter describes port trunking and contains the procedures for creating, deleting, and modifying port trunks with a local or Telnet management session. It contains the following sections:

- ❑ Port Trunking Overview on page 128
- ❑ Creating a Port Trunk on page 132
- ❑ Deleting a Port Trunk on page 134
- ❑ Modifying a Port Trunk on page 135

Port Trunking Overview

Port trunking is an economical way for you to increase the bandwidth between two Ethernet switches. For the AT-8400 Series switch, a port trunk can consist of up to eight ports that have been grouped together to function as one logical path. A port trunk increases the bandwidth between switches and is useful in situations where a single physical data link between switches is insufficient to handle the traffic load.

A port trunk sends packets from a particular source to a particular destination over the same link within the trunk. A single link is designated for flooding broadcasts and packets of unknown destination.

The example in Figure 35 consists of a 1,000 Mbps port trunk with four data links between two AT-8400 switches.

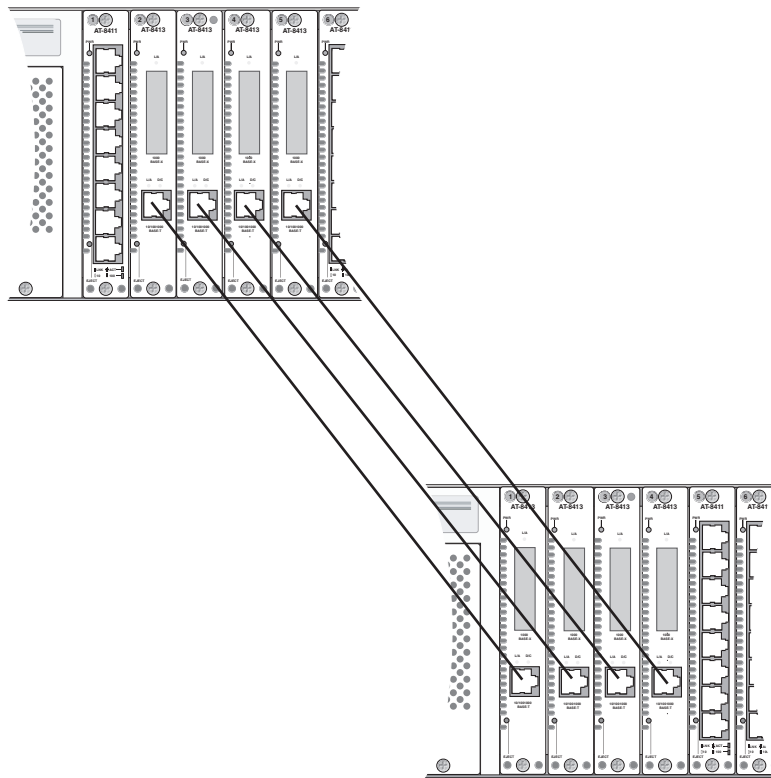


Figure 35 Port Trunk Example with 1000 Mbps Ports

The example in Figure 36 illustrates a 10/100 port trunk with 8 data links between two AT-8400 switches.

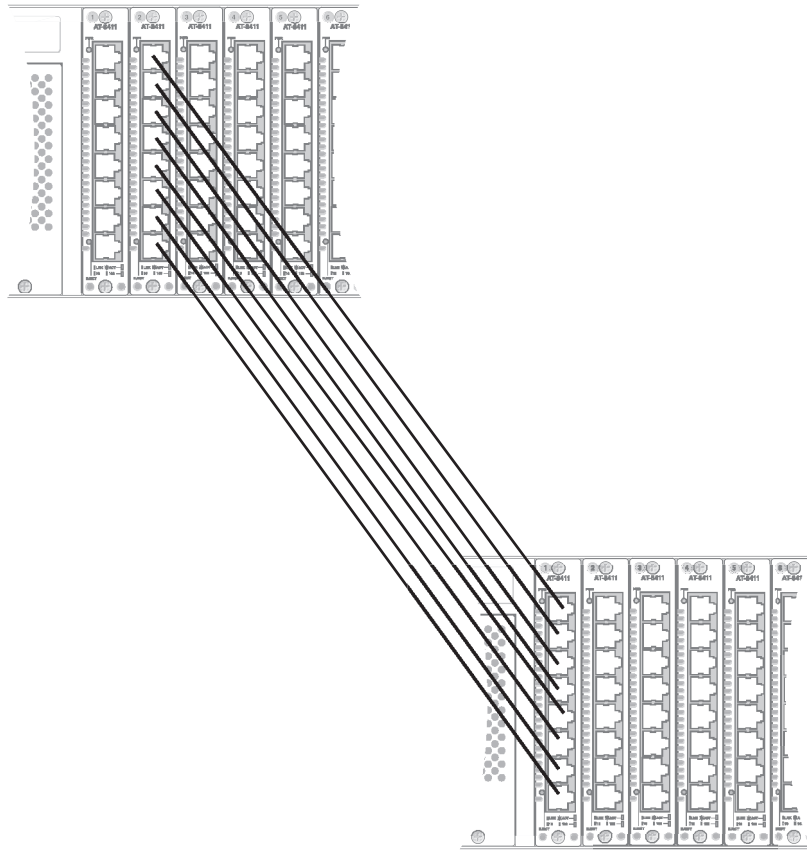


Figure 36 Port Trunk Example with 10/100 Mbps Ports

In addition, you can create a port trunk between an AT-8400 switch and other switches that support trunking.

Port Trunking Guidelines

When creating a port trunk, you need to follow a set of guidelines. Observe the following guidelines when creating a port trunk:

- An AT-8400 switch can support up to 8 trunks at a time.
- You can assign only one trunk to a line card. However, you can assign all, none, or some of the ports on a line card to a trunk.
- A port can belong to a single trunk only.
- A port trunk can consist of a maximum of 8 ports.
- The ports of a port trunk must be of the same medium type. For example, they can be all twisted-pair ports or all fiber optic ports.

- ❑ For 10/100 port trunks, such as those on an AT-8411 TX line card, all ports included in the trunk must reside on the same line card. See Figure 36 on page 129 for an illustration of a 10/100 Mbps port trunk.
- ❑ For 1,000 Mbps port trunks, such as those on an AT-8413 line card, all ports included in the trunk must reside on different line cards. Generally, there is one 1,000 Mbps port per line card as with the AT-8413 line card. See Figure 35 on page 128 for an illustration of a 1,000 Mbps port trunk.
- ❑ Although each AT-8413 line card contains two ports, only one port can be active at a time. Each AT-8413 line card can forward traffic on either the twisted pair or fiber optic port. When creating a port trunk with AT-8413 line cards, the trunked ports must be made up of either twisted pair or fiber optic ports.
- ❑ The speed, duplex mode, and flow control settings must be the same for all the ports in a trunk. In addition, the broadcast filter, override priority, HOL blocking, back pressure, MDI/MDIX, and negotiation settings must be the same for all the ports in a trunk.
- ❑ The ports of a port trunk must be members of the same VLAN. A port trunk cannot consist of ports from different VLANs.
- ❑ The ports of a port trunk must all have the same security setting.
- ❑ When cabling a trunk, the order of the connections should be maintained on both nodes. The lowest numbered port in a trunk on the switch should be connected to the lowest numbered port of the trunk on the other device, the next lowest numbered port on the switch should be connected to the next lowest numbered port on the other device, and so on.

For example, assume that you are connecting a trunk between two AT-8400 switches. On the first AT-8400 switch you chose ports 1.2, 1.3, 1.4, 1.5 for the trunk. On the second AT-8400 switch you chose ports 2.1, 2.2, 2.3, and 2.4. To maintain the order of the port connections, you would connect port 1.2 on the first AT-8400 switch to port 2.1 on the second AT-8400 switch, port 1.3 to port 2.2, and so on.

- ❑ You can create a port trunk using the fiber optic ports in an AT-8412/SC FX line card.

Before Creating Port Trunks

As mentioned in the above guidelines for creating port trunks, you need to ensure the settings on your ports are identical before adding them to a port trunk. To display your current port settings, see [Displaying Port Status](#) on page 102. Then, to update the port configuration so all of the ports in the trunk have the same configuration, see [Configuring Port Parameters](#) on page 106. For information about changing port security, see [Configuring Port Security](#) on page 473.

Load Distribution Methods

The AT-S60 management software provides the Source Address (SA) Trunking load distribution method. When a switch receives a packet from a network node, it examines the destination address to determine on which port, if any, the packet should be transmitted. If the packet is destined for a port trunk, the switch examines the source address of the packet. If this is the first packet from the source node to be transmitted over a port trunk, then the switch assigns the source address to a trunk link. All subsequent packets from the source node are sent from the assigned data link of the trunk.

The switch assigns source addresses so as to evenly distribute the addresses, as much as possible, across all the ports of the trunk. The intent is to ensure all the links in the trunk are used.

Creating a Port Trunk

This section contains the procedure for creating a port trunk on the switch. You must configure all the ports in your port trunk with the same settings. For more details, review the guidelines in Port Trunking Overview on page 128 before performing the procedure.



Caution

Connect the cables to the trunk ports on the switches after you have configured the trunk with the management software. Connecting the cables before configuring the software creates a loop in your network topology. Data loops can result in broadcast storms and poor network performance.

To create a port trunk, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
2. From the Port Menu, type **4** to select Port Trunking.

The Trunk Configuration menu is shown in Figure 37.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
High School Switch 142
User: Manager                                00:14:33 15-Jan-2004
Trunk Configuration
ID Name Type Ports
-----
1 - Create Trunk
2 - Delete Trunk
3 - Modify Trunk

R - Return to Previous Menu

Enter your selection?

```

Figure 37 Trunk Configuration Menu

3. Type **1** to select Create Trunk.

The following prompt is displayed.

```
Enter Trunk Name: ->
```

4. Enter an alphanumeric name that identifies the trunk, such as universitytrunk7. Press Return.

You can select a name with a maximum of 16 alphanumeric characters. In addition, the trunk name must contain one alphabetic character. Trunk names must be unique. You cannot enter a port name for this parameter.

The following prompt appears:

```
Enter Trunk Type: (1 - 10/100, 2 - GB): [1 to 2]
```

5. Enter a trunk type based on the speed of the ports and press Return.

Enter **1** for 10/100 Mbps ports.

Enter **2** for GBIC port or a port with speeds of up to 1,000 Mbps.

The following prompt appears:

```
Enter Trunk Ports:
```

6. Enter the ports that constitute the port trunk and press Return.

For information about how to specify ports, see [Specifying Ports](#) on page 34.

For 10/100 Mbps port trunks, all the ports that comprise the trunk must be on the same line card.

For 1,000 Mbps port trunks, all the ports that make up the trunk must be on different line cards.

Once you have specified the ports of the trunk, the following message is displayed:

```
Please wait while Trunk is being created...Done!
New ID = 1
```

The Trunk Configuration menu is updated with information about the new trunk.

7. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.
8. Configure the ports on the remote switch for port trunking.
9. Connect the cables to the ports of the trunk on the switch.

The port trunk is ready for network operation.

Deleting a Port Trunk

Use this procedure to delete an existing port trunk, including the trunk ID, name, and ports associated with the port trunk.



Caution

Before performing the following procedure, disconnect the cables from the port trunk on the switch. Deleting a port trunk with the cables attached 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 Main Menu, type **1** to select Port Menu.
The Port Menu is shown Figure 26 on page 102.
2. From the Port Menu, type **4** to select Port Trunking.
The Trunk Configuration menu is shown in Figure 37 on page 132.
3. Type **2** to delete a trunk.
The following prompt is displayed:

```
Enter Trunk ID: [1 to 22] -> 1
```
4. Enter the trunk ID number of the port trunk you want to delete and press Return.
After you delete a trunk, the following message is displayed:

```
Please wait while Trunk is being deleted...Done!  
Press any key to continue
```
5. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.
You have successfully deleted the port trunk from the switch.

Modifying a Port Trunk

Use this procedure to modify an existing port trunk. See the Port Trunking Guidelines on page 129 for information specific to 10/100 Mbps and 1000 Mbps port trunks.

When you select the Modify Port Trunk selection on the Port Trunking menu, you can perform the following actions:

- Changing the name of the trunk
- Adding ports to a trunk
- Deleting ports from a trunk
- Setting (or overwriting) the ports in a trunk
- Clearing (or removing) all the ports in a trunk

After you modify a port trunk, you need to return to the Main Menu and save your changes using the **S** - Save Configuration Changes selection.

To modify a port trunk on the switch, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
The Port Menu is shown in Figure 26 on page 102.
2. From the Port Menu, type **4** to select Port Trunking.
The Trunk Configuration menu is shown in Figure 37 on page 132.
3. Type **3** - Modify Trunk to modify a port trunk.

The Modify Trunk menu is shown in Figure 38. Notice the two current port trunks, called `highschool` and `elementary`, included in this figure.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
High School Switch 142

User: Manager                                00:14:33 15-Jan-2004

                                Modify Trunk
ID      Name      Type      Ports
-----
1       highschool 10/100MB  4.1-4
2       elementary 10/100MB  4.5-8

1 - Change Trunk Name
2 - Add ports to Trunk
3 - Delete ports from Trunk
4 - Set ports in Trunk
5 - Clear ports in Trunk

U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 38 Modify Trunk Menu

4. Select one of the following options:
 - Select **1** - Change Trunk Name to change the alphanumeric name of the trunk. See Changing the Name of the Port Trunk on page 137.
 - Select **2** - Add ports to Trunk to add ports to a trunk. See Adding Ports to an Existing Port Trunk on page 137.
 - Select **3** - Delete ports from Trunk to delete ports from a trunk. See Deleting Ports from a Port Trunk on page 139.
 - Select **4** - Set ports in Trunk to overwrite the ports in the trunk with a new list of ports. See Replacing Ports in a Trunk on page 140.
 - Select **5** - Clear ports in Trunk to delete all the ports in a trunk. See Clearing Ports in a Port Trunk on page 141.
5. After making changes, type **R** until you return the Main Menu. Then type **S** to select Save Configuration Changes.

Changing the Name of the Port Trunk

Use this procedure to change the name of an port trunk.

To change the name of an port trunk, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
The Port Menu is shown in Figure 26 on page 102.
2. From the Port Menu, type **4** to select Port Trunking.
The Trunk Configuration menu is shown in Figure 37 on page 132.
3. Type **3** to modify a trunk.
The Modify Trunk menu is shown in Figure 38 on page 136.
4. Select **1** - Change Trunk Name to change the alphanumeric name of the trunk.

The following prompt is displayed:

```
Enter Trunk ID: [1 to 22] -> 1
```

5. Enter the trunk ID number of the trunk you want to change the name of and press Return. A list of the current trunk IDs appears in the Modify Trunk menu. See Figure 38 on page 136.

After you enter the trunk ID, the following prompt is displayed:

```
Enter new trunk name:
```

6. Type in a new name and press Return.
You can select a name with a maximum of 16 alphanumeric characters. In addition, the trunk name must contain one alphabetic character. Trunk names must be unique. You cannot enter a port name for this parameter.
The Modify Trunk menu is updated with the new trunk name.
7. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes. The new trunk name is saved.

Adding Ports to an Existing Port Trunk

Use this procedure to add ports to an existing port trunk. Be sure to follow the guidelines regarding port trunks. For detailed information, see Before Creating Port Trunks on page 131. If you want to overwrite all of the current ports in port trunk and replace them with new ports, see Replacing Ports in a Trunk on page 140.

To add ports to an existing port trunk, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
The Port Menu is shown in Figure 26 on page 102.

2. From the Port Menu, type **4** to select Port Trunking.
The Trunk Configuration menu is shown in Figure 37 on page 132.

3. Type **3** to modify a trunk.
The Modify Trunk menu is shown in Figure 38 on page 136.

4. Select **2** - Add ports to Trunk to add ports to an existing trunk.

The following prompt appears:

```
Enter Trunk ID: [1 to 22] -> 1
```

5. Enter the trunk ID number of the trunk you want to modify and press Return. A list of the current trunk IDs appears in the Modify Trunk menu. See Figure 38 on page 136.

The following prompt appears:

```
Enter ports to add to trunk:
```

6. Enter the ports you want to add to the trunk and press Return.

For information about how to specify ports, see Specifying Ports on page 34.

For 10/100 port trunks, all the ports that comprise the trunk must be on the same line card.

For GBIC port trunks (or ports with speeds up to 1,000 Mbps), all the ports that make up the trunk must be on different line cards.

The Modify Trunk menu is updated with the new ports.

7. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes to save the new ports.

Deleting Ports from a Port Trunk

Use this procedure to delete ports from an existing port trunk. If you want to delete all the ports from an existing port trunk and replace them with a new set of ports, see *Replacing Ports in a Trunk* on page 140 and *Clearing Ports in a Port Trunk* on page 141.

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

1. From the Main Menu, type **1** to select Port Menu.
The Port Menu is shown in Figure 26 on page 102.
2. From the Port Menu, type **4** to select Port Trunking.
The Trunk Configuration menu is shown in Figure 37 on page 132.
3. Type **3** - Modify Trunk.
The Modify Trunk menu is shown in Figure 38 on page 136.
4. Select **3** - Delete ports from Trunk.
The following prompt appears:
`Enter Trunk ID: [1 to 22] -> 1`
5. Enter the trunk ID number of the trunk you want to modify and press Return. A list of the current trunk IDs appears in the Modify Trunk menu. See Figure 38 on page 136.
After you enter the trunk ID, the following prompt appears:
`Enter ports to delete:`
6. Enter the ports you want to delete from the trunk and press Return.
For information about how to specify ports, see *Specifying Ports* on page 34.
For 10/100 port trunks, all the ports that comprise the trunk must be on the same line card.
For GBIC port trunks (or ports with speeds up to 1,000 Mbps), all the ports that make up the trunk must be on different line cards.
The Modify Trunk menu is updated to reflect the ports you deleted.
7. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Replacing Ports in a Trunk

Use this procedure to overwrite, or replace, the current ports in a port trunk with a new list of ports. To add ports to an existing port trunk while retaining the current ports, see Adding Ports to an Existing Port Trunk on page 137.

To overwrite the current ports in a port trunk with a new list of ports, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
The Port Menu is shown in Figure 26 on page 102.
2. From the Port Menu, type **4** to select Port Trunking.
The Trunk Configuration menu is shown in Figure 37 on page 132.
3. Type **3** - Modify Trunk.
The Modify Trunk menu is shown in Figure 38 on page 136.
4. Type **4** - Set ports in Trunk.
The following prompt appears:
`Enter Trunk ID: [1 to 22] ->1`
5. Enter the trunk ID number of the trunk you want to update and press Return. A list of the current trunk IDs appears in the Modify Trunk menu. See Figure 38 on page 136.
After you enter the trunk ID, the following prompt appears:
`Enter trunk ports:`
6. Enter the new trunk ports that overwrite the current port trunks and press Return.
For information about how to specify ports, see Specifying Ports on page 34.
For 10/100 port trunks, all the ports that comprise the trunk must be on the same line card.
For GBIC port trunks (or ports with speeds up to 1,000 Mbps), all the ports that make up the trunk must be on different line cards.
The Modify Trunk menu is updated with the new ports.
7. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes to save the new ports.

Clearing Ports in a Port Trunk

Use this procedure to clear, or delete, **all** of the current ports in a port trunk while leaving the port trunk ID, name, and type. To delete individual ports, see Deleting Ports from a Port Trunk on page 139.

To clear or delete all the ports on a port trunk, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
The Port Menu is shown in Figure 26 on page 102.
2. From the Port Menu, type **4** to select Port Trunking.
The Port Trunking menu is shown in Figure 37 on page 132.
3. Type **3** - Modify Trunk.
The Modify Trunk menu is shown in Figure 38 on page 136.
4. Type **5** - Clear ports in Trunk to remove the current list of ports.
The following prompt appears:
Enter Trunk ID: [1 to 22] -> 1
5. Enter the trunk ID number and press Return. A list of the current trunk IDs appears in the Modify Trunk menu. See Figure 38 on page 136.
After you enter the trunk ID, the following message appears:
Please wait while clearing Trunk ports...Done!
Press any key to continue
The Modify Trunk menu is updated to show no ports associated with the Trunk ID.
6. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Chapter 9

Port Mirroring

This chapter describes port mirroring and provides the procedures for creating and deleting a port mirror using a local or Telnet management session. It contains the following sections:

- Port Mirroring Overview on page 143
- Creating a Port Mirror on page 144
- Modifying a Source Port Mirror on page 146
- Deleting a Destination Port Mirror on page 148
- Enabling a Destination Port Mirror on page 149
- Disabling a Destination Port Mirror on page 150

Port Mirroring Overview

The port mirroring feature allows you to monitor the traffic on one or more ports by copying the traffic to another port which is called the destination mirror port. Using port mirroring, you can connect a network analyzer to the mirror port to monitor both traffic received and transmitted from one or more ports (which are called source mirror ports). In the software, the destination mirror port is called the destination port while the source mirror ports are called source ports.

Observe the following guidelines when creating a port mirror:

- You can mirror from one to 12 ports on a switch at a time, depending on number and types of line cards installed in your chassis.
- The ports that are mirrored and the mirroring port must be located on the same switch.
- You can assign each line card one source mirroring port and one destination mirroring port. Each line card can participate in only one port mirror.
- When setting up a port mirror, you need to consider the transfer rate of the source ports and the receive rate of the destination port mirror. When you exceed the maximum receive rate of the destination port, you might not be able to monitor all of the frames. For example, two 100 Mbps source ports sending bidirectional traffic are mirrored to a 100 Mbps destination port. The maximum receive rate of the 100 Mbps destination port is 100 Mbps. As a result, frames are dropped (assuming a maximum transfer rate). If you replace the 100 Mbps destination port with a 1GB port in this scenario, then the receive rate of the 1GB destination port is 400 Mbps.

Creating a Port Mirror

Use the following procedure to create a port mirror. For information about how to specify a port, see Specifying Ports on page 34.

To create a port mirror, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
The Port Menu is shown in Figure 26 on page 102.
2. From the Port Menu, type **5** to select Port Mirroring.
The Port Mirroring menu is shown in Figure 39.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
High School Switch 142
User: Manager                                00:14:33 15-Jan-2004
Port Mirroring
Destination Port      Source Port(s)      Status
-----
1 - Create Mirror
2 - Modify Mirror
3 - Delete Mirror
4 - Enable Mirror
5 - Disable Mirror
U - Update Display
R - Return to Previous Menu
Enter your selection?
```

Figure 39 Port Mirroring Menu

3. Type **1** to select Create Mirror.
The following prompt is displayed:
Enter Destination Port:
4. Enter the number of the port that functions as the mirror port (that is, the port where the traffic is copied) and press Return.
You can specify only one mirror port. For information about how to specify a port, see Specifying Ports on page 34.
5. The following prompt is displayed:
Enter the Source Port(s) [port-list]:
6. Enter a single port or a list of nonconsecutive ports on different line cards whose traffic is to be mirrored. Press Return.

Note

You cannot assign a range of ports on the same line card as source mirror ports.

The source mirror port (or ports) is displayed at the top of the screen.

7. After making changes, Type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Your changes are saved. The port mirror is now functional.

Modifying a Source Port Mirror

Use the following procedure to add, delete, set (overwrite), or clear a source port mirror. For information about how to specify a port, see *Specifying Ports* on page 34.

To modify a source port mirror, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
The Port Menu is shown in Figure 26 on page 102.
2. From the Port Menu, type **5** to select Port Mirroring.
The Port Mirroring menu is shown in Figure 39 on page 144.
3. Type **2** to select Modify Mirror.
The Modify Mirror Menu is shown in Figure 40.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
High School Switch 142

User: Manager                                00:14:33 15-Jan-2004

                                Modify Mirror

Destination Mirror Port    Source Mirror Port(s)    Status
-----
3.4                        8.4, 9.6                Enabled
4.5                        10.1, 11.1, 12.1       Enabled

1 - Add Source Port(s)
2 - Delete Source Port(s)
3 - Set Source Port(s)
4 - Clear Source Port(s)

U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 40 Modify Mirror Menu

4. Select **1- Add Source Port(s)** to add a source port mirror to a current list.

The following prompt appears:

```
Enter Destination Port:
```

5. Enter the destination mirror port from the list at the top of the menu and press Return.

For information about how to specify a port, see *Specifying Ports* on page 34.

The following prompt appears:

```
Enter Source Port(s) [port-list]:
```

6. Enter the source mirror port (s) or port list and press Return.

Note

You cannot assign a range of ports as source mirror ports.

The display at the top of the Port Mirroring menu is updated.

7. To delete a source port mirror, enter **2**.

The following prompt appears:

```
Enter Destination Port:
```

8. Enter the destination port from the list at the top of the screen and press Return.

The following prompt appears:

```
Enter Source Port(s) [port-list]:
```

9. Enter source mirror port(s) or port list and press Return.

The source and destination mirror ports are removed from the display at the top of the menu.

10. To set, or overwrite, a source mirror port, enter **3**.

The following prompt appears:

```
Enter Destination Port:
```

11. Enter the destination port from the list at the top of the screen and press Return.

The following prompt appears:

```
Enter Source Port(s) [port-list]:
```

12. Enter the new source mirror port(s) or port list and press Return.

13. To clear, or remove, all source mirror ports from a port mirror, type **4**.

The following prompt appears:

```
Enter Destination Port:
```

14. Enter the destination mirror port from the list at the top of the screen and press Return.

All source mirror ports are removed from the Modify Mirror Menu.

15. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

The port mirror is updated with your changes.

Deleting a Destination Port Mirror

To delete a destination port mirror and its source mirror port(s), perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
The Port Menu is shown in Figure 26 on page 102.
2. From the Port Menu, type **5** to select Port Mirroring.
The Port Mirroring menu is shown in Figure 39 on page 144.
3. Type **3** to select Delete Mirror.
The following prompt is displayed.

```
Enter Destination Port:
```
4. Enter the destination mirror port from the list at the top of the menu and press Return.
For information about how to specify a port, see Specifying Ports on page 34.
The destination port and the source port(s) are removed from the display at the top of the Port Mirroring menu.
5. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.
The port mirror on the switch is deleted. The port that was functioning as the port mirror is now available for normal network operations.

Enabling a Destination Port Mirror

Use this procedure if you have previously disabled a destination port mirror (see Disabling a Destination Port Mirror on page 150) and you want to make it active again.

To enable a destination port mirror, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.

The Port Menu is shown in Figure 26 on page 102.

2. From the Port Menu, type **5** to select Port Mirroring.

The Port Mirroring menu is shown in Figure 39 on page 144.

3. Type **4** to select Enable Mirror.

The following prompt is displayed.

```
Enter Destination Port [port-list, all]:
```

4. Enter the mirror port that you want to enable and press Return.

port-list

For information about how to specify ports, see Specifying Ports on page 34.

all

Use this selection to enable all the mirror ports listed on the Port Mirroring Menu.

At the top of the Port Mirroring menu, the Status column changes to Enabled.

Note

By default, the mirror is enabled when it is created.

5. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

The port mirror (or port mirrors) is now enabled.

Disabling a Destination Port Mirror

Use this procedure to prevent traffic from the source mirror port from being mirrored to the destination port. You may want to use this procedure to temporarily stop mirroring the source traffic while reserving the destination port for mirroring.

To disable a port mirror, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.

The Port Menu is shown in Figure 26 on page 102.

2. From the Port Menu, type **5** to select Port Mirroring.

The Port Mirroring menu is shown in Figure 39 on page 144.

3. Type **5** to select Disable Mirror.

The following prompt is displayed.

```
Enter Destination Port [port-list, all]:
```

4. Enter the mirror port that you want to disable and press Return.

port-list

For information about how to specify ports, see Specifying Ports on page 34.

all

Use this selection to disable all the mirror ports listed on the Port Mirroring Menu.

At the top of the Port Mirroring menu, the Status column changes to Disabled.

5. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

The port mirror is now disabled.

Section II

Advanced Features

The chapters in Section II explain how to manage the advanced features on an AT-8400 switch from a local or Telnet management session. The chapters include:

- ❑ Chapter 10: File System Configuration on page 152
- ❑ Chapter 11: File Downloads and Uploads on page 167
- ❑ Chapter 12: Event Log on page 203
- ❑ Chapter 13: Class of Service (CoS) on page 214
- ❑ Chapter 14: IGMP Snooping on page 218
- ❑ Chapter 15: STP and RSTP on page 228
- ❑ Chapter 16: Multiple Spanning Tree Protocol (MSTP) on page 257

Chapter 10

File System Configuration

The chapter describes the file system operations you can perform on configuration and system files. It contains the following sections:

- ❑ File System Configuration Overview on page 153
- ❑ Setting, Creating, Editing, and Displaying System Configuration Files on page 156
- ❑ Copying and Renaming System Files on page 162
- ❑ Deleting System Files on page 163
- ❑ Displaying System Files on page 165

File System Configuration Overview

The File System Menus allow you to choose the active system configuration file, create a system configuration file, and perform basic file operations on system files.

You may want to create a configuration file to perform a routine task or to ensure all your AT-8400 switches have an identical configuration. There are two ways of obtaining new configuration files. Either you can create a configuration file with the File System Menus or you can upload a configuration file (see Setting, Creating, Editing, and Displaying System Configuration Files on page 156.) After you use either method, you can load the new configuration file onto the switch with the File System Menus. In addition, you can view the contents of the configuration file.

Note

The default name for the configuration file is boot.cfg.

In addition, the File System Menus, allow you to perform basic file operations on system files. You can display copy, rename, and delete system files. The following file types are the supported system files:

- certificate files
- certificate enrollment request files
- configuration files
- image files
- key files

For in-depth information about certificate and certificate enrollment request files, see Chapter 21: Public Key Infrastructure (PKI) on page 501. For information about the configuration file, see Chapter 10: File System Configuration on page 152. The image file is the AT-S60 management software. For information about the key file, see Chapter 20: Encryption on page 484.

All of the above system file types have the same naming conventions. See the next section for more details.

File Naming Conventions

The file subsystem provides a flat file system which means directories are not supported. Files are uniquely identified by a file name in the following format:

```
filename.ext
```

where:

- ❑ *filename* is a descriptive name for the file, and may be one to sixteen characters in length. Valid characters are lowercase letters (a–z), uppercase letters (A–Z), digits (0–9), and the following characters: ~ ' @ # \$ % ^ & () _ - { }. Invalid characters are: ! * + = " | \ [] ; : ? / , < > .
- ❑ *ext* is a file name extension which is three characters in length. Valid characters are lowercase letters (a–z), uppercase letters (A–Z), digits (0–9) and the hyphen character (-). The extension is used by the switch to determine the data type of the file and how to use the file. Each file name extension must be separated from the filename portion by a period (.)

Table 4 File Extensions and File Types

Extension	File Type
cfg	Configuration file (or boot script)
cer	Certificate file
csr	Certificate enrollment request
img	Image file
key	Key file

Note

The certificate file, certificate enrollment request file, and key file types are only appears in the AT-S60 version 2.0.0 software.

The following is an example of a valid file name for a configuration file:

```
standardconfig.cfg
```

The following is an example of an invalid file name:

```
sys/head_o.cfg
```

The backslash character (/) is not a valid delimiter character and directories are not supported.

Using Wildcards to Specify Groups of Files

You can use the asterisk character (*) as a wildcard character in some fields to identify groups of files. In addition, a wildcard can be combined with other characters. The following are examples of valid wildcard expressions:

*.cfg

*.key

28*.cfg

Setting, Creating, Editing, and Displaying System Configuration Files

Use the procedures in this section to load a system configuration file onto the switch, create a system configuration file, and view the contents of system configuration files. There are three procedures:

- ❑ Setting a System Configuration File on page 156
- ❑ Creating a System Configuration File on page 158
- ❑ Displaying System Configuration Files on page 159

Before you set or create a system configuration file, you may want to find out more information about configuration files on your switch. To display a list of current configuration file names, see [Displaying System Files](#) on page 165.

Note

For information about downloading and uploading files, see [Chapter 11: File Downloads and Uploads](#) on page 167.

Setting a System Configuration File

This procedure allows you to set, or select, the configuration file for the switch. You can select a configuration file that you have created or that you have downloaded onto the switch. After you set the configuration file, the switch uses it for the next reboot.

However, this procedure does not reboot the switch. For instructions on how to use the menus to reboot the switch, see [Rebooting a Switch](#) on page 63.

Perform the following procedure to set a specific configuration file to be the boot configuration file. This file is used to boot the system in the next session.

1. From the Main Menu, type **9** to select File Menu.

The File Menu is shown in Figure 41.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
High School Switch 142
User: Manager                                00:14:33 15-Jan-2004

File Menu

1 - Boot Configuration File ..... boot.cfg (Exist)
2 - Current Configuration ..... boot.cfg
3 - Create Configuration File
4 - View Configuration File
5 - Display File(s)
6 - Copy File
7 - Rename File
8 - Delete File

R - Return to Previous Menu

Enter your selection?

```

Figure 41 File Menu

2. Type **1** to select Boot Configuration File.

This field lists the configuration file that is to be used for the **next** reboot of the switch. In other words, the commands in the configuration file are executed when the switch is rebooted.

The following message is displayed:

```
Enter Boot Configuration File Name:
```

3. Enter the name of the configuration file that you want to load onto the AT-8400 Series Switch.

Note

The file name you enter here must already exist on the switch.

The file name must already exist on the switch. You can enter up to 16 alphanumeric characters followed by .cfg. See File Naming Conventions on page 154.

The following message is displayed.

```
Setting boot configuration name, please wait...
```

Note

The Current Configuration field is a read-only field. It displays the name of your current configuration file. This is the configuration file that was used to boot up the system in the current session.

Creating a System Configuration File

This procedure allows you to save your system configuration to a file on the switch. You may want to save a copy of your system configuration file to download it onto another switch. Or, you may want to create a backup of your current configuration file.

If the system configuration file does not reflect the current configuration on the system, the **S** - Save Configuration appears on the Main Menu. If you want to save your configuration changes, select **S** - Save Configuration from the Main Menu.

To create a system configuration file, perform the following procedure:

1. From the Main Menu, type **9** to select File Menu.
The File Menu is shown in Figure 41 on page 157.
2. From the File Menu, type **3** to select Create Configuration File to create a new configuration file.

The following prompt is displayed:

```
Enter Configuration File Name:
```

3. Enter a configuration file name.

You can enter up to 16 alphanumeric characters followed by .cfg. See File Naming Conventions on page 154.

Note

If a filename already exists, the system displays a message asking if you want to overwrite the existing file name. Follow the prompts.

Note

You cannot name a configuration file default.cfg. This file name is reserved by the switch.

The following message is displayed:

```
Saving...Please wait 15 seconds before rebooting the system.
```

Editing a System Configuration File

You can edit a system configuration file on your workstation, using a text editor such as Word pad, and then upload it to one or more switches. A system configuration file contains a structured list of commands. Because the system configuration file defines so many switch operations, it is crucial to follow these guidelines when you edit the file:

- Follow the syntax of the CLI commands exactly. Refer to the *AT-S60 Command Line User's Guide* for the command syntax. Displaying System Configuration Files on page 159 shows an example of a system configuration file.
- Never alter the order of the feature headings that are listed (or commented out with # signs).



Caution

Any deviation from the command syntax or order of features in the system configuration file can create serious switch malfunctions.

Displaying System Configuration Files

Use the following procedure to view configuration files. To display a list of configuration file names, see Displaying System Files on page 165.

To view configuration files, perform the following procedure:

1. From the Main Menu, type **9** to select File Menu.
The File Menu is shown in Figure 41 on page 157.
2. Type **4** to select View Configuration File to display the contents of the current configuration file.

The following prompt is displayed:

```
Enter Configuration File Name:
```

The View Configuration File Menu is shown in Figure 42.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
High School Switch 142

User: Manager                                00:14:33 15-Jan-2004

View Configuration File Menu

Configuration File: mydefault.cfg
-----

#
# Port Configuration
#
set switch port(s)=3.1 speed = 100mfull
set switch port(s)=3.2 speed = 100mfull
set switch port(s)=3.3 speed = 100mfull
set switch port(s)=3.4 speed = 100mfull
#
#
#Port Trunking Configuration
#
#
#Port Mirror Configuration
#

N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection?
```

Figure 42 View Configuration File Menu (page 1)

3. Press **N** to select Next Page to see the second page of the View Configuration File Menu.

The second page of the View Configuration File Menu is shown in Figure 43.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
                          High School Switch 142
User: Manager                                00:14:33 15-Jan-2004
                          View Configuration File Menu
                          Configuration File: boot.cfg
-----
#
#Port Security Configuration
#
#
#VLAN Configuration
#
create vlan=v3 vid=3 vlantype=portbased taggedports=1.2-8 untaggedport=3.1-
8
#
#STP Configuration
#
#
#Switch Configuration
#
N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection?
```

Figure 43 View Configuration File Menu (page 2)

4. Continue pressing **N** to advance to the next screen or **P** to display the previous screen.

Copying and Renaming System Files

Use this procedure to copy and rename system files that reside on the switch. You can copy and rename certificate, certificate request, configuration, image, and key files.

To display a list of system file names, see [Displaying System Files](#) on page 165.

To copy and rename system files, perform the following procedure:

1. From the Main Menu, type **9** to select File Menu.
The File Menu is shown in [Figure 41](#) on page 157.
2. From the File Menu, type **6** to select Copy File to copy a system file or list of files.

Note

Selecting Copy File does not allow you to overwrite files.

The following prompt is displayed:

```
Enter Source File Name:
```

3. Enter the name of the file you want to copy.

The following prompt is displayed:

```
Enter Destination File Name:
```

4. Enter the new file name.

You can enter a file name of up to 16 alphanumeric characters, followed by a 3 letter extension. You must keep the same extension. See [File Naming Conventions](#) on page 154.

The following message is displayed:

```
Copying file please wait...
```

5. Type **7** - Rename file to rename a system file.

The following prompt is displayed:

```
Enter File Name to be renamed:
```

6. Enter a file name.

```
Renaming please wait...
```

Deleting System Files

Use this procedure to delete a system file. You can delete any of the following file types:

- certificate files
- certificate enrollment request files
- configuration files
- image files
- key files

If you delete a configuration file that is set as the Boot Configuration file, then (Not Exist) appears next to the configuration file name on the File Menu. See Setting a System Configuration File on page 156. The (Not Exist) statements means the configuration file is not present on the switch. Even without selecting the **S** - Save option on the Main Menu, the switch's configuration is reset to the factory default settings if it is rebooted in this state. See Appendix A: AT-S60 Default Settings on page 820 for a complete list of the factory default configuration settings.

Note

If you delete a configuration file that is set as the boot configuration file, (Not Exist) appears next to the file name. In this case, the configuration file is not present on the switch. As a result, if you reboot in this state the switch is reset with factory defaults.

You may want to display the current system file names before you begin this procedure. To display a list of system file names, see Displaying System Files on page 165.

Note

You cannot retrieve a deleted file.

To delete a system file, perform the following procedure:

1. From the Main Menu, type **9** to select File Menu.
The File Menu is shown in Figure 41 on page 157.

2. From the File Menu, type **8** to select Delete file to delete a system file.

The following prompt is displayed:

```
Enter File Name to be deleted:
```

3. Enter the name of the file you want to delete.

The following message is displayed:

```
Deleting file...please wait
```

Displaying System Files

Use this procedure to display a list of current system files. You can use this procedure to display certificate, configuration, image, and key files. For information about shortcuts for specifying file names, see File Naming Conventions on page 154.

To display a list of current system file names, perform the following procedure:

1. From the Main Menu, type **9** to select File Menu.

The File Menu is shown in Figure 41 on page 157.

2. From the File Menu, type **5** to select Display files to display a list of system files.

The following prompt is displayed:

```
Enter File Name to list:
```

3. Enter a configuration file name.

You can enter up to 16 alphanumeric characters followed by a three letter extension. In addition, special characters, such as *, are permitted. For example, to display the current list of certificate files, enter:

```
*.cer
```

To display the current list of configuration files, enter:

```
*.cfg
```

To display the current list of key files, enter:

```
*.key
```

To display the system files that begin with the letter t, enter:

```
t*.*
```

The Display File(s) Menu is shown in Figure 44.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
High School Switch 142
User: Manager                                00:14:33 15-Jan-2004
Display File(s) Menu

Filename          Size (bytes)      Created
-----
default.cfg      805              01/10/2002 12:01:16
boot.cfg         1249             10/24/2003 16:50:40
newcfg.cg        1082             07/12/2003 16:59:06
serverkey150.key 768              11/30/2003 19:17:35
hostkey250.key   1024             11/30/2003 20:38:20
atikey350.key    560              12/11/2003 20:56:13

U - Update Display
R - Return to Previous Menu

Enter your selection?
```

Figure 44 Display File(s) Menu

The format of the Display File(s) Menu is described below:

- The Filename column indicates the name of the system file.
- The Size column indicates the size of the file, in bytes.
- The Created column lists the date and time in the following format: month/day/year hours:minutes:seconds.

Chapter 11

File Downloads and Uploads

This chapter contains procedures for downloading and uploading files to a switch, as well as information on obtaining AT-S60 software updates. It includes the following sections:

- ❑ Overview on page 168
- ❑ Obtaining Management Software Updates on page 171
- ❑ Downloading Files on page 172
- ❑ Uploading Files on page 187
- ❑ Downloading the AT-S60 Image Switch to Switch on page 201

Overview

Downloading and uploading are useful system features that make switch management efficient. For example, you can upload a configuration file from a switch to your management station, make changes with a text editor, and then download it onto a different switch. This can be useful in network environments that contain a number of AT-8400 chassis on different subnets that need to be configured at the same, or nearly the same time.

You can also download a new version of the AT-S60 management software onto a switch so that a switch always has the latest software available. Several file types can coexist on an AT-8400 chassis. These file types are specified in Table 5.

Table 5 File Types and Extensions

File Type	Extension
Certificate file	cer
Certificate enrollment request	csr
Configuration file (or boot script)	cfg
Image file	img
Key file	key

For in-depth information about certificate and certificate enrollment request files, see Chapter 24: Public Key Infrastructure (PKI) on page 501. For information about the configuration file, see Chapter 10: File System Configuration on page 152. The image file is the AT-S60 management software. For information about the key file, see Chapter 23: Encryption.

You can download or upload all of these file types, with some exceptions in downloading and uploading switch to switch. Two of the file types that you may want to download or upload most frequently are:

- AT-S60 management software image (.img file)

This image is a combination of the operating software for the switch and the bootloader code that initializes the switch when powered on or reset.

- System configuration file (.cfg file)

This file contains the settings for the different switch parameters, such as VLANs, port trunks, and so forth. If you have not entered configuration settings, then the system configuration file

contains the factory default settings. For more information, refer to Appendix A: AT-S60 Default Settings on page 820. For information about editing a system configuration file, see Editing a System Configuration File on page 159.

Obtaining Management Software Updates on page 171 describes where to find management software updates.

The Downloads & Uploads Menu is shown in Figure 45.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Production Switch 142
User: Manager                                00:14:33 01-Jan-2004
Downloads & Uploads

1 - Download Application Image/BootLoader
2 - Upload Application Image/BootLoader

3 - Download a File
4 - Upload a File

R - Return to Previous Menu

Enter your selection?
```

Figure 45 Downloads & Uploads Menu

The chapter is divided into two major sections, based on the options on the Downloads & Uploads Menu:

- Options 1 and 3 for downloading files are described in Downloading Files beginning on page 172.
- Options 2 and 4 for uploading files are described in Uploading Files beginning on page 187.

The final section, Downloading the AT-S60 Image Switch to Switch on page 201, contains the procedure for downloading the image file from one switch to another. This process is particularly useful if your network contains a large number of AT-8400 chassis. You can upgrade the software on one master switch and then instruct the master switch to upgrade the software on the other switches in the same subnet.

Note

Downloading a File on page 609 describes how to download files using a web browser management session.

Obtaining Management Software Updates

New releases of management software for our managed products can be downloaded from either of the following Internet sites:

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

To use the FTP server, go to the above web site. Then login to the FTP server by entering "anonymous" for the user name and your email address for the password.

Downloading Files

This section contains the procedures for downloading files onto a switch from a local or Telnet management session. Because the process for downloading files depends upon the file type (either an image file or another type of file), this section contains two parts:

- ❑ Downloading an Image File Using Xmodem or TFTP on page 173
- ❑ Downloading a File Using Xmodem or TFTP on page 180

You can transfer a file using either the Xmodem or TFTP protocol for a local management session, or the TFTP protocol only for a Telnet management session. In order to use TFTP, there must be a node on your network with the TFTP server software and the file to download must be stored on that node.

In general, installing a new AT-S60 software image does not change the current configuration settings of a switch (for example, IP address, subnet mask, and virtual LANs).

However, when you upgrade the AT-S60 management software from version 1.1.4 to version 2.0.0NE or later, you must reset the switch to the factory defaults and then update your configuration file.

This procedure assumes that you have already obtained the new AT-S60 management software from Allied Telesyn and stored it on the management workstation from which you are performing the procedure, or on the TFTP server.

Downloading an Image File Using Xmodem or TFTP

The following procedures describe how to download a .img file type (image file) only. To download a different file type, see Downloading a File Using Xmodem or TFTP on page 180. See Table 5 on page 168 for more information about file types.



Caution

The switch stops forwarding Ethernet traffic during the initialization of the AT-S60 software image.

Note

To download new software onto the switch using TFTP, your network must have a server or workstation with the TFTP server software. You must store the new AT-S60 image or configuration file and specify the file on that server or workstation.

To download a new software image file onto a switch, perform the following procedure:

1. Start a local management session on the switch where you intend to download the new management software image file.
2. From the Main Menu, type **4** to select Administration Menu.
3. From the Administration Menu, type **D** to select Downloads & Uploads.

The Downloads & Uploads Menu is shown in Figure 46.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
High School Switch 142
User: Manager                                00:14:33 01-Jan-2004
Downloads & Uploads

1 - Download Application Image/BootLoader
2 - Upload Application Image/BootLoader

3 - Download a File
4 - Upload a File

R - Return to Previous Menu

Enter your selection?

```

Figure 46 Downloads & Uploads Menu

Note

Menu options 2 and 4 in the menu are described in [Uploading Files](#) on page 187. Option 3 is described in [Downloading a File Using Xmodem or TFTP](#) on page 180.

4. Type **1** to download a new software image file onto the switch.

If you are using a local management session, the following prompt is displayed:

```
Download Method/Protocol [X-Xmodem, T-TFTP]:
```

If you are using a Telnet management session, the following prompt is displayed:

```
Only TFTP downloads are available for a Telnet access.
```

```
TFTP server IP address:
```

To download an image file using Xmodem, refer to [Downloading an Image File Using Xmodem](#), which follows. To download an image file using TFTP, refer to [Downloading an Image File Using TFTP](#) on page 178.

Downloading an Image File Using Xmodem

To download an image file using Xmodem (this procedure shows how to use the Hilgraeve HyperTerminal program), perform the following procedure:

1. Type **X** at the prompt displayed in Step 4 in the procedure that begins on page 173.

The following prompt is displayed:

```
You are going to invoke the Xmodem download utility.
Do you wish to continue? [Yes/No]
```

2. Type **Y**.

The following prompt is displayed:

```
Use HyperTerminal's 'Transfer/Send File' option to
select Filename & Protocol
```

3. In the HyperTerminal main window, select the **Transfer** menu. Then select **Send File** from the pull-down menu, as shown in Figure 47.

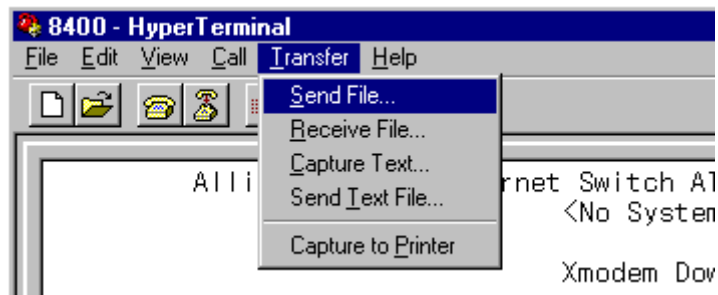


Figure 47 Transfer Menu

The Send File window is shown in Figure 48.

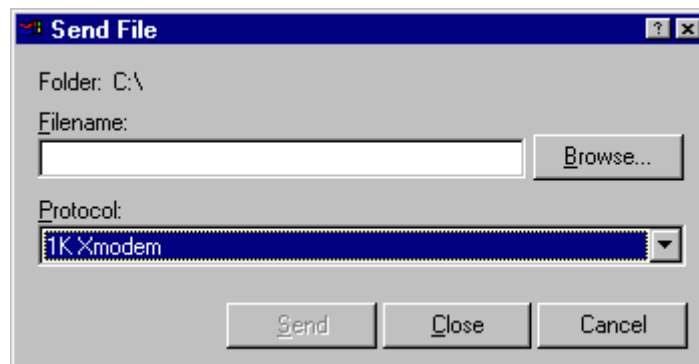


Figure 48 Send File Window

4. In the Filename field, type the path and filename, or click the Browse button to locate and select the file to be downloaded onto the switch.

- Click on the Protocol field and select as the transfer protocol either Xmodem or 1K XModem.

Note

The transfer protocol must be Xmodem or 1K Xmodem. The recommended transfer protocol is 1K Xmodem because it is much faster than the Xmodem protocol. For a faster download, set the console baud rate to 115200. Refer to Starting a Local Management Session on page 40 for information on setting the console baud rate.

- Click **Send**.

The software file immediately begins to download onto the switch. The Xmodem File Send window in Figure 49 displays the current status of the software file download. The download process takes several minutes to complete.

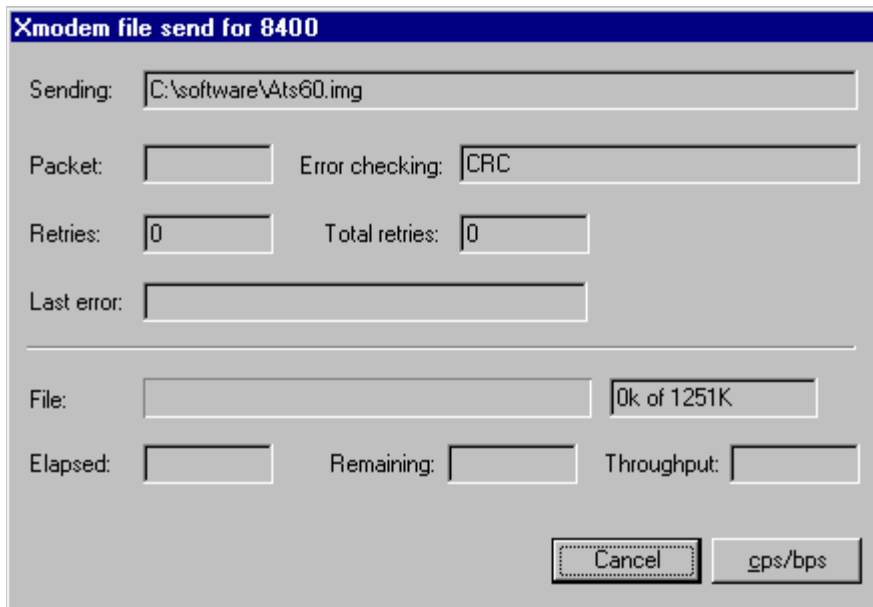


Figure 49 XModem File Send Window

When the downloading process is complete, the file is validated. The switch then compares the new image to the existing image that the switch is running. If the two files are the same, the following message is displayed:

```
Skipping this download...  
Press any key to continue
```

If this message is not displayed, proceed to step 8. Otherwise, go on to step 7.

- Press any key.

The Downloads & Uploads Menu is displayed, as shown in Figure 46 on page 173.

8. If the new image file differs from the existing one, the following message is displayed:

For a local management session:

```
Switch is about to reboot. Do you want to proceed?  
[Yes/No]
```

For a Telnet management session:

```
Remote access will be lost. Do you want to continue?  
[Yes/No]
```

9. Type **N** if you do not want to activate the new image file.

The Downloads & Uploads Menu is displayed, as shown in Figure 46 on page 173.

10. Type **Y** to activate the new image file and reset the switch.

The switch now decompresses and initializes the software, a process that takes less than two minutes to complete. After the management software is initialized, you can press any key to start a local management session. Or, restart the Telnet management session to display the login prompt.

Note

Do not interrupt the decompression and initialization process. Do not manually reboot the switch. The switch automatically reboots as part of the initialization process.

Downloading an Image File Using TFTP

To download a file using TFTP, perform the following procedure:

1. To begin:
 - a. If you are using a Telnet management session, the following prompt is already displayed from step 4 in the procedure that begins on page 173:


```
Only TFTP downloads are available for a Telnet
access.
TFTP server IP address:
```
 - b. If you are using a local management session, type **T** at the prompt displayed in step 4 in the procedure that begins on page 173:

The following prompt is displayed:

```
TFTP Server IP address:
```
2. Enter the IP address of the TFTP server.

The following prompt is displayed:

```
Remote File Name:
```
3. Enter the name of the image file to download.

Note

The image file name can be a maximum of 20 characters long.

Note

The file you are downloading must be stored in the download directory of the TFTP server.

After you specify the filename, the download begins. The download process takes several seconds to complete.

When the downloading process is complete, the file is validated. The switch compares the new image to the existing image file that the switch is running. If the two files are the same, the following message is displayed:

```
The downloading application image version is same as
current version
Skipping this download...
Press any key to continue...
```

If this message is not displayed, proceed to step 5. Otherwise, go on to step 4.

4. Press any key.

The Downloads & Uploads Menu is displayed, as shown in Figure 46 on page 173.

5. If the new image file differs from the existing one, the following message is displayed:

For the local management session:

```
Switch is about to reboot. Do you want to proceed?  
[Yes/No]
```

For the Telnet management session:

```
Remote access will be lost. Do you want to continue?  
[Yes/No]
```

6. Type **N** if you do not want to activate the new image file.
The Downloads & Uploads menu is displayed, as shown in Figure 46 on page 173.
7. Type **Y** to activate the new image file and reset the switch.

Note

If you type **Y** and are using a Telnet management session for this procedure, the Telnet session terminates. Allow at least two minutes for the process to complete before you restart the Telnet management session.

The switch now decompresses and initializes the software, a process that takes less than two minutes to complete. After the management software is initialized, you can press any key to start a local management session, or restart the Telnet management session to display the login prompt.

Note

Do not interrupt the decompression and initialization process. Do not manually reboot the switch. The switch automatically reboots as part of the initialization process.

Downloading a File Using Xmodem or TFTP

The following procedures describe how to download certificate, certificate enrollment requests, configuration, and key files. See Table 5 on page 168 for a list of file types and their extensions. To download an image file, see Downloading an Image File Using Xmodem or TFTP on page 173.

If you are downloading a configuration file, there are some precautions you need to take. Downloading a configuration file from one AT-8400 switch to another is useful in networks that contain a large number of AT-8400 chassis with identical hardware configurations-- that is, the same number of line cards and the same types of line cards installed in the same slots of the chassis. For example, two AT-8400 chassis with 8 AT-8411 line cards installed in slots 1 through 8 have identical hardware configurations.



Caution

If you download a configuration file onto a switch with a different hardware configuration, you may halt the operation of your switch.

To download a file using Xmodem or TFTP, perform the following procedure:

1. Start a local management session on the switch where you intend to download the new management software or configuration file.
2. From the Main Menu, type **4** to select Administration Menu.
3. From the Administration Menu, type **D** to select Downloads & Uploads.

The Downloads & Uploads menu is shown in Figure 50.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
High School Switch 142
User: Manager                                00:14:33 01-Jan-2004
Downloads & Uploads

1 - Download Application Image/BootLoader
2 - Upload Application Image/BootLoader

3 - Download a File
4 - Upload a File

R - Return to Previous Menu

Enter your selection?

```

Figure 50 Downloads & Uploads Menu

Note

Menu options 2 and 4 in the menu are described in Uploading Files on page 187.

4. Type **3** to download a new file onto the switch.

If you are using a local management session, the following prompt is displayed:

```
Download Method/Protocol [X-Xmodem, T-TFTP]:
```

If you are using a Telnet management session, the following prompt is displayed:

```
Only TFTP downloads are available for a Telnet
access.
```

```
TFTP server IP address:
```

To download a file other than an image file using Xmodem, refer to Downloading a File Using Xmodem, which follows. To download a file other than an image file using TFTP, refer to Downloading a File Using TFTP on page 185.

Downloading a File Using Xmodem

To download certificate, certificate enrollment requests, configuration, and key files using Xmodem, perform the following procedure:

1. Type **X** at the prompt displayed in Step 4 in the procedure that begins on page 180.

The following prompt is displayed

```
Local file name:
```

2. Enter the local file name.

This will be the name of the of the file after it is downloaded to the switch.

The following prompt is displayed:

```
You are going to invoke the Xmodem download utility.  
Do you wish to continue? [Yes/No]
```

3. Type **Y**.

The following prompt is displayed:

```
Use HyperTerminal's 'Transfer/Send File' option to  
select Filename & Protocol
```

4. In the HyperTerminal main window, select the **Transfer** menu. Then select **Send File** from the pull-down menu, as shown in Figure 51.

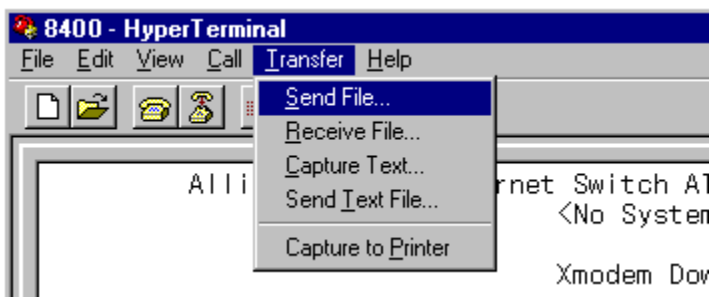


Figure 51 Transfer Menu

The Send File window is shown in Figure 52.

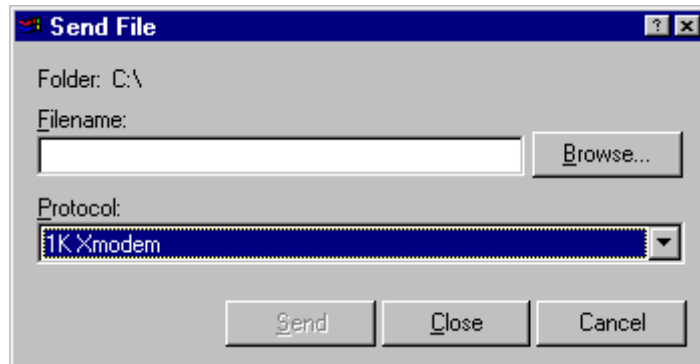


Figure 52 Send File Window

Note

The transfer protocol must be Xmodem or 1K Xmodem.

5. In the Filename field, type the path and filename, or click the Browse button to locate and select the file to be downloaded onto the switch.
6. Click on the Protocol field and select as the transfer protocol either Xmodem or, for a faster download, 1K XModem.

7. Click **Send**.

The file immediately begins to download onto the switch. The Xmodem File Send window in Figure 53 displays current status of the file download.

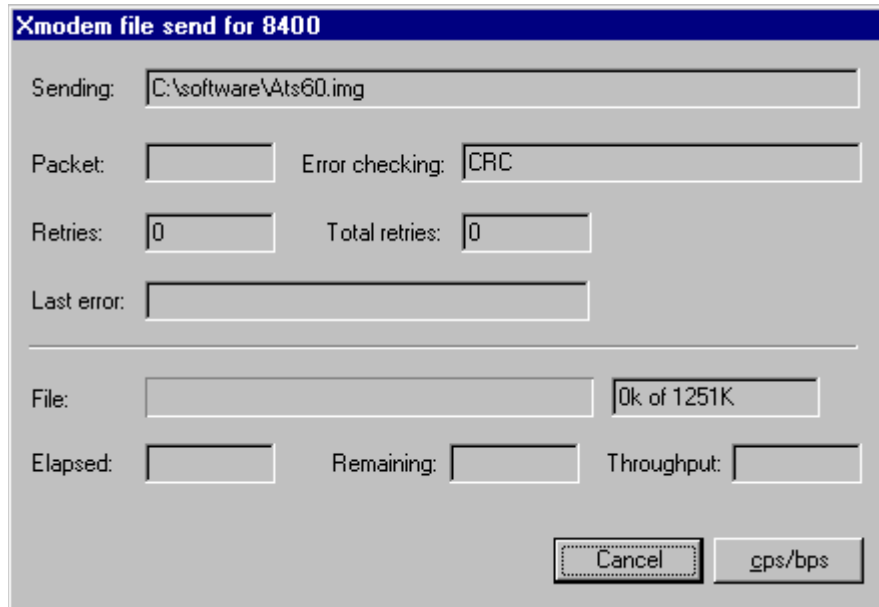


Figure 53 XModem File Send Window

When the download process is complete, a message is displayed that shows the file name and size.

Downloading a File Using TFTP

To download a certificate, certificate enrollment requests, configuration, and key files using TFTP, perform the following procedure:

1. If you are using a Telnet management session, go to step 2. If you are using a local management session, type **T** at the prompt displayed in Step 4 in the procedure that begins on page 180.

The following prompt is displayed:

```
TFTP server IP address:
```

2. Enter the IP address of the TFTP server.

The following prompt is displayed:

```
Remote File Name:
```

3. Enter the remote file name of the file on the TFTP server that you want to download.

Note

The file name can be a maximum of 20 characters long.

Note

The file you are downloading must be stored in the download directory of the TFTP server.

If the file name format is correct, the following prompt is displayed:

```
Local file name:
```

4. Enter a name for the file after it is downloaded to the switch.

Note

The file name can be a maximum of 20 characters long.

Note

The file you are downloading must be stored in the download directory of the TFTP server.

If the local file name you entered already exists on the switch, the following message is displayed:

```
The specified local file exists already.
Press any key to continue.
```

Press any key. The Downloads & Uploads Menu is displayed, as shown in Figure 50 on page 181.

If you specified an acceptable file name, the download begins. When the TFTP download is complete, the following message is displayed:

```
File successfully sent!  
Press any key to continue...
```

5. Press any key.

The Downloads & Uploads menu is displayed, as shown in Figure 50 on page 181.

Uploading Files

This section contains procedures for uploading the following files to a management station or TFTP server using a local or Telnet management session. You can upload:

- Current AT-S60 software image and bootloader software
- Certificate files
- Certificate Enrollment Request files
- Configuration files
- Key files

You can transfer a file using either the Xmodem or TFTP protocol for a local management session, or the TFTP protocol only for a Telnet management session. In order to use TFTP, there must be a node on your network with the TFTP server software.

This section contains two parts:

- [Uploading an Image File Using Xmodem or TFTP on page 188](#)
- [Uploading a File Using Xmodem or TFTP on page 194](#)

Uploading an Image File Using Xmodem or TFTP

The following procedures describe how to upload an `.img` file type (image file) only. To upload other file types, see *Uploading a File Using Xmodem or TFTP* on page 194. See Table 5 on page 168 for a list of file types.

To upload a file from a switch onto your management station, perform the following procedure:

Note

Allied Telesyn does not recommend that you upload an AT-S60 software image onto a management workstation for the purpose of downloading it onto another switch. Obtain new AT-S60 software images for downloading onto a switch from the Allied Telesyn web site.

1. Start a local management session on the switch where you intend to upload the management software image or configuration file.
2. From the Main Menu, type **4** to select Administration Menu.
3. From the Administration Menu, type **D** to select Downloads & Uploads.

The Downloads & Uploads menu is shown in Figure 54.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
                          High School Switch 142

User: Manager                               00:14:33 01-Jan-2004

                          Downloads & Uploads

1 - Download Application Image/BootLoader
2 - Upload Application Image/BootLoader

3 - Download a File
4 - Upload a File

R - Return to Previous Menu

Enter your selection?
```

Figure 54 Downloads & Uploads Menu

Note

Menu options 1 and 3 are described in *Downloading an Image File Using Xmodem or TFTP* on page 173. Option 4 is described in *Uploading a File Using Xmodem or TFTP* on page 194.

4. Type **2** to upload the AT-S60 software image from the switch.

If you are using a local management session, the following prompt is displayed:

```
Upload Method/Protocol [X-Xmodem, T-TFTP]:
```

If you are using a Telnet management session, the following prompt is displayed:

```
Only TFTP uploads are available for a Telnet access.  
TFTP server IP address:
```

To upload an image file using Xmodem, refer to [Uploading an Image File Using Xmodem](#), which follows. To upload an image file using TFTP, see [Uploading an Image File Using TFTP](#) on page 193.

Uploading an Image File Using Xmodem

To upload an image file using Xmodem (this procedure shows how to use the Hilgraeve HyperTerminal program), perform the following procedure:

1. Type **X** at the prompt displayed in Step 4 in the procedure that begins on page 187.

The following prompt is displayed:

```
You are going to invoke the Xmodem upload utility.  
Do you wish to continue? [Yes/No]
```

2. Type **Y**.

The following prompt is displayed:

```
Use HyperTerminal's 'Transfer/Receive File' option  
to select Protocol
```

3. In the HyperTerminal main window, select the **Transfer** menu. Then select **Receive File** from the pull-down menu, as shown in Figure 55.

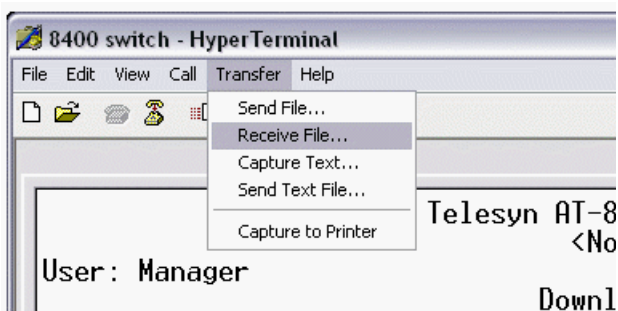


Figure 55 Transfer Menu

The Receive File window is shown in Figure 56.

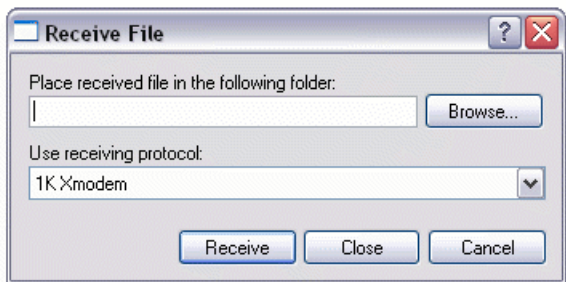


Figure 56 Receive File Window

4. In the Place received file in the following folder field, type the path to the destination folder, or click the Browse button to locate the destination folder.

- Click on the Protocol field and select as the transfer protocol either Xmodem or 1K XModem.

Note

The transfer protocol must be Xmodem or 1K Xmodem. The recommended transfer protocol is 1K Xmodem because it is much faster than the Xmodem protocol. For a faster download, set the console baud rate to 115200. Refer to Starting a Local Management Session on page 40 for information on setting the console baud rate.

- Click **Receive**.

The Receive filename window is displayed, as shown in Figure 57.

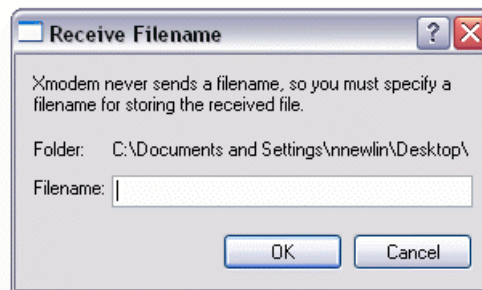


Figure 57 Receive Filename Window

- Enter a name for storing the uploaded file.

The Xmodem file receive window is displayed, as shown in Figure 58.

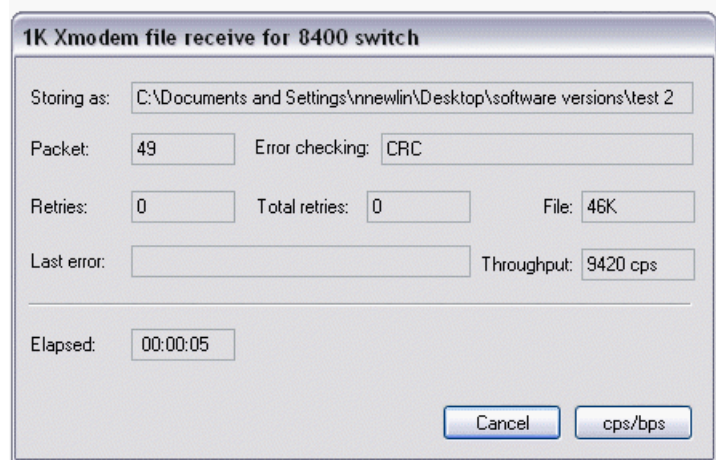


Figure 58 Xmodem File Receive Window

The file immediately begins to upload onto the system. The Xmodem File Receive window displays the current status of the file upload. The upload time depends upon the size of the file.

When the upload is complete, the following message is displayed:

```
Xmodem File Transfer Completed  
Press any key to continue...
```

8. Press any key.

The Downloads & Uploads Menu is displayed, as shown in Figure 54 on page 188.

Uploading an Image File Using TFTP

To upload an image file using TFTP, perform the following procedure:

1. If you are using a Telnet management session, go to step 2. If you are using a local management session, type **T** at the prompt displayed in Step 4 in the procedure that begins on page 187.

The following prompt is displayed:

```
TFTP Server IP address:
```

2. Enter the IP address of the TFTP server.

The following prompt is displayed:

```
Remote File Name:
```

3. Enter the file name of the image file that you want to upload.

Note

The file you are uploading must be stored in the upload directory of the TFTP server.

Once a file name has been specified, the upload begins. When the TFTP upload is complete, the following message is displayed:

```
File successfully sent!  
Press any key to continue...
```

4. Press any key.

The Downloads & Uploads menu is displayed, as shown in Figure 54 on page 188.

Uploading a File Using Xmodem or TFTP

The following procedures describe how to upload certificate, certificate enrollment requests, configuration, and key files. See Table 5 on page 168 for a list of file types and extensions. To upload an image file, see Uploading an Image File Using Xmodem or TFTP on page 188.

To upload files, perform the following procedure:

1. Start a local management session on the switch where you intend to upload the management software image or configuration file.
2. From the Main Menu, type **4** to select Administration Menu.
3. From the Administration Menu, type **D** to select Downloads & Uploads.

The Downloads & Uploads menu is shown in Figure 59.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
High School Switch 142
User: Manager                                00:14:33 01-Jan-2004
Downloads & Uploads
1 - Download Application Image/BootLoader
2 - Upload Application Image/BootLoader
3 - Download a File
4 - Upload a File
R - Return to Previous Menu
Enter your selection?
```

Figure 59 Downloads & Uploads Menu

Note
Menu options 1 and 3 are described in Downloading Files on page 172.

4. Type **2** to upload the AT-S60 software image from the switch.

If you are using a local management session, the following prompt is displayed:

```
Upload Method/Protocol [X-Xmodem, T-TFTP]:
```

If you are using a Telnet management session, the following prompt is displayed:

```
Only TFTP uploads are available for a Telnet access.  
TFTP server IP address:
```

To upload a file using Xmodem, refer to [Uploading a File Using Xmodem](#), which follows. To upload a file using TFTP, refer to [Uploading a File Using TFTP](#) on page 199.

Uploading a File Using Xmodem

To upload a file using Xmodem (this procedure shows how to use the Hilgraeve HyperTerminal program), perform the following procedure:

1. Type **X** at the prompt displayed in Step 4 in the procedure that begins on page 187.

The following prompt is displayed:

```
Local file name:
```

2. Enter a name for the file to be uploaded from the switch.

Note

The file name must already exist on the switch.

Note

If you receive the following message:

```
The specified local file name/type can not be  
uploaded.
```

```
Press any key to continue.
```

the file name extension is not correct or the file does not exist. See File Naming Conventions on page 154 for more information about file types.

The following prompt is displayed:

```
You are going to invoke the Xmodem upload utility.  
Do you wish to continue? [Yes/No]
```

3. Type **Y**.

The following prompt is displayed:

```
Use HyperTerminal's 'Transfer/Receive File' option  
to select Protocol
```

- In the HyperTerminal main window, select the **Transfer** menu. Then select **Receive File** from the pull-down menu, as shown in Figure 60.

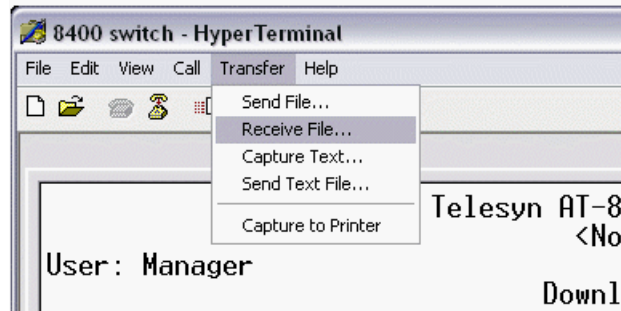


Figure 60 Transfer Menu

The Receive File window in Figure 61 is shown.

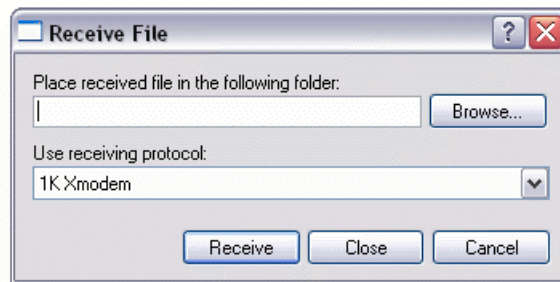


Figure 61 Receive File Window

- In the Place received file in the following folder field, type the path to the destination folder, or click the Browse button to locate the destination folder.
- Click on the Protocol field and select as the transfer protocol either Xmodem or, for a faster download, 1K XModem.
- Click Receive.

The Receive filename window is displayed, as shown in Figure 62.

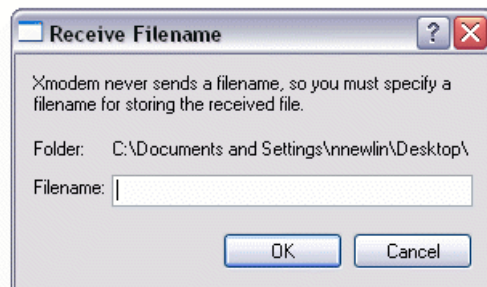


Figure 62 Receive Filename Window

8. Enter a name for storing the uploaded file.

This will be the name for the file on the management station after the upload process is complete.

The Xmodem file receive window opens, as shown in Figure 63

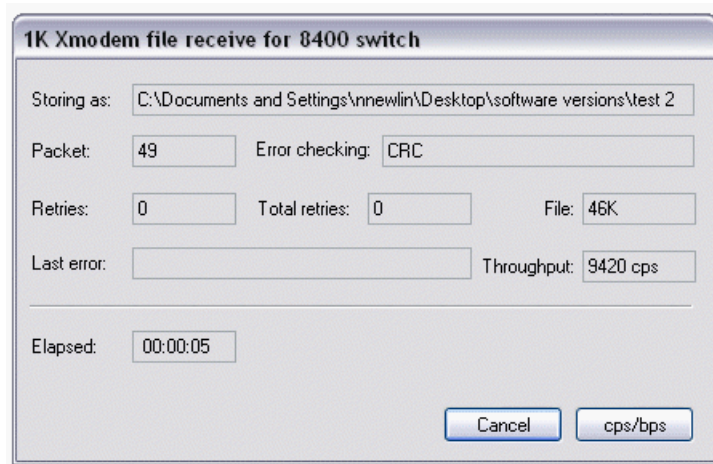


Figure 63 Xmodem File Receive Window

The file immediately begins to upload onto the system. The Xmodem File Receive window displays current status of the file upload. The upload time depends upon the size of the file.

When the upload is complete, the following message is displayed:

```
Xmodem File Transfer Completed  
Press any key to continue...
```

9. Press any key.

The Downloads & Uploads Menu is displayed, as shown in Figure 59 on page 194.

Uploading a File Using TFTP

To upload a file using TFTP, perform the following procedure:

1. To begin:
 - a. If you are using a Telnet management session, the following prompt is already displayed from step 4 in the procedure that begins on page 194:

```
Only TFTP downloads are available for a Telnet
access.
TFTP server IP address:
```
 - b. If you are using a local management session, type **T** at the prompt displayed in step 4 in the procedure that begins on page 194:

The following prompt is displayed:

```
TFTP Server IP address:
```
2. Enter the IP address of the TFTP server.

The following prompt is displayed:

```
Remote File Name:
```
3. Enter the remote file name.

This will be the name of the of the file on the TFTP server after you complete the upload process.

Note

The file you are uploading must be stored in the upload directory of the TFTP server.

If the file name format is correct, the following prompt is displayed:

```
Local file name:
```

4. Enter a name for the file to be uploaded from the switch.

Note

The file name must already exist on the switch.

Note

If you receive the following message:

```
The specified local file name/type can not be
uploaded.
```

```
Press any key to continue.
```

the file name extension is not correct or the file does not exist. See File Naming Conventions on page 154 for more information about file types.

After you specify an acceptable file name, the upload begins. When the TFTP upload is complete, the following message is displayed:

```
File successfully sent!
Press any key to continue...
```

5. Press any key.

The Downloads & Uploads menu is displayed, as shown in Figure 59 on page 194.

Downloading the AT-S60 Image Switch to Switch

This procedure explains how to download an AT-S60 software image from a master AT-8400 switch to another switch using enhanced stacking. You can update only AT-8400 Series switches. In other words, you cannot download AT-S60 management software onto an AT-8000 Series switch.

Downloading an image file from one AT-8400 to another is useful in networks that contain a large number of AT-8400 chassis. Once you have updated the software on the master switch of an enhanced stack, you can instruct the master switch to automatically upgrade the other AT-8400 chassis in the same subnet.

Note

The following procedure can be performed from either a local or Telnet management session.

To download a management software image from a master AT-8400 Series switches to other AT-8400 Series switches in the same subnet, perform the following procedure:

1. From the Main Menu, type **8** to select Enhanced Stacking.
The Enhanced Stacking menu is shown in Figure 19 on page 80.
2. From the Enhanced Stacking menu, type **2** to select Stacking Services.

Note

The **2** - Stacking Services selection is available only from a management session on a master switch.

The Stacking Services Menu is shown in Figure 20 on page 81.

3. From the Stacking Services menu, type **1** to select Get/Refresh List of Switches.
4. From the Stacking Services menu, type **4** to select Image Download Image/Bootloader.

A prompt similar to the following is displayed:

```
Enter the remote switch number -> [1 to 12]
```

5. Enter the number (Num column in menu) of the AT-8400 Series switches whose software you want to update. You can specify more than one switch at a time. You can specify the switches individually (e.g., 2,4,5), as a range (e.g., 3-6), or both (e.g., 1-4,7,10). You can download to up to 24 switches at a time.

Note

You can update only AT-8400 Series switches. You cannot download AT-S60 management software onto an AT-8000 Series switch.

The following prompt is displayed:

```
Do you want to show remote switch burning flash ->
[Yes/No]
```

You can use this prompt to view system messages as the software image is stored to flash memory.

6. You can respond with Yes or No to this prompt. It does not affect the download.

The following prompt is displayed:

```
Do you want confirmation before downloading each
switch -> [Yes/No]
```

If you are updating multiple switches, answering Yes to this prompt causes the management software to display a confirmation message before it upgrades a switch. If you answer No, the master switch downloads without a confirmation message.

The management software begins the download. The management software notifies you when the download is complete.



Caution

After a switch image file has been downloaded, the switch must write it to flash memory. This requires one to two minutes to complete. Do not reset or power off the switch while it is writing the file. After the file has been written to flash memory, the switch automatically resets.

Chapter 12

Event Log

This chapter describes the event log. Sections in the chapter include:

- Event Log Overview on page 204
- Configuring the Event Log on page 205
- Displaying Events on page 207
- Saving the Event Log on page 212
- Clearing the Event Log on page 213

Event Log Overview

A managed switch is a complex piece of computer equipment that includes both hardware and software. Multiple software features operate simultaneously, interoperating with each other and processing large amounts of network traffic. It is often difficult to determine exactly what is happening when a switch appears not to be operating normally, or what happened when the problem occurred.

A network manager's major task is to monitor the system functions and to deal with problems as they arise. The event log provides vital information about system activity on the AT-8400 switch that helps you identify and solve system problems. The event log includes the following information:

- the time and date of an event
- the severity of an event
- the AT-S60 software module that generated the event
- a description of the event

The event log can store up to 4,000 entries. All events are purged from the log when the switch is reset or power cycled. However, you can save an event log by using the S-Save option. See *Saving the Event Log* on page 212.

Allied Telesyn recommends that you set the switch's date and time if you intend to use the event log. Otherwise, the switch does not log the entries with the correct date and time. For instructions, refer to *Setting the System Time* on page 59.

Note

The event log, even when disabled, logs all AT-S60 initialization events that occur when the switch is reset or power cycled. Any switch events that occur after AT-S60 initialization are entered into the log only if you enable the event log. The default setting for the event log is disabled.

Configuring the Event Log

To enable or disable the event log and specify what the switch does when the log reaches its maximum capacity, perform the following procedure:

1. From the Main menu, type **E** to select Event Log.

The Event Log Menu is shown in Figure 64.

```

Allied Telesyn Ethernet Switch AT-S60 V2.1.0
      Production Switch 32
User: Manager                               11:20:02 02-Jan-2004

                          Event Log

1 - Event Logging.....Disabled
2 - Log Full Action.....Wrap
3 - Event Output.....Temporary
  (Memory)
4 - Event Order.....Chronological
5 - Event Mode.....Normal
6 - Event Severity.....E,W,I
7 - Event Module.....All

C - Clear Log
S - Save Log to File
V - View Log
R - Return to Previous Menu

```

Figure 64 Event Log Menu

2. To enable or disable the event log feature, type **1** to select Event Logging.

Choose between the following selections:

Enabled

Choose Enabled to immediately begin to add events to the log.

Disabled

Choose Disabled to immediately stop adding events to the log. This is the default.

3. To determine what action the switch takes when the event log reaches its maximum capacity, type **2** to select Log Full Action.

Choose between the following selections:

Wrap

Once the event log reaches its maximum capacity, this option deletes old entries and continues to add new entries. This is the default.

Halt

Once the event log reaches its maximum capacity, this option causes the log to stop adding new entries.

4. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

To display the events in the log, go to the next procedure.

Displaying Events

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

1. From the Main menu, type **E** to select Event Log.

The Event Log menu is shown in Figure 64 on page 205.

Note

The **3** - Event Output option is a read-only field. The selection is always set to Temporary.

2. To select the order of the events in the log, type **4** to select the Event Order.

Toggle between the following selections:

Chronological

This option displays the events in from the oldest event to the most recent event. The default is Chronological.

Reverse Chronological

This option displays the events from the most recent event to the oldest event.

3. To select the format of the event log, type **5** to select Event Mode.

Toggle between the following selections:

Normal

This option displays the time, software module, severity, and description for each event. The default is Normal.

Full

This option displays the same information as Normal, plus filename, line number, and event ID.

4. To display events of a selected severity, type **6** to select Event Severity.

The following prompt is displayed:

```
Enter Severity levels to display (ALL, E - Error, W -
Warning, I - Information, D - Debug) ->
```

5. Choose one or more of the following selections:

Table 6 Event Log Severity Levels

Value	Severity Level	Description
ALL	All levels	Displays all of the following message types.
E	Error	Switch operation is severely impaired.
W	Warning	An issue may require manager attention.
I	Information	Useful information that can be ignored during normal operation.
D	Debug	Detailed high-volume information that is intended for Technical Support.

The default is to display informational events, error messages, and warning messages. You can select more than one severity at a time by separating severities with a comma—for example, E,W.

6. To display the events of a selected AT-S60 software module, type **7** to select Event Module.

The following prompt is displayed:

```
Enter Modules to display (ALL, SYSTEM, CLI, EVTLOG, MAC,
STP, VLAN, GARP, PCFG, PMIRR, PTRUNK, PSEC, PACCESS, IP,
ESTACK, FILE, IGMP, TIME, TFTP, HTTP, TELNET, SNMP, RADIUS,
TACACS, ENCO, PKI, SSL, SSH) ->
```

7. Select one or more software modules to display.

Enter a list of modules separated by a comma—for example, "system, stp, ptrunk." For a list of the modules and their abbreviations, refer to Software Modules on page 210. The default is **ALL**, which displays the events for all modules.

8. Once you have set the log filters, type **V** to select View Log.

An example of an event log is show in Figure 65. This log is in the Full display mode. The Normal display mode does not include the Filename, Line Number, and Event ID items.

```

Allied Telesyn Ethernet Switch AT-S60 V2.1.0
Production Switch 32

User: Manager                               11:20:02 02-Jan-2004

Event Log

S      Date      Time      EventID      Source File:Line Number
Event
-----
I      2/01/04    09:11:02  073001      garpmain.c:259
garp: GARP initialized
I      2/01/04    09:55:15  083001      portconfig.c:961
pcfg: PortConfig initialized
I      2/01/04    12:24:12  093001      mirrorapp.c:158
pmirr: Mirror initialization succeeded
I      2/01/04    12:47:08  043016      macapp.c:1431
mac: Delete Dynamic MAC by Port[2.7]
succeeded

Temporary (Memory) Log Events 1 - 4 of 212
P - Previous Page N - Next Page F - First Page L - Last Page
R - Return to Previous Menu

Enter your selection?

```

Figure 65 Event Log Example

The columns in the log are described below:

- ❑ S (Severity) - The event's severity. Table 7 defines the different severity levels:

Table 7 Event Log Severity Levels

Value	Severity Level	Description
E	Error	Switch operation is severely impaired.
W	Warning	An issue may require manager attention.
I	Information	Useful information that can be ignored during normal operation.
D	Debug	Detailed high-volume information that is intended for Technical Support.

- ❑ Date - The date the event occurred.
- ❑ Time - The time the event occurred.
- ❑ Event - The module within the AT-S60 software that generated the event followed by a brief description of the event. For a list of the AT-S60 modules, see Software Modules on page 210.
- ❑ Event ID - A unique number that identifies the event. (Displayed only in the Full display mode.)
- ❑ Source File and Line Number - The name of the AT-S60 source file and line number that generated the event. (Displayed only in the Full display mode.)

Software Modules

The Mod column in the event log displays an abbreviation of the AT-S60 software module that generated the event. Table 8 lists the modules and their abbreviations.

Table 8 AT-S60 Software Modules

Module Name	Description
ALL	All modules
CLI	Command line interface commands
ENCO	Encryption keys
ESTACK	Enhanced stacking
EVTLOG	Event log
FILE	File system
GARP	GARP GVRP
HTTP	Web server
IGMP	IGMP snooping
IP	Switch IP Configuration, BOOTP, and DHCP
MAC	MAC address table
PACCESS	802.1x port-based access control
PCFG	Port configuration
PKI	Public Key Infrastructure
PMIRR	Port mirroring

Table 8 AT-S60 Software Modules

Module Name	Description
PSEC	Port security (MAC address-based)
PTRUNK	Port trunking
RADIUS	RADIUS authentication protocol
SNMP	SNMP
SSH	Secure Shell protocol
SSL	Secure Sockets Layer protocol
STP	Spanning Tree, Rapid Spanning, and Multiple Spanning Tree protocols
SYSTEM	Hardware status; Manager and Operator log in and log off events.
TACACS	TACACS+ authentication protocol
TELNET	Telnet
TFTP	TFTP
TIME	System Time and SNTP
VLAN	Port-based and tagged VLANs, and multiple VLAN modes

Saving the Event Log

To save the current contents of the event log as a file in the file system, you use the "S - Save Log to File" on the Event Log menu. Once you create an event log file, you can either view it or download it to your management workstation.

Before you create an event log file, configure the Event Log feature to specify which log entries you want to save. See Configuring the Event Log on page 205.

Configuring the Save Option

To create an Event Log file, perform the following procedure.

1. From the Main menu, type **E** to select Event Log.
The Event Log Menu is shown in Figure 64 on page 205.
2. To save an Event Log to a file, type **S** to select S - Save Log to File.

The following prompt is displayed:

```
This operation can take a long time. Do you want to  
continue [Yes/No]->
```

3. Choose from the following selections:

Yes: Indicates you want to create an Event Log file.

No: Indicates you do not want to create a Event Log file.

The following prompt is displayed:

```
Enter file name (*.log)->
```

4. Enter a filename of up to 16 alphanumeric characters, followed by the ".log" extension.

For information about how to create a file on the AT-S60 file system, refer to Setting, Creating, Editing, and Displaying System Configuration Files on page 156.

Clearing the Event Log

To clear all events from the log, perform the following procedure:

1. From the Main menu, type **E** to select Event Log
The Event Log menu is shown in Figure 64 on page 205.
2. Type **C** to select Clear Log.
A confirmation prompt is displayed,
3. Type **Y** to clear the log or **N** to cancel the procedure.
The log, if enabled, immediately begins to learn new events.

Chapter 13

Class of Service (CoS)

This chapter contains the procedures for configuring Class of Service (CoS). Sections in the chapter include:

- ❑ Class of Service Overview on page 215
- ❑ Configuring CoS on page 217

Class of Service Overview

When a port on an Ethernet switch becomes oversubscribed, meaning that its egress queues contain more frames than the port can handle in an timely and orderly manner, there is the possibility that frames may be delayed in reaching their destinations. A port may be forced to delay the transmission of some frames while it handles other traffic. And in some circumstances, some frames destined to be forwarded to an oversubscribed port from other switch ports may be discarded.

Minor delays are often of no consequence to a network or its performance. But there are some applications, referred to as delay or time sensitive applications, that can be impacted by frame delays. Voice transmission and video conferencing are two examples. When frames carrying data for these applications are delayed from reaching their destination, the audio or video quality may suffer.

This is where CoS is of value. It allows you to manage the flow of traffic through your switch by having the switch ports give higher priority to some frames, such as delay sensitive traffic, over other frames. This is referred to as prioritizing traffic.

CoS applies principally to tagged frames. If you have read Tagged VLAN Overview on page 412, then you know that a tagged frame contains information within it that specifies the VLAN to which the frame belongs. This information is located in the Ethernet header of a frame.

A tagged frame also contains priority data, also within the Ethernet header, which is used by network switches and other networking devices to know how important or delay sensitive the frame is compared to other frames. Frames of a high priority are typically handled by the switch ports before frames of a low priority.

CoS, as defined in the IEEE 802.1p standard, has eight levels of priority. The priorities are 0 to 7, with 0 the lowest priority and 7 the highest.

When a tagged frame is received on a port on the switch, it is examined by the AT-S60 software for its priority. The switch software uses the priority to determine which egress priority queue the frame should be directed to on the egress port.

Each switch port has two egress queues, low and high. When a tagged frame enters a switch port, the switch responds by placing the frame into one of the two egress queues according to following assignments:

IEEE 802.1p Priority Levels	AT-8400 Series Port Egress Queue
7	high
6	high
5	high
4	high
3	low
2	low
1	low
0	low

For example, a tagged frame with a priority tag of 6 is placed in the high priority queue, while a frame with a priority tag of 1 is placed in the low priority queue.

These priority-to-queue assignments can be overridden using the AT-S60 management software on a per-port basis.

It should be noted that the determination of which egress queue a frame is directed to is made when a frame is received on the ingress port and before the frame is forwarded to the egress port. Consequently, configuring this feature on a switch port influences the ingress frames.

For example, when you configure a switch port so that all ingress frames with a priority level of 3 are handled by the high priority queue, all frames with a priority level 3 that the port *receives* are directed to the low priority egress queue of the egress port.

You can also use CoS to control which priority queue handles untagged frames that ingress a port. By default, untagged frames (that is, frames without VLAN or priority level information) are automatically assigned to the low priority buffer. But you can configure CoS on a port so that all untagged frames received on the port are directed to the high priority queue on the egress ports.

Configuring CoS

To configure CoS for a port, perform the following procedure:

1. From the Main Menu, type **1** to select Port Menu.
The Port Menu is shown in Figure 26 on page 102.
2. From the Port Menu, type **1** to select Port Configuration. The following prompt is displayed:

```
Enter port-list:
```
3. Enter the port you want to configure. For information on entering ports, refer to Specifying Ports on page 34.
The Port Configuration menu for the selected port(s) is displayed. Option 3 control CoS.
4. Type **3** to toggle Option 3 - Override Priority through the possible settings. The settings are:
 - No Override - All ingress tagged frames with a priority of 0 to 3 are sent to the low priority egress queue and tagged frames with a priority of 4 to 7 are sent to the high priority egress queue. Ingress untagged frames are sent to the low priority queue.
 - Low Priority - All ingress tagged and untagged frames are directed to the low priority egress queue.
 - High Priority - All ingress tagged and untagged frames received on a port are directed to the high priority egress queue.
5. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Note

The tagged information in a frame is not changed as the frame traverses the switch. A tagged frame leaves a switch with the same priority level that it had when it entered, regardless of the priority queue that handled the frame.

Note

To view the priority queue assignment for a port, use the Port Status selection in the Port Menu.

Chapter 14

IGMP Snooping

This chapter provides a description of the Internet Group Management Protocol (IGMP) snooping feature. Also, it explains how to activate and configure the IGMP snooping feature on the switch using a local or Telnet management session. This chapter contains the following sections:

- ❑ IGMP Snooping Overview on page 219
- ❑ Configuring IGMP Snooping on page 221
- ❑ Displaying a List of Host Nodes on page 224
- ❑ Displaying a List of Multicast Routers on page 226

IGMP Snooping Overview

IGMP enables routers to create lists of nodes that are members of multicast groups. (A multicast group is a group of end nodes that request multicast packets from a multicast application.) The router creates a multicast membership list by periodically sending out queries to the local area networks connected to its ports.

A user activates IGMP by selecting a multicast application such as a radio, voice, or video application on their PC. This selection triggers a series of message exchanges. A node responds to a query from the PC by sending a *report* which indicates an end node's intention to become a member of a multicast group. Nodes that join a multicast group are referred to as *host nodes*. Once a host node has been made a member of a multicast group, it must continue to periodically issue reports to remain a member.

Once the router has received a report from a host node, it notes the multicast group that the host node wants to join and the port on the router where the node is located. Then multicast packets belonging to that multicast group are forwarded from the port by the router. If a particular port on the router has no nodes that want to be members of multicast groups, the router does not send multicast packets from the port. This improves network performance by restricting multicast packets only to router ports where host nodes are located.

There are two versions of IGMP, referred to as Version 1 and Version 2. One of the differences between the two versions is how a host node indicates that it no longer wants to be a member of a multicast group. In Version 1, it simply stops sending reports. If a router does not receive a report from a host node after a predefined length of time, referred to as a *time-out value*, the router assumes that the host node no longer wants to receive multicast frames and removes it from the membership list of the multicast group.

In Version 2, a host node exits from a multicast group by sending a *leave request*. Once a router receives a leave request from a host node, it removes the node from the appropriate membership list. If it determines there are no further host nodes on the port, the router also stops sending out multicast packets from the port connected to the node.

IGMP snooping enables the Fast Ethernet switch to monitor the flow of queries from a router and reports from host nodes to build its own multicast membership lists. The switch uses the lists to forward multicast packets only to switch ports where there are host nodes that are members of multicast groups. This improves switch performance and network security by restricting the flow of multicast packets only to those switch ports connected to host nodes.

Without IGMP snooping, a switch would flood multicast packets from all of its ports, except the port on which it received the packet. Such flooding of packets can negatively impact switch and network performance.

The AT-8400 Series switch supports both IGMP Version 1 and Version 2. The switch maintains its multicast groups through an adjustable time-out value, which controls how frequently it expects to see reports from end nodes that want to remain members of multicast groups, and by processing leave requests.

Note

The default setting for IGMP snooping is disabled.

Configuring IGMP Snooping

To configure, enable, or disable IGMP snooping on the switch and to configure IGMP snooping parameters, perform the following procedure:

1. From the Main Menu, type **5** to select System Menu.

The System Menu is shown in Figure 5 on page 51.

2. From the System Menu, type **1** to select Configure System.

The Configure System Menu is shown in Figure 11 on page 59.

3. From the Configure System menu, type **1** to select Configure System Software.

The Configure System Software Menu is shown in Figure 12 on page 60.

4. From the Configure System Software menu, type **7** to select Configure IGMP Snooping.

The IGMP Snooping Configuration menu is shown in Figure 66.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
High School Switch 142

User: Manager                                00:14:33 28-Jan-2004

                Configure IGMP Snooping

1 - IGMP Snooping Status ..... Disabled
2 - Multicast Host Topology ..... Single-Host/Port (Edge)
3 - Host/Router Timeout Interval . 260 seconds
4 - Maximum Multicast Groups ..... 256
5 - Multicast Router Ports Mode .. Auto Detect
6 - View Multicast Hosts List
7 - View Multicast Router List

R - Return to Previous Menu

Enter your selection:

```

Figure 66 Configure IGMP Snooping Menu

Note

Options 6 and 7 in the menu are discussed later in this chapter.

Options 1 through 5 are described below:

1 - IGMP Snooping Status

Enables and disables IGMP snooping on the switch. After selecting this option, type **E** to enable or **D** to disable this feature. The default is disabled.

2 - Multicast Host Topology

Defines whether there is one host node per switch port or multiple host nodes per port. Possible settings are Single-Host/Port (Edge) and Multi-Host/Port (Intermediate).

The Single-Host/Port setting is appropriate when there is only one host node connected to a port on the switch. With this setting, the switch immediately stops sending multicast packets from a port when a host node issues a leave request or when a host node stops sending reports.

The 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 where multiple host nodes are connected. With this setting, the switch continues sending multicast packets out from 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 the host nodes connected to a switch port have transmitted leave requests (or have timed out) does the switch stop sending multicast packets out from the port.

If a switch has a mixture of host nodes, that is, some connected directly to the switch and others through another switch or hub, you should select the Multi-Host Port (Intermediate) selection.

3 - 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 watches for queries from the router. If the switch does not detect any queries from a multicast router during the specified time interval, it assumes the router is no longer active on the port.

4 - Maximum Multicast Groups

Specifies the maximum number of multicast groups the switch learns. The range is 1 to 256 groups. The default is 64 multicast groups.

This parameter 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 becoming filled with multicast addresses, leaving no room for dynamic or static MAC addresses.

5 - Multicast Router Ports Mode

Controls whether the detection of ports on the switch that are connected to multicast routers is made automatically or manually.

You use this selection to specify which of the ports on the switch are connected to multicast routers. You can allow the switch to determine this automatically by selecting Auto Detect, which is the default setting, or you can specify the ports manually by selecting Manual Select. If you select the latter, the following option is added to the Configure IGMP Switching menu:

C - Configure Multicast Router Ports

Selecting this menu option displays the Configure Multicast Router Ports menu as shown in Figure 67.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
High School Switch 142
User: Manager                                00:14:33 28-Jan-2004
Configure Multicast Router Ports
Static Router Ports
-----
1 - Create/Modify Multicast Router Ports
R - Return to Previous Menu
Enter your selection:

```

Figure 67 Configure Multicast Router Ports Menu

To specify the multicast router ports, type **1** to select Create/Modify Multicast Router Ports and enter the ports when prompted. For information on entering ports, refer to Specifying Ports on page 34.

5. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Your changes are activated immediately on the switch.

Displaying a List of Host Nodes

This procedure displays a list of the multicast groups on a switch, as well as the host nodes. To display the list, perform the following procedure:

1. From the IGMP Snooping Configuration Menu, type **6** to select View Multicast Hosts List.

For instructions on how to display the IGMP Snooping Configuration Menu, perform Steps 1 to 4 of Configuring IGMP Snooping on page 221.

The View Multicast Hosts List Menu is shown in Figure 68.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142

User: Manager                                00:14:33 01-Jan-2004

View Multicast Hosts List

=====
MulticastGroup      VLAN      Port/TrunkId  HostIP      Status
=====
01:00:5E:00:01:01   1         1.2-5/-      172.16.10.51 Active
01:00:5E:7F:FF:FA   1         8.3/-        149.35.2.75  Active
                   149.35.2.65  Active
01:00:5E:00:00:02   1         27/-         149.35.2.69  Active
01:00:5E:00:00:09   1         35/-         172.16.10.51 Active

U - Update Display
R - Return to Previous Menu

Enter your selection?
    
```

Figure 68 View Multicast Hosts List Menu

The information in this menu is for viewing purposes only. The columns are defined below:

Multicast Group

The multicast address of the group.

VLAN

The VID of the VLAN where the port is an untagged member.

Port/TrunkId

This column displays host members present on either a port or a trunk of the switch.

HostIP

The IP address(es) of the host node(s) connected to the port.

Status

The status of the host node. The status can be either Active, meaning the node is an active member of a multicast group, or Left Group, meaning the node has recently left the group.

Displaying a List of Multicast Routers

A multicast router is a router that is receiving multicast packets from a multicast application and transmitting the packets to host nodes. You can use the AT-S60 software to display a list of the multicast routers that are connected to the switch.

To display a list of the multicast routers, perform the following procedure:

1. From the IGMP Snooping Configuration Menu, type **7** to select View Multicast Router List.

For instructions on how to display the IGMP Snooping Configuration menu, perform Steps 1 to 4 of Configuring IGMP Snooping on page 221.

The View Multicast Routers List Menu is displayed. The appearance of the menu differs depending on whether the ports connected to multicast routers are determined automatically or manually. Figure 69 is an example of how the menu looks if the multicast router ports are being determined automatically.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142

User: Manager                                00:14:33 01-Jan-2004

View Multicast Routers List

=====
VLAN ID      Port/TrunkId      RouterIP
=====
1            -/1               172.16.01.1
2            8.1-8/-          172.16.25.9
14          -/25             172.16.35.7

U - Update Display
R - Return to Previous Menu

Enter your selection?
    
```

Figure 69 View Multicast Routers List Menu

The information in this menu is for viewing purposes only. The columns are defined below:

VLAN ID

The VID of the VLAN where the port is an untagged member.

Port/TrunkId

This column displays router members present on either a port or a trunk of the switch.

RouterIP

The IP address of the multicast router.

If you enter the multicast router ports manually, the menu contains a single column labelled Static Router Ports and a list of the ports that you entered when you configured IGMP snooping.

Chapter 15

STP and RSTP

This chapter provides background information on the Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP). The chapter also contains procedures on how to adjust spanning tree bridge and port parameters. This chapter includes the following sections:

- ❑ STP and RSTP Overview on page 229
- ❑ Enabling or Disabling STP and RSTP on page 240
- ❑ Configuring STP on page 242
- ❑ Configuring RSTP on page 248

Note

For further information on Spanning Tree Protocol, refer to IEEE Std 802.1d. For further information on Rapid Spanning Tree Protocol, refer to IEEE Std 802.1w.

STP and RSTP Overview

A physical loop in a network topology can pose a significant problem to Ethernet network performance. A loop exists when two or more nodes on a network can transmit data to each other over more than one data link. The problem with physical loops is that data packets can become caught in repeating cycles, referred to as broadcast storms, that needlessly consume network bandwidth and significantly reduce network performance.

STP and RSTP prevent data loops from forming by ensuring that only one path exists between the end nodes in your network. Should one of the protocols detect multiple paths, it places the extra paths in a standby or blocking mode, leaving only one main active path.

STP and RSTP can also activate a redundant path if the main path goes down. So not only do these protocols guard against multiple links between segments and the risk of broadcast storms, but they can also maintain network connectivity by activating a backup redundant path in case a main link fails.

The principal difference between the two protocols is in the time each takes to complete the process commonly referred to as *convergence*. When a change is made to the network topology, such as the addition of a new bridge, a spanning tree protocol must determine whether there are redundant paths that must be blocked to prevent data loops, or activated to maintain intercommunications between the various network segments. This is the process of convergence.

With STP, convergence can take minutes to complete in a large network. This can result in lost data packets and the loss of intercommunication between various parts of the network during the convergence process.

RSTP is much faster. It can complete a convergence in seconds, and so diminish the possible impact the process can have on your network.

The STP implementation on the AT-8400 Series switch complies with the IEEE 802.1d standard. The RSTP implementation complies with the IEEE 802.1w standard. The following subsections provide a basic overview on how STP and RSTP operate and define the different parameters that you can adjust.

- ❑ Bridge Priority and the Root Bridge on page 230
- ❑ Mixed STP and RSTP Networks on page 237
- ❑ Spanning Tree and VLANs on page 237

Note

Spanning tree is disabled by default on the switch.

Note

For information about Multiple Spanning Tree, see Chapter 16, Multiple Spanning Tree Protocol (MSTP) on page 257.

Note

An AT-8411 TX line card with more than four ports functioning as redundant links to other network devices can significantly retard the speed of convergence for STP and RSTP. You can avoid this problem by selecting ports on different line cards to function as redundant links.

Bridge Priority and the Root Bridge

The first task that bridges perform when a spanning tree protocol is activated on a network is the selection of a *root bridge*. A root bridge distributes network topology information to the other network bridges and is used by the other bridges to determine if there are redundant paths in the network.

A root bridge is selected by a combination of a *bridge priority* number, also referred to as the bridge identifier, and sometimes the bridge's MAC address. The bridge with the lowest bridge priority number in the network is selected as the root bridge. If two or more bridges have the same bridge priority number, of those bridges the one with the lowest MAC address is designated as the root bridge.

The bridge priority number can be changed on an AT-8400 Series switch. You can designate a switch on your network as the root bridge by giving it the lowest bridge priority number. You might also consider which bridge should function as the backup root bridge in the event you need to take the primary root bridge off-line, and assign that bridge the second lowest bridge identifier number.

The range for STP and RSTP bridge priority is 0 to 61,440 in increments of 4,096. The range is divided into sixteen increments. You set the parameter by specifying the increment that represents the desired bridge priority value. Table 9 on page 231 lists the bridge priority value increments. For example, to set a bridge priority value on a switch to 45056, select increment 11. The default value is 32,768, increment 8.

Table 9 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

Path Costs and Port Costs

Once the Root Bridge has been selected, the bridges must determine if the network contains redundant paths and, if one is found, they must select a preferred path while placing the redundant paths in a backup or blocking state.

Where there is only one path between a bridge and the root bridge, the bridge is referred to as the *designated bridge* and the port through which the bridge is communicating with the root bridge is referred to as the *root port*.

If redundant paths exist, the bridges that are a part of the paths must determine which path is the primary, active path, and which path(s) are placed in the standby, blocking mode. This is accomplished by a determination of *path costs*. The path offering the lowest cost to the root bridge becomes the primary path and all other redundant paths are placed into blocking state.

Path cost is determined through an evaluation of *port costs*. Every port on a bridge participating in STP has a cost associated with it. The cost of a port on a bridge is typically based on port speed—the faster the port, the lower the port cost. The exception to this is the ports on the root bridge, where all ports have a port cost of 0.

Path cost is the sum of the port costs between a bridge and the root bridge.

The port costs of the ports on an AT-8400 Series switch can be adjusted through the management software. For STP and RSTP, the range is 0 to 200,000,000.

The default value of 0 activates auto-detection. This features sets port cost according to port speed, assigning lower costs to ports operating at higher speeds.

Table 10 lists the auto-detection default values for STP and RSTP.

Table 10 STP and RSTP Auto-Detect Port Costs

Port Speed	Port Cost
10 Mbps	2000000
100 Mbps	200000
1000 Mbps	20000

You can override Auto-Detect and set the port cost manually.

Port Priority

If two paths have the same port cost, the bridges must select a preferred path. In some instances this can involve the use of the *port priority* parameter. This parameter can be used as a tie-breaker when two paths have the same cost.

The range for port priority is 0 to 240 in increments of 16. Just as with the bridge priority value, you specify the increment that corresponds to the desired value. Table 11 lists the port priority increments. The default value is 128, with an increment of 8.

Table 11 Port Priority Value Increments

Increment	Port Priority	Increment	Port Priority
0	0	8	128
1	16	9	144
2	32	10	160
3	48	11	176
4	64	12	192
5	80	13	208
6	96	14	224
7	112	15	240

Forwarding Delay and Topology Changes

If there is a change in the network topology due to a failure, removal, or addition of any active components, the active topology may also change. This may trigger a change in the state of some blocked ports. However, a change in a port state is not activated immediately.

It might take time for the root bridge to notify all bridges that a topology change has occurred, especially if it is a large network. If a topology change is made before all bridges have been notified, a temporary data loop could occur, and that could adversely impact network performance.

To forestall the formation of temporarily data loops during topology changes, a port designated to change from blocking to forwarding passes through two additional states, listening and learning, before it begins to forward frames. The amount of time a port spends in these states is set by the *forwarding delay* value. This value controls the amount of time that a port spends in the listening and learning states prior to changing to the forwarding state.

The forwarding delay value is adjustable on the AT-8400 Series switch through the management software. The appropriate value for this parameter depends on a number of variables, with the size of your network being a primary factor. For large networks, you should specify a value large enough to allow the root bridge sufficient time to propagate a topology change throughout the entire network. For small networks, you should not specify a value so large that a topology change is unnecessarily delayed, which could result in the delay or loss of some data packets.

Note

The forwarding delay parameter applies only to STP.

Hello Time and Bridge Protocol Data Units (BPDU)

The bridges in a spanning tree domain communicate with each other using a bridge multicast frame that contains a special section devoted to carrying STP or RSTP information. This portion of the frame is referred to as the Bridge Protocol Data Unit (BPDU). When a bridge is brought on-line, it issues a BPDU in order to determine whether a root bridge has already been selected on the network. If a root bridge has not been selected, the BPDU determines whether it has the lowest bridge priority number of all the bridges and, consequently, should become the root bridge.

The root bridge periodically transmits a BPDU to determine whether there have been any changes to the network topology and to inform other bridges of topology changes. The frequency with which the root bridge sends out a BPDU is called the *Hello Time*. This is a value that you can set on the AT-8400 Series switch. The interval is measured in seconds and the default is 2 seconds. Consequently, if an AT-8400 Series switch is selected as the Root Bridge of a spanning tree domain, it transmits a BPDU every two seconds.

Point-to-Point Ports and Edge Ports

Note

This section applies only to RSTP.

Part of the task of configuring RSTP is defining the port types on the bridge. This relates to the device(s) connected to the port. With port type defined, RSTP can reconfigure a network much quicker than STP when a change in network topology is detected.

There are two possible selections:

- Point-to-point
- Edge port

If a bridge port is operating in full-duplex mode, then the port is functioning as point-to-point. Figure 70 illustrates an AT-8400 chassis and an AT-8024 switch that have been interconnected with one data link. With the link operating in full-duplex, the ports are said to be point-to-point ports.

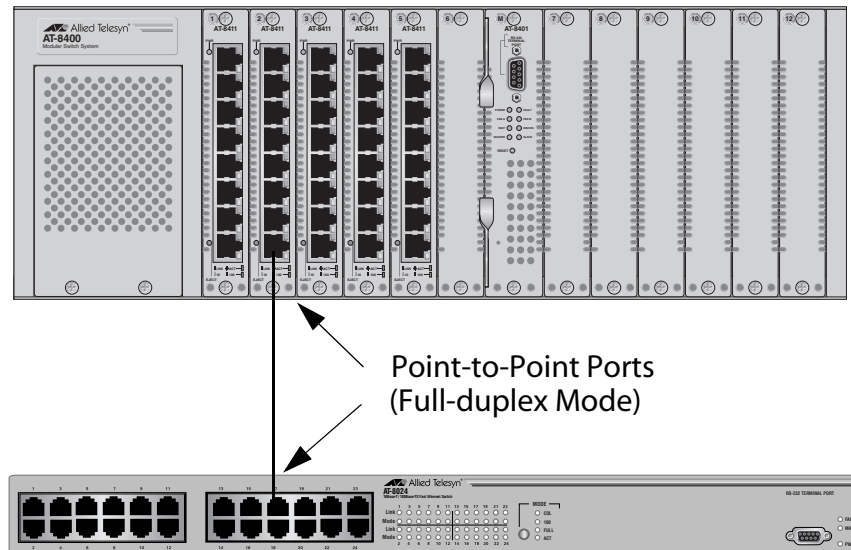


Figure 70 Point-to-Point Ports

If a port is operating in half-duplex mode and is not connected to any further bridges participating in STP or RSTP, then the port is an edge port. Figure 71 illustrates an edge port on an AT-8411 TX line card in an AT-8400 chassis. The port is connected to an Ethernet hub, which in turn is connected to a series of Ethernet workstations. This is an edge port because it is connected to a device operating at half-duplex mode and there are no participating STP or RSTP devices connected to it.

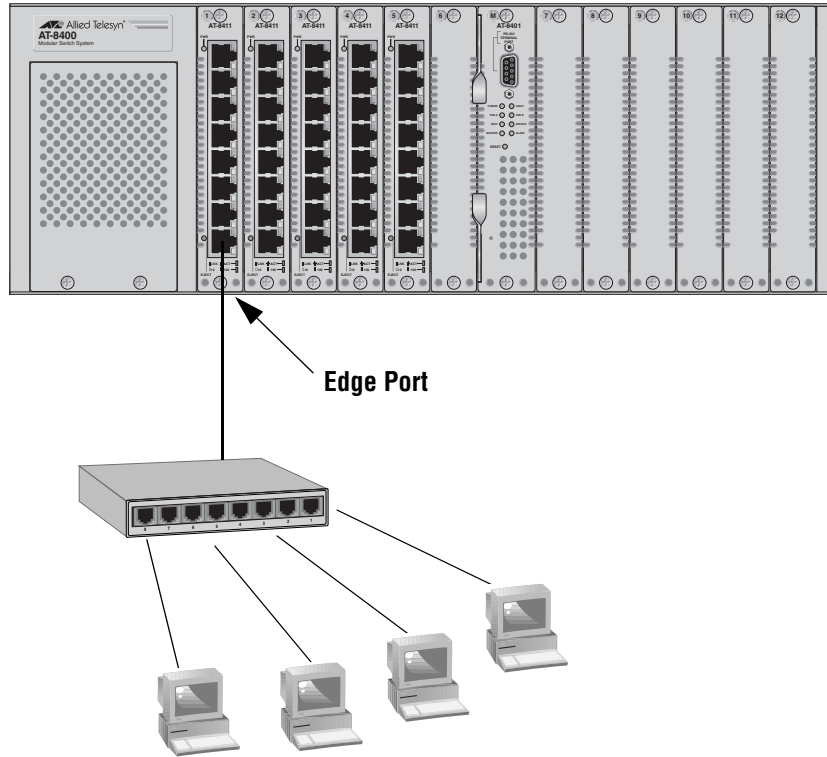


Figure 71 Edge Port

A port can be both point-to-point and edge at the same time. It would operate in full-duplex and have no STP or RSTP devices connected to it. Figure 72 illustrates a port on an AT-8411 TX line card functioning both as point-to-point and edge.

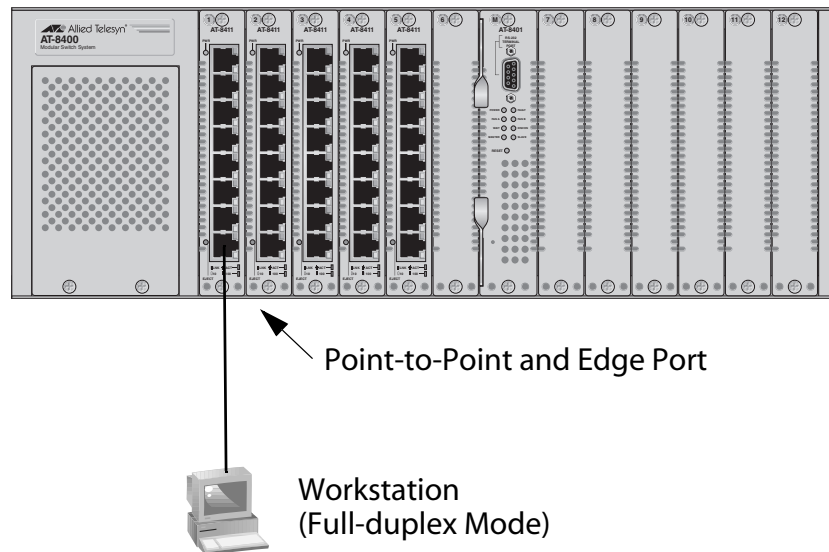


Figure 72 Point-to-Point and Edge Point

Determining whether a bridge port is point-to-point, edge, or both, can be a bit confusing. For that reason it might be best not to change the default values for this RSTP feature unless you have a good grasp of the concept. In most cases, the default values work fine.

Mixed STP and RSTP Networks

RSTP IEEE 802.1w is fully compliant with STP IEEE 802.1d. Your network can consist of bridges running both protocols. STP and RSTP in the same network should be able to operate together to create a single spanning tree domain.

You can activate RSTP on an AT-8400 Series switch even when all of the other switches are running STP. The AT-8400 Series switch can combine its RSTP with the STP of the other switches. An AT-8400 Series switch monitors the traffic on each port for BPDU packets. Ports that receive RSTP BPDU packets operate in RSTP while ports receiving STP BPDU packets operate in STP.

Spanning Tree and VLANs

The STP and RSTP implementations on an AT-8400 Series switch are single-instance spanning trees. They support one spanning tree domain. (To define multiple spanning trees, you can use MSTP. For information, refer to MSTP Overview on page 258.)

The single spanning tree encompasses all ports on the switch. If the ports are grouped into different VLANs, the spanning tree crosses the VLAN boundaries. This can pose a problem where multiple VLANs that span different switches are connected with untagged ports. What can occur is that spanning tree blocks a data link because it detects a physical data loop. This can cause fragmentation of your VLANs.

This is illustrated in Figure 73. Two VLANs, Sales and Production, span one AT-8400 Series switch and one AT-8024GB switch. Two links consisting of untagged ports interconnect the separate parts of each VLAN. If spanning tree is activated on the switches, one of the links would be disabled because spanning tree, which crosses the VLAN boundaries, would see the links as forming a physical loop, even though the VLAN traffic itself does not cross the boundaries.

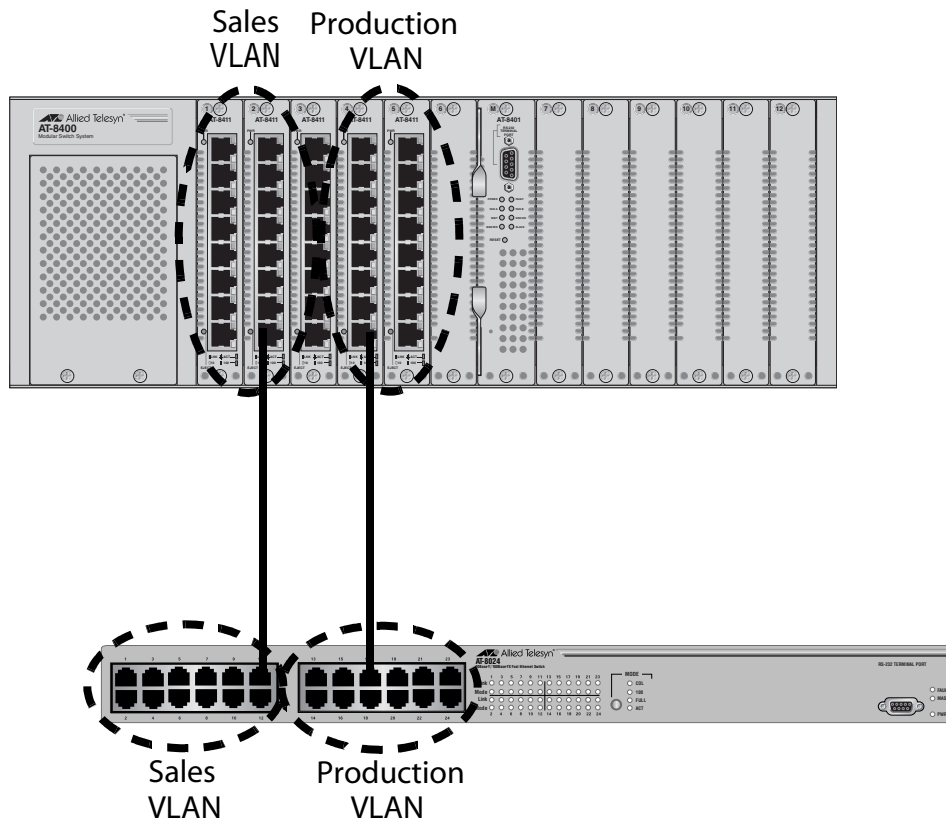


Figure 73 VLAN Fragmentation

There are several approaches that you can take to resolve this problem. One is not to activate STP or RSTP on your network. This solution mandates vigilance on your part not to create network loops when wiring your network.

Another approach is to connect your VLANs with tagged ports instead of untagged ports. A tagged port can handle traffic from more than one VLAN at a time. For information on tagged and untagged ports, refer to Chapter 18, Tagged and Port-based Virtual LANs on page 401.

You can also place different VLANs in different spanning trees. This is accomplished using the Multiple Spanning Tree Protocol, explained in MSTP Overview on page 258.

Enabling or Disabling STP and RSTP

The AT-8400 Series switch can support STP, RSTP, and MSTP. However, only one spanning tree protocol can be active on the switch at a time. Before you enable a spanning tree protocol, you must first select it as the active spanning tree protocol on the switch. Once you have selected it as the active protocol, you can enable or disable it.

To select 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 Main Menu, type **3** to select Spanning Tree Menu.

The Spanning Tree Menu is shown in Figure 74.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
                          High School Switch 142
User: Manager                               00:14:33 15-Jan-2004
                          Spanning Tree Menu
1 - Spanning Tree Status ..... Disabled
2 - Active Protocol Version ... RSTP
3 - STP Configuration
4 - RSTP Configuration
5 - MSTP Configuration

R - Return to Previous Menu

Enter your selection?
```

Figure 74 Spanning Tree Menu

Note

If you do not want to change the active spanning tree protocol, but you do want to enable or disable the protocol, go to step 6.

2. To change the active version of spanning tree protocol on the switch, type **2** to select Active Protocol Version.

The following prompt is displayed:

```
This operation will need a reboot of the system.
Do you want to continue [Y/N] ->
```

3. Type **Y** for yes.

The following prompt is displayed:

```
Enter new value (S-STP, R-RSTP, M-MSTP):
```

4. Type **S** to select STP, **R** to select RSTP, or **M** to select MSTP.

The following prompt is displayed:

```
Do you want to enable spanning tree? (Y/N) ->
```

If you respond with Yes to this prompt, the management software reboots the switch and enables the selected spanning tree protocol. If you respond with No, the management software reboots but does not activate spanning tree. The first response is appropriate if you do not want to configure the spanning tree parameter settings before spanning tree is activated. A response of No is appropriate if you want to configure spanning tree parameters before spanning tree is activated.

5. Type **Y** for yes or **N** for no.

The switch reboots and the selected spanning tree protocol becomes the active protocol on the switch. You can now configure the parameters of the selected spanning tree protocol. If you selected STP, go to Configuring STP on page 242 for further instructions. If you selected RSTP, go to Configuring RSTP on page 248. If you selected MSTP, go to MSTP Overview on page 258.

Unlike other management procedures with the AT-S60 software, this procedure does not require you to return to the Main Menu to save your changes. The change to the active spanning tree protocol is automatically saved before the switch reboots.

Note

Steps 6, 7, and 8 apply only if you did not enable the spanning tree when you selected it. The steps enable or disable the spanning tree protocol.

6. To enable or disable the active spanning tree, type **1** to select Spanning Tree Status.
7. Type **E** to enable spanning tree or **D** to disable it. The default is enabled.
8. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Configuring STP

This section contains the following procedures:

- ❑ Configuring STP Bridge Settings on page 242
- ❑ Configuring STP Port Parameters on page 245
- ❑ Displaying STP Port Settings on page 247

Configuring STP Bridge Settings

This section contains the procedure for configuring a bridge's STP settings.



Caution

The default STP parameters 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.

Note

You cannot configure the STP settings unless the protocol has been selected as the active spanning tree protocol on the switch. For instructions, refer to Enabling or Disabling STP and RSTP on page 240.

1. From the Main Menu, type **3** to select Spanning Tree Menu.
The Spanning Tree Menu is shown in Figure 74 on page 240.
2. From the Spanning Tree Menu, type **3** to select STP Configuration.

The STP Menu is shown in Figure 75.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
High School Switch 142
User: Manager                                00:14:33 15-Jan-2004

                                STP Menu

1 - Bridge Priority ..... 32768
2 - Bridge Hello Time ... 2
3 - Bridge Forwarding ... 15
4 - Bridge Max Age ..... 20
5 - Bridge Identifier ... 00:30:84:EE:31:01
6 - Root Bridge ..... 00:30:84:EE:31:01
7 - Root Priority ..... 32768

P - STP Port Parameters
R - Reset STP to Defaults

R - Return to Previous Menu

Enter your selection?:

```

Figure 75 STP Menu

3. Adjust the bridge STP settings as needed. The parameters are described below.

1 - 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 9 on page 231, Bridge Priority Value Increments on page 231.

2 - Bridge Hello Time

The time interval, in seconds, between generating and sending configuration messages by the bridge. This parameter can be from 1 to 10 seconds. The default is 2 seconds.

3 - Bridge Forwarding

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.

4 - Bridge Max Age

The length of time in seconds after which stored bridge protocol data units (BPDUs) are deleted by the bridge. All bridges in a bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). For example, if you use the default 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 $(2 \times (\text{ForwardingDelay} - 1))$

Note

The aging time for BPDUs is different from the aging time used by the MAC address table.

5 - Bridge Identifier

The MAC address of the AT-8401 management card. This is used as a tie breaker if two bridges have the same bridge priority number. You cannot change this value.

6 - Root Bridge

Indicates the MAC address of the switch in the network that is currently functioning as the root bridge for all the switches in the spanning tree domain. The MAC address is determined by the spanning tree protocol. This parameter provides an easy way for a network manager to determine which switch in the network is functioning as the root bridge. This is a read-only parameter.

7 - Root Priority

Indicates the bridge priority value on the root bridge. The bridge priority value is used by spanning tree to select the root bridge for the spanning tree domain. The bridge with the lowest value is the assigned as the root bridge. This is a read-only parameter.

4. To change STP port settings, go to the next procedure. If you do not want to change STP port settings, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Configuring STP Port Parameters

To adjust a port's STP parameters, perform the following procedure:

1. From the Main Menu, type **3** to select Spanning Tree Menu.
The Spanning Tree Menu is shown in Figure 74 on page 240.
2. From the Spanning Tree Menu, type **3** to select STP Configuration.
The STP Menu is shown in Figure 75 on page 243.
3. From the STP Menu, type **P** to select STP Port Parameters.
The STP Port Parameters Menu is shown in Figure 76.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
High School Switch 142
User: Manager                                00:14:33 15-Jan-2004
                                STP Port Parameters
1 - Configure STP Port Settings
2 - Display STP Port Configuration
R - Return to Previous Menu

Enter your selection?

```

Figure 76 STP Port Parameters Menu

4. Type **1** to select Configure STP Port Settings.
The following prompt is displayed:
Enter port-list:
5. Enter the port to configure. For instructions on how to specify port numbers, refer to Specifying Ports on page 34.

The STP Port Configuration menu is shown in Figure 77.

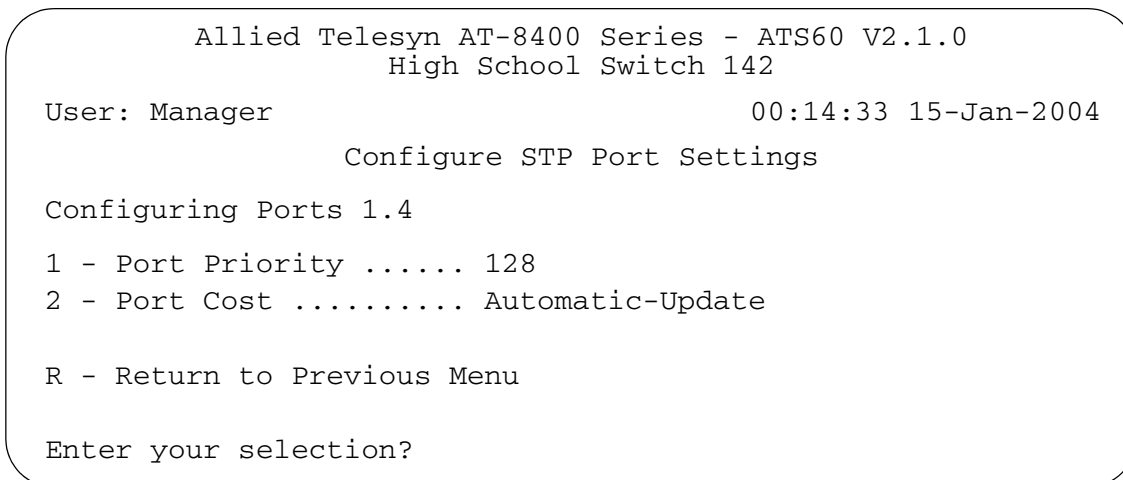


Figure 77 Configure STP Port Settings Menu

6. Adjust the settings as desired. The parameters are described below.

1 - 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 11**, Port Priority Value Increments on page 233.

2 - 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 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.

7. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Displaying STP Port Settings

To display port STP settings, perform the following procedure:

1. From the Spanning Tree Menu, type **3** to select STP Configuration.
The STP Menu is shown in Figure 75 on page 243.
2. From the STP Menu, type **P** to select STP Port Parameters.
The STP Port Parameters Menu is shown in Figure 76 on page 245.
3. From the STP Port Parameters Menu, type **2** to select Display STP Port Configuration.

The Display STP Port Configuration Menu is shown in Figure 78.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
High School Switch 142

User: Manager                                00:14:33 15-Jan-2004

Display STP Port Configuration

Port State      Cost          Priority
-----
1.1 Disabled    Auto-Update   128
1.2 Disabled    Auto-Update   128
1.3 Disabled    Auto-Update   128
1.4 Disabled    Auto-Update   128
1.5 Disabled    Auto-Update   128
1.6 Disabled    Auto-Update   128
1.7 Disabled    Auto-Update   128
1.8 Disabled    Auto-Update   128

N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 78 Display STP Port Configuration Menu

Configuring RSTP

This section contains the following procedures:

- ❑ Configuring RSTP Bridge Settings on page 248
- ❑ Configuring RSTP Port Parameters on page 252
- ❑ Displaying RSTP Port Configuration and Port State on page 254

Configuring RSTP Bridge Settings

This section contains the procedure for configuring a bridge's RSTP settings.



Caution

The default RSTP parameters 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. Consult the IEEE 802.1w standard before you change any RSTP parameters.

Note

You cannot configure RSTP settings unless the protocol has been selected as the active spanning tree protocol on the switch. For instructions, refer to Enabling or Disabling STP and RSTP on page 240.

1. From the Main Menu, type **3** to select Spanning Tree Menu.
The Spanning Tree Menu is shown in Figure 74 on page 240.
2. From the Spanning Tree Menu, type **4** to select RSTP Configuration.

The RSTP Menu is shown in Figure 79.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
High School Switch 142

User: Manager                                00:14:33 15-Jan-2004

                                RSTP Menu

1 - Force Version ..... RSTP
2 - Bridge Priority ..... 32768 <In multiples of 4096: 8>
3 - Bridge Hello Time ... 2
4 - Bridge Forwarding ... 15
5 - Bridge Max Age ..... 20
6 - Bridge Identifier ... 00:30:84:52:11:11
7 - Root Bridge ..... 00:30:84:52:11:11
8 - Root Priority ..... 32768

P - RSTP Port Parameters
D - Reset RSTP to Defaults

R - Return to Previous Menu

Enter your selection?

```

Figure 79 RSTP Menu

- Adjust the parameters as needed. The parameters are defined below.

1 - 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 sends only STP BPDU packets out the ports.

2 - 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 9 on page 231, Bridge Priority Value Increments on page 231.

3 - Bridge Hello Time

The time interval, in seconds, between generating and sending configuration messages by the bridge. This parameter can be from 1 to 10 seconds. The default is 2 seconds.

4 - 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.

5 - 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 $(2 \times (\text{ForwardingDelay} - 1))$

6 - 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.

7 - Root Bridge

Indicates the MAC address of the switch in the network that is currently functioning as the root bridge for all the switches in the spanning tree domain. The MAC address is determined by the spanning tree protocol. This parameter provides an easy way for a network manager to determine which switch in the network is functioning as the root bridge. This is a read-only parameter.

8 - Root Priority

Indicates the bridge priority value on the root bridge. The bridge priority value is used by spanning tree to select the root bridge for the spanning tree domain. The bridge with the lowest value is assigned as the root bridge. This is a read-only parameter.

4. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Configuring RSTP Port Parameters

To adjust a port's RSTP parameters, perform the following procedure:

1. From the Main Menu, type **3** to select Spanning Tree Menu.
The Spanning Tree Menu is shown in Figure 74 on page 240.
2. From the Spanning Tree Menu, type **4** to select RSTP Configuration.
The RSTP Menu is shown in Figure 79 on page 249.
3. From the RSTP Configuration menu, type **P** to select RSTP Port Parameters.

The RSTP Port Parameters Menu is shown in Figure 80.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
High School Switch 142
User: Manager                                00:14:33 15-Jan-2004
RSTP Port Parameters
1 - Configure RSTP Port Settings
2 - Display RSTP Port Configuration
3 - Display RSTP Port State
R - Return to Previous Menu
Enter your selection?
```

Figure 80 RSTP Port Parameters Menu

4. Type **1** to select Configure RSTP Port Settings.
The following prompt is displayed:
Enter port-list:
5. Enter the port to configure.
For instructions on how to specify port numbers, refer to Specifying Ports on page 34.

The Configure RSTP Port Settings Menu is shown in Figure 81.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
High School Switch 142
User: Manager                                00:14:33 15-Jan-2004
Configure RSTP Port Settings

Configuring Ports 4.8
1 - Port Priority ..... 128
2 - Path Cost ..... Auto Update
3 - Point-to-Point ..... Auto Detect
4 - Edge Port ..... Yes

C - Check Migration to RSTP on Selected Ports (MCHECK)
R - Return to Previous Menu

Enter your selection?

```

Figure 81 Configure RSTP Port Settings Menu

- Adjust the settings as needed. The parameters are explained below.

1 - 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 11 on page 233, Port Priority Value Increments on page 233.

2 - 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 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.

3 - Point-to-Point

This parameter defines whether the port is functioning as a point-to-point port. For an explanation of this parameter, refer to Point-to-Point Ports and Edge Ports on page 234.

4 - Edge Port

This parameter defines whether the port is functioning as an edge port. For an explanation of this parameter, refer to Point-to-Point Ports and Edge Ports on page 234.

C - Check Migration To RSTP on Selected Ports (MCHECK)

This parameter resets a RSTP port, allowing it to send RSTP BPDUs. When an RSTP bridge receives STP BPDUs on an RSTP port, the port transmits STP BPDUs. The RSTP port continues to transmit STP BPDUs indefinitely. Type **C** to reset the RSTP port to transmit RSTP BPDUs.

Each time a RSTP port is reset by receiving STP BPDUs, you need to type **C** to reset the RSTP port, allowing it to send RSTP BPDUs.

Note

MCHECK is only valid when the RSTP mode is enabled. This option does not apply when the switch is in STP mode.

7. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Displaying RSTP Port Configuration and Port State

The RSTP Port Parameters menu has two selections for displaying a variety of RSTP port information. The two menu selections are discussed below.

To display RSTP port configuration and port state, perform the following procedure:

1. From the Main Menu, type **3** to select Spanning Tree Menu.
The Spanning Tree Menu is shown in Figure 74 on page 240.
2. From the Spanning Tree Menu, type **4** to select RSTP Configuration.
The RSTP Menu is shown in Figure 79 on page 249.
3. From the RSTP Configuration menu, type **P** to select RSTP Port Parameters.
The RSTP Port Parameters Menu is shown in Figure 80 on page 252.
4. From the RSTP Port Parameters Menu, type **2** to select Display RSTP Port Configuration.

The Display RSTP Port Configuration Menu is shown in Figure 78.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Production Switch 142

User: Manager                                00:14:33 15-Jan-2004

Display RSTP Port Configuration

Port | Edge-Port | Point-to-Point | Cost          | Priority
-----|-----|-----|-----|-----
4.1   Yes      Auto Detect    Auto Update    128
4.2   Yes      Auto Detect    Auto Update    128
4.3   Yes      Auto Detect    Auto Update    128
4.4   Yes      Auto Detect    Auto Update    128
4.5   Yes      Auto Detect    Auto Update    128
4.6   Yes      Auto Detect    Auto Update    128
4.7   Yes      Auto Detect    Auto Update    128
4.8   Yes      Auto Detect    Auto Update    128

N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 82 Display RSTP Port Configuration Menu

This selection displays a menu that contains the current port settings for the following RSTP parameters:

- Edge-Port: Indicates if the port is an edge port or not. The values are yes or no.
 - Point-to-Point: Indicates if the port is a point-to-point port or not. The values are yes, no, or auto detect.
 - Cost - Indicates the port cost of the port.
 - Priority - Indicates the port priority.
5. To display the state of the RSTP port, type **3** to select Display RSTP Port State.

The Display RSTP Port State Menu is shown in Figure 78.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Production Switch 142
User: Manager                                00:14:33 15-Mar-2004
Display RSTP Port State
-----
Port      State      Role      P2P  Version  Port-Cost
-----
1.1      Disabled  -----
3.1      Disabled  -----
3.2      Disabled  -----
3.3      Disabled  -----
3.4      Forwarding Designated Yes   RSTP    200000
3.5      Disabled  -----
3.6      Disabled  -----
3.7      Disabled  -----

N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection?
    
```

Figure 83 Display RSTP Port State

This selection displays a menu that contains the following RSTP operating status for a port:

- State - Identifies the RSTP state of the port. The states are: disabled, discarding, learning, and forwarding. A state of disabled means the port has not established a link with its end node or the link is down.
- Role - Indicates the RSTP role of the port. The role are root, alternate, backup, and designated.
- P2P - Indicates whether the port is a point-to-point port. The values are yes, no, and auto-detect.
- Version - Indicates whether the port is operating in RSTP mode, STP-compatible mode, or MSTP mode. The values are rstp, stp, or mstp.
- Port-Cost - Indicates the port cost of the port.

Chapter 16

Multiple Spanning Tree Protocol (MSTP)

This chapter provides background information on the Multiple Spanning Tree Protocol (MSTP). The chapter also contains procedures on how to enable MSTP on the switch and configure MSTP parameters. The sections in this chapter include:

- ❑ MSTP Overview on page 258
- ❑ Configuring MSTP on page 274

Note

For further information on Multiple Spanning Tree Protocol, refer to IEEE Std 802.1s.

MSTP Overview

As mentioned in Chapter 15, STP and RSTP on page 228, STP and RSTP are referred to as single-instance spanning trees that search for physical loops across all VLANs in a bridged network. When loops are detected, the protocols stop the loops by placing one or more bridge ports in a blocking state.

As explained in Spanning Tree and VLANs on page 237, STP and RSTP can result in VLAN fragmentation where VLANs that span multiple bridges are connected together with untagged ports. The untagged ports creating the links can represent a physical loop in the network, which are blocked by spanning tree. The result can be a loss of communication between different parts of the same VLAN.

One way to resolve this, other than by not activating spanning tree on your network, is to link the switches using tagged ports, which can handle traffic from multiple VLANs simultaneously. The drawback to this approach is that the link formed by the tagged ports can create a bottleneck to your Ethernet traffic, resulting in reduced network performance.

Another approach is to use the Multiple Spanning Tree Protocol (MSTP). This spanning tree shares many of the same characteristics as RSTP. It features rapid convergence and has many of the same parameters. But the main difference is that while RSTP, just like STP, supports only a single-instance spanning tree, MSTP supports multiple spanning trees within a network.

The following sections describe some of the terms and concepts relating to MSTP. If you are not familiar with spanning tree or RSTP, you should first review the section on page 257.

Note

Do not activate MSTP on an AT-8400 Series switch without first familiarizing yourself with the following concepts and guidelines. Unlike STP and RSTP, you cannot activate this spanning tree protocol on a switch without first configuring the protocol parameters.

Note

Due to different vendor implementations of the new IEEE 802.1s standard, compatibility issues concerning MSTP instances between the AT-8400 Series switch and switches from other vendors may exist. This can result in compatibility issues between different MSTP implementations. For this release, MSTP is compatible only with other AT-8400 Series switches.

**Multiple
Spanning Tree
Instance (MSTI)**

The individual spanning trees in MSTP are referred to as Multiple Spanning Tree Instances (MSTIs). A MSTI can span any number of AT-8400 Series switches, and an AT-8400 Series switch can support up to 16 MSTIs at a time.

To create a MSTI, you first assign it a number, referred to as the MSTI ID. The range is 1 to 15. (The switch comes with a default MSTI with an MSTI ID of 0. This default spanning tree instance is discussed later in Common and Internal Spanning Tree (CIST) on page 267.)

Once you have selected an MSTI ID, you need to define the scope of the MSTI by assigning one or more VLANs to it. An instance can contain any number of VLANs, but a VLAN can belong to only one MSTI at a time.

Here are a couple of examples. Figure 84 illustrates two AT-8400 Series switches each containing the two VLANs Sales and Production. The two parts of each VLAN are connected with a direct link using untagged ports on both switches.

If the switches were running STP or RSTP, one of the links would be blocked because the links constitute a physical loop. Which link would be blocked depends on the STP or RSTP bridge settings. In the example, the link between the two parts of the Production VLAN is blocked, resulting in a loss of communications between the two parts of the Production VLAN.

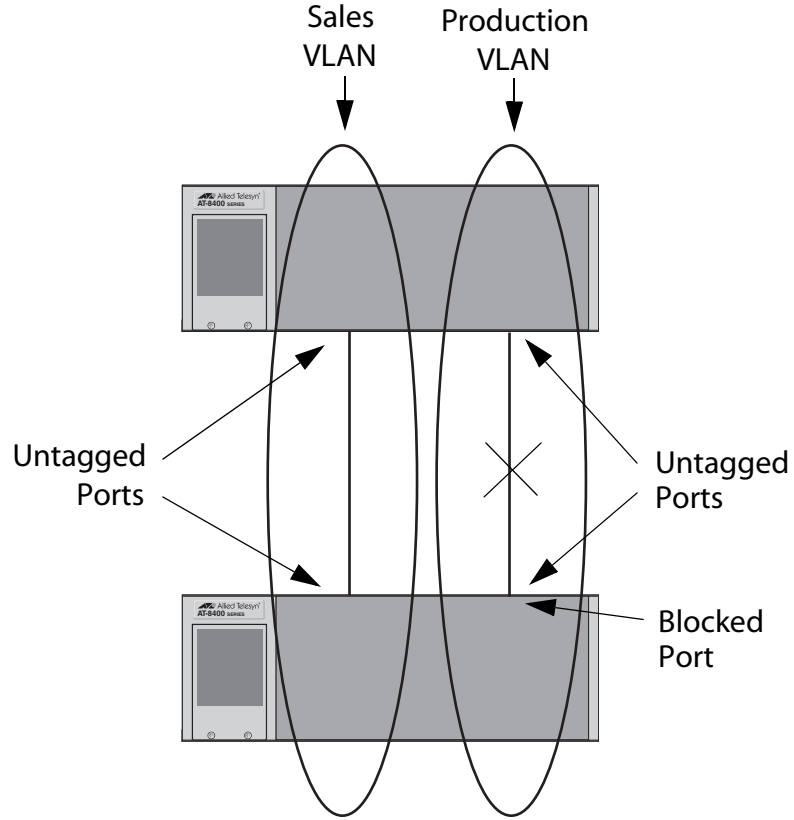


Figure 84 VLAN Fragmentation with STP or RSTP

Figure 85 illustrates the same two AT-8400 Series switches and the same two virtual LANs. But in this example, the two switches are running MSTP and the two VLANs have been assigned different spanning tree instances. Now that they reside in different MSTIs, both links remain active, enabling the VLANs to forward traffic over their respective direct link.

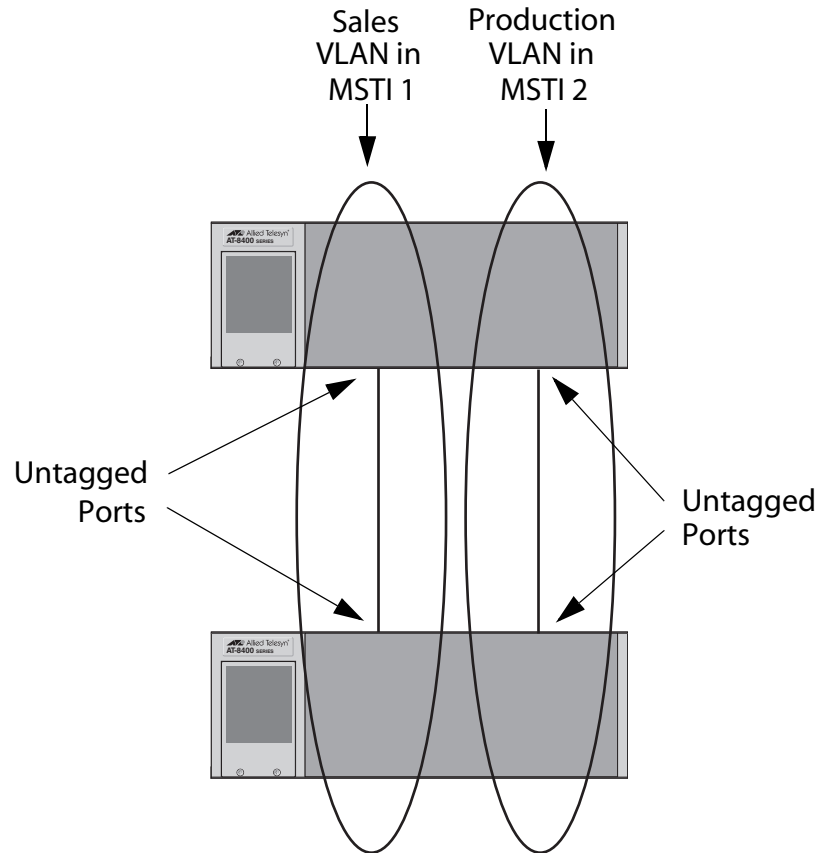


Figure 85 MSTP Example of Two Spanning Tree Instances

A MSTI can contain more than one VLAN. This is illustrated in Figure 86 where there are two AT-8400 Series switches with four VLANs. There are two MSTIs, each containing two VLANs. MSTI 1 contains the Sales and Presales VLANs and MSTI 2 contains the Design and Engineering VLANs.

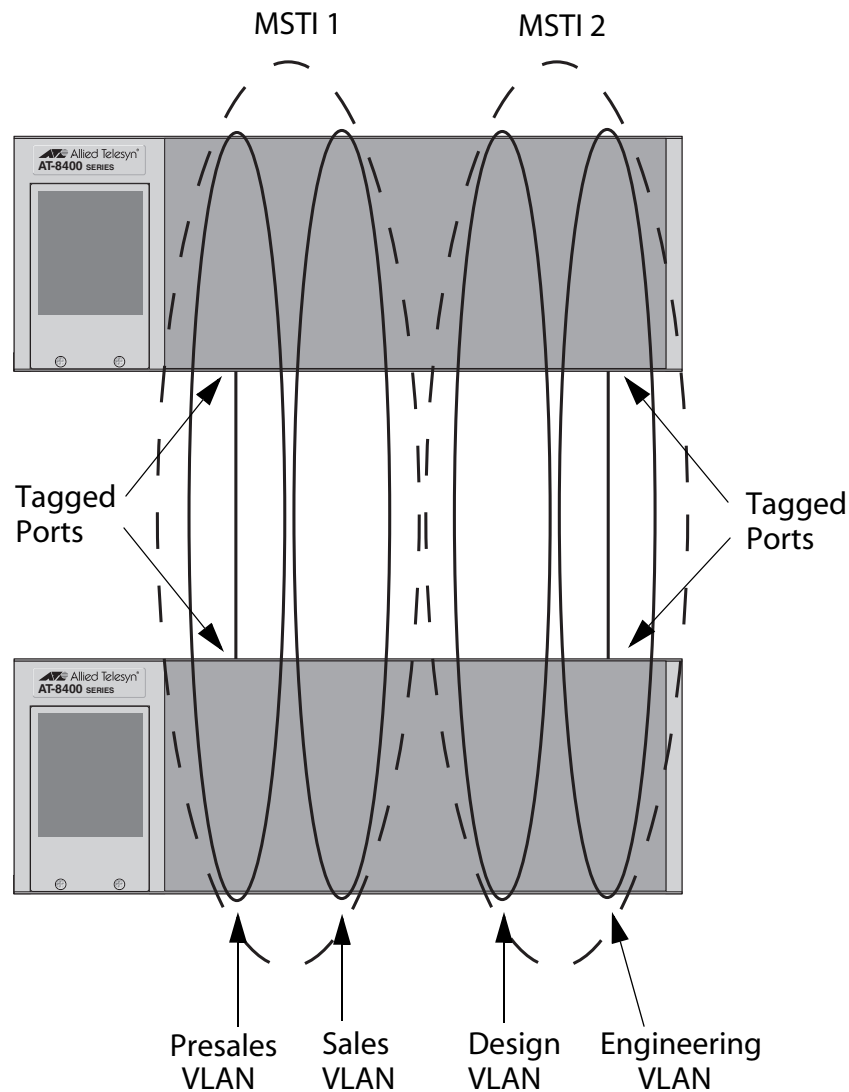


Figure 86 Multiple VLANs in a MSTI

You should note in this example that since an MSTI contains more than one VLAN, the links between the VLAN parts is made with tagged, not untagged, ports so that they can carry traffic from more than one virtual LAN. Referring again to Figure 86, the tagged link in MSTI 1 is carrying traffic for both the Presales and Sales VLANs while the tagged link in MSTI 2 is carrying traffic for the Design and Engineering VLANs.

This example illustrates Allied Telesyn's implementation of MSTP. It shows that a tagged port cannot be a member of VLANs that belong to different MSTIs. That is why each MSTI in the example has its own tagged link.

MSTI Guidelines

Here are several guidelines to keep in mind about MSTIs:

- An AT-8400 Series switch can support up to 16 spanning tree instances, including the CIST, at a time.
- A MSTI can contain any number of VLANs.
- A VLAN can belong to only one MSTI at a time.
- A port on the switch can belong to only one spanning tree instance at a time. This means that a port cannot be a tagged and untagged member of VLANs that belong to different MSTIs. For example, if Port 1 on a line card is an untagged port in one VLAN and a tagged port in three other VLANs, all four VLANs must be assigned to the same MSTI. This rule is required because a port can be either blocking or forwarding; a port cannot perform both functions simultaneously, which could occur if it was a member of VLANs that resided in different spanning tree instances.
- A router or Layer 3 network device is required to forward traffic between different VLANs.

VLAN and MSTI Associations

Part of the task to configuring MSTP involves assigning VLANs to spanning tree instances. The mapping of VLANs to MSTIs is called *associations*. A VLAN, either port-based or tagged, can belong to only one instance at a time, but an instance can contain any number of VLANs.

Multiple Spanning Tree Regions

Another important concept of MSTP is *regions*. A MSTP region is defined as a group of bridges that share exactly the same MSTI characteristics. Those characteristics are:

- Configuration name
- Revision number
- VLANs
- VLAN to MSTI ID associations

A *configuration name* is a name you assign to a region to help you identify it. You must assign each bridge in a region exactly the same name—even the same upper and lowercase lettering. Identifying the regions in your network is easier if you choose names that are characteristic of the functions of the nodes and bridges of the region. In addition, standardize the capitalization of the configuration name. Examples are Sales Region and Engineering Region.

The *revision number* is an arbitrary number you assign to a region. This number can be used to keep track of the revision level of a region's configuration. For example, you might use this value to maintain the number of times you revise a particular MSTP region. It is not important that you maintain this number, only that each bridge in a region have the same number.

The bridges of a particular region must also have the same VLANs. The names of the VLANs and the VLAN IDs must be same on all bridges of a region.

Finally, the VLANs in the bridges must be associated to the same MSTIs.

If any of the above information is different on two bridges, MSTP considers the bridges as residing in different regions.

Figure 87 illustrates the concept of regions. It shows one MSTP region consisting of two AT-8400 Series switches. Each switch in the region has the same configuration name and revision level. The switches also have the same five VLANs and the VLANs are associated with the same MSTIs.

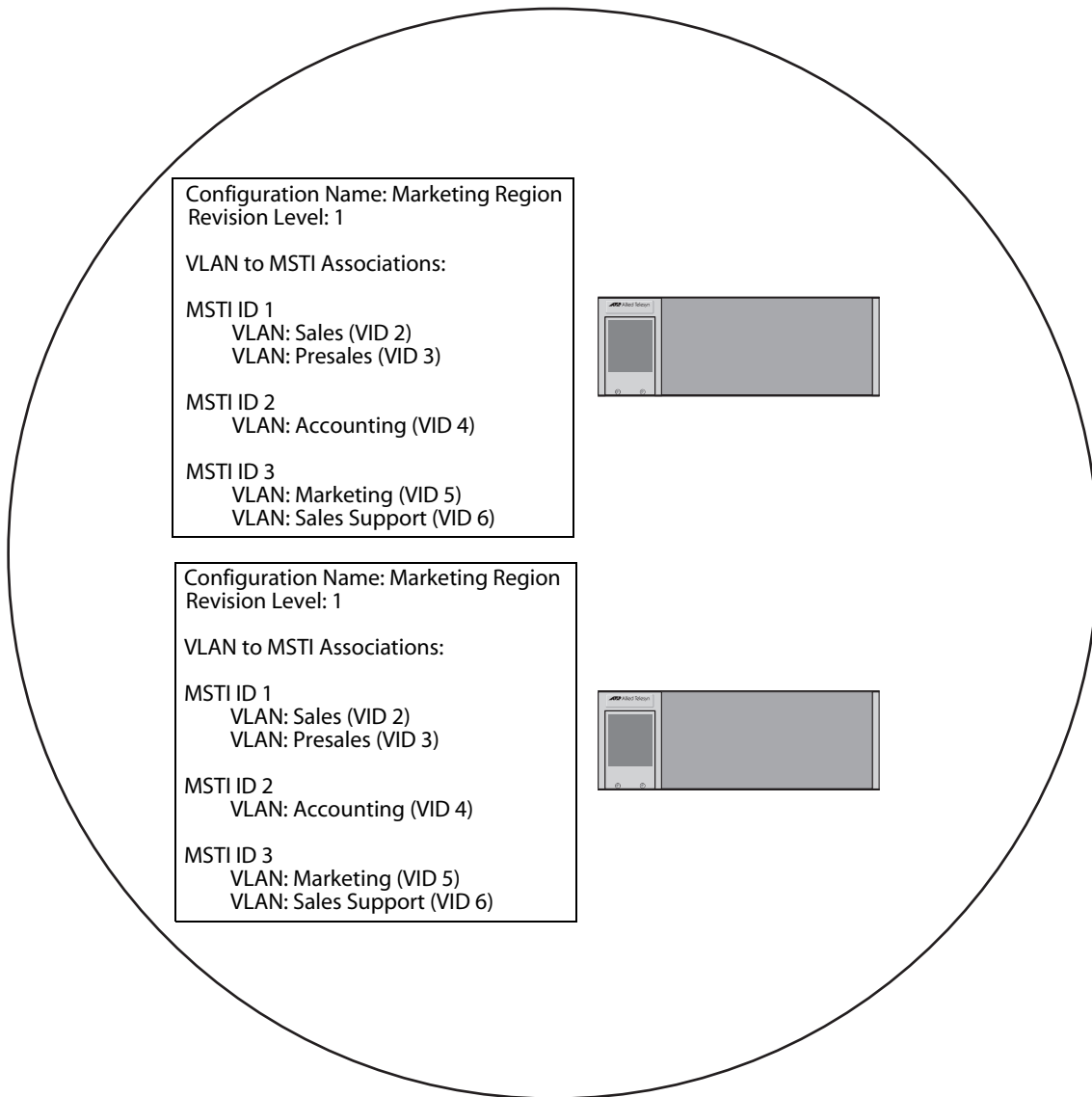


Figure 87 Multiple Spanning Tree Region

The AT-8400 Series switch determines regional boundaries by examining the MSTP BPDUs received on the ports. A port that receives a MSTP BDU from another bridge with regional information different from its own is considered to be a boundary port and the bridge connected to the port as belonging to another region.

The same is true for any ports connected to bridges running the single-instance spanning tree STP or RSTP. Those ports are also considered as part of another region.

Each MSTI functions as an independent spanning tree within a region. Consequently, each MSTI must have a root bridge to locate physical loops within the spanning tree instance. An MSTI's root bridge is called a *regional root*. The MSTIs within a region may share the same regional root or they can have different regional roots.

A regional root for an MSTI must be within the region where the MSTI is located. An MSTI cannot have a regional root that is outside its region.

A regional root is selected by a combination of the *MSTI priority* value and the bridge's MAC address. The MSTI priority is analogous to the RSTP bridge priority value. Where they differ is that while the RSTP bridge priority is used to determine the root bridge for an entire bridged network, MSTI priority is used only to determine the regional root for a particular MSTI.

The range for this parameter is the same as the RSTP bridge priority—from 0 to 61,440 in sixteen increments of 4,096. To set the parameter, you specify the increment that represents the desired MSTI priority value. Table 9 on page 231 lists the increments.

Region Guidelines

Here are several points to remember about regions.

- A network can contain any number of regions and a region can contain any number of AT-8400 Series switches.
- An AT-8400 Series switch can belong to only one region at a time.
- A region can contain any number of VLANs.
- All of the bridges in a region must have the same configuration name, revision level, VLANs, and VLAN to MSTI associations.
- An MSTI cannot span multiple regions.

- ❑ Each MSTI must have a regional root for locating loops in the instance. MSTIs can share the same regional root or have different roots. A regional root is determined by the MSTI priority value and a bridge's MAC address.
- ❑ The regional root of a MSTI must be in the same region as the MSTI.

Common and Internal Spanning Tree (CIST)

MSTP has a default spanning tree instance called the Common and Internal Spanning Tree (CIST). This instance has an MSTI ID of 0.

This instance has unique features and functions that make it different from the MSTIs that you create yourself. First, you cannot delete this instance and you cannot change its MSTI ID.

Second, when you create a new port-based or tagged VLAN, it is by default associated with the CIST and is automatically given an MSTI ID of 0. The Default_VLAN is also associated by default with CIST.

Another critical difference is that when you assign a VLAN to another MSTI, it still partially remains a member of CIST. This is because CIST is used by MSTP to communicate with other MSTP regions and with any RSTP and STP single-instance spanning trees in the network. MSTP uses CIST to participate in the creation of a spanning tree between different regions and between regions and single-instance spanning tree, to form one spanning tree for the entire bridged network.

The reason MSTP uses CIST to form the spanning tree of an entire bridged network is because CIST can cross regional boundaries, while a MSTI cannot. If a port is a boundary port, that is, if it is connected to another region, that port automatically belongs solely to CIST, even if it was assigned to an MSTI, because only CIST is active outside of a region.

As mentioned earlier, every MSTI must have a root bridge, referred to as a regional root, in order to locate loops that might exist within the instance. CIST must also have a regional root. However, the CIST regional root communicates with the other MSTP regions and single-instance spanning trees in the bridged network.

The CIST regional root is set with the *CIST Priority* parameter. This parameter, which functions similar to the RSTP bridge priority value, is used to select the root bridge for the entire bridged network. If an AT-8400 Series switch has the lowest CIST Priority value among all the spanning tree bridges, it functions as the root bridge for all the MSTP regions and STP and RSTP single-instance spanning trees in the network.

MSTP with STP and RSTP

MSTP is fully compatible with STP and RSTP. If a port on an AT-8400 Series switch running MSTP receives STP BPDUs, the port sends only STP BPDU packets. If a port receives RSTP BPDUs, the port sends MSTP BPDUs since RSTP can process MSTP BPDUs.

A port connected to a bridge running STP or RSTP is considered a boundary port of the MSTP region and the bridge as belonging to a different region.

An MSTP region can be considered as a virtual bridge. The implication is that other MSTP regions and STP and RSTP single-instance spanning trees cannot discern the topology or constitution of a MSTP region. The only bridge they are aware of is the regional root of the CIST instance.

Summary of Guidelines

Careful planning is essential for the successful implementation of MSTP. This section reviews all the rules and guidelines mentioned in earlier sections, and adds a few new ones:

- An AT-8400 Series switch can support up to 16 spanning tree instances, including the CIST, at a time.
- A MSTI can contain any number of VLANs.
- A VLAN can belong to only one MSTI at a time.
- An MSTI ID can be from 1 to 15.
- The CIST ID is 0. You cannot change this value.
- A port on the switch can belong to only one spanning tree instance at a time. This means that a port cannot be a tagged and untagged member of VLANs that belong to different MSTIs. For example, if Port 1 on a line card is an untagged port in one VLAN and a tagged port in three other VLANs, all four VLANs must be assigned to the same MSTI. This rule is required because a port can be either blocking or forwarding. A port cannot perform both functions simultaneously, which could occur if it was a member of VLANs that reside in different spanning tree instances.
- A router or Layer 3 network device is required to forward traffic between VLANs.
- A network can contain any number of regions and a region can contain any number of AT-8400 Series switches.
- An AT-8400 Series switch can belong to only one region at a time.
- A region can contain any number of VLANs.

- ❑ All of the bridges in a region must have the same configuration name, revision level, VLANs, and VLAN to MSTI associations.
- ❑ An MSTI cannot span multiple regions.
- ❑ Each MSTI must have a regional root for locating loops in the instance. MSTIs can share the same regional root or have different roots. A regional root is determined by the MSTI priority value and a bridge's MAC address.
- ❑ The regional root of a MSTI must be in the same region as the MSTI.
- ❑ The CIST must have a regional root for communicating with other regions and single-instance spanning trees.
- ❑ MSTP is compatible with STP and RSTP.
- ❑ A port transmits CIST information even when it's associated with another MSTI ID. However, in determining network loops, MSTI takes precedence over CIST. (This is explained in more detail in Associating VLANs to MSTIs on page 269.)

Note

Due to different vendor implementations of the new IEEE 802.1s standard, compatibility issues concerning MSTP instances between the AT-8400 Series switch and switches from other vendors may exist. This can result in compatibility issues between different MSTP implementations. For this release, MSTP is compatible only with other AT-8400 Series switches.

Associating VLANs to MSTIs

Allied Telesyn recommends that you assign all VLANs on a switch to an MSTI. You should not leave a VLAN assigned to just the CIST, including the Default_VLAN. This is to prevent the blocking of a port that should be in the forwarding state. The reason for this guideline is explained below.

An MSTP BPDU contains the instance to which the port transmitting the packet belongs. By default, all ports belong to the CIST instance. So CIST would be included in the BPDU. If the port is a member of a VLAN that has been assigned to another MSTI, that information is also included in the BPDU.

This is shown in Figure 88. Port 8 on a line card in Switch A is a member of a VLAN assigned to MSTI ID 7. Port 1 on another line card in the same switch is a member of a VLAN assigned to MSTI ID 10. The BPDUs transmitted by port 8 to Switch B would indicate that the port is a member of both CIST and MSTI 7, while the BPDUs from Port 1 would indicate the port is a member of the CIST and MSTI 10.

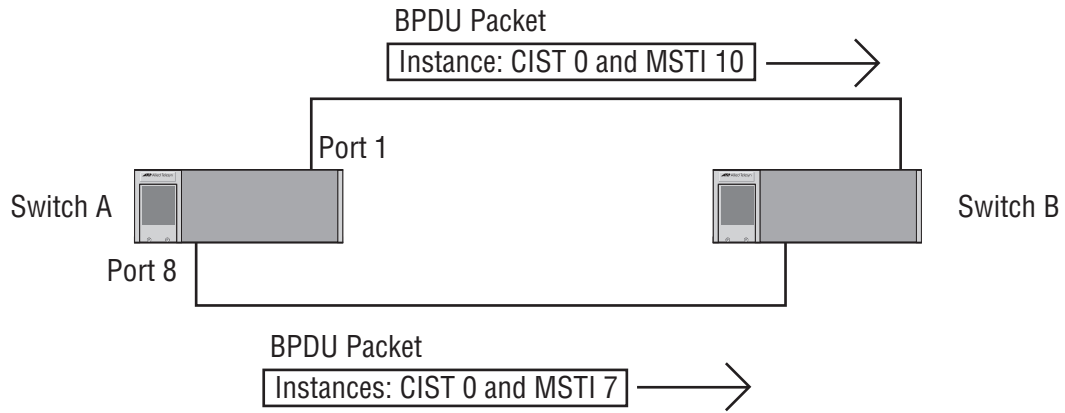


Figure 88 CIST and VLAN Guideline - Example 1

At first glance, it might appear that since both ports belong to CIST, a loop would exist between the switches and that MSTP would block a port to stop the loop. However, within a region, MSTI takes precedence over CIST. When Switch B receives a packet from Switch A, it uses MSTI, not CIST, to determine whether a loop exists. And since both ports on Switch A belong to different MSTIs, Switch B determines that no loop exists.

A problem can arise if you assign some VLANs to MSTIs while leaving others assigned to CIST. The problem is illustrated in Figure 89. The network is the same as the previous example. The only difference is that the VLAN containing Port 8 on Switch A has not been assigned to an MSTI, and belongs only to CIST with its MSTI ID 0.

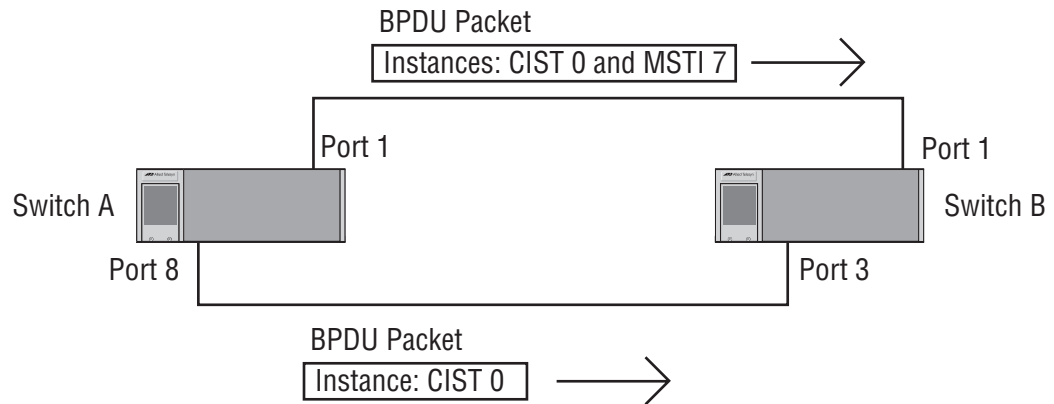


Figure 89 CIST and VLAN Guideline - Example 2

When port 3 on Switch B receives a BPDUs, the switch notes the port sending the packet belongs only to CIST. Consequently, Switch B uses CIST in determining whether a loop exists. The result would be that the switch detects a loop because the other port is also receiving BPDUs packets from CIST 0. Switch B would block a port to cancel the loop.

To avoid this issue, always assign all VLANs on a switch, including the Default_VLAN, to an MSTI. This guarantees that all ports on the switch have an MSTI ID and that helps to ensure that loop detection is based on MSTI, not CIST.

Connecting VLANs Across Different Regions

Special consideration needs to be taken into account when connecting different MSTP regions or an MSTP region and a single-instance STP or RSTP region. Unless planned properly, VLAN fragmentation can occur between the VLANs of your network.

As mentioned previously, only the CIST can span regions. A MSTI cannot. Consequently, you may run into a problem if you use more than one physical data link to connect together various parts of VLANs that reside in bridges in different regions. The result can be a physical loop, which spanning tree disables by blocking ports.

This is illustrated in Figure 90. The example shows two switches, each residing in a different region. Port 1 on a line card in Switch A is a boundary port. It is an untagged member of the Accounting VLAN, which has been associated with MSTI 4. Port 8 on another line card is a tagged and untagged member of three different VLANs, all associated to MSTI 12.

If both switches were a part of the same region, there would be no problem since the ports reside in different spanning tree instances. However, the switches are part of different regions and MSTIs do not cross regions. Consequently, the result would be that spanning tree would determine that a loop exists between the regions, and Switch B would block a port.

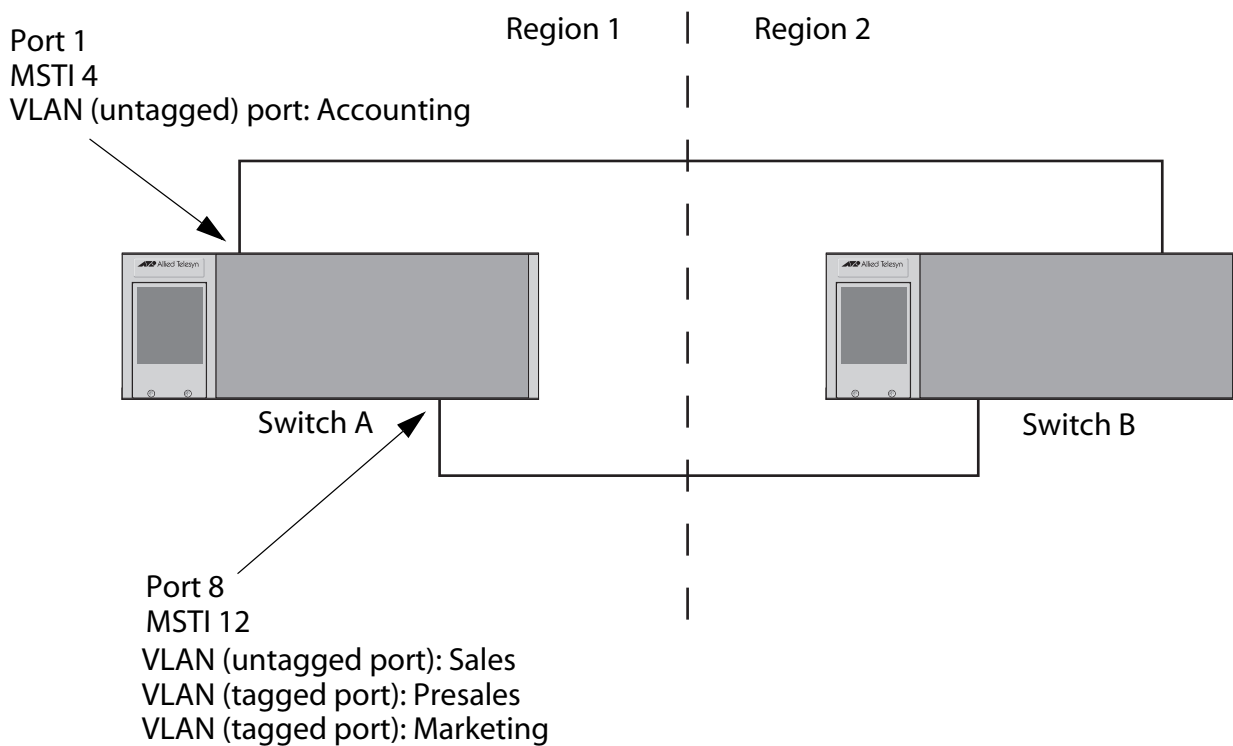


Figure 90 Spanning Regions - Example 1

There are several ways to address this issue. One is to have only one MSTP region for each subnet in your network.

Another approach is to group those VLANs that need to span regions into the same MSTI. Those VLANs that do not span regions can be assigned to other MSTIs.

Here is an example. Let's assume that you have two regions that contain the following VLANs:

Region 1 VLANs

Sales
Presales
Marketing
Advertising
Technical Support
Product Management
Project Management
Accounting

Region 2 VLANs

Hardware Engineering
Software Engineering
Technical Support
Product Management
CAD Development
Accounting

The two regions share three VLANs: Technical Support, Product Management, and Accounting. You could group those VLANs into the same MSTI in each region. For instance, for Region 1 you might group the three VLANs in MSTI 11 and in Region 2 you could group them into MSTI 6. Once grouped, you can connect the VLANs across the regions using a link of tagged ports.

Configuring MSTP

This section contains the following procedures:

- Enabling or Disabling MSTP on page 274
- Configuring MSTP Bridge Settings on page 277
- Configuring the CIST Priority on page 279
- Creating, Deleting, and Modifying MSTI IDs on page 280
- Associating VLANs to MSTI IDs on page 283
- Configuring MSTP Port Settings on page 288
- Displaying MSTP Port Settings and Status on page 290

Note

You cannot configure MSTP unless the protocol has been selected as the active spanning tree protocol on the switch.

Enabling or Disabling MSTP

The AT-8400 Series switch can support STP, RSTP, and MSTP. However, only one spanning tree protocol can be active on the switch at a time. Before you can enable a spanning tree protocol, you must first select it as the active spanning tree protocol on the switch. Once you have selected it as the active protocol, you can then enable or disable it.

To select 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 Main Menu, type **3** to select Spanning Tree Menu.

The Spanning Tree Menu is shown in Figure 91.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142
User: Manager                                00:14:33 15-Jan-2004
Spanning Tree Menu
1 - Spanning Tree Status ..... Disabled
2 - Active Protocol Version ... RSTP
3 - STP Configuration
4 - RSTP Configuration
5 - MSTP Configuration

R - Return to Previous Menu

Enter your selection?

```

Figure 91 Spanning Tree Menu

Note

If you do not want to change the active spanning tree protocol and just want to enable or disable it, go to step 6.

- To change the active version of spanning tree protocol on the switch, type **2** to select Active Protocol Version.

The following prompt is displayed:

```

This operation will need a reboot of the system.
Do you want to continue [Y/N] ->

```

- Type **Y** for yes.

The following prompt is displayed:

```

Enter new value (S-STP, R-RSTP, M-MSTP):

```

- Type **S** to select STP, **R** to select RSTP, or **M** to select MSTP.

The following prompt is displayed:

```

Do you want to enable spanning tree? (Y/N) ->

```

If you select Yes to enable spanning tree, the management software reboots the switch and enables the selected spanning tree protocol. Enable spanning tree if you want to activate spanning tree before you configure the MSTP parameter settings.

If you select No to disable spanning tree, the management software reboots, but does not activate spanning tree. This response is appropriate if you want to configure spanning tree parameters before activating spanning tree.

5. Type **Y** for yes or **N** for no.

The switch reboots and if you select Yes, the selected spanning tree protocol becomes the active protocol on the switch. You can now configure the parameters of the selected spanning tree protocol.

Unlike other management procedures with the AT-S60 software, this procedure does not require you to return to the Main Menu to save your changes. The change to the active spanning tree protocol is automatically saved before the switch reboots.

Note

Steps 6, 7, and 8 apply only if you did not enable the spanning tree when you selected it. These steps enable or disable the spanning tree protocol.

6. To enable or disable the active spanning tree, type **1** to select Spanning Tree Status.
7. Type **E** to enable spanning tree or **D** to disable it. The default is enabled.
8. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Configuring MSTP Bridge Settings

This section contains the procedure for configuring a bridge's MSTP settings.

1. From the Main Menu, type **3** to select Spanning Tree Menu.
The Spanning Tree Menu is shown in Figure 91 on page 275.
2. From the Spanning Tree Menu, type **5** to select MSTP Configuration.
The MSTP Menu is shown in Figure 92.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142

User: Manager                                00:14:33 15-Jan-2004

                                MSTP Menu

1 - Force Version ..... MSTP
2 - Hello Time ..... 2
3 - Forwarding Delay ..... 15
4 - Max Age ..... 20
5 - Max Hops ..... 20
6 - Configuration Name .....
7 - Revision Level ..... 0
8 - Bridge Identifier ..... 00:30:24:1E:EE:11

C - CIST Menu
M - MSTI Menu
V - VLAN-MSTI Association Menu
P - MSTP Port Parameters

R - Return to Previous Menu

Enter your selection?

```

Figure 92 MSTP Menu

Menu selections 1 to 8 are described below. Selections C, M, V, and P are described in later sections in this chapter.

3. Adjust the MSTP settings as needed. The selections are described below.

1 - 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 for 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.

2 - Hello Time

The time interval between generating and sending configuration messages by the bridge. The range of this parameter is 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.

3 - Forwarding Delay

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.

4 - 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 6 to 40 seconds. The default is 20 seconds.

In selecting a value for maximum age, the following must be observed:

MaxAge must be less than $(2 \times (\text{HelloTime} + 1))$

MaxAge must be less than $(2 \times (\text{ForwardingDelay} - 1))$

5 - 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. Once the counter reaches zero, the BPDU is deleted.

6 - 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 include Sales Region and Production Region.

7 - Revision Level

The revision level of an MSTP region. The range is 0 (zero) to 255. 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.

8 - Bridge Identifier

The MAC address of the bridge. The bridge identifier is used as a tie breaker in the selection of a root bridge when two or more bridges have the same bridge priority value. This value cannot be changed.

4. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Configuring the CIST Priority

This procedure explains how to adjust the bridge's CIST priority.

To change the CIST priority, do the following:

1. From the Main Menu, type **3** to select Spanning Tree Menu.
The Spanning Tree Menu is shown in Figure 91 on page 275.
2. From the Spanning Tree Menu, type **5** to select MSTP Configuration.
The MSTP Menu is shown in Figure 92 on page 277.
3. From the MSTP Menu, type to select **C** to select CIST Menu.
The CIST Menu is shown in Figure 93.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142

User: Manager                                00:14:33 15-Jan-2004

                                CIST Menu

CIST Priority ..... 32768
Associated VLANs ..... 1,2,4,11

1 - Modify CIST Priority

R - Return to Previous Menu

Enter your selection?

```

Figure 93 CIST Menu

The CIST Priority field in the menu displays the current value for this MSTP parameter. This number is used in determining the root bridge of the network spanning tree. 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.

The Associated VLANs field displays the VIDs of the VLANs that are currently associated with CIST and have not been assigned to a MSTI.

4. To change the CIST priority, type **1**.

The following prompt is displayed:

```
Enter new priority [the value will be multiplied by
4096]: [0 to 15] ->
```

5. Enter the increment that represents the new CIST priority value.

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 9 on page 231.

6. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Creating, Deleting, and Modifying MSTI IDs

The following procedures explain how to create, delete, and modify MSTI IDs:

- Creating MSTI IDs on page 280
- Deleting an MSTI ID on page 282
- Modifying an MSTI ID on page 283

Creating MSTI IDs

To create MSTI IDs, perform the following procedure.

1. From the Main Menu, type **3** to select Spanning Tree Menu.
The Spanning Tree Menu is shown in Figure 91 on page 275.
2. From the Spanning Tree Menu, type **5** to select MSTP Configuration.
The MSTP Menu is shown in Figure 92 on page 277.
3. From the MSTP Menu, type **M** to select MSTI Menu.

The MSTI Menu is shown in Figure 94.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142

User: Manager                                00:14:33 15-Jan-2004

MSTI Menu

MSTI | Priority | Regional Root ID | Path Cost | Associated VLANs
-----
1      32768      00A0D2 1454B3      0           1,2
2      32768      00A0D2 1454B3      0           4,11

1 - Create MSTI
2 - Delete MSTI
3 - Modify MSTI

U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 94 MSTI Menu

The fields in the table are defined below:

MSTI

Lists the MSTI IDs existing on the switch.

Priority

Specifies the MSTI priority value for the MSTI. The steps in this procedure explain how you can assign this value when you create an MSTI ID and how to modify the value for an existing MSTI ID.

Regional Root ID

Identifies the regional root for the MSTI by its MAC address.

Path Cost

Specifies the path cost from the bridge to the regional root. If the bridge is the regional root, the value is 0.

Associated VLANs

Specifies the VIDs of the VLANs that have been associated with the MSTI ID.

The table does not include the CIST. The table is empty if no MSTI IDs have been created.

4. Type **1** to select Create MSTI.

The following prompt is displayed:

```
Enter the MSTI ID to be created: [1 to 15] ->
```

5. Enter the new MSTP ID.

The MSTI IDs range is from 1 to 15. You can specify only one MSTI ID at a time.

The following prompt is displayed:

```
Success...Do you want to associate VLANs with this
MSTI ID: [Yes/No] ->
```

6. If you want to associate VLANs to the MSTI now, type **Y** for yes. If you want to do it later, type **N** for no.

To add or remove VLANs from an existing MSTI, go to Associating VLANs to MSTI IDs on page 283.

If you respond with yes, the following prompt is displayed:

```
Enter the list of VLANs:
```

7. Enter the VIDs of the VLANs that you want to associate with the MSTI ID.

You can specify more than one VLAN at a time (for example, 4,6,11) To view VIDs, refer to Displaying VLANs on page 418.

8. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Deleting an MSTI ID

To delete an MSTI ID, do the following:

1. From the Main Menu, type **3** to select Spanning Tree Menu.
The Spanning Tree Menu is shown in Figure 91 on page 275.
2. From the Spanning Tree Menu, type **5** to select MSTP Configuration.
The MSTP Menu is shown in Figure 92 on page 277.
3. From the MSTI Menu, type **2** to select Delete MSTI.

The following prompt is displayed:

```
Enter the MSTI ID to be deleted: [1 to 15] ->
```

4. Enter the MSTP IDs that you want to delete.

The range is 1 to 15. (You cannot delete CIST, which has a value of 0.)

All VLANs associated with a deleted MSTP ID are returned to CIST.

5. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Modifying an MSTI ID

To change the MSTI priority value for an MSTI, do the following:

1. From the Main Menu, type **3** to select Spanning Tree Menu.
The Spanning Tree Menu is shown in Figure 91 on page 275.
2. From the Spanning Tree Menu, type **5** to select MSTP Configuration.
The MSTP Menu is shown in Figure 92 on page 277.
3. From the MSTI Menu, type **3** to select MSTI Configuration Menu.
The following prompt is displayed:
Enter the MSTI ID to be modified: [1 to 15] ->
4. Enter the MSTP IDs that you want to modify.
The range is 1 to 15. You can specify only one MSTI ID at a time.
The following prompt is displayed:
Enter new priority [the value will be multiplied by 4096] [0 to 15] -> 8
5. Enter a new MSTI priority number for this MSTI on the bridge.
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 9 on page 231.
6. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Associating VLANs to MSTI IDs

When you create a new MSTI ID, you are given the opportunity to associating VLANs to it. But, once a MSTI ID is created, there might come a time when you want to add more VLANs to it, or perhaps remove VLANs.

This section provides the following procedures:

- Adding or Removing a VLAN from an MSTI ID on page 284
- Associating a VLAN to an MSTI ID on page 286
- Removing a VLAN from an MSTI ID on page 286
- Associating VLANs to an MSTI ID and Deleting All Associated VLANs on page 287

Adding or Removing a VLAN from an MSTI ID

This procedure explains how to associate VLANs on the switch to an existing MSTI ID and also how to remove VLANs. Before performing this procedure, note the following:

- You must create a MSTI ID before you can assign VLANs to it. To create a MSTI ID, refer to *Creating, Deleting, and Modifying MSTI IDs* on page 280.
- You can assign a VLAN to only one MSTI. By default, a VLAN, when created, is associated with the CIST instance, which has a MSTI ID of 0.
- An MSTI can contain any number of VLANs.

To add or remove a VLAN from an MSTI ID, do the following:

1. From the Main Menu, type **3** to select Spanning Tree Menu.
The Spanning Tree Menu is shown in Figure 91 on page 275.
2. From the Spanning Tree Menu, type **5** to select MSTP Configuration.
The MSTP Menu is shown in Figure 92 on page 277.
3. From the MSTP Menu, type **V** to select VLAN-MSTI Association Menu.

The VLAN-MSTI Association Menu is shown in Figure 95.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142

User: Manager                                00:14:33 15-Jan-2004

VLAN-MSTI Association Menu

MSTI/CIST      Associated VLANs
-----
0
4              1,2
5              6
7              7,22

1 - Add VLANs to MSTI
2 - Delete VLANs from MSTI
3 - Set VLAN to MSTI association
4 - Clear VLAN to MSTI association

U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 95 VLAN-MSTI Association Menu

The fields in the table are defined below:

MSTI / CIST

Lists the CIST and current MSTI IDs on the switch.

Associated VLANs

Specifies the VIDs of the VLANs associated with the CIST and MSTI IDs. For instance, referring to the figure above, the VLANs with the VIDs 7 and 22 are assigned to MSTI 7.

Associating a VLAN to an MSTI ID

To associate a VLAN to an MSTP ID, do the following:

1. From the Main Menu, type **3** to select Spanning Tree Menu.
The Spanning Tree Menu is shown in Figure 91 on page 275.
2. From the Spanning Tree Menu, type **5** to select MSTP Configuration.
The MSTP Menu is shown in Figure 92 on page 277.
3. From the MSTP Menu, type **V** to select VLAN-MSTI Association Menu.
The VLAN-MSTI Association Menu is shown in Figure 95 on page 285.
4. From the VLAN-MSTI Association Menu, type **1** to select Add VLANs to MSTI.

The following prompt is displayed:

```
Enter the MSTI ID <enter 0 for CIST> [0 to 15] ->
```

5. Enter the MSTI ID to which you want to associate a VLAN.

A prompt similar to the following is displayed:

```
Enter the list of VLANs:
```

6. Enter the VLAN ID of the virtual LAN you want to associate with the MSTI ID.

You can enter more than one VLAN at a time (for example, 2,4,7).
To view VIDs, refer to Displaying VLANs on page 418.

The MSTI ID retains any VLANs already associated with it when new VLANs are added.

7. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Removing a VLAN from an MSTI ID

To remove a VLAN from an MSTP ID, do the following:

1. From the Main Menu, type **3** to select Spanning Tree Menu.
The Spanning Tree Menu is shown in Figure 91 on page 275.
2. From the Spanning Tree Menu, type **5** to select MSTP Configuration.
The MSTP Menu is shown in Figure 92 on page 277.
3. From the MSTP Menu, type **V** to select VLAN-MSTI Association Menu.
The VLAN-MSTI Association Menu is shown in Figure 95 on page 285.

4. From the VLAN-MSTI Association Menu, type **2** to select Delete VLANs from MSTI.

The following prompt is displayed:

```
Enter the MSTI ID <enter 0 for CIST> [0 to 15] ->
```

5. Enter the MSTI ID to which you want to associate a VLAN.

A prompt similar to the following is displayed:

```
Enter the list of VLANs:
```

6. Enter the VLAN ID of the virtual LAN that you want to remove from the MSTI ID.

You can enter more than one VLAN at a time (for example, 2,4,7)
To view VLANs, refer to Displaying VLANs on page 418.

A removed VLAN is returned to CIST.

7. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Associating VLANs to an MSTI ID and Deleting All Associated VLANs

To associate VLANs to an MSTP ID while deleting all VLANs that are already associated with it, do the following:

1. From the Main Menu, type **3** to select Spanning Tree Menu.
The Spanning Tree Menu is shown in Figure 91 on page 275.
2. From the Spanning Tree Menu, type **5** to select MSTP Configuration.
The MSTP Menu is shown in Figure 92 on page 277.
3. From the MSTP Menu, type **V** to select VLAN-MSTI Association Menu.
The VLAN-MSTI Association Menu is shown in Figure 95 on page 285.
4. From the VLAN-MSTI Association Menu, type **1** to select Add VLANs to MSTI.

The following prompt is displayed:

```
Enter the MSTI ID <enter 0 for CIST> [0 to 15] ->
```

5. Enter the MSTI ID to which you want to associate a VLAN.

6. A prompt similar to the following is displayed:

```
Enter the list of VLANs:
```

7. Enter the VLAN ID of the virtual LAN that you want to associate with the MSTI ID.

You can enter more than one VLAN at a time (for example, 2,4,7)
(To view VLANs, refer to Displaying VLANs on page 418.)

The VLANs already associated with the MSTI ID are removed when the new VLANs are added. The removed VLANs are returned to CIST.

8. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Configuring MSTP Port Settings

To configure a port's MSTP parameters, perform the following procedure:

1. From the Main Menu, type **3** to select Spanning Tree Menu.
The Spanning Tree Menu is shown in Figure 91 on page 275.
2. From the Spanning Tree Menu, type **5** to select MSTP Configuration.
The MSTP Menu is shown in Figure 92 on page 277.
3. From the MSTP Menu, type **P** to select MSTP Port Parameters.
The MSTP Port Parameters menu is shown in Figure 96.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142
User: Manager                                00:14:33 15-Jan-2004
MSTP Port Parameters
1 - Configure MSTP Port Settings
2 - Display MSTP Port Configuration
3 - Display MSTP Port State
R - Return to Previous Menu
Enter your selection?

```

Figure 96 MSTP Port Parameters Menu

4. Type **1** to select Configure MSTP Port Settings.
The following prompt is displayed:
Enter port-list:
5. Enter the port to configure. For instructions on how to specify port numbers, refer to Specifying Ports on page 34.

The Configure MSTP Port Settings menu is shown in Figure 97.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142
User: Manager                                00:14:33 15-Jan-2004
Configure MSTP Port Settings
1 - Port Priority ..... 128
2 - Port Internal Path Cost ..... Auto Update
3 - Port External Path Cost ..... 200000
4 - Point-to-Point ..... Auto Detect
5 - Edge Port ..... Yes

C - Check Migration to RSTP on Selected Ports (MCHECK)
R - Return to Previous Menu

Enter your selection?

```

Figure 97 Configure MSTP Port Settings Menu

- Adjust the port settings as needed. The selections are described below:

1 - 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 128). For a list of the increments, refer to Table 11 on page 233.

2- 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.

3- 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.

4 - Point-to-Point

This parameter defines whether the port is functioning as a point-to-point port. For an explanation of this parameter, refer to Point-to-Point Ports and Edge Ports on page 234.

5 - Edge Port

This parameter defines whether the port is functioning as an edge port. For an explanation of this parameter, refer to Point-to-Point Ports and Edge Ports on page 234.

C - Check Migration To RSTP on Selected Ports (MCHECK)

The MCHECK parameter appears only when MSTP is enabled. This parameter resets a RSTP port, allowing it to send RSTP BPDUs. When an RSTP bridge receives STP BPDUs on an RSTP port, the port transmits STP BPDUs. The RSTP port continues to transmit STP BPDUs indefinitely. Type **C** to reset the RSTP port to transmit RSTP BPDUs.

Each time a RSTP port is reset by receiving STP BPDUs, you need to type **C** to reset the RSTP port, allowing it to send RSTP BPDUs.

7. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Displaying MSTP Port Settings and Status

The MSTP Port Parameters menu, shown in Figure 96 on page 288, has two selections for displaying a variety of MSTP port information. The two menu selections are described below.

To display MSTP port settings and status, perform the following procedure.

1. From the Main Menu, type **3** to select Spanning Tree Menu.
The Spanning Tree Menu is shown in Figure 91 on page 275.
2. From the Spanning Tree Menu, type **5** to select MSTP Configuration.
The MSTP Menu is shown in Figure 92 on page 277.
3. From the MSTP Menu, type **P** to select MSTP Port Parameters.
The MSTP Port Parameters menu is shown in Figure 96 on page 288.
4. From the MSTP Port Parameters Menu, type **2** to select Display MSTP Port Configuration.

This selection displays a menu that contains the current port settings for the following MSTP parameters:

- Edge-Port
- Point-to-Point Port
- External or Internal Port Cost
- Port Priority

5. To display MSTP port state information, type **3** to select Display MSTP Port State.

This selection displays a menu that contains the following MSTP operating status for a port:

- State - Identifies the MSTP state of the port. Possible states are: discarding, learning, and forwarding. A state of disabled means the port has not established a link with its end node.
- MSTI-ID - The MSTI ID of the VLAN containing the port. (The MSTI ID for a regional boundary port is always 0, even if the VLAN containing the port has been associated with a MSTI other than CIST.)
- Role - Indicates the MSTP role of the port. Possible roles are: root, alternate, backup, and designated.
- Port Cost - The port cost of the port.
- Version - Indicates whether the port is operating in MSTP mode or STP-compatible mode.

Section III

SNMPv3 Protocol

There is one chapter in this section that describes the SNMPv3 Protocol. This chapter explains how to configure an AT-8400 switch with the SNMPv3 Protocol from a local or Telnet management session.

Chapter 17

SNMPv3 Configuration

This chapter provides a description of the AT-S60 implementation of the SNMPv3 protocol. In addition, it provides procedures that allow you to create and modify SNMPv3 users. The following sections are provided:

- SNMPv3 Overview on page 294
- Configuring the SNMPv3 Protocol on page 304
- Configuring the SNMPv3 User Table on page 305
- Configuring the SNMPv3 View Table on page 315
- Configuring the SNMPv3 Access Table on page 324
- Configuring the SNMPv3 SecurityToGroup Table on page 340
- Configuring the SNMPv3 Notify Table on page 348
- Configuring the SNMPv3 Target Address Table on page 355
- Configuring the SNMPv3 Target Parameters Table on page 368
- Configuring the SNMPv3 Community Table on page 381
- Displaying SNMPv3 Table Menus on page 391

Note

Several SNMPv3 parameters appear only in the AT-S60 version 2.1.0 software.

SNMPv3 Overview

The SNMPv3 protocol builds on the existing SNMPv1 and SNMPv2c protocol implementation which is described in Chapter 5: “SNMPv1 and SNMPv2c Configuration.” In the SNMPv3 protocol, User-based Security Model (USM) authentication is implemented along with encryption, allowing you to configure a secure SNMP environment.

The SNMP terminology changes in the SNMPv3 protocol. In the SNMPv1 and SNMPv2c protocols, there are two actors in an SNMP network—a manager and an agent. A *manager* is a server that runs SNMP management software. The manager is often called the Network Management System (NMS). An *agent* is the SNMP software that runs on a network device, such as the AT-8400 switch. An NMS is responsible for querying, or polling, agents in the network. In addition, the agent sends messages to the NMS indicating events. In the AT-S60 implementation of SNMPv3, the switch sends trap and inform messages.

In SNMPv3, managers and agents are both called *entities*. Each entity consists of an Engine Id and SNMP applications. Each AT-8400 switch has a unique Engine ID number. The roles of authoritative entity and non-authoritative entity can change depending on the type of message that is sent. Consider the following three cases:

- ❑ The NMS sends an inform message to the switch. Once a network device (either an NMS or the switch) sends an inform message, the network device expects a response to this type of message. When the switch receives an inform message, then the switch is considered an authoritative entity. In this case, the NMS is the non-authoritative entity.
- ❑ If the switch sends a trap message (a type of message that does not expect a response), then the switch is considered the authoritative entity. In this case, the NMS is the non-authoritative entity.
- ❑ If the switch sends an inform message, then the NMS is considered the authoritative entity. In this case, the switch is the non-authoritative entity.

The concept of entities is important because they help define an internal architecture for the SNMPv3 protocol—as opposed to just defining a set of messages. This new architecture makes the protocol more secure. For more details about the architecture, consult the SNMPv3 RFCs. For the SNMP RFCs supported by this release of the AT-S60 software, see SNMP Management Session on page 32.

With the SNMPv3 protocol, you create users, determine the protocol used for message authentication as well as determine if data transmitted between an SNMP agent and an NMS is encrypted. In addition, you have the ability to restrict user privileges by determining the user's view of the Management Information Bases (MIBs). In this way, you restrict which MIBs the user can display and modify. In addition, you can restrict the types of messages the switch can send on behalf of a user.

After you have created a user, you define SNMPv3 message notification. This consists of determining where messages are sent and what types of messages can be sent. This configuration is similar to the SNMPv1 and SNMPv2c configuration because you configure IP addresses of trap receivers, or hosts. In addition, with the SNMPv3 implementation you decide what types of messages can be sent.

This section further describes the features of the SNMPv3 protocol. The following subsections are included:

- SNMPv3 Authentication Protocols on page 295
- SNMPv3 Privacy Protocol on page 296
- SNMPv3 MIB Views on page 296
- SNMPv3 Storage Types on page 297
- SNMPv3 Message Notification on page 297
- SNMPv3 Tables on page 298
- SNMPv3 Configuration Example on page 303

SNMPv3 Authentication Protocols

The SNMPv3 protocol supports two authentication protocols—HMAC-MD5-96 (MD5) and HMAC-SHA-96 (SHA). Both MD5 and SHA use an algorithm to generate a message digest. Each authentication protocol authenticates a user by checking the message digest. In addition, both protocols use keys to perform authentication. The keys for both protocols are generated locally using the Engine ID, a unique identifier that is assigned to each switch automatically, and the user password. You modify a key only by modifying the user password.

In addition, you have the option of assigning no user authentication. In this case, no authentication is performed for this user. Allied Telesyn does not recommend this configuration for security reasons.

Note

The keys generated by the MD5 and SHA protocols are specific to the SNMPv3 protocol. They have no relation to the SSL and SSH keys for encryption.

SNMPv3 Privacy Protocol

After you have configured an authentication protocol, you have the option of assigning a privacy protocol if you have the encrypted version of the AT-S60 software. In SNMPv3 protocol terminology, privacy is equivalent to encryption. Currently, the DES protocol is the only encryption protocol supported. The DES privacy protocol requires the authentication protocol to be configured as either MD5 or SHA.

If you assign a DES privacy protocol to a user, then you are also required to assign a privacy password. If you choose to not assign the privacy to DES, then SNMPv3 messages are sent in plain text format.

Note

You are able to configure the Privacy Protocol only if you are using the encrypted version of the AT-S60 software.

SNMPv3 MIB Views

The SNMPv3 protocol allows you to configure MIB views for users and groups. The MIB tree is defined by RFC 1155 (Structure of Management Information). See Figure 98.

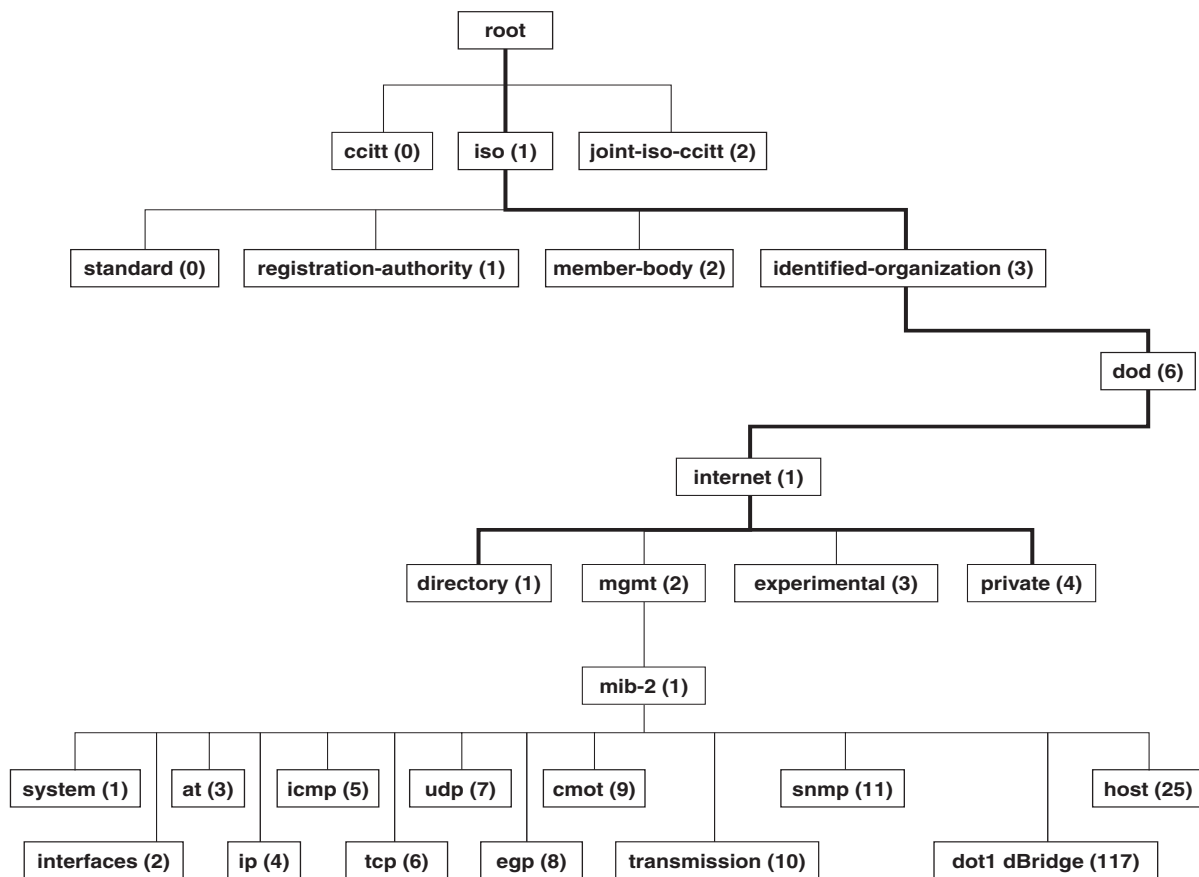


Figure 98 MIB Tree

The AT-S60 software supports the MIB tree, starting with the Internet MIBs, as defined by 1.3.6.1. There are two ways to specify a MIB view. You can enter the OID number of the MIB view or its equivalent text name. For example, to specify MIBs in the Internet view, you can enter the OID format "1.3.6.1" or the text name "internet."

In addition, you can define a MIB view that the user can access or a MIB view that the user cannot access. When you want to permit a user to access a MIB view, you include a particular view. When you want to deny a user access to a MIB view, you exclude a particular view.

After you specify a MIB Subtree view you have the option of further restricting a view by defining a Subtree Mask. The relationship between a MIB Subtree View and a Subtree Mask is analogous to the relationship between an IP address and a subnet mask. The switch uses the subnet mask to determine which portion of an IP address represents the network address and which portion represents the node address. In a similar way, the Subtree Mask further refines the Subtree View and enables you to restrict a MIB view to a specific row of the OID MIB table. Naturally, you need a thorough understanding of the OID MIB table to define a Subtree Mask.

SNMPv3 Storage Types

Each SNMPv3 table entry has its own storage type. You can choose between NonVolatile storage which allows you to save the table entry or Volatile storage which does not allow you to save an entry. If you select the Volatile storage type, when you power off the switch your SNMPv3 configuration is lost and cannot be recovered.

At each SNMPv3 menu, you are prompted to configure a storage type. You do not have to configure the same storage type value for each table entry.

SNMPv3 Message Notification

When you generate an SNMPv3 message from the switch, there are three basic pieces of information included in the message:

- The type of message
- The destination of the message
- SNMP security information

To configure the type of message, you need to define if you are sending a Trap or Inform message. Basically, the switch expects the authoritative entity (or NMS) to respond to an Inform message. The switch does not expect the authoritative entity to respond to a Trap message. These two message types are defined in the SNMPv3 (RFC 2571-6).

To determine the destination of the message, you configure the IP address of the host. This configuration is similar to the SNMPv1 and SNMPv2c configuration.

The SNMP security information consists of information about the following:

- User
- View of the MIB Tree
- Security Level
- Security Model
- Authentication Level
- Privacy Protocol
- Group

To configure the SNMP security information, you associate a user and its related information—View, Security Level, Security Model, Authentication Level, Privacy Protocol and Group—with the type of message and the host IP address.

SNMPv3 Tables

The SNMPv3 configuration is neatly divided into configuring SNMPv3 user information and configuring the message notification. You must configure all seven tables to successfully configure the SNMPv3 protocol. Use the following tables for user configuration:

- Configure SNMPv3 User Table
- Configure SNMPv3 View Table
- Configure SNMPv3 Access Table
- Configure SNMPv3 SecurityToGroup Table

First, you create a user in the Configure SNMPv3 User Table. Then you define the MIB view this user has access to in the Configure SNMPv3 View Table. To configure a security group and associate a MIB view to a security group, you configure the Configure SNMPv3 Access Table. Finally, configure the Configure SNMPv3 SecurityToGroup Menu to associate a user to a security group. See Figure 99 for an illustration of how the user configuration tables are linked.

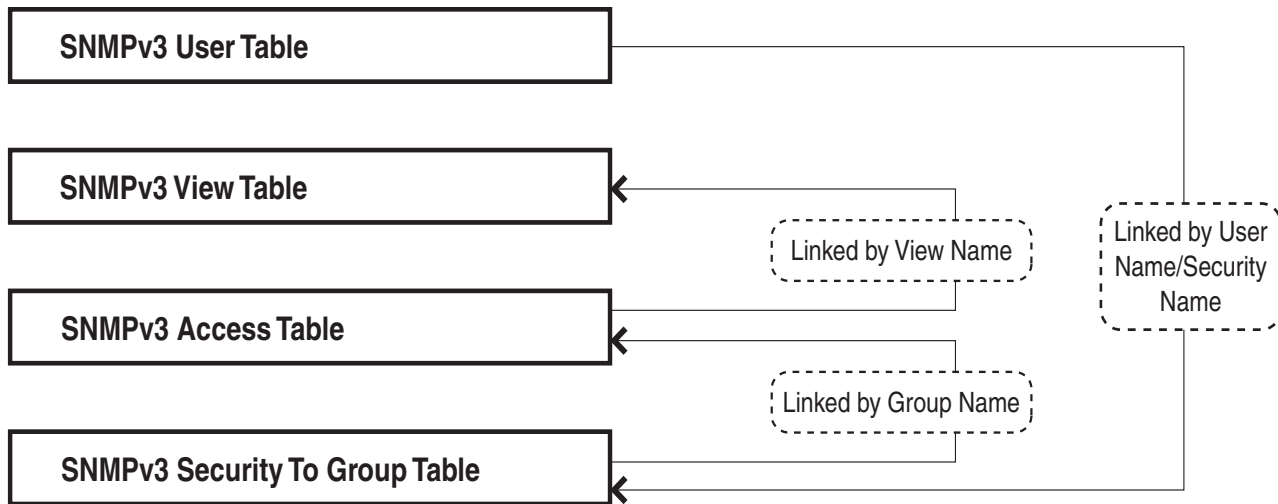


Figure 99 SNMPv3 User Configuration Process

In general, you focus on configuring security groups and then add and delete users from the groups as needed. For example, you may want to have two groups—one for Manager privileges and a second one for Operator privileges. See Appendix B, *SNMPv3 Configuration* on page 293 for an example of Manager and Operator configurations.

After you configure an SNMPv3 user, you need to configure SNMPv3 message notification. This configuration is accomplished with the following tables:

- Configure SNMPv3 Notify Table
- Configure SNMPv3 Target Address Table
- Configure SNMPv3 Target Parameters Table

You start the message notification configuration by defining the type of message you want to send with the SNMPv3 Notify Table. Then you define a IP address that is used for notification in the Configure SNMPv3 Target Address Table. This is the IP address of the SNMPv3 manager. Finally, you associate the trap information with a user by configuring the Configure SNMPv3 Target Parameters Table.

See Figure 100 for an illustration of how the message notification tables are linked.

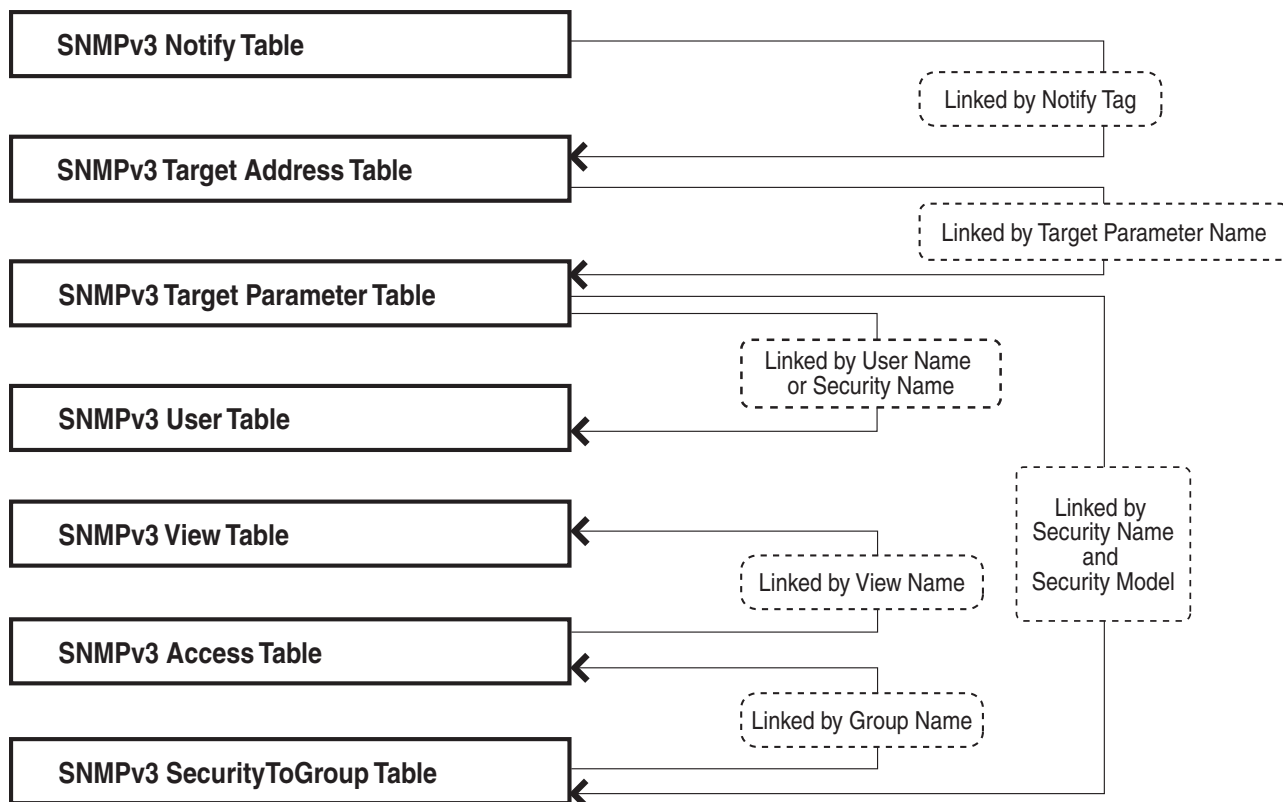


Figure 100 SNMPv3 Message Notification Process

For a more detailed description of the SNMPv3 Tables, see the following subsections:

- ❑ SNMPv3 User Table on page 301
- ❑ SNMPv3 View Table on page 301
- ❑ SNMPv3 SecurityToGroup Table on page 302
- ❑ SNMPv3 Notify Table on page 302
- ❑ SNMPv3 Target Address Table on page 302

- ❑ SNMPv3 Target Parameters Table on page 302
- ❑ SNMPv3 Community Table on page 303

SNMPv3 User Table

The Configure SNMPv3 User Table menu allows you to create an SNMPv3 user and provides the options of configuring authentication and privacy protocols. With an authentication protocol configured, users are authenticated when they send and receive messages. In addition, you can configure a privacy protocol and password so messages a user sends and receives are encrypted. The DES privacy algorithm uses the privacy password and the Engine ID to generate a key that is used for encryption. Lastly, you can configure a storage type for this table entry which allows you to save this user and its related configuration to flash memory.

SNMPv3 View Table

The Configure SNMPv3 View Table Menu allows you to create a view of the MIB OID Table. First, you configure a view of a subtree. Then you have the option of configuring a Subtree Mask that further refines the subtree view. For example, you can use a Subtree Mask to restrict a user's view to one row of the MIB OID Table. In addition, you can chose to include or exclude a view. As a result, you can let a user see a particular view or prevent a user from seeing a particular view. Lastly, you can configure a storage type for this table entry which allows you to save this view to flash memory.

SNMPv3 Access Table

The Configure SNMPv3 Access Table Menu allows you to configure a security group. After you create a security group, you assign a set of users with the same access privileges to this group using the SNMPv3 SecurityToGroup Table. It is useful to consider the types of groups you want to create and the types of access privileges each group will have. In this way, it is easy to keep track of your users as belonging to one or two groups.

For each group, you can assign read, write, and notify views of the MIB table. The views you assign here have been previously defined in the Configure SNMPv3 View Table Menu. For example, the Read View allows group members to view the specified portion of the OID MIB table. The Write View allows group members to write to, or modify, the MIBs in the specified MIB view. The Notify View allows group members to send trap messages defined by the MIB view. Lastly, you can configure a storage type for this table entry which allows you to save this view to flash memory.

SNMPv3 SecurityToGroup Table

The Configure SNMPv3 SecurityToGroup Table Menu allows you to associate a User Name with a security group called a Group Name. The User Name is previously configured with the Configure SNMPv3 User Table Menu. The security group is previously configured with the Configure SNMPv3 Access Table Menu. Lastly, you can configure a storage type for this table entry which allows you to save the entry to flash memory.

SNMPv3 Notify Table

The Configure SNMPv3 Notify Table Menu allows you to define the type of message that is sent from the switch (or non-authoritative entity) to the authoritative entity. You have the option of defining the message type as either an Inform or a Trap message. When a switch sends an Inform message, it expects a response from the authoritative entity. In comparison, when the switch sends a Trap message, it does not require a response from the authoritative entity.

In addition, you define a Notify Tag that links an SNMPv3 Notify Table entry to the host IP address defined in the Configure SNMPv3 Target Address Table Menu. Lastly, you can configure a storage type for this table entry which allows you to save the entry to flash memory.

SNMPv3 Target Address Table

The Configure SNMPv3 Target Address Table Menu allows you to configure the IP address of the host. Also, in an SNMPv3 Target Address Table entry, you configure the values of the Tag List parameter with the previously defined Notify Tag parameter values. The Notify Tag parameter is configured in the Configure SNMPv3 Notify Table. In this way, the Notify and Target Address tables are linked. Lastly, you can configure a storage type for this table entry which allows you to save the entry to flash memory.

SNMPv3 Target Parameters Table

The Configure SNMPv3 Target Parameters Table Menu allows you to define which user can send messages to the host IP address defined in the Configure SNMPv3 Target Address Table. The user and its associated information is previously configured in the Configure SNMPv3 User Table, SNMPv3 View Table, SNMPv3 Access Table, and SNMPv3 SecurityToGroup Table. Lastly, you can configure a storage type for this table entry which allows you to save the entry to flash memory.

SNMPv3 Community Table

The Configure SNMPv3 Community Table Menu allows you to configure SNMPv1 and SNMPv2c communities. If you are going to use the SNMPv3 Tables to configure SNMPv1 and SNMPv2c communities, start with the SNMPv3 Community Table. See Configuring the SNMPv3 Community Table on page 381.

Note

Allied Telesyn recommends that you use the procedures described in Chapter 4, SNMPv1 and SNMPv2c Configuration on page 84 to configure the SNMPv1 and SNMPv2c protocols.

SNMPv3 Configuration Example

You may want to have two classes of SNMPv3 users—Managers and Operators. In this scenario, you would configure one group, called Managers, with full access privileges. Then you would configure a second group, called Operators, with monitoring privileges only. For a detailed example of this configuration, see Appendix B, SNMPv3 Configuration Examples on page 840.

Configuring the SNMPv3 Protocol

This section describes how to configure the SNMPv3 protocol using the SNMPv3 Tables. To successfully configure this protocol, you must perform the procedures in the order given. For overview information about SNMPv3, see the SNMPv3 Overview on page 294.

In order to allow an NMS to access the switch, you need to enable SNMP access. In addition, to allow the switch to send a trap when it receives a request message, you need to enable authentication failure traps. See Enabling the SNMP Protocol on page 86.

The following SNMPv3 tables are described in this chapter:

- Configuring the SNMPv3 User Table on page 305
- Configuring the SNMPv3 View Table on page 315
- Configuring the SNMPv3 Access Table on page 324
- Configuring the SNMPv3 SecurityToGroup Table on page 340
- Configuring the SNMPv3 Notify Table on page 348
- Configuring the SNMPv3 Target Address Table on page 355
- Configuring the SNMPv3 Target Parameters Table on page 368
- Configuring the SNMPv3 Community Table on page 381

The SNMPv3 User, View, Access, and SecurityToGroup tables are concerned with setting up a user, determining authentication and privacy, and associating a user to a security group. The SNMPv3 Notify, Target Address, and Target Parameters tables are concerned with message notification. You use the SNMPv3 Community Table to configure SNMPv1 and SNMPv2 communities.

Due to the complexity of the SNMPv3 configuration, Allied Telesyn recommends that you configure the SNMPv3 protocol with the procedures listed above, in the order they are listed. However, it is possible to configure the SNMPv3 protocol using the above procedures in any order.

Note

New entries to the SNMPv3 tables are added alphabetically.

Configuring the SNMPv3 User Table

This section contains a description of the SNMPv3 User Table and how to create, delete, and modify table entries. Configure the SNMPv3 User Table first. Creating this table, allows you to create an entry in an SNMPv3 User Table for a User Name. In addition, this table allows you to associate a User Name with the following parameters:

- Authentication Protocol
- Authentication Password
- Privacy Protocol
- Privacy Password

Note

You are prompted to configure the Privacy Protocol only if you are using the encrypted version of the AT-S60 software.

There are three functions you can perform with the SNMPv3 User Table.

- Creating an SNMPv3 User Table Entry on page 305
- Deleting an SNMPv3 User Table Entry on page 309
- Modifying an SNMPv3 User Table Entry on page 310

Creating an SNMPv3 User Table Entry

To create an entry in the SNMPv3 User Table, perform the following procedure:

1. From the Main Menu, type **5** to select System Menu.
The System Menu is shown in Figure 5 on page 51.
2. From the System Menu, type **1** to select Configure System.
The Configure System Menu is shown Figure 11 on page 59.
3. From the Configure System Menu, type **1** to select Configure System Software.
The Configure System Software Menu is shown in Figure 12 on page 60.
4. From the Configure System Software Menu, type **8** to select Configure SNMP.
The Configure System Software Menu is shown in Figure 101 on page 306.
5. From the Configure SNMP Menu, type **5** to select Configure SNMPv3 Table.

The Configure SNMPv3 Table Menu is shown in Figure 101.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142
User: Manager                                00:14:33 15-Jan-2004
Configure SNMPv3 Table
1 - SNMP Engine.....80:00:00:CF:31:00:30:84:FD:57:DA
2 - Configure SNMPv3 User Table
3 - Configure SNMPv3 View Table
4 - Configure SNMPv3 Access Table
5 - Configure SNMPv3 SecurityToGroup Table
6 - Configure SNMPv3 Notify Table
7 - Configure SNMPv3 Target Address Table
8 - Configure SNMPv3 Target Parameters Table
9 - Configure SNMPv3 Community Table
R - Return to Previous Menu
Enter your selection?
```

Figure 101 Configure SNMPv3 Table Menu

Note

The SNMP Engine field is a read-only field. You cannot change the setting. The field displays the SNMP engine identifier that is assigned automatically to the switch.

6. From the Configure SNMPv3 Table Menu, type **2** to select Configure SNMPv3 User Table.

The Configure SNMPv3 User Table Menu is shown in Figure 102.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142
User: Manager                                00:14:33 15-Jan-2004
                Configure SNMPv3 User Table
Engine ID ..... 80:00:00:CF:03:00:30:84:FD:57:DA
User Name ..... jenny
Authentication Protocol ... MD5
Privacy Protocol ..... DES
Storage Type ..... NonVolatile
Row Status ..... Active

1 - Create SNMPv3 Table Entry
2 - Delete SNMPv3 Table Entry
3 - Modify SNMPv3 Table Entry

U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 102 Configure SNMPv3 User Table Menu

7. To create a new user table, type **1** to select Create SNMPv3 Table Entry.

The following prompt is displayed:

```
Enter User (Security) Name:
```

8. Enter a descriptive name of the user.

You can enter a name that consists of up to 32-alphanumeric characters.

The following prompt is displayed:

```
Enter Authentication Protocol [M-MD5, S-SHA,
N-None]:
```

9. Enter one of the following:

M-MD5

This value represents the MD5 authentication protocol. With this selection, users 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.

S-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.

N-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.

If you select NONE, you are prompted for the Storage Type. Go to Step 13.

If you select MD5 or SHA, the following prompt is displayed:

```
Enter Authentication Password:
```

10. Enter an authentication password of up to 32-alphanumeric characters and press Return.

You are prompted to re-enter the password.

The following prompt is displayed:

```
Enter Privacy Protocol [D-DES, N-None]:
```

Note

If you have the non encrypted 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.

11. Select one of the following options:

D -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.

N -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.

If you select NONE, you are prompted for the Storage Type. Go to Step 13.

If you select DES, the following prompt is displayed:

```
Enter Privacy Password:
```

12. Enter a privacy password of up to 32-alphanumeric characters.

You are prompted to re-enter the password.

The following prompt is displayed:

```
Enter Storage Type [V-Volatile, N-NonVolatile]:
```

13. Select one of the following storage types for this table entry:

V - Volatile

Select this storage type if you do not want the ability to save an entry in the SNMPv3 User Table to nonvolatile memory. After making changes to an SNMPv3 User Table entry with a Volatile storage type, the **S** - Save Configuration Changes option does not appear on the Main Menu.

N-NonVolatile

Select this storage type if you want the ability to save an entry in the SNMPv3 User Table to nonvolatile memory. After making changes to an SNMPv3 User Table entry with a NonVolatile storage type, the **S** - Save Configuration Changes option appears on the Main Menu, allowing you to save your changes.

Note

The Row Status parameter is a read-only field in the Telnet and Local interfaces. The Active value indicates the SNMPv3 User Table entry takes effect immediately.

14. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Deleting an SNMPv3 User Table Entry

You may want to delete an entry from the SNMPv3 User Table. When you delete an entry in the SNMPv3 User Table, there is no way to undelete, or recover it.

To delete an entry in the SNMPv3 User Table, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in Configuring the SNMPv3 User Table on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is shown in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **2** to select Configure SNMPv3 User Table.

The SNMPv3 User Table is shown in Figure 102.

3. From the SNMPv3 User Table, type **2** to select Delete SNMPv3 Table Entry.

The following prompt is displayed:

```
Enter User (Security) Name:
```

4. Enter the User Name of the User Table entry you want to delete.

The following prompt is displayed:

```
Do you want to delete this table entry? (Y/N):
[Yes/No]->
```

5. Enter **Y** to delete the user or **N** to save the user.
6. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Modifying an SNMPv3 User Table Entry

This section describes how to modify parameters in an SNMPv3 Notify Table entry. See the following procedures:

- Modifying the Authentication Protocol and Password on page 310
- Modifying the Privacy Protocol and Password on page 312
- Modifying the Storage Type on page 314

Modifying the Authentication Protocol and Password

To modify the Authentication Protocol and Password in an SNMPv3 User Table entry, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in Configuring the SNMPv3 User Table on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 User Table Menu is shown in Figure 101

2. From the Configure SNMPv3 Table Menu, type **2** to select Configure SNMPv3 User Table.

The SNMPv3 User Table is shown in Figure 102.

3. From the SNMPv3 User Table, type **3** to select Modify SNMPv3 Table Entry.

The Modify SNMPv3 User Table is shown in Figure 103.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142
User: Manager                                00:14:33 15-Jan-2004
Modify SNMPv3 User Table
Engine ID ..... 80:00:00:CF:03:00:30:84:FD:57:DA
User Name ..... wilson
Authentication Protocol ... SHA
Privacy Protocol ..... DES
Storage Type ..... NonVolatile
Row Status ..... Active

1 - Set Authentication Protocol & Password
2 - Set Privacy Protocol & Password
3 - Set Storage Type

U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 103 Modify SNMPv3 User Table Menu

- To change the authentication protocol and password, type **1** to select Set Authentication Protocol & Password.

The following prompt is displayed:

```
Enter User Name:
```

- Enter the User Name of the User Table you want to modify.

The following prompt is displayed:

```
Enter Authentication Protocol [M-MD5, S-SHA,
N-None]:
```

- Enter one of the following:

M-MD5

This value represents the MD5 authentication protocol. With this selection, users 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.

S-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.

N-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.

If you select None, go to step 9.

If you select MD5 or SHA, the following prompt is displayed:

Enter Authentication Password:

7. Enter an authentication password of up to 32-alphanumeric characters.

The following prompt is displayed:

Re-enter Authentication password:

8. Re-enter the password.

The following message is displayed:

Authentication protocol algorithm has been changed.

The following prompt is displayed:

Please enter privacy password to regenerate privacy key.

9. Enter the Privacy Password for this User Name.

The following prompt is displayed:

Re-enter Privacy password:

10. Re-enter the password.
11. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Modifying the Privacy Protocol and Password

To modify the Privacy Protocol and Password in an SNMPv3 User Table entry, perform the following procedure.

Note

You can only configure the Privacy Protocol if you have configured the Authentication Protocol with the MD5 or SHA values.

1. Follow steps 1 through 5 in the procedure described in Configuring the SNMPv3 User Table on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 User Table Menu is shown in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **2** to select Configure SNMPv3 User Table.

The SNMPv3 User Table is shown in Figure 102 on page 307.

3. From the SNMPv3 User Table, type **3** to select Modify SNMPv3 Table Entry.

The Modify SNMPv3 Table Menu is shown in Figure 103 on page 311.

4. Type **2** to select Privacy Protocol & Password.

The following prompt is displayed:

```
Enter User (Security) Name:
```

5. Enter the User Name.

The following prompt is displayed:

```
Enter Privacy Protocol [D-DES, N-None]:
```

6. Choose one of the following Privacy Protocols:

D -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.

N -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.

If you select None, proceed to step 9.

If you select DES, the following prompt is displayed:

```
Enter Privacy Password:
```

7. Enter a privacy password of up to 32-alphanumeric characters.

The following prompt is displayed:

```
Re-enter Authentication password:
```

8. Re-enter the password.
9. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Modifying the Storage Type

To modify the Storage Type in an SNMPv3 User Table entry, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in Configuring the SNMPv3 User Table on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 User Table Menu is shown in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **2** to select Configure SNMPv3 User Table.

The SNMPv3 User Table is shown in Figure 102 on page 307.

3. From the SNMPv3 User Table, type **3** to select Modify SNMPv3 Table Entry.

The Modify SNMPv3 Table Menu is shown in Figure 103 on page 311.

4. To change the storage type, type **3** to select Set Storage Type.

The following prompt is displayed:

```
Enter User (Security) Name:
```

5. Enter the User Name.

The following prompt is displayed:

```
Enter Storage Type [V-Volatile, N-NonVolatile]:
```

6. Select one of the following storage types for this table entry:

V - Volatile

Select this storage type if you do not want the ability to save an entry in the SNMPv3 User Table to nonvolatile memory. After making changes to an SNMPv3 User Table entry with a Volatile storage type, the **S** - Save Configuration Changes option does not appear on the Main Menu.

N-NonVolatile

Select this storage type if you want the ability to save an entry in the SNMPv3 User Table to nonvolatile memory. After making changes to an SNMPv3 User Table entry with a NonVolatile storage type, the **S** - Save Configuration Changes option appears on the Main Menu, allowing you to save your changes.

7. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Configuring the SNMPv3 View Table

This section contains a description of the SNMPv3 View Table and how to create, delete, and modify table entries. Creating this table, allows you to specify a view using the following parameters:

- Subtree OID
- Subtree Mask
- MIB OID Table View

To configure the SNMPv3 View Table, you need to be very familiar with the MIB tree. You can be very specific about the view a user can or cannot access—down to a column or row of the tree. AT-S60 supports the Internet subtree of the MIB tree. See RFC 2575 for detailed information about defining a view.

There are three functions you can perform with the SNMPv3 User Table.

- Creating an SNMPv3 View Table Entry on page 315
- Deleting an SNMPv3 View Table Entry on page 318
- Modifying an SNMPv3 View Table Entry on page 319

Creating an SNMPv3 View Table Entry

To create an entry in the SNMPv3 View Table, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is displayed.

2. From the Configure SNMPv3 Table Menu, type **3** to select Configure SNMPv3 View Table.

The Configure SNMPv3 View Table Menu is shown in Figure 104.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142
User: Manager                                00:14:33 15-Jan-2004
Configure SNMPv3 View Table
View Name ..... internet
Subtree OID ..... 1.3.6.1
Subtree Mask .....
View Type ..... Included
Storage Type ..... NonVolatile
Row Status ..... Active

1 - Create SNMPv3 Table Entry
2 - Delete SNMPv3 Table Entry
3 - Modify SNMPv3 Table Entry

U - Update Display
R - Return to Previous Menu

Enter your selection?
```

Figure 104 Configure SNMPv3 View Table Menu

3. From the Configure SNMPv3 View Table Menu, type **1** to select Create SNMPv3 Table Entry.

The following prompt is displayed:

Enter View Name:

4. Enter a descriptive name of this View.

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.

The following prompt is displayed:

Enter View Subtree (OID format/Text Name):

5. Enter 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
```

The following prompt is displayed:

```
Enter Subtree Mask (Hex format):
```

6. Enter a subtree mask.

This is an optional parameter that is used to further refine the value in the View Subtree parameter. This parameter is in binary format.

The View Subtree parameter defines a MIB View and the Subtree Mask further restricts a user's view, for example, to a specific row of the MIB tree. The value of the Subnet Mask parameter is dependent on the subtree you select. See RFC 2575 for detailed information about defining a subnet mask.

The following prompt is displayed:

```
Enter View Type [I-Included, E-Excluded]:
```

7. Enter one of the following view types:

I - Included

Enter this value to permit a user to see the subtree specified above.

E - Excluded

Enter this value to not permit a user to see the subtree specified above.

The following prompt is displayed:

```
Enter Storage Type [V-Volatile, N-NonVolatile]:
```

8. Select one of the following storage types for this table entry:

V - Volatile

Select this storage type if you do not want the ability to save an entry in the SNMPv3 View Table to the configuration file. After making changes to an SNMPv3 View Table entry with a Volatile storage type, the **S** - Save Configuration Changes option does not appear on the Main Menu.

N-NonVolatile

Select this storage type if you want the ability to save an entry in the SNMPv3 View Table to the configuration file. After making changes to an SNMPv3 View Table entry with a NonVolatile storage type, the **S** - Save Configuration Changes option appears on the Main Menu, allowing you to save your changes.

Note

The Row Status parameter is a read-only field in the Telnet and Local interfaces. The Active value indicates the SNMPv3 View Table entry takes effect immediately.

9. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Deleting an SNMPv3 View Table Entry

You may want to delete an entry from the SNMPv3 View Table. After you delete an SNMPv3 View Table entry, there is no way to undelete, or recover it.

To delete an entry in the SNMPv3 View Table, perform the following procedure:

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is shown in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **3** to select Configure SNMPv3 View Table.

The SNMPv3 View Table is shown in Figure 104 on page 316.

3. From the SNMPv3 View Table, type **2** to select Delete SNMPv3 Table Entry.

The following prompt is displayed:

```
Enter View Name:
```

4. Enter the View Name of the View Table entry you want to delete.

The following prompt is displayed:

```
Enter View Subtree (OID format/Text Name):
```

5. Enter the subtree for this view.

```
Do you want to delete this table entry? (Y/N):
[Yes/No]->
```

6. Enter **Y** to delete the view or **N** to save the view.
7. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Modifying an SNMPv3 View Table Entry

This section describes how to modify parameters in an SNMPv3 Notify Table entry. See the following procedures:

- Modifying a Subtree Mask on page 319
- Modifying a View Type on page 321
- Modifying a Storage Type on page 322

Modifying a Subtree Mask

To modify the Subtree Mask parameter in an SNMPv3 View Table entry, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is shown in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **3** to select Configure SNMPv3 View Table.

The Configure SNMPv3 View Table Menu is shown in Figure 104 on page 316.

3. From the Configure SNMPv3 View Table Menu, type **3** to select Modify SNMPv3 Table Entry.

The Modify SNMPv3 View Table Menu is shown in Figure 105.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142
User: Manager                                00:14:33 15-Jan-2004
Modify SNMPv3 View Table

View Name ..... tcp
Subtree OID ..... 1.3.6.1.2.1.6
Subtree Mask ..... ff:ff
View Type ..... Included
Storage Type ..... NonVolatile
Row Status ..... Active

1 - Set Subtree Mask
2 - Set View Type
3 - Set Storage Type

U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 105 Modify SNMPv3 View Table Menu

- To modify the Subtree Mask for this view, type **1** to select Set Subtree Mask.

The following prompt is displayed:

```
Enter View Name:
```

- Enter an existing View Name.

The following prompt is displayed:

```
Enter View Subtree (OID format/Text Name):
```

- Enter 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
```

The following prompt is displayed:

```
Enter Subtree Mask (Hex format):
```

- Enter a Subtree Mask.

This is an optional parameter that is used to further refine the value in the View Subtree parameter. This parameter is in binary format.

The View Subtree parameter defines a MIB View and the Subtree Mask further restricts a user's view, for example, to a specific row of the MIB tree. The value of the Subnet Mask parameter is dependent on the subtree you select. See RFC 2575 for detailed information about defining a subnet mask.

8. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Modifying a View Type

To modify the View Type parameter in an SNMPv3 View Table entry, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is shown in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **3** to select Configure SNMPv3 View Table.

The Configure SNMPv3 View Table Menu is shown in Figure 104 on page 316.

3. From the Configure SNMPv3 View Table Menu, type **3** to select Modify SNMPv3 Table Entry.

The Modify SNMPv3 Table Menu is shown in Figure 105 on page 320.

4. To modify the View Type, type **2** to select Set View Type.

The following prompt is displayed:

```
Enter View Name:
```

5. Enter a View Name that was previously configured.

The following prompt is displayed:

```
Enter View Subtree (OID format/Text Name):
```

6. Enter the View Subtree value for this View Name.

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
```

The following prompt is displayed:

```
Enter View Type [I-Included, E-Excluded]:
```

7. Choose one of the following view types:

I - Included

Enter this value to permit a user to see the subtree specified above.

E - Excluded

Enter this value to not permit a user to see the subtree specified above.

8. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Modifying a Storage Type

To modify the Storage Type parameter in an SNMPv3 View Table entry, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is shown in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **3** to select Configure SNMPv3 View Table.

The Configure SNMPv3 View Table Menu is shown in Figure 104 on page 316.

3. From the Configure SNMPv3 View Table Menu, type **3** to select Modify SNMPv3 Table Entry.

The Modify SNMPv3 Table Menu is shown in Figure 105 on page 320.

4. To modify the storage type, type **3** to select Set Storage Type.

The following prompt is displayed:

```
Enter View Name:
```

5. Enter the View Name you want to modify.

The following prompt is displayed:

```
Enter View Subtree (OID format/Text Name):
```

6. Enter the View Subtree for this View Name.

The following prompt is displayed:

```
Enter Storage Type [V-Volatile, N-Nonvolatile]:
```

7. Select one of the following storage types for this table entry:

V - Volatile

Select this storage type if you do not want the ability to save an entry in the SNMPv3 View Table to the configuration file. After making changes to an SNMPv3 View Table entry with a Volatile storage type, the **S** - Save Configuration Changes option does not appear on the Main Menu.

N-NonVolatile

Select this storage type if you want the ability to save an entry in the SNMPv3 View Table to the configuration file. After making changes to an SNMPv3 View Table entry with a NonVolatile storage type, the **S** - Save Configuration Changes option appears on the Main Menu, allowing you to save your changes.

8. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Configuring the SNMPv3 Access Table

This section contains a description of the SNMPv3 Access Table and how to create, delete, and modify table entries. The SNMPv3 Access Table allows you to configure a security group. Each user must belong to a security group. After you have configured a security group, use the SecurityToGroup Table to assign users to security groups. See Creating an SNMPv3 SecurityToGroup Table Entry on page 340.

For each security group, you can assign the following attributes:

- a Security Model (SNMPv1, SNMPv2c, SNMPv3)
- Read, write, and notify views
- A security level
- A storage type

Before you begin this procedure, you will need to configure entries in the View Table. These values are used to configure the Read, Write, and Notify View parameters in this procedure. See Configuring the SNMPv3 View Table on page 315.

There are three functions you can perform with the SNMPv3 Access Table.

- Creating an SNMPv3 Access Table Entry on page 324
- Deleting an SNMPv3 Access Table Entry on page 329
- Modifying an SNMPv3 Access Table Entry on page 330

Creating an SNMPv3 Access Table Entry

To create an entry in the SNMPv3 Access Table, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is shown in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **4** to select Configure SNMPv3 Access Table.

The Configure SNMPv3 Access Table Menu is shown in Figure 106.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142

User: Manager                                00:14:33 15-Jan-2004

                Configure SNMPv3 Access Table

Group Name .... softwareengineering   Security Model . v3
Context Prefix.                        Security Level . AuthPriv
Read View..... internet              Context Match .. Exact
Write View .... tcp                  Storage Type ... NonVolatile
Notify View ... tcp                  Row Status ..... Active

1 - Create SNMPv3 Table Entry
2 - Delete SNMPv3 Table Entry
3 - Modify SNMPv3 Table Entry

U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 106 Configure SNMPv3 Access Table Menu

- To create a group in the SNMPv3 Access Table, type **1** to select Create SNMPv3 Table Entry.

The following prompt is displayed:

```
Enter Group Name:
```

- 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, unique group names makes it easier to tell the groups apart.

There are four default values for this field:

- defaultV1GroupReadOnly
- defaultV1GroupReadWrite
- defaultV2cGroupReadOnly
- defaultV2cGroupReadWrite

These values are reserved for SNMPv1 and SNMPv2c implementations.

Note

The Context Prefix and the Context Match fields are a read only fields. The Context Prefix field is always set to null. The Context Match field is always set to exact.

The following prompt is displayed:

```
Enter Security Model [1-v1, 2-v2c, 3-v3]:
```

5. Select one of the following SNMP protocols as the Security Model for this Group Name.

1-v1

Select this value to associate the Group Name with the SNMPv1 protocol.

2-v2c

Select this value to associate the Group Name with the SNMPv2c protocol.

3-v3

Select this value to associate the Group Name with the SNMPv3 protocol. The SNMPv3 protocol allows you to configure the group to authenticate SNMPv3 users and encrypt messages.

The following prompt is displayed:

```
Enter Security Level [N-NoAuthNoPriv, A-AuthNoPriv, P-AuthPriv]:
```

6. Select one of the following security levels:

N-NoAuthNoPriv

This option represents no authentication and no privacy protocol. Select this security level if you do not want to authenticate SNMP users 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, N-NoAuthNoPriv is the only security level you can select.

A-AuthNoPriv

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.

P-AuthPriv

This option represents authentication and the privacy protocol. Select this security level to encrypt messages using a privacy protocol and authenticate SNMP users. This level provides the

greatest level of security. You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

The following prompt is displayed:

```
Enter Read View Name:
```

7. Enter a value that you configured with the View Name parameter in the SNMPv3 View Table.

A Read View Name 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.

The following prompt is displayed:

```
Enter Write View Name:
```

8. Enter a value that you configured with the View Name parameter in the SNMPv3 View Table.

A Write View Name 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.

The following prompt is displayed:

```
Enter Notify View Name:
```

9. Enter a value that you configured with the View Name parameter in the SNMPv3 View Table.

A Notify View Name allows the users assigned to this Group Name to send traps permitted in the specified View. This value does not need to be unique.

The following prompt is displayed:

```
Enter Storage Type [V-Volatile, N-NonVolatile]:
```

10. Select one of the following storage types for this table entry:

V - Volatile

Select this storage type if you do not want the ability to save an entry in the SNMPv3 Access Table to the configuration file. After making changes to an SNMPv3 Access Table entry with a Volatile storage type, the

S - Save Configuration Changes option does not appear on the Main Menu.

N-NonVolatile

Select this storage type if you want the ability to save an entry in the SNMPv3 Access Table to the configuration file. After making changes to an SNMPv3 Access Table entry with a NonVolatile storage type, the **S** - Save Configuration Changes option appears on the Main Menu, allowing you to save your changes.

Note

The Row Status parameter is a read-only field in the Telnet and Local interfaces. The Active value indicates the SNMPv3 Access Table entry will take effect immediately.

11. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Deleting an SNMPv3 Access Table Entry

You may want to delete an entry from the SNMPv3 Access Table. After you delete an SNMPv3 Access Table, there is no way to undelete, or recover, it.

To delete an entry in the SNMPv3 Access Table, perform the following procedure:

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is shown in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **4** to select Configure SNMPv3 Access Table.

The SNMPv3 Access Table is shown in Figure 106 on page 325.

Note

To display a particular Group Name and its associated parameters from the Configure SNMPv3 Access Table Menu, type **N** to display the Next Page and **P** to display the previous page.

3. From the SNMPv3 Access Table, type **2** to select Delete SNMPv3 Table Entry.

The following prompt is displayed:

```
Enter Group Name:
```

4. Enter the Group Name that you want to delete.

The following prompt is displayed:

```
Enter Security Model [1-v1, 2-v2c, 3-v3]:
```

5. Enter the Security Model of this Group Name.

Select one of the following security levels:

1-v1

Select this value to associate the Group Name with the SNMPv1 protocol.

2-v2c

Select this value to associate the Group Name with the SNMPv2c protocol.

3-v3

Select this value to associate the Group Name with the SNMPv3 protocol. The following prompt is displayed:

```
Enter the Security Level [N-NoAuthNoPriv, A-AuthNoPriv, P-AuthPriv]:
```

6. Enter the Security Level of this Group Name.

Select one of the following Security Levels:

N-NoAuthNoPriv

This option represents no authentication and no privacy protocol. Select this security level if you do not want to authenticate SNMP users 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, N-NoAuthNoPriv is the only security level you can select.

A-AuthNoPriv

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.

P-AuthPriv

This option represents authentication and the privacy protocol. Select this security level to encrypt messages using a privacy protocol and authenticate SNMP users. This level provides the greatest level of security. You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

The following prompt is displayed:

```
Do you want to delete this table entry? (Y/N):
[Yes/No]->
```

7. Enter **Y** to delete the view or **N** to save the view.

The following prompt is displayed:

8. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Modifying an SNMPv3 Access Table Entry

This section describes how to modify parameters in an SNMPv3 Access Table entry. For each entry in the SNMPv3 Access Table, you can modify the following parameters:

- Read View Name
- Write View Name
- Notify View Name
- Storage Type

Configure the values of the Read View Name, Write View Name, and Notify View Name parameters with values previously configured with the View Name parameter in the SNMPv3 View Table. This is the only way to associate a Group Name with these Views. See *Creating an SNMPv3 View Table Entry* on page 315.

See the following procedures:

- Modifying the Read View Name on page 331
- Modifying the Write View Name on page 334
- Modifying the Notify View Name on page 336
- Modifying the Storage Type on page 338

Modifying the Read View Name

To modify the Read View Name parameter in an SNMPv3 Access Table entry, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in *Creating an SNMPv3 User Table Entry* on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is shown in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **4** to select Configure SNMPv3 Access Table.

The Configure SNMPv3 Access Table is shown in Figure 106 on page 325.

3. From the Configure SNMPv3 Access Table, type **3** to select Modify SNMPv3 Table Entry.

The Modify SNMPv3 Access Table is shown in Figure 107.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142

User: Manager                                00:14:33 15-Jan-2004

Modify SNMPv3 Access Table

Group Name .... sales                        Security Model . v3
Context Prefix.                               Security Level . AuthNoPriv
Read View..... systemmanagers                Context Match .. Exact
Write View .... salespeople                   Storage Type ... Volatile
Notify View ... salespeople                   Row Status ..... Active

1 - Set Read View Name
2 - Set Write View Name
3 - Set Notify View Name
4 - Set Storage Type

U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 107 Modify SNMPv3 Access Table Menu

- To modify the Read View Name parameter, type **1** to select Set Read View Name.

The following prompt is displayed:

```
Enter Group Name:
```

- Enter a Group Name that was previously configured.

The following prompt is displayed:

```
Enter Security Model [1-v1, 2-v2c, 3-v3]:
```

- Enter the Security Model configured for this Group Name. You cannot change the value of the Security Model parameter.

Select one of the following SNMP protocols:

1-v1

Select this value to associate the Group Name with the SNMPv1 protocol.

2-v2c

Select this value to associate the Group Name with the SNMPv2c protocol.

3-v3

Select this value to associate the Group Name with the SNMPv3 protocol.

The following prompt is displayed:

```
Enter Security Level [N-NoAuthNoPriv, A-AuthNoPriv,
P-AuthPriv]:
```

7. Select one of the following security levels:

N-NoAuthNoPriv

This option represents no authentication and no privacy protocol. Select this security level if you do not want to authenticate SNMP users 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, N-NoAuthNoPriv is the only security level you can select.

A-AuthNoPriv

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.

P-AuthPriv

This option represents authentication and the privacy protocol. Select this security level to encrypt messages using a privacy protocol and authenticate SNMP users. This level provides the greatest level of security. You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

The following prompt is displayed:

```
Enter Read View Name:
```

8. Enter a value that you configured with the View Name parameter in the SNMPv3 View Table. See [Creating an SNMPv3 View Table Entry](#) on page 315.

A Read View Name allows the users assigned to this Security Group to view the information specified in the View Table. This value does not need to be unique.

9. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Modifying the Write View Name

To modify the Write View Name parameter in an SNMPv3 Access Table entry, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is shown in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **4** to select Configure SNMPv3 Access Table.

The Configure SNMPv3 Access Table is shown in Figure 106 on page 325.

3. From the Configure SNMPv3 Access Table, type **3** to select Modify SNMPv3 Table Entry.

The Modify SNMPv3 Table Menu is shown in Figure 107 on page 332.

4. To modify the Write View Name parameter, type **2** to select Set Write View Name.

The following prompt is displayed:

```
Enter Group Name:
```

5. Enter a Group Name that was previously configured.

The following prompt is displayed:

```
Enter Security Model[1-v1, 2-v2c, 3-v3]:
```

6. Enter the Security Model configured for this Group Name. You cannot change the value of the Security Model parameter.

Select one of the following SNMP protocols:

1-v1

Select this value to associate the Group Name with the SNMPv1 protocol.

2-v2c

Select this value to associate the Group Name with the SNMPv2c protocol.

3-v3

Select this value to associate the Group Name with the SNMPv3 protocol.

The following prompt is displayed:

```
Enter Security Level [N-NoAuthNoPriv, A-AuthNoPriv,
P-AuthPriv]:
```

7. Enter the Security Level configured for this Group Name. You cannot change the value of the Security Level parameter.

Select one of the following security levels:

N-NoAuthNoPriv

This option represents no authentication and no privacy protocol. Select this security level if you do not want to authenticate SNMP users 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, N-NoAuthNoPriv is the only security level you can select.

A-AuthNoPriv

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.

P-AuthPriv

This option represents authentication and the privacy protocol. Select this security level to encrypt messages using a privacy protocol and authenticate SNMP users. This level provides the greatest level of security. You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

The following prompt is displayed:

```
Enter Write View Name:
```

8. Enter a value that you configured with the View Name parameter in the SNMPv3 View Table.

A Write View Name allows the people assigned to this Security Group to write, or modify, to the information in the specified View Table. This value does not need to be unique.

9. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Modifying the Notify View Name

To modify the Notify View Name parameter in an SNMPv3 Access Table entry, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is shown in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **4** to select Configure SNMPv3 Access Table.

The Configure SNMPv3 Access Table is shown in Figure 106 on page 325.

3. From the Configure SNMPv3 Access Table, type **3** to select Modify SNMPv3 Table Entry.

The Modify SNMPv3 Table Menu is shown in Figure 107 on page 332.

4. To modify the Notify View Name parameter, type **3** to select Set Notify View Name.

The following prompt is displayed:

```
Enter Group Name:
```

5. Enter a Group Name that was previously configured.

The following prompt is displayed:

```
Enter Security Model[1-v1, 2-v2c, 3-v3]:
```

6. Enter the Security Model configured for this Group Name. You cannot change the value of the Security Model parameter.

Select one of the following SNMP protocols:

1-v1

Select this value to associate the Group Name with the SNMPv1 protocol.

2-v2c

Select this value to associate the Group Name with the SNMPv2c protocol.

3-v3

Select this value to associate the Group Name with the SNMPv3 protocol.

The following prompt is displayed:

```
Enter Security Level [N-NoAuthNoPriv, A-AuthNoPriv,
P-AuthPriv]:
```

7. Enter the Security Level configured for this Group Name. You cannot change the value of the Security Level parameter.

Select one of the following security levels:

N-NoAuthNoPriv

This option represents no authentication and no privacy protocol. Select this security level if you do not want to authenticate SNMP users 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, N-NoAuthNoPriv is the only security level you can select.

A-AuthNoPriv

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.

P-AuthPriv

This option represents authentication and the privacy protocol. Select this security level to encrypt messages using a privacy protocol and authenticate SNMP users. This level provides the greatest level of security. You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

The following prompt is displayed:

```
Enter Notify View Name:
```

8. Enter a value that you configured with the View Name parameter in the SNMPv3 View Table.

A Notify View Name permits the users assigned to this Security Group to send traps specified in this view of the MIB tree. This value does not need to be unique.

9. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Modifying the Storage Type

To modify the Storage Type parameter in an SNMPv3 Access Table entry, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is shown in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **4** to select Configure SNMPv3 Access Table.

The Configure SNMPv3 Access Table is shown in Figure 106 on page 325.

3. From the Configure SNMPv3 Access Table, type **3** to select Modify SNMPv3 Table Entry.

The Modify SNMPv3 Table Menu is shown in Figure 107 on page 332.

4. To modify the Storage Type parameter, type **4** to select Set Storage Type.

The following prompt is displayed:

```
Enter Group Name:
```

5. Enter a Group Name that was previously configured.

The following prompt is displayed:

```
Enter Security Model[1-v1, 2-v2c, 3-v3]:
```

6. Enter the Security Model configured for this Group Name. You cannot change the value of the Security Model parameter.

Select one of the following SNMP protocols:

1-v1

Select this value to associate the Group Name with the SNMPv1 protocol.

2-v2c

Select this value to associate the Group Name with the SNMPv2c protocol.

3-v3

Select this value to associate the Group Name with the SNMPv3 protocol.

The following prompt is displayed:

```
Enter Security Level [N-NoAuthNoPriv, A-AuthNoPriv, P-AuthPriv]:
```

7. Enter the Security Level configured for this Group Name. You cannot change the value of the Security Level parameter.

Select one of the following security levels:

N-NoAuthNoPriv

This option represents no authentication and no privacy protocol. Select this security level if you do not want to authenticate SNMP users 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, N-NoAuthNoPriv is the only security level you can select.

A-AuthNoPriv

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.

P-AuthPriv

This option represents authentication and the privacy protocol. Select this security level to encrypt messages using a privacy protocol and authenticate SNMP users. This level provides the greatest level of security. You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

The following prompt is displayed:

```
Enter Storage Type [V-Volatile, N-NonVolatile]:
```

8. Select one of the following storage types for this table entry:

V - Volatile

Select this storage type if you do not want the ability to save an entry in the SNMPv3 Access Table to the configuration file. After making changes to an SNMPv3 Access Table entry with a Volatile storage type, the **S** - Save Configuration Changes option does not appear on the Main Menu.

N-NonVolatile

Select this storage type if you want the ability to save an entry in the SNMPv3 Access Table to the configuration file. After making changes to an SNMPv3 Access Table entry with a NonVolatile storage type, the **S** - Save Configuration Changes option appears on the Main Menu, allowing you to save your changes.

9. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Configuring the SNMPv3 SecurityToGroup Table

This section contains a description of the SNMPv3 SecurityToGroup Table and how to create, delete, and modify table entries. The SNMPv3 SecurityToGroup Table allows you to associate a User Name with a Group Name. The User Name is configured in the Configure SNMPv3 User Table Menu while the Group Name is configured in the Configure SNMPv3 Access Table Menu. In addition, the configuration in the Configure SNMPv3 Access Table Menu defines which MIB views this User can read, write (modify), and send traps from. For each User Name, you can assign:

- A Security Model (SNMPv1, SNMPv2c, SNMPv3)
- A Group Name
- A Storage Type

There are three functions you can perform with the SNMPv3 Access Table.

- Creating an SNMPv3 SecurityToGroup Table Entry on page 340
- Deleting an SNMPv3 SecurityToGroup Table Entry on page 343
- Modifying an SNMPv3 SecurityToGroup Table Entry on page 344

Creating an SNMPv3 SecurityToGroup Table Entry

To create an entry in the SecurityToGroup Table, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is shown in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **5** to select Configure SNMPv3 SecurityToGroup Table.

The Configure SNMPv3 SecurityToGroup Table Menu is shown in Figure 108.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Marketing Switch 17

User: Manager                                00:14:33 15-Jan-2004

Configure SNMPv3 SecurityToGroup Table

Security Model..... v3
Security Name ..... spike
Group Name ..... marketing
Storage Type ..... NonVolatile
Row Status ..... Active

1 - Create SNMPv3 Table Entry
2 - Delete SNMPv3 Table Entry
3 - Modify SNMPv3 Table Entry

N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 108 Configure SNMPv3 SecurityToGroup Table Menu

3. To configure a group in the SNMPv3 SecurityToGroup Table, type **1** to select Create SNMPv3 Table Entry.

The following prompt is displayed:

```
Enter User (Security) Name:
```

4. Enter the User Name that you want to associate with a group.

Enter a User Name that you configured in Creating an SNMPv3 User Table Entry on page 305.

The following prompt is displayed:

```
Enter Security Model [1-v1, 2-v2c, 3-v3]:
```

5. Select the SNMP protocol that was configured for this User Name.

Choose from the following:

1-v1

Select this value to associate the Group Name with the SNMPv1 protocol.

2-v2c

Select this value to associate the Group Name with the SNMPv2c protocol.

3-v3

Select this value to associate the Group Name with the SNMPv3 protocol.

The following prompt is displayed:

```
Enter Group Name:
```

6. Enter a Group Name that you configured in the SNMPv3 Access Table. See. Creating an SNMPv3 Access Table Entry on page 324.

There are four default values for this field:

- defaultV1GroupReadOnly
- defaultV1GroupReadWrite
- defaultV2cGroupReadOnly
- defaultV2cGroupReadWrite

These values are reserved for SNMPv1 and SNMPv2c implementations.

The following prompt is displayed:

```
Enter Storage Type [V-Volatile, N-NonVolatile]:
```

7. Select one of the following storage types for this table entry:

V - Volatile

Select this storage type if you do not want the ability to save an entry in the SNMPv3 SecurityToGroup Table to the configuration file. After making changes to an SNMPv3 SecurityToGroup Table entry with a Volatile storage type, the **S** - Save Configuration Changes option does not appear on the Main Menu.

N-NonVolatile

Select this storage type if you want the ability to save an entry in the SNMPv3 SecurityToGroup Table to the configuration file. After making changes to an SNMPv3 SecurityToGroup Table entry with a NonVolatile storage type, the **S** - Save Configuration Changes option appears on the Main Menu, allowing you to save your changes.

Note

The Row Status parameter is a read-only field in the Telnet and Local interfaces. The Active value indicates the SNMPv3 SecurityToGroup Table entry will take effect immediately.

8. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Deleting an SNMPv3 SecurityToGroup Table Entry

You may want to delete an entry from the SNMPv3 SecurityToGroup Table. When you delete an SNMPv3 SecurityToGroup Table entry, there is no way to undelete, or recover, it.

To delete an entry in the SNMPv3 SecurityToGroup Table, perform the following procedure:

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is shown in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **5** to select Configure SNMPv3 SecurityToGroup Table.

The SNMPv3 SecurityToGroup Table is shown in Figure 108 on page 341.

Note

To display a Group Name and its associated parameters from the Configure SNMPv3 SecurityToGroup Table Menu, type **N** to display the Next Page and **P** to display the previous page.

3. From the SNMPv3 SecurityToGroup Table, type **2** to select Delete SNMPv3 Table Entry.

The following prompt is displayed:

```
Enter User (Security) Name:
```

4. Enter a User Name.

The following prompt is displayed:

```
Enter Security Model [1-v1, 2-v2c, 3-v3]:
```

5. Enter the Security Model of this User Name.

Choose from the following:

1-v1

Select this value to associate the Group Name with the SNMPv1 protocol.

2-v2c

Select this value to associate the Group Name with the SNMPv2c protocol.

3-v3

Select this value to associate the Group Name with the SNMPv3 protocol.

The following prompt is displayed:

```
Do you want to delete this table entry? (Y/N):
[Yes/No]->
```

6. Enter **Y** to delete this SecurityToGroup entry or **N** to save it.
7. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Modifying an SNMPv3 SecurityToGroup Table Entry

This section describes how to modify parameters in an SNMPv3 SecurityToGroup Table entry. See the following procedures:

- Modifying the Group Name on page 344
- Modifying the Storage Type on page 346

Modifying the Group Name

To modify the Group Name in an SNMPv3 SecurityToGroup Table entry, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is shown in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **5** to select Configure SNMPv3 SecurityToGroup Table.

The Configure SNMPv3 SecurityToGroup Table is shown in Figure 106 on page 325.

3. From the Configure SNMPv3 SecurityToGroup Table, type **3** to select Modify SNMPv3 Table Entry.

The Modify SecurityToGroup Table is displayed as shown Figure 108.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Marketing Switch 17

User: Manager                                00:14:33 15-Jan-2004

Modify SNMPv3 SecurityToGroup Table

Security Model..... v3
Security Name ..... cleo72
Group Name ..... engineering
Storage Type ..... Volatile
Row Status ..... Active

1 - Set Group Name
2 - Set Storage Type

N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 109 Modify SNMPv3 SecurityToGroup Table Menu

- To modify the Group Name, type **1** to select Set Group Name.

The following prompt is displayed:

```
Enter User (Security) Name:
```

- Enter a User Name.

The User Name must be previously configured in the Configure SNMPv3 User Table Menu. See Creating an SNMPv3 User Table Entry on page 305.

The following prompt is displayed:

```
Enter Security Model [1-v1, 2-v2c, 3-v3]:
```

- Enter the Security Model configured for this User Name. You cannot change the value of the Security Model parameter.

Select one of the following SNMP protocols:

1-v1

Select this value if this User Name is configured with the SNMPv1 protocol.

2-v2c

Select this value to associate the User Name with the SNMPv2c protocol.

3-v3

Select this value to associate the User Name with the SNMPv3 protocol.

The following prompt is displayed:

```
Enter Group Name:
```

7. Enter the new Group Name.

This value must match a value configured in the Group Name parameter in the Configure SNMPv3 Access Table. See Creating an SNMPv3 Access Table Entry on page 324.

8. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Modifying the Storage Type

To modify the Storage Type in an SNMPv3 SecurityToGroup Table entry, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is shown in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **5** to select Configure SNMPv3 SecurityToGroup Table.

The Configure SNMPv3 SecurityToGroup Table is shown in Figure 106 on page 325.

3. From the Configure SNMPv3 SecurityToGroup Table, type **3** to select Modify SNMPv3 Table Entry.
4. To modify the storage type, type **2** to select Set Storage Type.

The following prompt is displayed:

```
Enter User (Security) Name:
```

5. Enter a User Name.

The User Name must be previously configured in the Configure SNMPv3 User Table Menu. See Creating an SNMPv3 User Table Entry on page 305.

The following prompt is displayed:

```
Enter Security Model [1-v1, 2-v2c, 3-v3]:
```

6. Enter the Security Model configured for this User Name. You cannot change the value of the Security Model parameter.

Select one of the following SNMP protocols:

1-v1

Select this value if this User Name is configured with the SNMPv1 protocol.

2-v2c

Select this value if this User Name is configured with the SNMPv2c protocol.

3-v3

Select this value if this User Name is configured with the SNMPv3 protocol.

The following prompt is displayed:

```
Enter Storage Type [V-Volatile, N-NonVolatile]:
```

7. Select one of the following storage types for this table entry:

V - Volatile

Select this storage type if you do not want the ability to save an entry in the SNMPv3 SecurityToGroup Table to the configuration file. After making changes to an SNMPv3 SecurityToGroup Table entry with a Volatile storage type, the **S** - Save Configuration Changes option does not appear on the Main Menu.

N-NonVolatile

Select this storage type if you want the ability to save an entry in the SNMPv3 SecurityToGroup Table to the configuration file. After making changes to an SNMPv3 SecurityToGroup Table entry with a NonVolatile storage type, the **S** - Save Configuration Changes option appears on the Main Menu, allowing you to save your changes.

8. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Configuring the SNMPv3 Notify Table

This section contains a description of the SNMPv3 Notify Table Menu and how to create, delete, and modify table entries. The Configure SNMPv3 Notify Table Menu allows you to define a name for sending traps. In each Notify Table entry, you define if the switch sends a trap or an inform message. The two message types, trap and inform, have different packet formats.

For each Notify group, you can configure:

- Notify Name
- Notify Tag
- Notify Type
- Storage Type

The value of the Notify Tag is linked with the Tag List parameter in the Configure SNMPv3 Target Address Table Menu. After you configure a value for the Notify Tag parameter, you use the same value in the Target List parameter that is located on the Target Address Table Menu. As a result of this connection between the two tables, the Notify Tag parameter assigns a Target IP address to the Notify Table internally.

There are three functions you can perform with the Configure SNMPv3 Notify Table Menu.

- Creating an SNMPv3 Notify Table Entry on page 348
- Deleting an SNMPv3 Notify Table Entry on page 350
- Modifying an SNMPv3 Notify Table Entry on page 351

Creating an SNMPv3 Notify Table Entry

To create an entry in the SNMPv3 Notify Table Menu, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is displayed in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **6** to select Configure SNMPv3 Notify Table.

The Configure SNMPv3 Notify Table Menu is shown in Figure 110.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Marketing Switch 17

User: Manager                                00:14:33 15-Jan-2004

                Configure SNMPv3 Notify Table

Notify Name ..... hardwareengineeringTrap
Notify Tag ..... hardwareengineeringtag
Notify Type ..... Trap
Storage Type ..... NonVolatile
Row Status ..... Active

1 - Create SNMPv3 Table Entry
2 - Delete SNMPv3 Table Entry
3 - Modify SNMPv3 Table Entry

U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 110 Configure SNMPv3 Notify Table Menu

- To create an entry in the table, type **1** to select Create SNMPv3 Table Entry.

The following prompt is displayed:

```
Enter Notify Name:
```

- Enter the name associated with this trap message.

Enter a 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.

The following prompt is displayed:

```
Enter Notify Tag:
```

- Enter the name of the Notify Tag.

Enter a name of up to 32 alphanumeric characters. The following prompt is displayed:

```
Enter Notify Type [T-Trap, I-Inform]:
```

- Enter one of the following message types:

T-Trap

Indicates this notify table is used to send traps. With this message type, the switch does not expects a response from the authoritative entity.

I-Inform

Indicates this notify table is used to send inform messages. With this message type, the switch expects a response from the authoritative entity.

The following prompt is displayed:

```
Enter Storage Type [V-Volatile, N-NonVolatile]:
```

7. Select one of the following storage types for this table entry:

V - Volatile

Select this storage type if you do not want the ability to save an entry in the SNMPv3 Notify Table to the configuration file. After making changes to an SNMPv3 Notify Table entry with a Volatile storage type, the **S** - Save Configuration Changes option does not appear on the Main Menu.

N-NonVolatile

Select this storage type if you want the ability to save an entry in the SNMPv3 Notify Table to the configuration file. After making changes to an SNMPv3 Notify Table entry with a NonVolatile storage type, the **S** - Save Configuration Changes option appears on the Main Menu, allowing you to save your changes.

Note

The Row Status parameter is a read-only field in the Telnet and Local interfaces. The Active value indicates the SNMPv3 Notify Table entry takes effect immediately.

8. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Deleting an SNMPv3 Notify Table Entry

You may want to delete an entry from the Configure SNMPv3 Notify Table Menu. When you delete a Configure SNMPv3 Notify Table entry, there is no way to undelete, or recover, it.

To delete an entry in the Configure SNMPv3 Notify Table Menu, perform the following procedure:

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is shown in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **6** to select Configure SNMPv3 Notify Table.

The Configure SNMPv3 Notify Table Menu is shown in Figure 110 on page 349.

Note

To display a Group Name and its associated parameters from the Configure SNMPv3 SecurityToGroup Table Menu, type **N** to display the Next Page and **P** to display the previous page.

- To delete an SNMPv3 Notify Table entry, type **2** to select Delete SNMPv3 Table Entry.

The following prompt is displayed:

```
Enter Notify Name:
```

- Enter a Notify Name.

The following prompt is displayed:

```
Do you want to delete this table entry? (Y/N):
[Yes/No] ->
```

- Enter **Y** to delete the SNMPv3 Notify Table entry or **N** to save it.
- After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Modifying an SNMPv3 Notify Table Entry

This section describes how to modify parameters in an SNMPv3 Notify Table entry. See the following procedures:

- Modifying a Notify Tag on page 351
- Modifying a Notify Type on page 353
- Modifying a Storage Type on page 354

Modifying a Notify Tag

To modify the Notify Tag parameter in an SNMPv3 Notify Table entry, perform the following procedure.

- Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is shown in Figure 101 on page 306.

- From the Configure SNMPv3 Table Menu, type **6** to select Configure SNMPv3 Notify Table.

The Configure SNMPv3 Notify Table Menu is shown in Figure 110 on page 349.

- From the Configure SNMPv3 Notify Table Menu, type **3** to select Modify SNMPv3 Table Entry.

The Modify SNMPv3 Notify Table Menu is displayed as shown in Figure 111.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Marketing Switch 17

User: Manager                                00:14:33 15-Jan-2004

                Modify SNMPv3 Notify Table

Notify Name ..... softwareengineering
Notify Tag..... softwareengineeringtag
Notify Type..... Inform
Storage Type ..... NonVolatile
Row Status ..... Active

1 - Set Notify Tag
2 - Set Notify Type
3 - Set Storage Type

N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection?
```

Figure 111 Modify SNMPv3 Notify Table Menu

Note

To display a Group Name and its associated parameters from the Configure SNMPv3 SecurityToGroup Table Menu, type **N** to display the Next Page and **P** to display the previous page.

4. To modify the Notify Tag, type **1** to select Set Notify Tag.
The following prompt is displayed:
Enter Notify Name:
5. Enter a Notify Name.
The following prompt is displayed:
Enter Notify Tag:
6. Enter the new Notify Tag.
Enter an alphanumeric value of up to 32 characters.
7. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Modifying a Notify Type

To modify the Notify Type parameter in an SNMPv3 Notify Table entry, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is shown in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **6** to select Configure SNMPv3 Notify Table.

The Configure SNMPv3 Notify Table Menu is shown in Figure 110 on page 349.

3. From the Configure SNMPv3 Notify Table Menu, type **3** to select Modify SNMPv3 Table Entry.

The Modify SNMPv3 Notify Table is shown in Figure 111 on page 352.

4. To modify the Notify Type, type **2** to select Set Notify Type.

The following prompt is displayed:

```
Enter Notify Name:
```

5. Enter a Notify Name.

The following prompt is displayed:

```
Enter Notify Type [T-Trap, I-Inform]:
```

6. Enter one of the following message types:

T-Trap

Indicates this notify table is used to send traps. With this message type, the switch does not expect a response from the host.

I-Inform

Indicates this notify table is used to send inform messages. With this message type, the switch expects a response from the host.

7. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Modifying a Storage Type

To modify the Storage Type parameter in an SNMPv3 Notify Table entry, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is shown in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **6** to select Configure SNMPv3 Notify Table.

The Configure SNMPv3 Notify Table Menu is shown in Figure 110 on page 349.

3. From the Configure SNMPv3 Notify Table Menu, type **3** to select Modify SNMPv3 Table Entry.

The Modify SNMPv3 Notify Table is shown in Figure 111 on page 352.

4. To modify the Storage Type, type **3** to select Set Storage Type.

The following prompt is displayed:

```
Enter Notify Name:
```

5. Enter a Notify Name.

The following prompt is displayed:

```
Enter Storage type [V-Volatile, N-NonVolatile]:
```

6. Select one of the following storage types for this table entry:

V - Volatile

Select this storage type if you do not want the ability to save an entry in the SNMPv3 Notify Table to the configuration file. After making changes to an SNMPv3 Notify Table entry with a Volatile storage type, the **S** - Save Configuration Changes option does not appear on the Main Menu.

N-NonVolatile

Select this storage type if you want the ability to save an entry in the SNMPv3 Notify Table to the configuration file. After making changes to an SNMPv3 Notify Table entry with a NonVolatile storage type, the **S** - Save Configuration Changes option appears on the Main Menu, allowing you to save your changes.

7. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Configuring the SNMPv3 Target Address Table

This section contains a description of the SNMPv3 Target Address Table Menu and how to create, delete, and modify table entries. You use the SNMPv3 Target Address Table Menu to assign the IP address of a host that is used for generating notifications. The Configure SNMPv3 Target Address Table Menu is linked internally to the Configure SNMPv3 Notify Table through the Tag List parameter. The Configure SNMPv3 Notify Table Menu receives the host IP address through the configuration of the SNMPv3 Target Address Table Menu.

For each Target Address Table entry, you can configure the following parameters:

- Target Address Name
- Target IP Address
- UDP Port
- Timeout Value
- Number of Retries
- Tag List
- Target Parameters
- Storage Type

You must configure the Tag List parameter with values previously configured in the Notify Tag parameter. The Notify Tag parameter is located on the Notify Table Menu. See [Creating an SNMPv3 Notify Table Entry](#) on page 348.

There are three functions you can perform with the Configure SNMPv3 Target Address Table Menu.

- [Creating an SNMPv3 Target Address Table Entry](#) on page 356
- [Deleting an SNMPv3 Target Address Table Entry](#) on page 358
- [Modifying an SNMPv3 Target Address Table Entry](#) on page 359

Creating an SNMPv3 Target Address Table Entry

To create an entry in the Configure SNMPv3 Target Address Table Menu, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is shown in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **7** to select Configure SNMPv3 Target Address Table.

The Configure SNMPv3 Target Address Table Menu is shown in Figure 112.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Marketing Switch 17

User: Manager                                00:14:33 15-Jan-2004

Configure SNMPv3 Target Address Table

Target Addr Name ... host451                 Timeout ..... 1500
Target Parameters .. SNMPmanagerPC          Retries ..... 3
IP Address ..... 198.35.11.1                UDP Port# ... 162
Storage Type ..... NonVolatile              Row Status .. Active
Tag List ..... hwengTrap hwengInform swengTrap swengInform

1 - Create SNMPv3 Table Entry
2 - Delete SNMPv3 Table Entry
3 - Modify SNMPv3 Table Entry

U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 112 Configure SNMPv3 Target Address Table Menu

3. To create an entry in the SNMPv3 Target Address Table, type **1** to select Create SNMPv3 Table Entry.

The following prompt is displayed:

```
Enter Target Address Name:
```

4. 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.

The following prompt is displayed:

```
Enter IP Address:
```

5. Enter the IP address of the host.

Use the following format for an IP address:
XXX.XXX.XXX.XXX

The following prompt is displayed:

```
Enter UDP Port#: [0 to 65535]-> 162
```

6. Enter a UDP port.

You can enter a UDP port in the range of 0 to 65,535. The default UDP port is 162.

The following prompt is displayed:

```
Enter Timeout (10mS): [0 to 2147483647]-> 1500
```

7. 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.

The following prompt is displayed:

```
Enter Retries:[0 to 255]-> 3
```

8. Enter the number of times the switch will retry, or resend, 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.

The following prompt is displayed:

```
Enter Tag List:
```

9. Enter a Tag List.

This list consists of a tag or list of tags you configured in a Configure SNMPv3 Notify Table entry with the Notify Tag parameter. See Creating an SNMPv3 Notify Table Entry on page 348. Enter a Tag List of up to 256 alphanumeric characters. Use a space to separate entries, for example:

```
hwengtag swengtag testengtag
```

The following prompt is displayed:

```
Enter Target Parameters:
```

10. 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 Configure SNMPv3 Target Parameters Table.

The following prompt is displayed:

```
Enter Storage Type [V-Volatile, N-NonVolatile]:
```

11. Select one of the following storage types for this table entry:

V - Volatile

Select this storage type if you do not want the ability to save an entry in the SNMPv3 Target Address Table to the configuration file. After making changes to an SNMPv3 Target Address Table entry with a Volatile storage type, the **S** - Save Configuration Changes option does not appear on the Main Menu.

N-NonVolatile

Select this storage type if you want the ability to save an entry in the SNMPv3 Target Address Table to the configuration file. After making changes to an SNMPv3 Target Address entry with a NonVolatile storage type, the **S** - Save Configuration Changes option appears on the Main Menu, allowing you to save your changes.

Note

The Row Status parameter is a read-only field in the Telnet and Local interfaces. The Active value indicates the SNMPv3 Target Address Table entry will take effect immediately.

12. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Deleting an SNMPv3 Target Address Table Entry

You may want to delete an entry from the SNMPv3 Target Address Table. After you delete an SNMPv3 Target Address Table entry, there is no way to undelete, or recover, it.

To delete an entry in the SNMPv3 Target Address Table, perform the following procedure:

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is shown in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **7** to select Configure SNMPv3 Target Address Table.

The Configure SNMPv3 Target Address Table Menu is shown in Figure 114 on page 369.

Note

To display a Group Name and its associated parameters from the Configure SNMPv3 SecurityToGroup Table Menu, type **N** to display the Next Page and **P** to display the previous page.

3. To delete an SNMPv3 Target Address Table entry, type **2** to select Delete SNMPv3 Table Entry.

The following prompt is displayed:

```
Enter Target Address Name:
```

4. Enter a Target Address Name.

The following prompt is displayed:

```
Do you want to delete this table entry? (Y/N):
[Yes/No] ->
```

5. Enter **Y** to delete the SNMPv3 Target Address Table entry or **N** to save it.
6. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Modifying an SNMPv3 Target Address Table Entry

This section describes how to modify parameters in an SNMPv3 Target Address Table entry. See the following procedures:

- Modifying the Target IP Address on page 360
- Modifying the Target Address UDP Port on page 361
- Modifying the Target Address Timeout on page 362
- Modifying the Target Address Retries on page 363
- Modifying the Target Address Tag List on page 364
- Modifying the Target Parameters Field on page 365
- Modifying the Storage Type on page 366

Note

You cannot modify the Target Address Name parameter.

Modifying the Target IP Address

To modify the target IP address in an SNMPv3 Target Address Table entry, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is shown in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **7** to select Configure SNMPv3 Target Address Table.

The Configure SNMPv3 Target Address Table Menu is shown in Figure 112 on page 356.

3. From the Configure SNMPv3 Target Address Table Menu, type **3** to select Modify SNMPv3 Table Entry.

The Modify SNMPv3 Target Address Table Menu is shown in Figure 113.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 98

User: Manager                                00:14:33 15-Jan-2004

          Modify SNMPv3 Target Address Table

Target Addr Name ... host451                 Timeout ..... 1500
Target Parameters .. SNMPmanagerPC          Retries ..... 3
IP Address ..... 198.35.11.1                UDP Port# ... 162
Storage Type ..... NonVolatile              Row Status .. Active
Tag List ..... hwengTrap hwengInform swengTrap swengInform

1 - Set Target IP Address
2 - Set Target Address UDP Port
3 - Set Target Address Timeout
4 - Set Target Address Retries
5 - Set Target Address TagList
6 - Set Target Parameters
7 - Set Storage Type

U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 113 Modify SNMPv3 Target Address Table Menu

- To change the Target IP Address, type **1** to select Set Target IP Address.

The following prompt is displayed:

```
Enter Target Address Name:
```

- Enter a previously configured Target Address Name.

This is 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.

The following prompt is displayed:

```
Enter IP Address:
```

- Enter the IP address of the host.

Use the following format for an IP address:

```
XXX.XXX.XXX.XXX
```

- After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Modifying the Target Address UDP Port

To modify the Target Address UDP Port parameter in an SNMPv3 Target Address Table entry, perform the following procedure:

- Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is shown in Figure 101 on page 306.

- From the Configure SNMPv3 Table Menu, type **7** to select Configure SNMPv3 Target Address Table.

The Configure SNMPv3 Target Address Table Menu is shown in Figure 112 on page 356.

- From the Configure SNMPv3 Target Address Table Menu, type **3** to select Modify SNMPv3 Table Entry.

The Modify SNMPv3 Target Address Table Menu is shown in Figure 113 on page 360.

- To change the Target Address UDP Port, type **2** to select Set Target Address UDP Port.

The following prompt is displayed:

```
Enter Target Address Name:
```

- Enter a previously configured Target Address Name.

This is 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.

The following prompt is displayed:

```
Enter UDP Port#: [0 to 65535]-> 162
```

6. Enter a UDP port.

You can enter a UDP port in the range of 0 to 65,535. The default UDP port is 162.

7. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Modifying the Target Address Timeout

The Target Address Timeout parameter only applies when the message type is an Inform message. To modify the Target Address Timeout parameter in an SNMPv3 Target Address Table entry, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is shown in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **7** to select Configure SNMPv3 Target Address Table.

The Configure SNMPv3 Target Address Table Menu is shown in Figure 112 on page 356.

3. From the Configure SNMPv3 Target Address Table Menu, type **3** to select Modify SNMPv3 Table Entry.

The Modify SNMPv3 Target Address Table Menu is shown in Figure 113 on page 360.

4. To modify the Target Address Timeout, type **3** to select Set Target Address Timeout.

The following prompt is displayed:

```
Enter Target Address Name:
```

5. Enter a previously configured Target Address Name.

This is 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.

The following prompt is displayed:

```
Enter Timeout (10mS): [0 to 2147483647]-> 1500
```

6. 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.

7. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Modifying the Target Address Retries

The Target Address Retries parameter only applies when the message type is an Inform message. To modify the Target Address Retries parameter in an SNMPv3 Target Address Table entry, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is shown in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **7** to select Configure SNMPv3 Target Address Table.

The Configure SNMPv3 Target Address Table Menu is shown in Figure 112 on page 356.

3. From the Configure SNMPv3 Target Address Table Menu, type **3** to select Modify SNMPv3 Table Entry.

The Modify SNMPv3 Target Address Table Menu is shown in Figure 113 on page 360.

4. To modify the Target Address Retries, type **4** to select Set Target Address Retries.

The following prompt is displayed:

```
Enter Target Address Name:
```

5. Enter a previously configured Target Address Name.

This is 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.

The following prompt is displayed:

```
Enter Retries:[0 to 255]-> 3
```

6. Enter the number of times the switch will retry, or resend, the Inform message.

The range is 0 to 255 retries. The default is 3 retries.

7. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Modifying the Target Address Tag List

To modify the Target Address Tag List parameter in an SNMPv3 Target Address Table entry, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is shown in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **7** to select Configure SNMPv3 Target Address Table.

The Configure SNMPv3 Target Address Table Menu is shown in Figure 112 on page 356.

3. From the Configure SNMPv3 Target Address Table Menu, type **3** to select Modify SNMPv3 Table Entry.

The Modify SNMPv3 Target Address Table Menu is shown in Figure 113 on page 360.

4. To modify the Target Address Tag List, type **5** to select Set Target Address TagList.

The following prompt is displayed:

```
Enter Target Address Name:
```

5. Enter a previously configured Target Address Name.

This is 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.

The following prompt is displayed:

```
Enter Tag List:
```

Enter a Tag List of up to 256 alphanumeric characters. Use a space to separate entries. This list consists of a tag or list of tags you configured in a Configure SNMPv3 Notify Table entry with the Notify Tag parameter. See Creating an SNMPv3 Notify Table Entry on page 348.

6. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Modifying the Target Parameters Field

To modify the Target Parameters field in an SNMPv3 Target Address Table entry, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is shown in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **7** to select Configure SNMPv3 Target Address Table.

The Configure SNMPv3 Target Address Table Menu is shown in Figure 112 on page 356.

3. From the Configure SNMPv3 Target Address Table Menu, type **3** to select Modify SNMPv3 Table Entry.

The Modify SNMPv3 Target Address Table Menu is shown in Figure 113 on page 360.

4. To modify the Target Parameters field, type **6** to select Set Target Parameters.

The following prompt is displayed:

```
Enter Target Address Name:
```

5. Enter a previously configured Target Address Name.

This is 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.

The following prompt is displayed:

```
Enter Target Parameters:
```

6. Enter a Target Parameters Name.

The value configured here must match the value configured with the Target Parameters Name parameter in the Configure SNMPv3 Target Parameters Table. This name can consist of up to 32-alphanumeric characters.

7. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Modifying the Storage Type

To modify the Storage Type parameter in an SNMPv3 Target Address Table entry, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is shown in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **7** to select Configure SNMPv3 Target Address Table.

The Configure SNMPv3 Target Address Table Menu is shown in Figure 112 on page 356.

3. From the Configure SNMPv3 Target Address Table Menu, type **3** to select Modify SNMPv3 Table Entry.

The Modify SNMPv3 Target Address Table Menu is shown in Figure 113 on page 360.

4. To modify the Storage Type, type **7** to select Set Storage Type.

The following prompt is displayed:

```
Enter Target Address Name:
```

5. Enter a previously configured Target Address Name.

This is 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.

The following prompt is displayed:

```
Enter Storage Type [V-Volatile, N-NonVolatile]:
```

6. Select one of the following storage types for this table entry:

V - Volatile

Select this storage type if you do not want the ability to save an entry in the SNMPv3 Target Address Table to the configuration file. After making changes to an SNMPv3 Target Address Table entry with a Volatile storage type, the **S** - Save Configuration Changes option does not appear on the Main Menu.

N-NonVolatile

Select this storage type if you want the ability to save an entry in the SNMPv3 Target Address Table to the configuration file. After making changes to an SNMPv3 Target Address entry with a NonVolatile storage type, the **S** - Save Configuration Changes option appears on the Main Menu, allowing you to save your changes.

7. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Configuring the SNMPv3 Target Parameters Table

This section contains a description of the SNMPv3 Target Parameters Table and how to create, delete, and modify table entries. The SNMPv3 Target Parameters Table links the user security information with the message notification information configured in the Configure SNMPv3 Notify Table Menu and Configure SNMPv3 Target Address Table Menu.

In the SNMPv3 Target Parameters Table, you specify the SNMP parameters that are used when a message is generated to a target, or host, IP address. The SNMPv3 Target Parameters Table also links a User Name and its related security information, called *user security information*, with a host. The user security information consists of the following parameters listed in the SNMPv3 tables where they are configured:

- User Name parameter configured in the SNMPv3 User Table Menu
- View Name parameter configured in the SNMPv3 View Table Menu
- Group Name, Security Model, and Security Level parameters configured in the SNMPv3 Access Table
- User Name, Security Model, and Group Name configured in the SNMPv3 SecurityToGroup Table

When you enter user security information in an SNMPv3 Target Parameters Table entry, it must match the configuration in the SNMPv3 tables listed above. If the user security information in the SNMPv3 Target Parameters Table entry does not match the configuration in the tables listed above, messages are not sent on behalf of the user.

Note

In the SNMPv3 Target Parameters Table, the Security Name parameter is the equivalent to the User Name parameter in the SNMPv3 User Table.

For each Target Address Table entry, you can configure:

- Target Parameters Name
- Security Name (User Name)
- Security Model
- Security Level
- Storage Type

There are three functions you can perform with the Configure SNMPv3 Target Parameters Table Menu.

- Creating an SNMPv3 Target Parameters Table Entry on page 369
- Deleting an SNMPv3 Target Parameters Table Entry on page 372
- Modifying an SNMPv3 Target Parameters Table Entry on page 373

Creating an SNMPv3 Target Parameters Table Entry

To create an entry in the Configure SNMPv3 Target Parameters Table, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is displayed in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **8** to select Configure SNMPv3 Target Parameters Table Menu.

The Configure SNMPv3 Target Parameters Table Menu is shown in Figure 114.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Marketing Switch 17

User: Manager                                00:14:33 15-Jan-2004

Configure SNMPv3 Target Parameters Table

Target Parameters Name ... host125parm
Message Processing Model . v3
Security Model..... v3
Security Name ..... murthy
Security Level ..... AuthPriv
Storage Type ..... NonVolatile
Row Status ..... Active

1 - Create SNMPv3 Table Entry
2 - Delete SNMPv3 Table Entry
3 - Modify SNMPv3 Table Entry

U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 114 Configure SNMPv3 Target Parameters Table Menu

3. To create an SNMPv3 Target Parameters Table, type **1** to select Create SNMPv3 Table Entry.

The following prompt is displayed:

```
Enter Target Parameters Name:
```

4. Enter a name of the Target Parameters.

Enter a value of up to 32-alphanumeric characters.

Note

You are prompted to 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.

The following prompt is displayed:

```
Enter User (Security) Name:
```

5. Enter a User Name.

The value of this parameter is previously configured with the Configure SNMPv3 User Table. See Creating an SNMPv3 User Table Entry on page 305.

The following prompt is displayed:

```
Enter Security Model [1-v1, 2-v2c, 3-v3]:
```

6. Select one of the following SNMP protocols as the Security Model for this Security Name, or User Name.

1-v1

Select this value to associate the Security Name, or User Name, with the SNMPv1 protocol.

2-v2c

Select this value to associate the Security Name, or User Name, with the SNMPv2c protocol.

3-v3

Select this value to associate the Security Name, or User Name, with the SNMPv3 protocol. The SNMPv3 protocol allows you to configure the group to authenticate SNMPv3 users and to encrypt messages.

The following prompt is displayed:

```
Enter Security Level [N-NoAuthNoPriv, A-AuthNoPriv, P-AuthPriv]:
```

7. 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 Configure SNMPv3 User Table Menu. See Creating an SNMPv3 User Table Entry on page 305.

N-NoAuthNoPriv

This option represents no authentication and no privacy protocol. Select this security level if you do not want to authenticate SNMP users 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, N-NoAuthNoPriv is the only security level you can select.

A-AuthNoPriv

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.

P-AuthPriv

This option represents authentication and the privacy protocol. Select this security level to encrypt messages using a privacy protocol and authenticate SNMP users. This level provides the greatest level of security. You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

The following prompt is displayed:

```
Enter Storage Type [V-Volatile, N-NonVolatile]:
```

8. Select one of the following storage types for this table entry:

V - Volatile

Select this storage type if you do not want the ability to save an entry in the SNMPv3 Target Parameters Table to the configuration file. After making changes to an SNMPv3 Target Parameters Table entry with a Volatile storage type, the **S** - Save Configuration Changes option does not appear on the Main Menu.

N-NonVolatile

Select this storage type if you want the ability to save an entry in the SNMPv3 Target Parameters Table to the configuration file. After making changes to an SNMPv3 Target Parameters Table

entry with a NonVolatile storage type, the **S** - Save Configuration Changes option appears on the Main Menu, allowing you to save your changes.

Note

The Row Status parameter is a read-only field in the Telnet and Local interfaces. The Active value indicates the SNMPv3 Target Parameters Table entry will take effect immediately.

9. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Deleting an SNMPv3 Target Parameters Table Entry

You may want to delete an entry from the SNMPv3 Target Parameters Table. When you delete an SNMPv3 Target Parameters Table entry, there is no way to undelete, or recover, it.

To delete an entry in the SNMPv3 Target Parameters Table, perform the following procedure:

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is shown in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **8** to select Configure SNMPv3 Target Parameters Table.

The Configure SNMPv3 Parameters Table Menu is shown in Figure 114 on page 369.

Note

To display a Group Name and its associated parameters from the Configure SNMPv3 SecurityToGroup Table Menu, type **N** to display the Next Page and **P** to display the previous page.

3. To delete an SNMPv3 Target Parameters Table entry, type **2** to select Delete SNMPv3 Table Entry.

The following prompt is displayed:

```
Enter Target Parameters Name:
```

4. Enter a Target Parameters Name.

The following prompt is displayed:

```
Do you want to delete this table entry? (Y/N):
[Yes/No]->
```

5. Enter **Y** to delete the SNMPv3 Target Address Table entry or **N** to save it.
6. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Modifying an SNMPv3 Target Parameters Table Entry

This section provides procedures for modifying parameters in an SNMPv3 Target Parameters Table entry. The parameter values configured in the Target Parameters Table must match those configured in the other tables. For a more detailed explanation, see *Creating an SNMPv3 Target Parameters Table Entry* on page 369.

In an SNMPv3 Target Parameters Table entry, the Security Name parameter is linked to the User Name parameter on the SNMPv3 User Table. In an SNMPv3 User Table entry, the User Name parameter is used as an index for the entry. Because the User Name and Security Name parameters are linked, the information you configure that relates to a User Table entry must match the information you configure in the SNMPv3 Target Parameters Table entry. In addition, the values configured for the following parameters in an SNMPv3 Target Parameters Table entry must match those configured in the corresponding table entry:

- User Name parameter in the SNMPv3 User Table
- View Name parameter in the SNMPv3 View Table
- Group Name, Security Model, and Security Level parameters in the SNMPv3 Access Table
- User Name, Security Model, Group Name parameters in the SNMPv3 SecurityToGroup Table

See the following procedures:

- Modifying the Security Name (User Name)* on page 374
- Modifying the Security Model* on page 376
- Modifying the Security Level* on page 377
- Modifying the Message Process Model* on page 378
- Modifying the Storage Type* on page 380

Note

You cannot modify the Target Params Name parameter.

Note

You cannot modify an entry in the SNMPv3 Target Parameter Table that contains a value of “default” in the Target Parameters Name field.

Modifying the Security Name (User Name)

In the AT-S60 implementation of the SNMPv3 protocol, the Security Name and the User Name parameters are equivalent. In the SNMPv3 Target Parameters Table Menu, the Security Name and the User Name parameters are used interchangeably.

When you modify the Security Name parameter, you must use a value that you configured with the User Name parameter in the Configure SNMPv3 User Table Menu. If you do not use a value configured with the User Name parameter, messages are not sent on behalf of this User Name. See Creating an SNMPv3 User Table Entry on page 305.

To modify the Security Name parameter in an SNMPv3 Target Parameter Table entry, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is shown in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **8** to select Configure SNMPv3 Target Address Table.

The Configure SNMPv3 Target Parameters Table Menu is shown in Figure 114 on page 369.

3. From the Configure SNMPv3 Target Parameters Table Menu, type **3** to select Modify SNMPv3 Table Entry.

The Modify SNMPv3 Target Parameters Table Menu is shown in Figure 115.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Marketing Switch 17

User: Manager                                00:14:33 15-Jan-2004

          Modify SNMPv3 Target Parameters Table

Target Parameters Name ... host27
Message Processing Model . v3
Security Model..... v3
Security Name ..... hoa
Security Level ..... AuthNoPriv
Storage Type ..... NonVolatile
Row Status ..... Active

1 - Set Security Name
2 - Set Security Model
3 - Set Security Level
4 - Set Message Processing Model
5 - Set Storage Type

U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 115 Modify SNMPv3 Target Parameters Table Menu

4. To change the Security Name parameter, type **1** to select Set Security Name.

The following prompt is displayed:

```
Enter Target Parameters Name:
```

5. Enter a previously configured Target Parameters Name.

Enter a value of up to 32-alphanumeric characters.

The following prompt is displayed:

```
Enter User (Security) Name:
```

6. Enter a User Name.

Enter a value that you previously configured with the Configure SNMPv3 User Table Menu. You can enter a value of up to 32-alphanumeric characters.

7. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Modifying the Security Model

For the Security or User Name you have selected, the value of the Security Model parameter in an SNMPv3 Target Parameter Table entry must match the value of the Security Model parameter in the SNMPv3 Access Table entry.



Caution

If the values of the Security Model parameter in the SNMPv3 User Table and the SNMPv3 Target Parameter Table entry do not match, notification messages are not generated on behalf of this User (Security) Name.

To modify the Security Model parameter in an SNMPv3 Target Parameter Table entry, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is shown in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **8** to select Configure SNMPv3 Target Address Table.

The Configure SNMPv3 Target Parameters Table Menu is shown in Figure 114.

3. From the Configure SNMPv3 Target Parameters Table Menu, type **3** to select Modify SNMPv3 Table Entry.

The Modify SNMPv3 Target Parameters Table Menu is shown in Figure 115 on page 375.

4. To change the Security Model, type **2** to select Security Model.

The following prompt is displayed:

```
Enter Target Parameters Name:
```

5. Enter a previously configured Target Parameters Name.

Enter a value of up to 32-alphanumeric characters.

The following prompt is displayed:

```
Enter Security Model [1-v1, 2-v2c, 3-v3]:
```

6. Select one of the following SNMP protocols that was previously configured as the Security Model for this Security Name, or User Name.

1-v1

Select this value if this User Name is associated with the SNMPv1 protocol.

2-v2c

Select this value if this User Name is associated with the SNMPv2c protocol.

3-v3

Select this value if this User Name is associated with the SNMPv3 protocol.

7. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Modifying the Security Level

For the Security or User Name you have selected, the value of the Security Level parameter in an SNMPv3 Target Parameter Table entry must match the value of the Security Level parameter in the SNMPv3 User Table entry.

To modify the Security Level parameter in an SNMPv3 Target Parameter Table entry, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is shown in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **8** to select Configure SNMPv3 Target Address Table.

The Configure SNMPv3 Target Parameters Table Menu is shown in Figure 114.

3. From the Configure SNMPv3 Target Parameters Table Menu, type **3** to select Modify SNMPv3 Table Entry.

The Modify SNMPv3 Target Parameters Table Menu is shown in Figure 115 on page 375.

4. To modify the Security Level, type **3** to select Set Security Level.

The following prompt is displayed:

```
Enter Target Parameters Name:
```

5. Enter a previously configured Target Parameters Name.

Enter a value of up to 32-alphanumeric characters.

The following prompt is displayed:

```
Enter Security Level [N-NoAuthNoPriv, A-AuthNoPriv, P-AuthPriv]:
```

6. Enter the Security Level.

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 Configure SNMPv3 User Table Menu. See Creating an SNMPv3 User Table Entry on page 305.

N-NoAuthNoPriv

This option represents no authentication and no privacy protocol. Select this security level if you do not want to authenticate SNMP users 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, N-NoAuthNoPriv is the only security level you can select.

A-AuthNoPriv

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.

P-AuthPriv

This option represents authentication and the privacy protocol. Select this security level to encrypt messages using a privacy protocol and authenticate SNMP users. This level provides the greatest level of security. You can select this value if you configured the Security Model parameter with the SNMPv3 protocol.

7. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Modifying the Message Process Model

You can modify the Message Process Model for SNMPv1 and SNMPv2c protocol configurations only. When you configure the SNMPv3 protocol, the Message Process Model is automatically assigned to the SNMPv3 protocol.

To modify the Message Process Model parameter in an SNMPv3 Target Parameter Table entry, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is shown in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **8** to select Configure SNMPv3 Target Address Table.

The Configure SNMPv3 Target Parameters Table Menu is shown in Figure 114.

3. From the Configure SNMPv3 Target Parameters Table Menu, type **3** to select Modify SNMPv3 Table Entry.

The Modify SNMPv3 Target Parameters Table Menu is shown in Figure 115 on page 375.

4. To modify the Message Process Model, type **4** to select Set Message Processing Model.

The following prompt is displayed:

```
Enter Target Parameters Name:
```

5. Enter a previously configured Target Parameters Name.

Enter a value of up to 32-alphanumeric characters.

The following prompt is displayed:

```
Enter Message Processing Model[1-v1,2-v2c,3-v3]:
```

6. Select one of the following SNMP protocols that is used to process, or send messages:

1-v1

Select this value to process messages with the SNMPv1 protocol.

2-v2c

Select this value to process messages with the Security Name, or User Name, with the SNMPv2c protocol.

3-v3

Select this value to process messages with the SNMPv3 protocol.

7. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Modifying the Storage Type

To modify the Storage Type parameter in an SNMPv3 Target Parameter Table entry, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is shown in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **8** to select Configure SNMPv3 Target Address Table.

The Configure SNMPv3 Target Parameters Table Menu is shown in Figure 114.

3. From the Configure SNMPv3 Target Parameters Table Menu, type **3** to select Modify SNMPv3 Table Entry.

The Modify SNMPv3 Target Parameters Table Menu is shown in Figure 115 on page 375.

4. To modify the Storage Type, type **5** to select Storage Type.

The following prompt is displayed:

```
Enter Target Parameters Name:
```

5. Enter a previously configured Target Parameters Name.

Enter a value of up to 32-alphanumeric characters.

The following prompt is displayed:

```
Enter Storage Type [V-Volatile, N-NonVolatile]:
```

6. Select one of the following storage types for this table entry:

V - Volatile

Select this storage type if you do not want the ability to save an entry in the SNMPv3 Target Parameters Table to the configuration file. After making changes to an SNMPv3 Target Parameters Table entry with a Volatile storage type, the **S** - Save Configuration Changes option does not appear on the Main Menu.

N-NonVolatile

Select this storage type if you want the ability to save an entry in the SNMPv3 Target Parameters Table to the configuration file. After making changes to an SNMPv3 Target Parameters Table entry with a NonVolatile storage type, the **S** - Save Configuration Changes option appears on the Main Menu, allowing you to save your changes.

7. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Configuring the SNMPv3 Community Table

This section contains a description of the SNMPv3 Community Table and how to create, delete, and modify table entries. The SNMPv3 Community Table allows you to create SNMPv1 and SNMPv2c Communities using the SNMPv3 Tables.

Allied Telesyn does not recommend that you use the menu described in this section to configure SNMPv1 and SNMPv2c communities. Instead, use the procedures described in *Configuring the SNMPv1 and SNMPv2c Protocols* on page 86.

However, if you want to configure SNMPv1 and SNMPv2c with the SNMPv3 Tables you need to start your configuration with the SNMPv3 Community Table and then create entries in the following tables:

- SNMPv3 View Table—See *Creating an SNMPv3 View Table Entry* on page 315.
- SNMPv3 Access Table—See *Creating an SNMPv3 Access Table Entry* on page 324.
- SNMPv3 SecurityToGroup Table—See *Creating an SNMPv3 SecurityToGroup Table Entry* on page 340.
- SNMPv3 Notify Table—See *Configuring the SNMPv3 Notify Table* on page 348.
- SNMPv3 Target Address Table—See *Creating an SNMPv3 Target Address Table Entry* on page 356.
- SNMPv3 Target Parameters Table—See *Creating an SNMPv3 Target Parameters Table Entry* on page 369.

It is important to note that you do not create an entry in the SNMPv3 User Table when you are configuring SNMPv1 and SNMPv2c with the SNMPv3 Tables. When you configure the SNMPv3 protocol, the various tables are linked with the User Name parameter and its related information. With the SNMPv1 and SNMPv2c configuration, the Security Name parameter and its related information (configured in the SNMPv3 Community Table Menu) links an SNMPv3 Community Table entry to the other SNMPv3 Table entries.

Note

In the SNMPv3 Community Table entry, the Security Name parameter is not related to the User Name parameter.

For each SNMPv3 Community Table entry, you can configure the following parameters:

- Community Index
- Community Name
- Security Name
- Transport Tag
- Storage Type

In addition, you can display the entries configured with the Configure SNMPv1 & SNMPv2c Community Menu in the Configure SNMPv3 Community Table Menu. However, you cannot modify an SNMPv1 & SNMPv2c Community Table entry with the Configure SNMPv3 Community Table Menu.

There are three functions you can perform with the Configure SNMPv3 Target Parameters Table Menu.

- Creating an SNMPv3 Community Table Entry on page 382
- Deleting an SNMPv3 Community Table Entry on page 385
- Modifying an SNMPv3 Community Table Entry on page 386

Creating an SNMPv3 Community Table Entry

To create an entry in the Configure SNMPv3 Community Table Menu, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is displayed Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **9** to select Configure SNMPv3 Community Table.

The Configure SNMPv3 Community Table Menu is shown in Figure 116.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Marketing Switch 17

User: Manager                                00:14:33 15-Jan-2004

Configure SNMPv3 Community Table

Community Index ..... ATIIndex1
Community Name ..... 451engineering75
Security Name ..... debashi48
Transport Tag ..... sampletag
Storage Type ..... NonVolatile
Row Status ..... Active

1 - Create SNMPv3 Table Entry
2 - Delete SNMPv3 Table Entry
3 - Modify SNMPv3 Table Entry

N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 116 Configure SNMPv3 Community Table Menu

- To create an entry in the SNMPv3 Community Table, type **1** to select Create SNMPv3 Table Entry.

The following prompt is displayed:

```
Enter Community Index:
```

- Enter the name of this Community Index.

This parameter describes the name of this community. It is used to index the other parameters in an SNMPv3 Community Table entry. Enter a value of up to 32-alphanumeric characters.

The following prompt is displayed:

```
Enter Community Name:
```

- 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.

The following prompt is displayed:

```
Enter Security Name:
```

6. Enter the 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.

The following prompt is displayed:

```
Enter Transport Tag:
```

7. Enter a name of up to 32-alphanumeric characters for the Transport Tag.

The Transport Tag parameter is similar to the Notify Tag parameter in the SNMPv3 Notify Table. Add the value you configure for the Transport Tag parameter to the Tag List parameter in the Target Address Table. In this way, the Transport Tag parameter links an SNMPv3 Community Table entry with an entry in the SNMPv3 Target Address Table. See SNMPv3 Target Address Table on page 302.

The following prompt is displayed:

```
Enter Storage type [V-volatile, N-NonVolatile]:
```

8. Select one of the following storage types for this table entry:

V - Volatile

Select this storage type if you do not want the ability to save an entry in the SNMPv3 Community Table to the configuration file. After making changes to an SNMPv3 Community Table entry with a Volatile storage type, the **S** - Save Configuration Changes option does not appear on the Main Menu.

N-NonVolatile

Select this storage type if you want the ability to save an entry in the SNMPv3 Community Table to the configuration file. After making changes to an SNMPv3 Community Table entry with a NonVolatile storage type, the **S** - Save Configuration Changes option appears on the Main Menu, allowing you to save your changes.

Note

The Row Status parameter is a read-only field in the Telnet and Local interfaces. The Active value indicates the SNMPv3 Community Table entry takes effect immediately.

9. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Deleting an SNMPv3 Community Table Entry

You may want to delete an entry from the SNMPv3 Community Table. When you delete an entry in the SNMPv3 Community Table, there is no way to undelete or recover it.

To delete an entry in the SNMPv3 Community Table, perform the following procedure:

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is shown in Figure 102 on page 307.

2. From the Configure SNMPv3 Table Menu, type **9** to select Configure SNMPv3 Community Table.

The Configure SNMPv3 Community Table Menu is shown in Figure 116 on page 383.

3. To delete an entry in the SNMPv3 Community Table, type **2** to select Delete SNMPv3 Table Entry.

The following prompt is displayed:

```
Enter Community Index:
```

4. Enter the Community Index that you want to delete.

The following prompt is displayed:

```
Do you want to delete this table entry? (Y/N):  
[Yes/No]->
```

5. Choose one of the following:

Y

Type Y to delete an SNMPv3 Community table entry.

N

Type N to retain the SNMPv3 Community table entry.

6. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Modifying an SNMPv3 Community Table Entry

For each entry in the SNMPv3 Community Table, you can modify the following parameters:

- Community Name
- Security Name
- Transport Tag
- Storage Type

However, you cannot modify the Community Index parameter.

Although you can display the SNMPv1 and SNMPv2c configuration created with the procedures described in Configuring the SNMPv1 and SNMPv2c Protocols on page 86, you cannot modify these Community Table entries with the SNMPv3 Tables.

See the following procedures:

- Modifying the Community Name on page 386
- Modifying the Security Name on page 388
- Modifying the Transport Tag on page 388
- Modifying the Storage Type on page 389

Modifying the Community Name

To modify the Community Name parameter in an SNMPv3 Community Table entry, perform the following procedure:

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is displayed Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **9** to select Configure SNMPv3 Community Table.

The Configure SNMPv3 Community Table Menu is shown in Figure 116 on page 383.

3. From the Configure SNMPv3 Community Table, type **3** to select Modify SNMPv3 Table Entry.

The Modify SNMPv3 Community Table Menu is shown in Figure 117.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Marketing Switch 17

User: Manager                                00:14:33 15-Jan-2004

Modify SNMPv3 Community Table

Community Index ..... alliedtelesynindex
Community Name ..... 789bothel23wa
Security Name ..... buster
Transport Tag ..... 72
Storage Type ..... Volatile
Row Status ..... Active

1 - Set Community Name
2 - Set Security Name
3 - Set Transport Tag
4 - Set Storage Type

N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 117 Modify SNMPv3 Community Table Menu

4. To change the Community Name, type **1** to select Set Community Name.

The following prompt is displayed:

```
Enter Community Index:
```

5. Enter the Community Index that you want to modify.

The following prompt is displayed:

```
Enter Community Name:
```

6. Enter the new Community Name.

The value of the Community Name parameter acts as a password for the SNMPv3 Community Table entry. This parameter is case sensitive. Enter a value of up to 64 alphanumeric characters.

Note

Allied Telesyn recommends that you select SNMP Community Names carefully to ensure these names are known only to authorized personnel.

- After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Modifying the Security Name

To modify the Security Name parameter in an SNMPv3 Community Table entry, perform the following procedure:

- Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is displayed as shown in Figure 101 on page 306.

- From the Configure SNMPv3 Table Menu, type **9** to select Configure SNMPv3 Community Table.

The Configure SNMPv3 Community Table Menu is shown in Figure 116 on page 383.

- From the Configure SNMPv3 Community Table, type **3** to select Modify SNMPv3 Table Entry.

The Modify SNMPv3 Community Table Menu is shown in Figure 117 on page 387.

- To change the Security Name, type **2** to select Set Security Name.

The following prompt is displayed:

```
Enter Community Index:
```

- Enter the Community Index of the Security Name you want to change.

The following prompt is displayed:

```
Enter Security Name:
```

- Enter the new Security Name.

Enter a value of up to 32-alphanumeric characters.

- After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Modifying the Transport Tag

To modify the Transport Tag parameter in an SNMPv3 Community Table entry, perform the following procedure:

- Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is displayed as shown in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **9** to select Configure SNMPv3 Community Table.

The Configure SNMPv3 Community Table Menu is shown in Figure 116 on page 383.

3. From the Configure SNMPv3 Community Table, type **3** to select Modify SNMPv3 Table Entry.

The Modify SNMPv3 Community Table Menu is shown in Figure 117 on page 387.

4. To change the Transport Tag, type **3** to select Set Transport Tag.

The following prompt is displayed:

```
Enter Community Index:
```

5. Enter the Community Index of the Transport Tag you want to change.

The following prompt is displayed:

```
Enter Transport Tag:
```

6. Enter the new value for the Transport Tag.

Enter a name of up to 32-alphanumeric characters.

7. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Modifying the Storage Type

To modify the Storage Type parameter in an SNMPv3 Community Table entry, perform the following procedure:

1. Follow steps 1 through 5 in the procedure described in Creating an SNMPv3 User Table Entry on page 305. Or, from the Main Menu type **5->1->1->8->5**.

The Configure SNMPv3 Table Menu is displayed as shown in Figure 101 on page 306.

2. From the Configure SNMPv3 Table Menu, type **9** to select Configure SNMPv3 Community Table.

The Configure SNMPv3 Community Table Menu is shown in Figure 116 on page 383.

3. From the Configure SNMPv3 Community Table, type **3** to select Modify SNMPv3 Table Entry.

The Modify SNMPv3 Community Table Menu is shown in Figure 117 on page 387.

4. To change the Storage Type, type **4** to select Set Storage Type.

The following prompt is displayed:

```
Enter Community Index:
```

5. Enter the Community Index of the Storage Type you want to change.

The following prompt is displayed:

```
Enter Storage type [V-volatile, N-NonVolatile]:
```

6. Select one of the following storage types for this table entry:

V - Volatile

Select this storage type if you do not want the ability to an entry in the SNMPv3 Community Table to the configuration file. After making changes to an SNMP Community Table entry with a Volatile storage type, the **S** - Save Configuration Changes option does not appear on the Main Menu.

N-NonVolatile

Select this storage type if you want the ability to save an entry in the SNMPv3 Community Table to the configuration file. After making changes to an SNMPv3 Community Table entry with a NonVolatile storage type, the **S** - Save Configuration Changes option appears on the Main Menu, allowing you to save your changes.

7. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Displaying SNMPv3 Table Menus

The procedures in this section describe how to display the SNMPv3 Tables. The following procedures are provided:

- Displaying the Display SNMPv3 User Table Menu on page 391
- Displaying the Display SNMPv3 View Table Menu on page 393
- Displaying the Display SNMPv3 Access Table Menu on page 394
- Displaying the Display SNMPv3 SecurityToGroup Table Menu on page 395
- Displaying the Display SNMPv3 Notify Table Menu on page 396
- Displaying the Display SNMPv3 Target Address Table Menu on page 397
- Displaying the Display SNMPv3 Target Parameters Table Menu on page 398
- Displaying the Display SNMPv3 Community Table Menu on page 399

Displaying the Display SNMPv3 User Table Menu

This section describes how to display the Display SNMPv3 User Table Menu. For information about the SNMPv3 User Table, see Creating an SNMPv3 User Table Entry on page 305.

To display the Display SNMPv3 User Table Menu, perform the following procedure.

1. From the Main Menu, type **5** to select System Menu.
The System Menu is shown in Figure 5 on page 51.
2. From the System Menu, type **1** to select Configure System.
The Configure System Menu is shown Figure 11 on page 59.
3. From the Configure System Menu, type **1** to select Configure System Software.
The Configure System Software Menu is shown in Figure 12 on page 60.
4. From the Configure System Software Menu, type **8** to select Configure SNMP.
The Configure SNMP Menu is shown in Figure 101 on page 306.
5. From the Configure SNMP Menu, type **6** to select Display SNMPv3 Table.

The Display SNMPv3 Table Menu is shown in Figure 118.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Marketing Switch 17
User: Manager                                00:14:33 15-Jan-2004
Display SNMPv3 Table
1 - Display SNMPv3 User Table
2 - Display SNMPv3 View Table
3 - Display SNMPv3 Access Table
4 - Display SNMPv3 SecurityToGroup Table
5 - Display SNMPv3 Notify Table
6 - Display SNMPv3 Target Address Table
7 - Display SNMPv3 Target Parameters Table
8 - Display SNMPv3 Community Table
R - Return to Previous Menu
Enter your selection?
```

Figure 118 Display SNMPv3 Table Menu

6. From the Display SNMPv3 Table Menu, type **1** to select Display SNMPv3 User Table.

The Display SNMPv3 User Table is shown in Figure 119.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Marketing Switch 17
User: Manager                                00:14:33 15-Jan-2004
Display SNMPv3 User Table
Engine Id ..... 80:00:00:CF:31:00:30:84:FD:57:DA
User Name ..... spike
Authentication Protocol ... MD5
Privacy Protocol ..... DES
Storage Type ..... NonVolatile
Row Status ..... Active
N - Next Page
U - Update Display
R - Return to Previous Menu
Enter your selection?
```

Figure 119 Display SNMPv3 User Table Menu

Displaying the Display SNMPv3 View Table Menu

This section describes how to display the Display SNMPv3 View Table Menu. For information about the SNMPv3 View Table parameters, see Creating an SNMPv3 View Table Entry on page 315.

To display the Display SNMPv3 View Table Menu, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in Displaying the Display SNMPv3 User Table Menu on page 391. Or, from the Main Menu type **5->1->1->8->6**.
2. From the Display SNMPv3 Table Menu, type **2** to select Display SNMPv3 View Table.

The Display SNMPv3 View Table Menu is shown in Figure 120.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
High School Switch 142

User: Manager                                00:14:33 15-Jan-2004

Display SNMPv3 View Table

View Name ..... tcp
Subtree OID ..... 1.3.6.1
Subtree Mask .....
View Type ..... Included
Storage Type ..... NonVolatile
Row Status ..... Active

N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 120 Display SNMPv3 View Table Menu

Displaying the Display SNMPv3 Access Table Menu

This section describes how to display the Display SNMPv3 Access Table Menu. For information about the SNMPv3 Access Table parameters, see Creating an SNMPv3 Access Table Entry on page 324.

To display the Display SNMPv3 Access Table Menu, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in Displaying the Display SNMPv3 User Table Menu on page 391. Or, from the Main Menu type **5->1->1->8->6**.
2. From the Display SNMPv3 Table Menu, type **3** to select Display SNMPv3 Access Table.

The Display SNMPv3 Access Table Menu is shown in Figure 121.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
High School Switch 142

User: Manager                                00:14:33 15-Jan-2004

Display SNMPv3 Access Table

Group Name .... technicalsales                Security Model . v3
Context Prefix.                               Security Level . AuthPriv
Read View..... internet                      Context Match .. Exact
Write View ....                               Storage Type ... NonVolatile
Notify View ...                               Row Status ..... Active

N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection?
```

Figure 121 Display SNMPv3 Access Table Menu

Displaying the Display SNMPv3 SecurityToGroup Table Menu

This section describes how to display the Display SNMPv3 SecurityToGroup Table Menu. For more information about the parameters in the SNMPv3 SecurityToGroup Table Menu, see *Creating an SNMPv3 SecurityToGroup Table Entry* on page 340.

To display the Display SNMPv3 SecurityToGroup Table Menu, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in *Displaying the Display SNMPv3 User Table Menu* on page 391. Or, from the Main Menu type **5->1->1->8->6**.
2. From the Display SNMPv3 Table Menu, type **4** to select Display SNMPv3 SecurityToGroup Table.

The Display SNMPv3 SecurityToGroup Table Menu is shown in Figure 122.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Marketing Switch 17

User: Manager                                00:14:33 15-Jan-2004

Display SNMPv3 SecurityToGroup Table

Security Model..... v3
Security Name ..... praveen
Group Name ..... hardwareengineering
Storage Type ..... NonVolatile
Row Status ..... Active

N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 122 Display SNMPv3 SecurityToGroup Table Menu

Displaying the Display SNMPv3 Notify Table Menu

This section describes how to display the Display SNMPv3 Notify Table Menu. For information about the SNMPv3 Notify Table parameters, see Creating an SNMPv3 Notify Table Entry on page 348.

To display the Display SNMPv3 Notify Table Menu, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in Displaying the Display SNMPv3 User Table Menu on page 391. Or, from the Main Menu type **5->1->1->8->6**.
2. From the Display SNMPv3 Table Menu, type **5** to select Display SNMPv3 Notify Table.

The Display SNMPv3 Notify Table Menu is shown in Figure 122.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Marketing Switch 17

User: Manager                                00:14:33 15-Jan-2004

Display SNMPv3 Notify Table

Notify Name ..... testengineeringTrap
Notify Tag ..... testengineeringtag
Notify Type ..... Inform
Storage Type ..... NonVolatile
Row Status ..... Active

N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection?
```

Figure 123 Display SNMPv3 Notify Table Menu

Displaying the Display SNMPv3 Target Address Table Menu

This section describes how to display the Display SNMPv3 Target Address Table Menu. For information about the SNMPv3 Target Address Table parameters, see *Creating an SNMPv3 Target Address Table Entry* on page 356.

To display the Display SNMPv3 Target Address Table Menu, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in *Displaying the Display SNMPv3 User Table Menu* on page 391. Or, from the Main Menu type **5->1->1->8->6**.
2. From the Display SNMPv3 Table Menu, type **6** to select Display SNMPv3 Target Address Table.

The Display SNMPv3 Target Address Table Menu is shown in Figure 122.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Marketing Switch 17

User: Manager                                00:14:33 15-Jan-2004

Display SNMPv3 Target Address Table

Target Addr Name ... host99                 Timeout ..... 1500
Target Parameters .. SNMPmanagerPC         Retries ..... 5
IP Address ..... 198.35.11.1               UDP Port# ... 162
Storage Type ..... NonVolatile             Row Status .. Active
Tag List ..... engTrap engInform

U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 124 Display SNMPv3 Target Address Table Menu

Displaying the Display SNMPv3 Target Parameters Table Menu

This section describes how to display the Display SNMPv3 Target Parameters Table Menu. For information about of the SNMPv3 Target Parameters Table parameters, see Creating an SNMPv3 Target Parameters Table Entry on page 369.

To display the Display SNMPv3 Target Parameters Table Menu, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in Displaying the Display SNMPv3 User Table Menu on page 391. Or, from the Main Menu type **5->1->1->8->6**.
2. From the Display SNMPv3 Table Menu, type **7** to select Display SNMPv3 Target Parameters Table.

The Display SNMPv3 Target Parameters Table Menu is shown in Figure 122.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Marketing Switch 17

User: Manager                                00:14:33 15-Jan-2004

Display SNMPv3 Target Parameters Table

Target Parameters Name ... TargetIndex21
Message Processing Model . v3
Security Model ..... v3
Security Name ..... wilson
Security Level ..... AuthPriv
Storage Type ..... NonVolatile
Row Status ..... Active

U - Update Display
R - Return to Previous Menu

Enter your selection?
```

Figure 125 Display SNMPv3 Target Parameters Table Menu

Displaying the Display SNMPv3 Community Table Menu

This section describes how to display the Display SNMPv3 Community Table Menu. For information about the SNMPv3 Community Table parameters, see Creating an SNMPv3 Community Table Entry on page 382.

To display the Display SNMPv3 Community Table Menu, perform the following procedure.

1. Follow steps 1 through 5 in the procedure described in Displaying the Display SNMPv3 User Table Menu on page 391. Or, from the Main Menu type **5->1->1->8->6**.
2. From the Display SNMPv3 Table Menu, type **8** to select Display SNMPv3 Community Table.

The Display SNMPv3 Community Table Menu is shown in Figure 122.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Marketing Switch 17

User: Manager                                00:14:33 15-Jan-2004

Display SNMPv3 Community Table

Community Index ..... atiindex14
Community Name ..... sunnyvale
Security Name ..... hoa
Transport Tag..... sampletag14
Storage Type ..... NonVolatile
Row Status ..... Active

U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 126 Display SNMPv3 Community Table Menu

Section IV

VLANs

The chapters in Section IV explain how to configure VLANs on an AT-8400 switch using a local or Telnet management session. The chapters include:

- ❑ Chapter 18: Tagged and Port-based Virtual LANs on page 401
- ❑ Chapter 19: Multiple VLAN Modes on page 435
- ❑ Chapter 20: GARP VLAN Registration Protocol on page 444

Chapter 18

Tagged and Port-based Virtual LANs

This chapter contains basic information about virtual LANs (VLANs). It also contains procedures for creating, modifying, and deleting VLANs from a local or Telnet management session. There is also a procedure on how to change a switch's VLAN operating mode. This chapter contains the following sections:

- VLAN Overview on page 402
- Port-based VLAN Overview on page 404
- Tagged VLAN Overview on page 412
- Basic VLAN Mode Overview on page 417
- Displaying VLANs on page 418
- Creating a Port-based or Tagged VLAN on page 421
- Example of Creating a Port-Based VLAN on page 425
- Example of Creating a Tagged VLAN on page 426
- Modifying a VLAN on page 427
- Deleting a VLAN on page 431
- Setting a Switch's VLAN Mode on page 432
- Specifying a Management VLAN on page 433

Note

For information about other types of VLAN types, see Chapter 19, Multiple VLAN Modes on page 435. Chapter 20, GARP VLAN Registration Protocol on page 444. Chapter 19, MAC-Based Virtual LANs on page 426. Chapter 20, Protocol-Based Virtual LANs on page 454.

VLAN Overview

A VLAN is a group of ports on an Ethernet switch that form a logical Ethernet segment. The ports of a VLAN form an independent traffic domain where the unicast, multicast, and broadcast packets generated by the nodes of a VLAN remain within the VLAN.

With VLANs, you can segment your network through the switch's management software and so be able to group nodes with related functions into their own separate, logical LAN segments. These VLAN groupings can be based on similar data needs or security requirements. For example, you could create separate VLANs for the different departments in your company, such as one for Sales and another for Accounting.

VLANs offer several important benefits:

- Improved network performance

Network performance often suffers as networks grow in size and as data traffic increases. The more nodes on a LAN segment vying for bandwidth, the more likely that overall network performance decreases.

VLANs improve network performance because VLAN traffic stays within the VLAN. The nodes of a VLAN receive traffic only from nodes of the same VLAN. This reduces the need for nodes to handle traffic not destined for them. It also frees up bandwidth within all the logical workgroups.

- Increased security

Since traffic generated by a node in a VLAN is restricted only to the other nodes of the same VLAN, VLANs can be used to control the flow of data in your network and prevent data from flowing to unauthorized end nodes.

- Simplified network management

VLANs can also simplify network management. Before the advent of VLANs, physical changes to the network often had to be made at the switches in the wiring closets. For instance, if an employee changed departments, changing the employee's LAN segment assignment might require a change to the wiring at the switches.

But with VLANs, you can change the LAN segment assignment of an end node connected to the switch through the switch's AT-S60 management software. VLAN memberships can be changed at any time through the management software without moving the

workstations physically, or having to change group memberships by moving cables from one switch port to another.

A virtual LAN can also span more than one switch. This means that the end nodes of a VLAN do not need to be connected to the same switch and so are not restricted to being in the same physical location.

The AT-8400 Series switch supports the following types of VLANs that you can create and modify yourself:

- Port-based VLANs
- Tagged VLANs
- Multiple VLANs
- GVRP VLANs

The Port-based and Tagged VLANs are described in the following sections in this section. For information about the other types of VLANs, see the following chapters:

- Chapter 19, Multiple VLAN Modes on page 435
- Chapter 20, GARP VLAN Registration Protocol on page 444

Port-based VLAN Overview

As explained in the VLAN Overview section, a VLAN consists of a group of ports on one or more Ethernet switches that form an independent traffic domain. The unicast, broadcast, and multicast packets generated by the end nodes of a VLAN remain within the VLAN and do not cross over to the end nodes of other VLANs unless there is an interconnecting device, such as a router or Layer 3 switch.

A port-based VLAN is a group of ports on a Fast Ethernet Switch that form a logical Ethernet segment. Each port of a port-based VLAN can belong to only one VLAN at a time.

A port-based VLAN can have as many or as few ports as needed. The VLAN can consist of all the ports on an Ethernet switch, or a few ports. A port-based VLAN also can span switches and consist of ports from multiple Ethernet switches.

Note

All of the Ethernet line cards for the AT-8400 Series switch are pre-configured with one port-based VLAN. All ports are members of this VLAN, called the Default_VLAN.

The parts that make up a port-based VLAN are:

- VLAN name
- VLAN Identifier
- Untagged ports
- Port VLAN Identifier

VLAN Name

To create a port-based VLAN, you must give it a name. The name should reflect the function of the network devices that are members of the VLAN. Examples include Sales, Production, and Engineering. The names of the VLANs on a switch must be unique. You cannot give two VLANs on the same switch the same name. A VLAN name can be up to 19 alphanumeric characters in length.

VLAN Identifier

Each VLAN in a network must have a unique number assigned to it. This number is called the VLAN identifier (VID). This number uniquely identifies a VLAN in the switch and the network.

If a VLAN consists only of ports located on one physical switch in your network, you would assign it a VID unique from all other VLANs in your network.

If a VLAN spans multiple switches, then the VID for the VLAN on the different switches must be the same. In this manner, the switches are able to recognize and forward frames belonging to the same VLAN even though the VLAN spans multiple switches. For example, if you had a port-based VLAN titled Marketing that spanned three AT-8400 Series switches, you would assign the Marketing VLAN on each switch the same VID.

You can assign this number manually or allow the management software to do it automatically. If you allow the management software to do it automatically, it simply selects the next available VID. This is acceptable when you are creating a new, unique VLAN.

If you are creating a VLAN on a switch that is part of a larger VLAN that spans several switches, then you need to assign the number yourself so that the VLAN has the same VID on all switches.

Untagged Ports

Naturally, you need to specify which ports on the switch are to be members of a port-based VLAN. Ports in a port-based VLAN are referred to as *untagged ports* and the frames received on the ports as *untagged frames*. The names derive from the fact that the frames received on a port do not contain any information that indicates VLAN membership, and that VLAN membership is determined solely by the port's PVID.

A port on a switch can be an untagged member of only one port-based VLAN at a time. An untagged port cannot be assigned to two port-based VLANs simultaneously.

Port VLAN Identifier

Each port in a port-based VLAN must have a port VLAN identifier (PVID). The switch associates a frame to a port-based VLAN by the PVID assigned to the port on which the frame is received, and forwards the frame only to those ports with the same PVID. Consequently, all ports of a port-based VLAN must have the same PVID. Additionally, the PVID of the ports in a VLAN must match the VLAN's VID.

For example, assume that you were creating a port-based VLAN on a switch and you had assigned the VLAN the VID a value of 5. Consequently, the PVID for each port in the VLAN would need to be assigned the value of 5.

Some switches and switch management programs require that you assign the PVID value for each port manually. However, the AT-S60 management software performs this task automatically. The software automatically assigns a PVID to a port, making it identical to the VID of the VLAN to which the port is a member.

General Rules for Creating a Port-based VLAN

Below is a summary of the general rules to observe when creating a port-based VLAN.

- Each port-based VLAN must be assigned a unique VID. If a particular VLAN spans multiple switches, each part of the VLAN on the different switches must be assigned the same VID.
- A port can be an untagged member of only one port-based VLAN at a time.
- The ports on an AT-8400 line card can belong to the same VLAN or to different VLANs.
- Each port must have a PVID. This value must be the same for all ports in a port-based VLAN and must match a VLAN's VID. This value is assigned automatically by the AT-S60 management software.
- A port-based VLAN that spans multiple switches requires a dedicated port on each switch to function as an interconnection between the switches where the various parts of the VLAN reside.
- If end nodes in different VLANs need to communicate with each other, a router or Layer 3 switch is required to interconnect the VLANs.
- An AT-8400 Series switch can support up to 256 VLANs.

Drawbacks of Port-based VLANs

There are several drawbacks to port-based VLANs:

- It is not easy to share network resources, such as servers and printers, across multiple VLANs. A router or Layer 3 switch must be added to the network to provide a means for interconnecting the port-based VLANs.

- ❑ The introduction of a router into your network could create security issues from unauthorized access to your network.
- ❑ A VLAN that spans several switches requires a port on each switch for the interconnection of the various parts of the VLAN. For example, a VLAN that spans three switches requires one port on each switch to interconnect the various sections of the VLAN. In network configurations where there are many individual VLANs that span switches, many ports can end up being used ineffectively just to interconnect the various VLANs.

Port-Based Examples

What follows are two examples of port-based VLANs that illustrate the basic principles discussed earlier in this chapter.

Example 1

Our first example is illustrated in Figure 127. It shows two port-based VLANs on an AT-8400 switch.

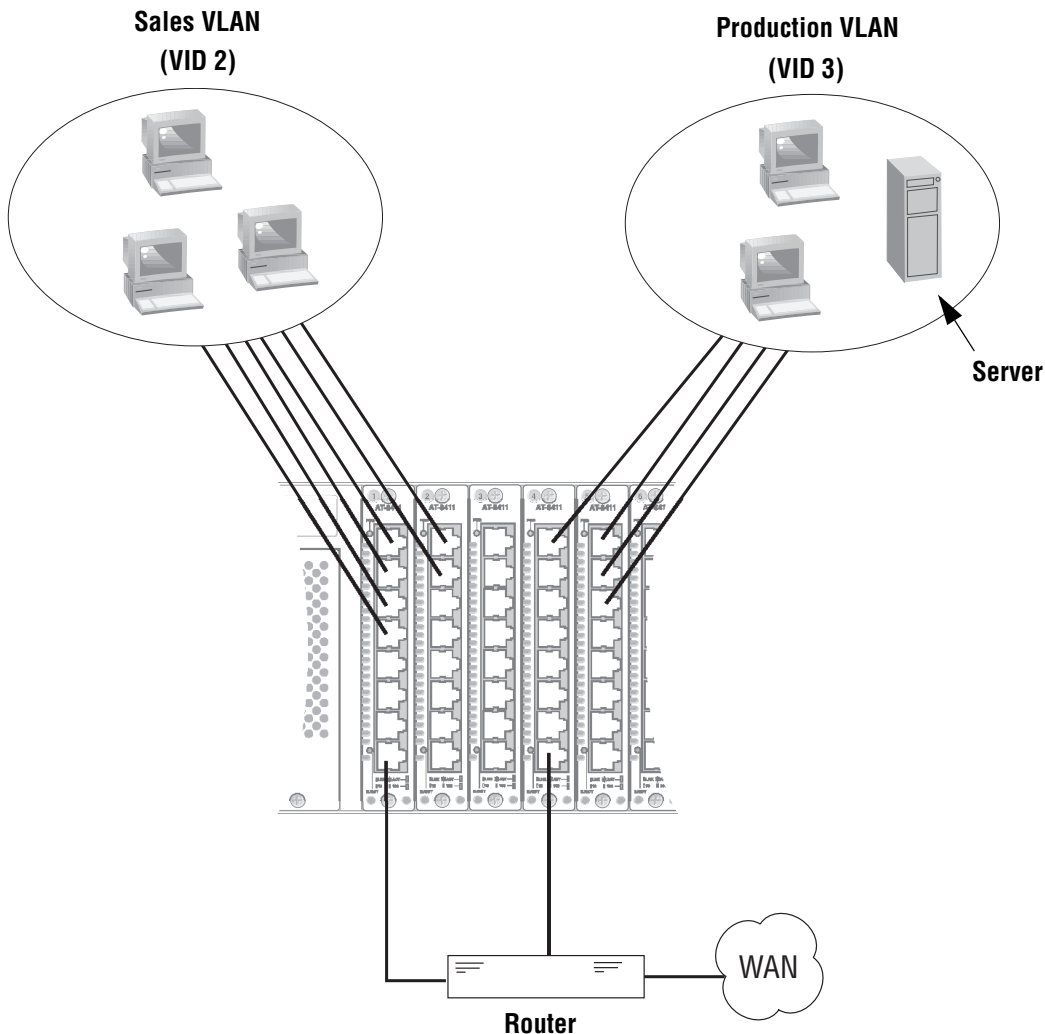


Figure 127 Port-based VLAN - Example 1

The two VLANs are Sales and Production. They were assigned unique VIDs of 2 and 3, respectively, when they were created. (The VID of 1 is reserved for the Default_VLAN.) The ports were also assigned a PVID value that matches the VID of the VLAN in which they were made a member. This is performed automatically by the management software. For instance, all the ports of the Sales VLAN were automatically assigned a PVID of 2 when the ports were made a member of the VLAN.

The table below lists the port assignments for the Sales and Production VLANs on the AT-8400 Series switch.

	Sales VLAN (VID 2)	Production VLAN (VID 3)
AT-8400 Series switch	Slot 1: AT-8411TX Ports: 1 - 4, 8 (PVID=2)	Slot 4: AT-8411TX Ports: 1, 8 (PVID=3)
	Slot 2: AT-8411TX Ports 1 - 2 (PVID=2)	Slot 5: AT-8411TX Ports 1 - 3 (PVID=3)

Each VLAN also has a port connected to the router. The router interconnects the VLANs. For instance, if a workstation in the Sales VLAN needs to access the server in the Production VLAN, the traffic passes through the router. Without the router (or a Layer 3 switch), the VLANs could not communicate with each other. The router also provides access for the VLANs to the WAN.

Example 2

Figure 128 illustrates our second port-based example. The two VLANs, Sales and Production, now span two Ethernet switches, an AT-8400 and an AT-8024.

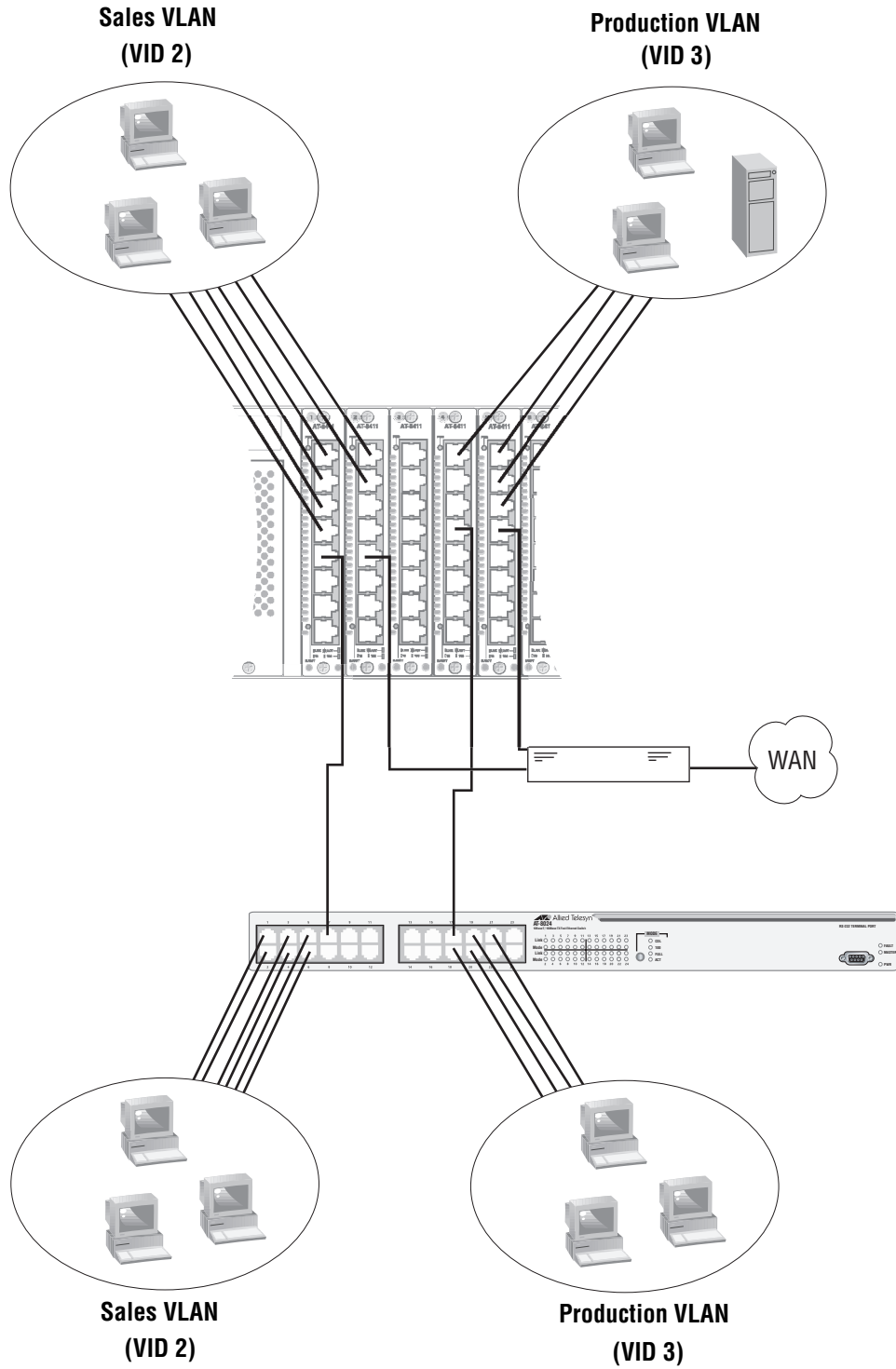


Figure 128 Port-based VLAN - Example 2

The table below lists the port assignments for the Sales and Production VLANs on the switches:

	Sales VLAN (VID 2)	Production VLAN (VID 3)
AT-8400 Series switch	Slot 1 Ports: 1-5 (PVID= 2)	Slot 4 Ports: 1, 4 (PVID= 3)
	Slot 2 Ports: 1-2, 5 (PVID= 2)	Slot 5 Ports: 4 (PVID= 3)
AT-8024 Switch	Ports 1-7 (PVID=2)	Ports 17-21 (PVID= 3)

As mentioned earlier, a VLAN that spans more than one switch requires a data link(s) to connect its different parts together. In our example, both VLANs span multiple switches. So both VLANs need to have a separate link.

For the Sales VLAN, that link is provided by Port 5 on the AT-8411 TX line card in Slot 1 in the AT-8400 Series switch and by Port 7 in the AT-8024 switch. The connection between the two ports allows the two parts of the Sales VLAN to function as one logical VLAN.

For the Production VLAN, the connection is supplied by Port 4 on the AT-8411 TX line card in Slot 4 of the AT-8400 Series switch and by Port 17 in the AT-8024 switch.

The two VLANs also need to be connected to the router so they can exchange packets and access the WAN. The Sales VLAN is connected to the router with Port 5 on the AT-8411 TX line card in Slot 2 of the AT-8400 Series switch. The Production VLAN is connected to the router with Port 4 on the line card in Slot 5.

Tagged VLAN Overview

The second type of VLAN supported by the AT-8400 Series switch is the *tagged VLAN*. Tagged VLANs use information inside tagged frames as they are received on the ports to determine VLAN membership. This contrasts with port-based VLANs, where the PVIDs assigned to the ports determine VLAN membership.

The VLAN information within an Ethernet frame is referred to as a *tag* or *tagged header*. A tag, which follows the source and destination addresses in a frame, contains the VID of the VLAN to which the frame belongs. As explained earlier in this chapter in VLAN Identifier on page 404, this number uniquely identifies each VLAN in a network.

When a switch receives a frame with a VLAN tag, referred to as a *tagged frame*, the switch forwards the frame only to those ports that share the same VID.

A port to receive or transmit tagged frames is referred to as a *tagged port*. Any network device connected to a tagged port must be IEEE 802.1Q-compliant. This is the standard that outlines the requirements and standards for tagging. The device must be able to process the tagged information on received frames and add tagged information to transmitted frames.

The benefit of a tagged VLAN is that the tagged ports within the VLAN can belong to more than one VLAN at one time. This can greatly simplify the task of adding shared devices to the network. For example, a server can be configured to accept and return packets from many different VLANs simultaneously.

Tagged VLANs are also useful where multiple VLANs span across switches. You can use one port per switch for connecting all VLANs on the switch to another switch.

The IEEE 802.1Q standard deals with how this tagging information is used to forward the traffic throughout the switch. The handling of frames tagged with VIDs coming into a port is straightforward. If the incoming frame's VID tag matches one of the VIDs of a VLAN that the port is a tagged member of, the frame is accepted and forwarded to the appropriate ports. If the frame's VID does not match any of the VLANs that the port is a member of, the frame is discarded.

The parts of a tagged VLAN are much the same as those for a port-based VLAN. They are:

- VLAN Name
- VLAN Identifier
- Tagged and Untagged Ports
- Port VLAN Identifier

Note

For explanations of VLAN name and VLAN identifier, refer to **VLAN Name** and VLAN Identifier on page 404.

Tagged and Untagged Ports

You need to specify which ports are members of the VLAN. In the case of a tagged VLAN, it is usually a combination of both untagged ports and tagged ports. You specify which ports are tagged and which untagged when you create the VLAN.

An untagged port, whether a member of a port-based VLAN or a tagged VLAN, can be in only one VLAN at a time. However, a tagged port can be a member of more than one VLAN. A port can also be an untagged member of one VLAN and a tagged member of different VLANs, simultaneously. However, a port cannot be a tagged and untagged member of the same VLAN.

Port VLAN Identifier

As explained earlier in the discussion on port-based VLANs, the management software automatically assigns a PVID to each port when a port is made a member of a VLAN. The PVID is always identical to the VLAN's VID, and that in a port-based VLAN packets are forwarded based on the PVID.

Since a tagged port determines VLAN membership by examining the tagged header within the frames that it receives, there would seem to be no need for a PVID. But, actually there is a need. The PVID is used if a tagged port receives an untagged frame (that is, a frame without any tagged information). The port forwards the frame based on the port's PVID. But this is only in cases where untagged frames arrive on tagged ports. Otherwise, the PVID of a port is ignored on a tagged port.

General Rules for Creating a Tagged VLAN

Below is a summary of the rules to observe when creating a tagged VLAN.

- Each tagged VLAN must be assigned a unique VID. If a particular VLAN spans multiple switches or stacks, each part of the VLAN on the different switches or stacks must be assigned the same VID.
- A tagged port can be a member of multiple VLANs.
- An untagged port can be an untagged member of only one VLAN at a time.
- The ports on an AT-8400 line card can belong to the same VLAN or different VLANs.
- A port cannot be an untagged and tagged member of the same VLAN.
- An AT-8400 Series switch can support up to 256 VLANs.

Tagged VLAN Example

Figure 129 illustrates how tagged ports can be used to interconnect IEEE 802.1Q-based products.

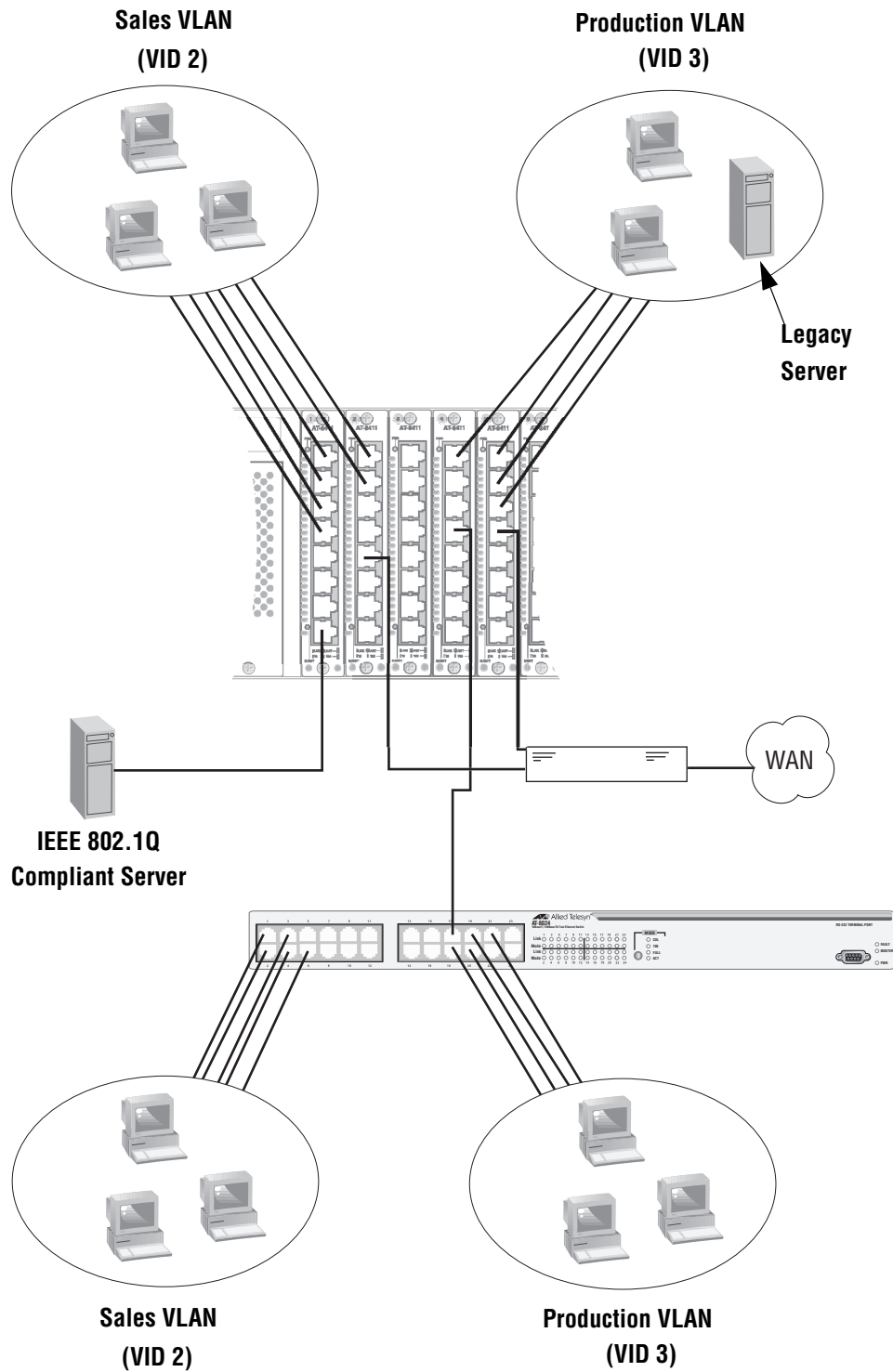


Figure 129 Example of a Tagged VLAN

This example is nearly identical to the port-based VLAN Example 2 earlier in this chapter. Tagged ports have been added to simplify network implementation and management.

The port assignments for the VLANs are as follows:

	Sales VLAN (VID 2)		Production VLAN (VID 3)	
	Untagged Ports	Tagged Ports	Untagged Ports	Tagged Ports
AT-8400 Switch	Slot 1 Ports: 1 - 4	Slot 1 Port: 8	Slot 4 Port: 1	Slot 1 Port: 8
	Slot 2 Ports: 1 - 2, 5	Slot 4 Port 4	Slot 5 Ports: 1 - 4	Slot 4 Port 4
AT-8024 Switch	1 - 4, 6	17	18 - 21	17

One of the changes is the addition of an IEEE 802.1Q-compliant server. This server can handle frames from multiple VLANs. It is connected to Port 8 on the AT-8411 TX line card in Slot 1 of the AT-8400 Series switch. Port 8 has been made a tagged port of both the Sales and Production VLANs. This allows the workstations of the VLANs to access the server without having to use the router.

It is important to note that even though the server accepts frames from and transmits frames to more than one VLAN, data separation and security remain. The frames from the server to the switch contain VID information that tell the switch which VLAN the packet belongs to. This prevents packets from crossing VLAN boundaries.

Another use of tagged ports in the example eliminates the need for separate, dedicated links to connect together VLANs that span multiple switches. Back in the port-based Example 2 on page 410, the Sales and Production VLANs each had separate links to connect together their different parts.

But in this example, tagged ports allow one data link to carry packets from different VLANs, but network security is maintained. Tagged frames, when received by the switch, are delivered only to those ports that belong to the VLAN from which the frames originated.

This shared data link is provided by Port 4 on the AT-8411 TX line card in Slot 4 of the AT-8400 Series switch and by Port 17 on the AT-8024 switch. Both ports have been made tagged ports of both the Sales VLAN and the Production VLAN.

Each VLAN still has a dedicated connection to the router for access by the Sales VLAN to the legacy server, and also so the two VLANs can access the WAN.

Basic VLAN Mode Overview

The Fast Ethernet Switches support a special VLAN configuration referred to as the Basic VLAN Mode. When the Basic VLAN Mode is activated, frames are forwarded based solely on MAC addresses. All VLAN information, including PVIDs assigned to ports and VLAN tags in tagged frames, is ignored. Tagged frames are analyzed only for priority level.

Packets are passed through the switch unchanged. Tagged and untagged frames exit the switch the same as they entered, either tagged or untagged, regardless of the type of ports on which the frames are received and transmitted.

You should be aware of the following before you activate the Basic VLAN mode:

- ❑ If a packet received on a switch port contains a MAC address not already stored in the MAC address table, the packet is flooded out all ports in the AT-8400 Series switch, except for the port on which the packet was received.
- ❑ You can create and modify port-based or tagged VLANs when the Basic VLAN Mode is activated, but the VLANs are not active. Port-based and tagged VLANs are active only when the switch is operating in the Tagged mode. Additionally, pre-existing port-based or tagged VLANs are retained in the event you later disabled Basic VLAN Mode, but the VLANs are not used.

Note

For instructions on how to activate the Basic VLAN mode, refer to *Setting a Switch's VLAN Mode* on page 432.

Displaying VLANs

The procedure in this section displays all the port-based and tagged VLANs on the AT-8400 Series switch. In addition, you can display the Management VLAN ID and the VLAN Mode.

To view the VLANs, perform the following procedure:

1. From the Main Menu, type **2** to select VLAN Menu.

The VLAN Menu is shown in Figure 130.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142
User: Manager                                00:14:33 20-Jan-2004
                                           VLAN Menu
1 - Configure VLAN
2 - Display VLAN
3 - Configure GARP-GVRP
R - Return to Previous Menu
Enter your selection?
```

Figure 130 VLAN Menu

2. From the VLAN Menu, type **2** to select Display VLAN.

The Display VLAN Menu is shown in Figure 131.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142
User: Manager                                00:14:33 20-Jan-2004
                                           Display VLAN
1 - Management VLAN ID..... 1 (Default_VLAN)
2 - VLAN Mode ..... User Configured
3 - Display Port Based VLAN
R - Return to Previous Menu
Enter your selection?
```

Figure 131 Display VLAN Menu

The Management VLAN ID and the VLAN Mode are displayed in the Display VLAN Menu.

- From the Display VLAN Menu, type **3** to select Display Port Based VLAN.

The Display Port Based VLAN Menu is displayed. An example of the menu is shown in Figure 132.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142

User: Manager                                00:14:33 01-Jan-2004

Display Port Based VLAN
VID VLAN Name      VLAN Type  Protocol  Untagged(U)/Tagged Ports
-----
1  Default_VLAN    Port Based
                        Port Based      U: 11.1-8, 12.8
                        Port Based      T: 5.1, 6.3
12 Sales           Port Based
                        Port Based      U: 1.1-8, 2.1-8, 3.4-8
                        Port Based      T: 5.1, 6.3
20 Production      Port Based
                        Port Based      U: 3.1-3, 4.3-8, 5.2-8, 6.1-8
                        Port Based      T: 5.1, 6.3

U - Update display
R - Return to Previous Menu

Enter your selection?

```

Figure 132 Display Port Based VLAN Menu

This menu displays all the tagged and port-based VLANs that exist on the switch. Also included are any VLANs created by GVRP, referred to as dynamic GVRP VLANs. The columns in the menu are defined below:

VID

This is the VID of the VLAN.

VLAN Name

This is the VLAN's name.

VLAN Type

If the VLAN type is Port Based, the VLAN is either a port-based or tagged VLAN. If the VLAN type is GARP, then the VLAN was created by GVRP.

Protocol

If the protocol is GARP, then either the VLAN was created by GVRP or the VLAN had a tagged port added to it by GVRP. Here is how you can tell which it is.

If VLAN Type and Protocol both say GARP, then the VLAN was created by GVRP. An example of a dynamic GVRP VLAN is the VLAN GVRP_VLAN_22 in the example menu above.

If only the Protocol is GARP, then the corresponding tagged port in the menu was added by GVRP to an existing VLAN. An example of this is the Engineering VLAN in the menu Display Port Based VLAN Menu on page 419. Notice, port 11.5 was added as a dynamic port to the tagged Engineering VLAN.

Tagged(T)/Untagged(U)

This column lists the ports of the VLAN.

Creating a Port-based or Tagged VLAN

To create a new port-based or tagged VLAN, perform the following procedure:

1. From the Main Menu, type **2** to select VLAN Menu.
The VLAN Menu is shown in Figure 130 on page 418.
2. From the VLAN Menu, type **1** to select Configure VLAN.
The Configure VLAN Menu is shown in Figure 133.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
High School Switch 142
User: Manager                                00:14:33 01-Jan-2003
                                Configure VLAN
1 - Set Management VLAN ID ..... 1 (Default_VLAN)
2 - Set VLAN Mode ..... User Configured
3 - Set Uplink Port ..... None
4 - Configure Port-Based VLAN

D - Reset to Default VLAN
R - Return to Previous Menu

Enter your selection?
```

Figure 133 Configure VLAN Menu

- From the Configure VLAN menu, type **4** to select Configure Port-Based VLAN.

The Configure Port Based VLAN Menu is shown in Figure 134.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
High School Switch 142

User: Manager                                00:14:33 01-Jan-2004

Configure Port-Based VLAN
-----
VIDVLAN Name   VLAN Type   Protocol Tagged(T)/Untagged(U) Ports
-----
1  Default_VLAN Port Based           U: 11.1-8, 12.8
                               T: 5.1, 6.3
12 Sales        Port Based           U: 1.1-8, 2.1-8, 3.4-8, 4.1-2, 7.1-2
                               T: 5.1, 6.3
20 Production  Port Based           U: 3.1-3, 4.3-8, 5.2-8, 6.1-8

1 - Create Port Based VLAN
2 - Delete Port Based VLAN
3 - Modify Port Based VLAN

U - Update display
R - Return to Previous Menu

Enter your selection?

```

Figure 134 Configure Port Based VLAN Menu

The top portion of the menu displays the current VLANs on the switch. For an explanation of the columns, refer to Displaying VLANs on page 418. If you have not created any VLANs, this menu contains only the Default_VLAN.

- Type **1** to select Create Port Based VLAN.

The following prompt is displayed:

```
Enter VLAN Name:
```

- Enter a name for the new VLAN.

The name can be from one to nineteen 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 to be 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

You must assign a name to a VLAN.

After you have entered a name, the following prompt is displayed:

```
Enter VLAN VID: [2 to 4094]
```

6. Enter a VID value for the new VLAN. The permitted range of the VID value is 2 to 4094.

The management software uses the next available VID number on the switch as the default value. If the VLAN is to be unique in your network, then its VID must also be unique. If this VLAN is to be 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

You must assign a VID to a VLAN.

The switch is only aware of the VIDs of the VLANs that exist on the line cards in the chassis. The switch is not aware of the VIDs of other VLANs in your network. You may need to take this into account when selecting a VID for a new VLAN.

For instance, let's assume that you added an AT-8400 Series switch to an existing network that already has VLANs on other switches that use VIDs 2 through 24. When you start to create your first VLAN on the new AT-8400 Series switch, the management software chooses VID 2 to assign to the VLAN, because that is the first VID available on the chassis. It does not automatically know that the VID is already in use by another VLAN on the network.

To avoid inadvertently assigning a new VLAN a VID already being used, you might consider keeping a list of your network VLANs and their associated VIDs.

After you have entered a VID, the following prompt is displayed:

```
Enter Tagged Port-list:
```

7. Specify the tagged ports of the VLAN.

If this VLAN does not contain any tagged ports, leave this field empty and simply press Return. For information on entering ports, refer to *Specifying Ports* on page 34.

After you have entered the tagged ports of the VLAN, the following prompt is displayed:

```
Enter Untagged Port-list:
```

8. Specify the ports on the switch to function as untagged ports in the VLAN.

If this VLAN does not contain any untagged ports, leave this field empty. For information on entering ports, refer to Specifying Ports on page 34.

After you have specified the untagged ports, the management software automatically creates the VLAN. The Configure Port Based VLAN Menu (Figure 134 on page 422) is updated with your new VLAN.

9. Check to see that the VLAN was created correctly and that it contains the appropriate ports.

The new VLAN is now ready for use.

Note

Ports designated as untagged ports of a new VLAN are automatically removed from their current untagged VLAN assignment. For example, if you are creating a new VLAN on a switch that contains only the Default_VLAN, the ports that you specify as untagged ports of the new VLAN are automatically removed from the Default_VLAN when the new VLAN is created.

Tagged ports are not removed from any current VLAN assignments because tagged ports can belong to more than one VLAN at a time.

10. Repeat this procedure starting with Step 4 to create additional VLANs.
11. After making changes, type **R** to return to the Main Menu. Then type **S** to select Save Configuration Changes.

Example of Creating a Port-Based VLAN

The following procedure creates the Sales VLAN illustrated in Port-Based Examples on page 408. This VLAN is assigned a VID of 2. It consists of seven untagged ports, Ports 1 to 4 and 8 from the AT-8411 TX line card in Slot 1 and Ports 1 and 2 from the AT-8411 TX line card in Slot 2. The VLAN does not contain any tagged ports.

To create the example Sales VLAN, perform the following procedure:

1. From the Main Menu, type **2** to select VLAN Menu.
The VLAN Menu is shown in Figure 133 on page 421.
2. From the VLAN Menu, type **1** to select Configure VLAN.
The Configure VLAN menu is shown in Figure 133 on page 421.
3. From the Configure VLAN menu, type **4** to select Configure Port Based VLAN.
The Configure VLAN Menu is shown in Figure 134 on page 422.
4. Type **1** to select Create Port Based VLAN.
The following prompt is displayed:
`Enter VLAN Name:`
5. Enter *Sales*. Press Return.
The following prompt is displayed:
`Enter VID [2 to 4094]:`
6. Enter **2**. This is the VID value for the new VLAN. Press Return.
The following prompt is displayed:
`Enter Tagged Port-list:`
7. Because the Sales VLAN does not contain any tagged ports, you do not enter any ports for this prompt. Press Return.
The following prompt is displayed:
`Enter Untagged Port-list:`
8. Enter "1.1-4,8,2.1-2". These are the untagged ports of the Sales VLAN.
The management software automatically creates the new VLAN and adds it to the list of VLANS in the menu.
9. Return to the Main Menu and type **S** to select Save Configuration Changes.

Example of Creating a Tagged VLAN

The following procedure creates the Production VLAN in the AT-8400 Series switch illustrated in Tagged VLAN Example on page 415. This VLAN is assigned the VID 3. It consists of five untagged ports: Port 1 from the AT-8411 TX line card in slot 5 and Ports 1 to 4 from the AT-8411 line card in Slot 6. The VLAN also consists of two tagged ports: Port 8 from Slot 1, which gives the VLAN access to an IEEE 802.1q-compliant server, and Port 4 from Slot 4, which is a shared link to the AT-8024 switch, where another part of the Production VLAN resides.

To create the Production VLAN example, perform the following procedure:

1. From the Main Menu, type **2** to select VLAN Menu.
The VLAN Menu is shown in Figure 130 on page 418.
2. From the VLAN Menu, type **1** to select Configure VLAN.
The Configure VLAN menu is shown in Figure 133 on page 421.
3. From the Configure VLAN menu, type **4** to select Configure Port Based VLAN.
The Configure VLAN Menu is shown in Figure 134 on page 422.
4. Type **1** to select Create Port Based VLAN. The following prompt is displayed:
Enter VLAN Name:
5. Enter *Production*. Press Return. The following prompt is displayed:
Enter VID [2 to 4094]:
6. Enter 3. This is the VID value for the new VLAN. Press Return. The following prompt is displayed:
Enter Tagged Port-list:
7. Enter *1,8,4,4*.
These are the tagged ports of the Production VLAN. Port 8 on the line card in Slot 1 is connected to an IEEE 802.1q-compliant server. Port 4 on the line card in Slot 4 is a shared link to the AT-8024 switch, where more nodes of the Production VLAN reside. The following prompt is displayed:
Enter Untagged Port-list:
8. Enter *4,1,5,1-4*. These are the untagged ports of Production VLAN.
The management software automatically creates the new VLAN and adds it to the list of VLANs in the menu.
9. After making changes, type **R** to return to the Main Menu. Then type **S** to select Save Configuration Changes.

Modifying a VLAN

The section contains the procedure for adding or deleting ports from a tagged or port-based VLAN.

To modify a VLAN, perform the following procedure:

1. From the Configure Port Based VLAN menu, type **3** to select Modify Port Based VLAN.

The Modify Port Based VLAN menu is shown in Figure 135.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
                          Engineering Switch 142

User: Manager                                00:14:33 01-Jan-2004

                          Modify Port Based VLAN

VID  VLAN Name      VLAN Type Protocol Tagged <T>/Untagged <U> Ports
-----
1    Default_VLAN  Port Based          U: 11.1-8, 12.8
                                T: 5.1, 6.3
12   Sales         Port Based          U: 1.1-8, 2.1-8, 3.4-8

1 - Add Ports to VLAN
2 - Delete Ports from VLAN
3 - Set Ports to VLAN
4 - Clear Ports from VLAN
5 - Change GARP VLAN

U - Update display
R - Return to Previous Menu

Enter your selection?

```

Figure 135 Modify Port Based VLAN Menu

The top portion of the menu displays the current VLANs on the switch. For an explanation of the columns, refer to the procedure Displaying VLANs on page 418.

Note

You cannot add or remove ports from a dynamic GVRP VLAN and you cannot remove a dynamic GVRP port from a port-based or tagged VLAN. For information on GVRP, refer to Chapter 20, GARP VLAN Registration Protocol on page 444.

Each menu selection is explained below.

1 - Add Ports to VLAN

To add ports to a VLAN, do the following:

- a. Type **1** to select Add Ports to VLAN.

The following prompt is displayed:

```
Enter VLAN ID: [2 to 4094] ->
```

- b. Enter the VID of the VLAN you want to change.

The following prompt is displayed:

```
Enter Tagged Port-list to add:
```

- c. If you want to add one or more tagged ports to the VLAN, enter them at this prompt. If you are not adding tagged ports, press Return. For information on entering ports, refer to Specifying Ports on page 34.

The following prompt is displayed:

```
Enter Untagged Port-list to add:
```

- d. If you want to add one or more untagged ports to the VLAN, enter them at this prompt. If you are not adding untagged ports, press Return.

Changes are immediately activated on the VLAN.

Note

Untagged ports that are added to a VLAN are automatically removed from their current untagged VLAN assignment. Adding a tagged port to a VLAN does not effect the tagged port's current VLAN assignments.

- e. Repeat this step to modify other VLANs.
- f. After modifying a VLAN, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

2 - Delete Ports from VLAN

To remove ports from a VLAN, do the following:

- a. Type **2** to select Delete Ports from VLAN.

The following prompt is displayed:

```
Enter VLAN ID: [2 to 4094] ->
```

- b. Enter the VID of the VLAN you want to change.

The following prompt is displayed:

```
Enter Tagged Port-list to delete:
```

- c. If you want to remove one or more tagged ports from the VLAN, enter the ports at this prompt. If you are not removing tagged ports, press Return. For information on entering ports, refer to *Specifying Ports* on page 34.

The following prompt is displayed:

```
Enter Untagged Port-list to delete:
```

- d. If you want to remove one or more untagged ports from the VLAN, enter them at this prompt. If you are not removing untagged ports, press Return.

Changes are immediately activated on the VLAN.

Note

Untagged ports that are removed from a VLAN are automatically returned to the Default_VLAN.

You cannot remove an untagged port directly from the Default_VLAN. Instead, you must assign it as an untagged port to another VLAN.

- e. Repeat this step to modify other VLANs.
- f. After modifying a VLAN, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

3 - Set Ports to VLAN

To remove all ports from a VLAN while assigning new ports, do the following:

- a. Type **3** to select Set Ports to VLAN.

The following prompt is displayed:

```
Enter VLAN ID: [2 to 4094] ->
```

- b. Enter the VID of the VLAN you want to change.

The following prompt is displayed:

```
Enter Tagged Port-list:
```

- c. Enter the new tagged ports for the VLAN. To remove all tagged ports without assigning new ports, press Return.

The following prompt is displayed:

```
Enter Untagged Port-list:
```

- d. Enter the new untagged ports from the VLAN. To remove all untagged ports without assigning new ports, press Return.

Changes are immediately activated on the VLAN.

- e. After modifying a VLAN, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

4 - Clear Ports from VLAN

To remove all ports from the VLAN, do the following:

- a. Type **4** to select Clear Ports from VLAN.

The following prompt is displayed:

```
Enter VLAN ID: [2 to 4094] ->
```

- b. Enter the VID of the VLAN you want to change.

All tagged and untagged ports are removed from the VLAN.

- c. After modifying a VLAN, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

5 - Change GARP VLAN

To convert a dynamic GVRP VLAN or a dynamic GVRP port to a static VLAN or port, do the following:

- a. Type **5** to select Change GARP VLAN.

The following prompt is displayed:

```
Enter VLAN ID: [2 to 4094] ->
```

- b. Enter the VID of the dynamic GVRP VLAN or the static VLAN containing the dynamic port you want to convert. You can specify only one VLAN.

The dynamic VLAN or port is changed to a static VLAN or port. You can now modify or delete the VLAN like any other tagged VLAN.

Note

For background information on GVRP, refer to Chapter 20, GARP VLAN Registration Protocol on page 444.

- c. After modifying a VLAN, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Deleting a VLAN

To delete a VLAN, perform the following procedure:

1. From the Configure Port Based VLAN menu, type **2** to select Delete Port Based VLAN.

The following prompt is displayed:

```
Enter VLAN ID: [2 to 4094] ->
```

2. Enter the VID of the VLAN you want to delete and press Return.

Note

You cannot delete the Default_VLAN, which has a VID of 1, or a dynamic GVRP VLAN.

The following confirmation prompt is displayed:

```
Do you want to delete this VLAN? [Yes/No] ->
```

3. Type **Y** to delete the VLAN or **N** to cancel the procedure. Press Return.

The VLAN is deleted. All untagged ports in the deleted VLAN are returned to the Default_VLAN as untagged ports.

4. Repeat this procedure to delete additional VLANs.
5. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Setting a Switch's VLAN Mode

This section contains the procedure for setting a switch's VLAN mode. You can configure a switch to support port-based and tagged VLANs or to operate in the Basic VLAN mode. Port-based and tagged VLANs and the Basic VLAN mode are described in earlier sections in this chapter.

Note

Changing a switch's VLAN mode resets the switch. The switch does not forward traffic during the brief period required to reload the AT-S60 management software.

To configure a switch's VLAN mode, perform the following procedure:

1. From the Main Menu, type **5** to select System Menu.
2. From the System Menu, type **1** to select Configure System.
3. From the Configure System menu, type **1** to select Configure System Software.
4. From the Configure System Software menu, type **1** to toggle the Switch Mode setting as desired.

Option 1 - Switch Mode in the Configure System Software menu toggles the switch between port-based and tagged VLANs and the Basic VLAN mode. When the option is showing Tagged, the switch supports port-based and tagged VLANs. When the option is showing Basic, the switch is operating in the Basic VLAN mode.

The system displays a confirmation prompt.

5. Type **Y** to change the switch VLAN mode or **N** to cancel this procedure.

If you responded with Y for yes, the switch automatically reboots and your management session is ended. To continue managing the switch, you must reestablish your management session once the switch has completed reloading the AT-S60 management software.

Specifying a Management VLAN

The management VLAN is the VLAN through which an AT-8400 Series switch expects to receive management packets. This VLAN is important if you are using the enhanced stacking feature of the switch or if you are managing a switch remotely.

Management packets are packets generated by a management workstation while managing a switch. The management card in the switch acts upon the packets only if they are received on the management VLAN.

The default management VLAN on an AT-8400 Series switch is the Default_VLAN. If you do not create any additional VLANs and link the switches together using untagged ports, then there is no need to specify a new management VLAN. You should be able to manage the AT-8400 Series switches in your network using the enhanced stacking feature.

However, if you create additional VLANs on your switches, it may be necessary for you to create a management communications path and then specify that path as the new management VLAN.

Below are several rules to observe when using this feature:

- The management VLAN must exist on each AT-8400 Series switch that you want to manage.
- Using the following procedure, you must specify the management VLAN in the AT-S60 software on each slave and master switch of an enhanced stack.
- The uplink and downlink ports on the switch that are the data links between the switches must be untagged members of the management VLAN.
- The port on the switch to which the management station is connected must be an untagged member of the management VLAN. (This does not apply if the management station is connected to the RS-232 port on the management card.)

Here is an example. Let's assume that you have an enhanced stack of three AT-8400 Series switches with one master switch. If the uplink and downlink ports between the various switches are untagged members of the Default_VLAN and if the management station is connected to a untagged port of the Default_VLAN, you can manage all the switches since the Default_VLAN is by default the management VLAN.

Now let's assume that you decided to create a VLAN called NMS with a VID of 24 for the sole purpose of remote network management. For this, you would need to create the NMS VLAN on each AT-8400 Series switch that you want to manage remotely, being sure to assign each NMS VLAN the VID of 24. You would need to be sure that the uplink and downlink ports connecting the switches together are untagged members of the NMS VLAN. And you would also need to specify the NMS VLAN as the management VLAN on each switch using the management software. Finally, you must be sure to connect your management station to a port on a switch that is an untagged member of the management VLAN. (This last step does not apply if you are managing the enhanced stack through the RS-232 port on the management card in one of the switches.)

To specify the management VLAN in the AT-S60 software, do the following:

1. From the Main Menu, type **2** to select VLAN Menu.
The VLAN Menu is shown in Figure 133 on page 421.
2. From the VLAN Menu, type **1** to select Configure VLAN.
The Configure VLAN Menu is shown in Figure 133 on page 421.
3. From the Configure VLAN menu, type **1** to select Set Management VLAN ID.
The following prompt is displayed:
Enter Management VLAN ID [1 to 4094] ->
4. Specify the VID of the VLAN that is to function as the management VLAN.

Note

The VLAN must already exist on the switch.

The following prompt is displayed:

SUCCESS - Press any key to continue...

5. Press any key.
6. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Chapter 19

Multiple VLAN Modes

This chapter explains the Multiple VLAN modes and how to select a mode. This chapter contains the following sections:

- ❑ **Multiple VLAN Mode Overview** on page 436
- ❑ **Selecting a VLAN Mode** on page 440
- ❑ **Changing the Uplink Port** on page 442
- ❑ **Displaying VLAN Information** on page 443

Multiple VLAN Mode Overview

The Multiple VLAN modes simplify the task of configuring a switch in a network environment that requires a high degree of network segmentation. These modes are useful in isolating the traffic on each port from all other ports. They are fixed VLAN configurations that cannot be changed.

When a Multiple VLAN mode is activated, the switch automatically places each port in a separate VLAN as an untagged port. Each VLAN is given a unique name and VID number based on the port number. For example, the VLAN for Port 1 on the module in Slot 1 is called Client_1 and is given the VID of 1, the VLAN for Port 2 is called Client_2 and has a VID of 2, and so on.

PVIDs are assigned automatically. For example, the PVID for Port 1 on the module in Slot 1 is assigned as 1, to match the VID of 1.

A user-specified port on the switch is designated as an uplink port and is made a member of all the VLANs. The uplink port can be connected to a shared device, such as a router for access to a WAN.

This highly segmented configuration is useful in situations where traffic generated by each end node or network segment connected to a port on the switch needs to be kept separate from all other network traffic, while allowing access to an uplink port. Unicast traffic received by the uplink port is effectively directed to the appropriate port and end node, and is not directed to any other port on the switch.

The AT-S60 software supports two types of Multiple VLAN modes:

- 802.1Q-compliant multiple VLANs
- Non-802.1Q compliant multiple VLANs

The VLAN modes are discussed in the following sections. Procedures for selecting a VLAN mode is in **Selecting a VLAN Mode** on page 440.

Note

The Multiple VLAN modes are supported only in single switch (that is, an edge switch) environments. This means that cascading of switches while in a Multiple VLAN mode is not allowed.

Activating a Multiple VLAN mode on a cascaded switch can possibly result in disconnection of network paths between switches unless the port used to link the switches is configured as the uplink port.

Configuring Multiple VLANs on cascaded switches can also affect Enhanced Stacking as the Master switch may not be able to detect member switches beyond the first cascaded switch.

802.1Q-Compliant Multiple VLANs Mode

802.1Q Multiple VLAN configuration is appropriate when the device connected to the uplink port is 802.1Q compatible, meaning that the device can handle tagged packets.

When 802.1Q Multiple VLANs mode is selected, the AT-S60 software configures all ports on the switch as Client VLANs except for one user-specified port that is designated as an uplink VLAN. Each Client VLAN contains one untagged port and one tagged port. The latter functions as the uplink port.

When you select the 802.1Q-compliant VLAN mode, you are asked to specify the uplink port. After you specify the port, the switch automatically creates the VLANs.

Table 12 illustrates this VLAN mode on an AT-8400 Series switch. It lists a few of the ports on the switch and shows how each port has been added as an untagged port to its own separate VLAN. Port 2.2 (Slot 2, Port 2) was selected as the uplink port. It was added as a tagged port to each VLAN.

Table 12 802.1Q-Compliant Multiple VLAN Example

VLAN Name	VID	Untagged Port	Tagged Port
Client_1	1	1.1	2.2
Client_2	2	1.2	2.2
Client_3	3	1.3	2.2
Client_4	4	1.4	2.2
Client_5	5	1.5	2.2
Client_6	6	1.6	2.2

Table 12 802.1Q-Compliant Multiple VLAN Example

VLAN Name	VID	Untagged Port	Tagged Port
Client_7	7	1.7	2.2
Client_8	8	1.8	2.2
Client_9	9	2.1	2.2
Client_10	10	2.2	
Client_11	11	2.3	2.2

Note

In 802.1Q Multiple VLAN mode, the device connected to the uplink port must be 802.1Q-compliant and must be able to handle tagged packets.

Non-802.1Q Compliant Multiple VLANs

The Non-802.1Q Multiple VLAN mode is appropriate when the device connected to the uplink port is non-802.1Q compatible, meaning that the device cannot handle tagged packets.

When the Non-802.1Q Multiple VLAN mode is selected, each port is placed as an untagged port in a separate Client VLAN. One port, selected as the uplink port, is also added to each VLAN, also as an untagged port.

The fact that the uplink port is untagged and that it is placed in more than one VLAN is why this mode is referred to as non-802.1Q compliant. Untagged ports are suppose to belong to only one VLAN at a time. Only tagged ports can belong to multiple VLANs.

When you select the Non-802.1Q Multiple VLAN mode, you are asked to specify the uplink port. After you specify the port, the switch automatically creates the VLANs.

Table 13 illustrates this VLAN mode on an AT-8400 Series switch. It lists a few of the ports on the switch and shows how each port has been added as an untagged port to its own separate VLAN. Port 2.2 was selected as the uplink port. It was added as an untagged port to each VLAN.

Table 13 Non-802.1Q Compliant Multiple VLAN Example

VLAN Name	VID	Untagged Port	Tagged Port
Client_1	1	1.1, 2.2	
Client_2	2	1.2, 2.2	
Client_3	3	1.3, 2.2	

Table 13 Non-802.1Q Compliant Multiple VLAN Example

VLAN Name	VID	Untagged Port	Tagged Port
Client_4	4	1.4, 2.2	
Client_5	5	1.5, 2.2	
Client_6	6	1.6, 2.2	
Client_7	7	1.7, 2.2	
Client_8	8	1.8, 2.2	
Client_9	9	2.1, 2.2	
Client_10	10	All ports	
Client_11	11	2.3, 2.2	

**Caution**

The non-802.1Q-Compliant Multiple VLAN mode does not protect the switch from VLAN leakage. If the switch receives a packet on the uplink port containing a destination MAC address that is not in the MAC address table, the switch broadcasts the packet out all ports, except the uplink port. This means that all end nodes on the switch receive the packet.

Multiple VLAN Modes and the Management VLAN

Although both multiple VLAN modes support remote management of the switch via a management VLAN, the management VLAN is restricted to one VLAN. It cannot be changed. In the 802.1Q-compliant mode, the management VLAN is the VLAN where the uplink port is an untagged member. In the non-802.1Q compliant mode, the management VLAN is the VLAN that contains all of the ports.

For background information in the management VLAN, refer to **Specifying a Management VLAN** on page 433.

Selecting a VLAN Mode

The following procedure explains how to select a VLAN mode on an AT-8400 Series Switch.

Note

You should create a backup file of the configuration of the switch before changing the switch to a Multiple VLAN mode. Changing the VLAN mode automatically deletes any port-based or tagged VLANs that you created on the switch.

1. From the Main Menu, type **2** to select VLAN Menu.

The VLAN Menu is displayed as shown in Figure 133 on page 421.

2. From the VLAN Menu, type **1** to select Configure VLAN.

The Configure VLAN Menu is displayed as shown in Figure 133 on page 421.

3. From the Configure VLAN Menu, type **2** to select Set VLAN Mode.

The following prompt is displayed:

```
Enter VLAN Mode (U-User Configured, Q-Multiple  
802.1Q, M-Multiple) ->
```

4. Select one of the following:

U - Activates the user configuration mode. Select this value to create your own port-based and tagged VLANs. This is the default setting.

Q - Activates the Q-802.1Q Multiple VLAN mode.

M - Activates the non-802.1Q compliant multiple VLANs mode.

If you selected a multiple VLAN mode, the following prompt is displayed:

```
Please backup current configuration before changing  
to multiple VLAN mode:  
Do you want to continue? [Y/N]
```

5. Enter **Y** to continue or **N** to cancel the procedure.

If you selected a Multiple VLAN mode, the following prompt is displayed:

```
Enter uplink port-list:
```

6. Enter the number of the port on the switch to function as the uplink port for the other ports. You can specify only one port.

The following confirmation is displayed:

```
Setting VLAN mode to Multiple VLAN. Please wait...
```

The VLAN mode is changed.

7. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Changing the Uplink Port

Once the switch is operating in a Multiple VLAN mode, you can always change the uplink port, if needed. You simply specify the new uplink port and the switch automatically reconfigures the VLANs.

To change the uplink port, perform the following procedure:

1. From the Main Menu, type **2** to select VLAN Menu.

The VLAN Menu is displayed as shown Figure 133 on page 421.

2. From the VLAN Menu, type **1** to select Configure VLAN.

The Configure VLAN Menu is displayed as shown in Figure 133 on page 421.

3. From the Configure VLAN menu, type **3** to select Set Uplink Port.

The following prompt is displayed:

```
Enter uplink port-list:
```

4. Enter the number of the port on the switch that is to function as the new uplink port. You can specify only one port.

The following confirmation is displayed:

```
Setting VLAN mode to Multiple VLAN. Please wait...
```

The uplink port is changed.

5. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Displaying VLAN Information

To view the name, VID number, and member ports of the VLANs on a switch, perform the following procedure:

1. From the Main Menu, type **2** to select VLAN Menu.
 The VLAN Menu is displayed as shown in Figure 133 on page 421.
2. From the VLAN Menu, type **2** to select Display VLAN.
 The Display VLAN Menu is displayed as shown in Figure 131 on page 418.
3. From the Display VLAN menu, type **3** to select Display Port Based VLAN.

An example of the Display Port Based VLAN Menu is shown in Figure 136.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 4
Login Privilege: Manager           00:14:33 01-Apr-2004
Display Port Based VLAN

VID      VLAN Name      VLAN Type      Protocol      Tagged(T)/Untagged(U)
-----
1        Client_1        Port Based
           Port Based
           Port Based      U: 1.1
           Port Based      T: 4.2
2        Client_2        Port Based
           Port Based
           Port Based      U: 1.2
           Port Based      T: 4.2
3        Client_3        Port Based
           Port Based
           Port Based      U: 1.3
           Port Based      T: 4.2
4        Client_4        Port Based
           Port Based
           Port Based      U: 1.4
           Port Based      T: 4.2

N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 136 Display Port Based VLAN Menu

The example shows a switch operating in the 802.1Q-compliant VLAN mode, with port 4.2 acting as the uplink port.

Chapter 20

GARP VLAN Registration Protocol

This chapter describes the GARP VLAN Registration Protocol (GVRP). It contains the following sections:

- ❑ GARP VLAN Registration Protocol (GVRP) Overview on page 445
- ❑ Configuring GVRP on page 453
- ❑ Enabling or Disabling GVRP on a Port on page 455
- ❑ Displaying GVRP Parameters and Statistics on page 458

GARP VLAN Registration Protocol (GVRP) Overview

The GARP VLAN Registration Protocol (GVRP) allows network devices to share VLAN information. The main purpose of GVRP is to allow switches to automatically discover some of the VLAN information that would otherwise have to be manually configured in each switch. This is helpful in networks where VLANs span more than one switch. Without GVRP, you must manually configure your switches to ensure that the various parts of a VLAN can communicate across the different switches. GVRP, which is an application of the Generic Attribute Registration Protocol (GARP), can do this for you automatically.

The AT-S60 management software uses GVRP protocol data units (PDUs) to share VLAN information among GVRP-active devices. The PDUs contain the VID numbers of the VLANs on the switch. A PDU contains the VIDs of all the VLANs on the switch, not just the VID to which the transmitting port is a member.

When a switch receives a GVRP PDU on a port, it examines the PDU to determine the VIDs of the VLANs on the device that sent it. It then does the following:

- ❑ If the VLAN does not exist on the switch, it creates the VLAN and adds the port as a tagged member to the VLAN. A VLAN created by GVRP is called a *dynamic GVRP VLAN*.
- ❑ If the VLAN already exists on the switch but the port is not a member of it, the switch adds the port as a tagged member. A port that has been added by GVRP to a static VLAN (that is a user-created VLAN) is called a *dynamic GVRP port*.

You cannot modify a dynamic GVRP VLAN. Once created, only GVRP can modify or delete it. A dynamic GVRP VLAN exists only so long as there are active nodes in the network that belong to the VLAN. If all nodes of a dynamic GVRP VLAN are shutdown and there are no active links, the VLAN is deleted from the switch. A dynamic GVRP exists only so long as the switch deems it is needed.

A dynamic GVRP port in a static VLAN remains a member of the VLAN as long as there are active VLAN members. If all members of the VLAN become inactive or there are no active links, GVRP removes the dynamic port from the VLAN, but does not delete the VLAN if the VLAN is a static VLAN.

Figure 137 provides an example of how GVRP works.

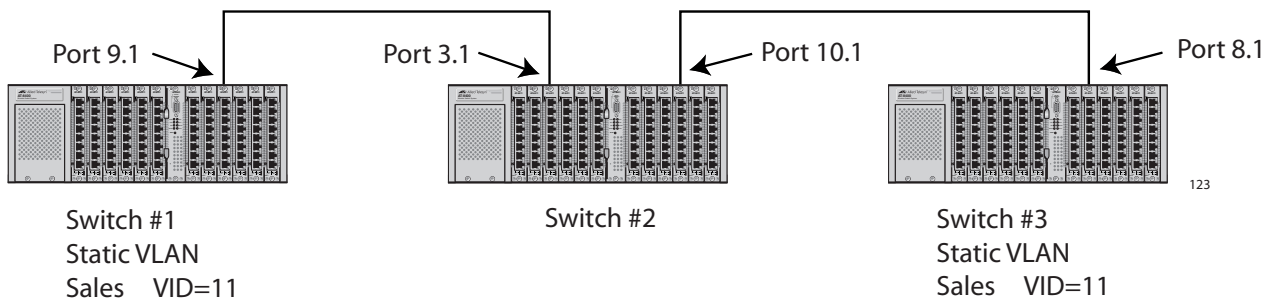


Figure 137 GVRP Example

Switches #1 and #3 contain the Sales VLAN, but Switch #2 does not. Consequently, the end nodes of the two parts of the Sales VLANs are unable to communicate with each other.

Without GVRP, you would need to configure Switch #2 by creating the Sales VLAN on the switch and adding ports 2 and 3 as members of the VLAN. If you happen to have a large network with a large number of VLANs, such manual configurations can be cumbersome and time consuming.

GVRP can make the configurations for you. Here is how GVRP would resolve the problem in the example.

1. Port 1 on Switch #1 sends a PDU to Port 2 on Switch #2, containing the VIDs of all the VLANs on the switch. One of the VIDs in the PDU would be that of the Sales VLAN, VID 11.
2. Switch #2 examines the PDU it receives on Port 2 and notes that it does not have a VLAN with a VID 11. So it creates the VLAN as a dynamic GVRP VLAN and assigns it a VID 11 and the name GVRP_VLAN_11. (The name of a dynamic GVRP VLAN has the prefix "GVRP_VLAN_", followed by the VID number.) The switch then adds Port 2, the port that received the PDU, as a tagged member of the VLAN.
3. Switch #2 sends a PDU out port 3 containing all of the VIDs of the VLANs on the switch, including the new gvrp11 VLAN with its VID of 11. (It should be noted that port 3 is not yet a member of the VLAN. Ports are added to VLANs when they receive, not send a PDU.)
4. Switch #3 receives the PDU on port 4 and, after examining it, notes that one of the VLANs on Switch #2 has the VID 11, which matches the VID of an already existing VLAN on the switch. So it does not create the VLAN since it already exists. It then determines whether the port that received the PDU, in this case port 4, is a member of the VLAN. If

it is not a member, it automatically adds the port to the VLAN as an tagged dynamic GVRP port. If the port is already a member of the VLAN, then no change is made.

5. Switch #3 sends a PDU out port 4 to Switch #2.
6. Switch #2 receives the PDU on port 3 and then adds the port as a tagged dynamic GVRP port to the dynamic GVRP_VLAN_11 VLAN.

There is now a communications path for the end nodes of the Sales VLAN on Switches #1 and #3. GVRP created the new GVRP_VLAN_11 dynamic GVRP VLAN with a VID of 11 on Switch #2 and added ports 2 and 3 to the VLAN as tagged dynamic GVRP ports.

Guidelines

Here are guidelines to observe when using this feature:

- GVRP is supported with STP and RSTP, or without spanning tree. However, GVRP is not supported with MSTP.
- GVRP is supported when the switch is operating in the Tagged VLAN mode, which is the VLAN mode for creating your own tagged and port-based VLANs.
- GVRP is not supported when the switch is operating in either of the Multiple VLAN modes or in the Basic VLAN mode.
- Both ports that constitute a data link between the switch and the other device must be running GVRP.
- You cannot modify or delete a dynamic GVRP VLAN.
- You cannot remove a dynamic GVRP port from a static or dynamic VLAN.
- GVRP is only aware of those VLANs that have active nodes, or where at least one end node of a VLAN has established a valid link with a switch. GVRP is not aware of a VLAN if there are no active end nodes or if no end nodes have established a link with the switch.
- Resetting a switch erases all dynamic GVRP VLANs and dynamic GVRP port assignments. The switch relearns the dynamic assignments as it receives PDUs from the other switches.
- GVRP has three timers that you can set: join timer, leave timer, and leave all timer. The values for these timers must be set the same on all switches running GVRP. Timers with different values on different switches can result in GVRP compatibility problems.

- ❑ You can convert dynamic GVRP VLANs and dynamic GVRP port assignments to static VLANs and static port assignments. The procedure for this is found in Modifying a VLAN on page 427.
- ❑ The default port settings on the switch for GVRP is active, meaning that the ports participate in GVRP. Allied Telesyn recommends disabling GVRP on those ports that are connected to GVRP-inactive devices, meaning that they do not feature GVRP.
- ❑ PDUs are transmitted to only those switch ports where GVRP is enabled.

GVRP and Network Security

GVRP should be used with caution because it can expose your network to unauthorized access. A network intruder can access restricted parts of the network by connecting to a switch port running GVRP and transmitting a bogus GVRP PDU containing VIDs of restricted VLANs. GVRP would make the switch port a member of the VLANs and that could give the intruder access to restricted areas of your network.

To protect against this type of network intrusion, you might consider the following:

- ❑ Activating GVRP only on those switch ports that are connected to other devices that support GVRP. Do not activate GVRP on ports that are connected to GVRP-inactive devices.
- ❑ Converting all dynamic GVRP VLANs and dynamic GVRP ports to static assignments, and then turning off GVRP on all switches. This preserves the new VLAN assignments while protecting against network intrusion.

GVRP-inactive Intermediate Switches

If two GVRP-active devices are separated by a GVRP-inactive switch, the GVRP-active devices may not be able to share VLAN information. There are two issues involved.

The first is whether the intermediate switch forwards the GVRP PDUs that it receives from the GVRP-active switches. GVRP PDUs are management frames, intended for a switch's CPU. In all likelihood, a GVRP-inactive switch discards the PDUs because it does not recognize them.

The second issue is that even if the GVRP-inactive switch forwards GVRP PDUs, it does not create the VLANs, at least not automatically. Consequently, even if the GVRP-active switches receive the PDUs and create the necessary VLANs, the intermediate switch may block the VLAN traffic, unless you modify its VLANs and port assignments manually.

Generic Attribute Registration Protocol (GARP) Overview

The following is a technical overview of GARP. An understanding of GARP may prove helpful when using GVRP.

The purpose of the *Generic Attribute Registration Protocol (GARP)* is to provide a generic framework whereby devices in a bridged LAN, for example, end stations and switches, can register and de-register *attribute* values, such as VLAN Identifiers, with each other. In doing so, the attributes are propagated to devices in the bridged LAN, and these devices form a "reachability" tree that is a subset of an active topology. For a bridged LAN, the active topology is normally that created and maintained by the Spanning Tree Protocol (STP).

To use GARP, a GARP application must be defined. The Layer 2 switch has one GARP application presently implemented, GVRP.

The GARP application specifies what the attribute represents.

GARP defines the architecture, rules of operation, state machines and variables for the registration and de-registration of attribute values. By itself, GARP is not directly used by devices in a bridged LAN. It is the applications of GARP that perform meaningful actions. The use of GVRP allows dynamic filter entries for VLAN membership to be distributed among the forwarding databases of VLAN-active switches.

A GARP Participant in a switch or an end station consists of a GARP Application component, and a *GARP Information Declaration (GID)* component associated with each port of the switch. One such GARP Participant exists per port, per GARP Application. The propagation of information between GARP Participants for the same Application in a switch is carried out by the *GARP Information Propagation (GIP)* component. Protocol exchanges take place between GARP Participants by means of LLC Type 1 services, using the group MAC address and PDU format defined for the GARP Application concerned.

Every instance of a GARP application includes a database to store the values of the attributes. Within GARP, attributes are mapped to GID indexes.

The architecture of GARP is shown in Figure 138.

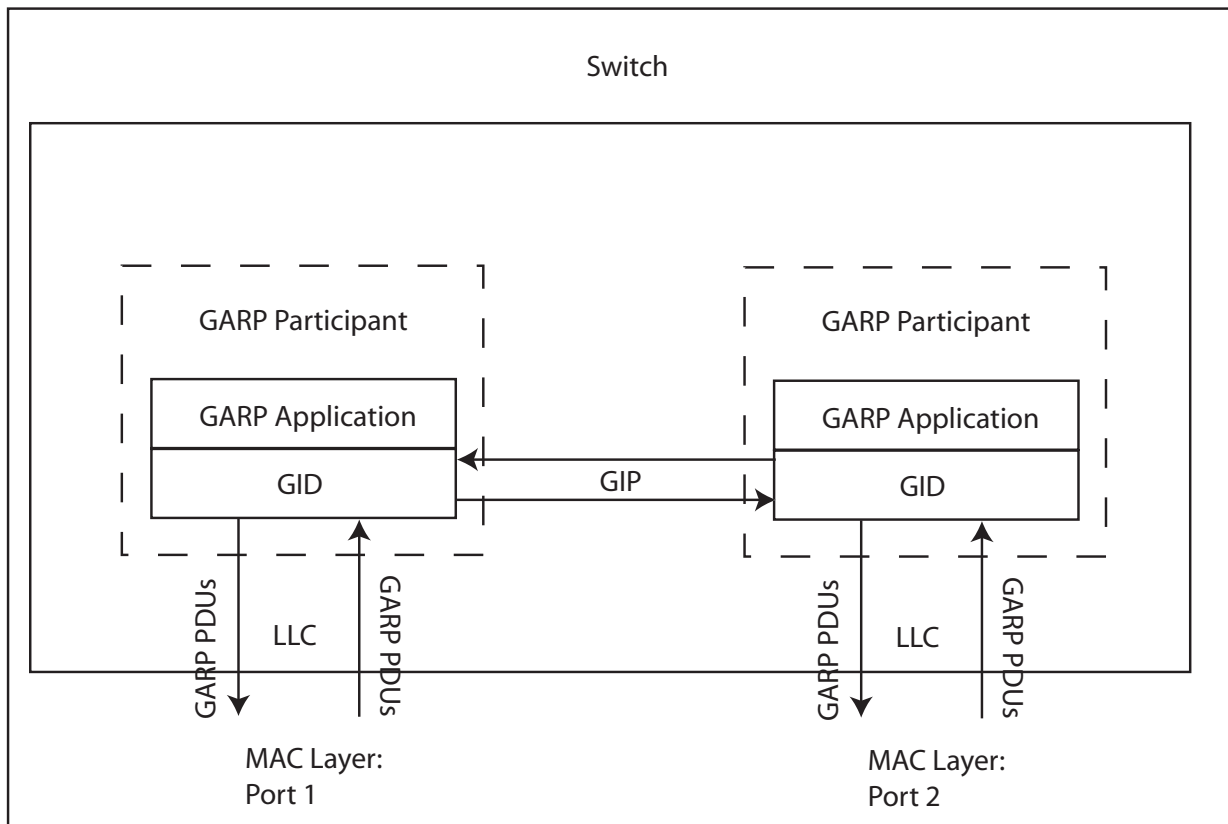


Figure 138 GARP Architecture

The GARP Application component of the GARP Participant is responsible for defining the semantics associated with the parameter values and operators received in GARP PDUs, and for generating GARP PDUs for transmission. The Application makes use of the GID component, and the state machines associated with the operation of GID, in order to control its protocol interactions.

An instance of GID consists of the set of state machines that define the current registration and declaration state of all *attribute* values associated with the GARP Participant. Separate state machines exist for the Applicant and Registrar. This is shown in Figure 139.

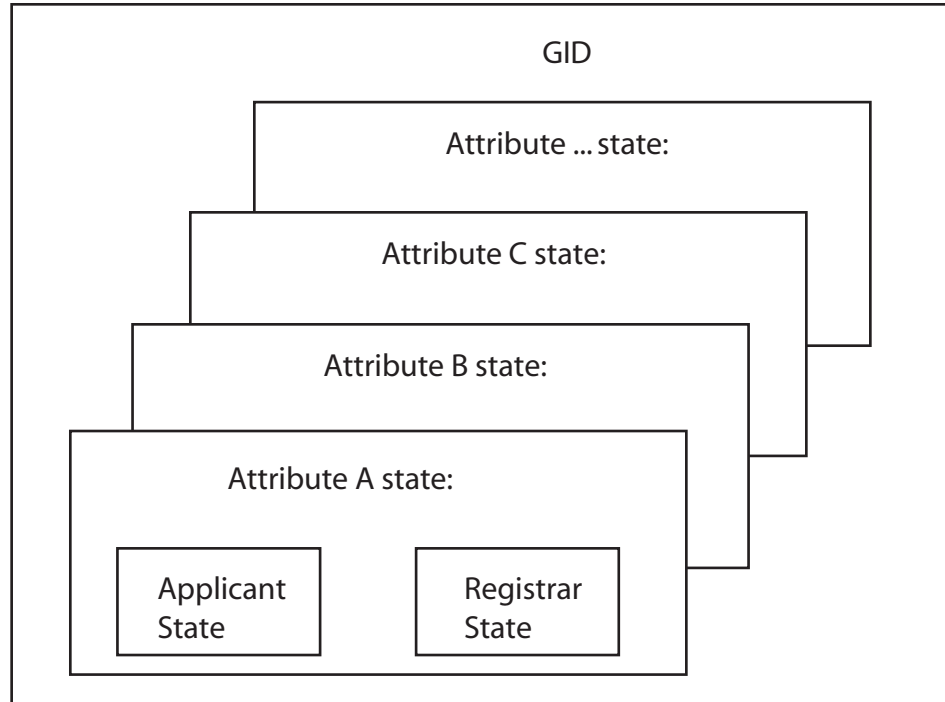


Figure 139 GID Architecture

GARP registers and de-registers *attribute* values through GARP messages sent at the GID level. A GARP Participant that wishes to make a declaration (an Applicant registering an *attribute* value) sends a JoinIn or JoinEmpty message. An Applicant that wishes to withdraw a declaration (de-registering an *attribute* value) sends a LeaveEmpty or LeaveIn message. Following the de-registration of an *attribute* value, the Applicant sends a number of Empty messages. The purpose of the Empty message is to prompt other Applicants to send JoinIn/JoinEmpty messages. For the GARP protocol to be resilient against multiple lost messages, a LeaveAll message is available. Timers are used in the state machines to generate events and control state transitions.

The job of the Applicant is twofold:

- To ensure that this Participant's declarations are registered by other Participants' Registrars
- To ensure that other Participants have a chance to re-declare (rejoin) after anyone withdraws a declaration (leaves).

The Applicant is therefore looking after the interests of all would-be Participants. This allows the Registrar to be very simple.

The job of the Registrar is to record whether an attribute is registered, in the process of being de-registered, or is not registered for an instance of GID.

To control the Applicant state machine, an Applicant Administrative Control parameter is provided. This parameter determines whether or not the Applicant state machine participates in GARP protocol exchanges. The default value has the Applicant participating in the exchanges.

To control the Registrar state machine, a Registrar Administrative Control parameter is provided. Basically this parameter determines whether or not the Registrar state machine listens to incoming GARP messages. The default value has the Registrar listening to incoming GARP messages.

The propagation of information between GARP Participants for the same Application in a switch is carried out by the GIP component. The operation of GIP is dependent upon STP being enabled on a port, as only ports in the STP Forwarding state are eligible for membership to the GIP connected ring. Ports in the GIP connected ring propagate GID Join and Leave requests to notify each other of attribute registrations and de-registrations. The operation of GIP allows ports in the switch to share information between themselves and the LANs/end stations to which the ports are connected.

If a port enters the STP Forwarding state and the GARP application that the port belongs to is enabled, then the port is added to the GIP connected ring for the GARP application. All attributes registered by other ports in the GIP connected ring is propagated to the recently connected port. All attributes registered by the recently connected port is propagated to all other ports in the GIP connected ring.

Similarly, if a port leaves the STP Forwarding state and the GARP application that the port belongs to is enabled, then the port is removed from the GIP connected ring for the GARP application. Prior to removal, GID leave requests are propagated to all other ports in the GIP connected ring if the port to be removed has previously registered an attribute and no other port in the GIP connected ring has registered that attribute. The operations of GIP can be enabled or disabled by user command.

Configuring GVRP

Use the following procedure to configure GVRP.

The timers in the following menus are in increments of centi seconds which is a hundredth of a second.

To configure GVRP, perform the following procedure:

1. From the Main Menu, type **2** to select VLAN Menu.
The VLAN Menu is shown in Figure 130 on page 418.
2. From the VLAN Menu, type **3** to select Configure GARP-GVRP.
The GARP-GVRP Menu is shown in Figure 140.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Production Switch 4

User: Manager                                00:14:33 24-May-2004

                                GARP-GVRP Menu

1 - GVRP Status ..... Disabled
2 - GVRP GIP Status ..... Enabled
3 - GVRP Join Timer ..... 20
4 - GVRP Leave Timer ..... 60
5 - GVRP Leave All Timer .. 1000

P - GVRP Port Parameters
O - Other GVRP Parameters Menu
D - Reset GVRP to Defaults

U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 140 GARP-GVRP Menu

3. Type **1** - GVRP Status to enable or disable GVRP.

The following prompt is displayed:

Enter your new value (E-Enabled, D-Disabled):

4. Choose one of the following:

E to enable GVRP.

D to disable GVRP. This is the default setting.

5. Type **2** - GVRP GIP Status to enable or disable GIP.

Enter your new value (E-Enabled, D-Disabled):

6. Choose one of the following:

E to enable GIP.

D to disable GIP.

Note

Do not disable GIP if you intend to use GVRP. GIP is required to propagate VLAN information among the ports of the switch.



Caution

The following steps change the three GVRP timers. Please note that the settings for these timers must be the same on all GVRP-active network devices.

7. To change the value of the Join Timer, type **3**.

The following prompt is displayed:

```
Enter new value (in centi seconds): [10 to 60] -> 20
```

8. Enter a new value for the Join Timer field in centi seconds which are one hundredths of a second. The default is 20 centiseconds.

If you change this field, it must in relation to the GVRP Leave Timer according to the following equation:

$$\text{Join Timer} \leq (2 \times (\text{GVRP Leave Timer}))$$

9. To set the GVRP Leave Timer, type **4** to select GVRP Leave Timer.

The following prompt is displayed:

```
Enter new value (in centi seconds): [30 to 180] -> 60
```

10. To set the GVRP Leave All Timer, type **5** to select GVRP Leave All Timer. The default is 60 centiseconds.

The following prompt is displayed:

```
Enter new value (in centi seconds): [500 to 3000] -  
> 1000
```

11. Enter a value in centiseconds. The default is 1000 centiseconds.

Enabling or Disabling GVRP on a Port

This procedure enables and disables GVRP on a switch port. The default setting for GVRP on a port is enabled. Only those ports where GVRP is enabled transmit PDUs.

Note

Allied Telesyn recommends disabling GVRP on unused ports and those ports that are connected to GVRP-inactive devices. This is to protect against unauthorized access to restricted areas of your network. For further information, refer to GVRP and Network Security on page 448.

1. From the Main Menu, type **2** to select VLAN Menu.
The VLAN Menu is shown in Figure 130 on page 418.
2. From the VLAN Menu, type **3** to select Configure GARP-GVRP.
The GARP-GVRP menu is shown in Figure 140 on page 453.
3. Type **P** - GVRP Port Parameters to configure the switch ports.
The GVRP Port Parameters Menu is shown in Figure 141.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
                          Production Switch 4
User: Manager                               00:14:33 24-May-2004
                          GVRP Port Parameters
1 - Configure GVRP Port Settings
2 - Display GVRP Port Configuration
R - Return to Previous Menu
Enter your selection?

```

Figure 141 GVRP Port Parameters Menu

4. Type **1** to configure GVRP Port Settings.
The following prompt is displayed:
Enter port-list:

- 5. Enter a port or a list of ports. For information about how to specify ports, see Specifying Ports on page 34.

The Configure GVRP Port Settings Menu is shown in Figure 142.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Production Switch 4
User: Manager                                00:14:33 24-May-2004
Configure GVRP Port Settings
Configuring Port 2.1-8
1 - Port Mode ..... Normal
R - Return to Previous Menu
Enter your selection?
```

Figure 142 Configure GVRP Port Settings Menu

- 6. Type **1** - Port Mode.

The following prompt is displayed:

```
Enter mode (0-Normal, 1-None): [0 to 1] -> 0
```

- 7. Type either **0** to select Normal or **1** to select None. A setting of Normal means the port processes and propagates GVRP information. This is the default setting. A setting of None prevents the port from processing GVRP information and from transmitting PDUs.
- 8. If you want to view the current port settings, from the GVRP Port Parameters menu, type **2** to display the GVRP port configuration.

The Display GVRP Port Configuration Menu is shown in Figure 143.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Production Switch 4
User: Manager                                00:14:33 24-May-2004
Display GVRP Port Configuration
GARP Port Parameters
Mode Normal ..... 2.1-8, 8.1-8
Mode None ..... 3.1-8, 4.1-8, 5.1-8, 6.1-8,9.1, 10.1-8
U - Update
R - Return to Previous Menu
Enter your selection?
```

Figure 143 Display GVRP Port Configuration Menu

9. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Displaying GVRP Parameters and Statistics

To display GVRP counters, database, state machine, and GIP connected ports ring, perform the following procedure:

1. From the Main Menu, type **2** to select VLAN Menu.
The VLAN Menu is shown in Figure 130 on page 418.
2. From the VLAN Menu, type **3** to select Configure GARP-GVRP.
The GARP-GVRP Menu is shown in Figure 140 on page 453.
3. From the GARP-GVRP Menu, type **0** to select Other GVRP Parameters Menu.

The Other GARP Port Parameters Menu is shown in Figure 144.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
                          Production Switch 4
User: Manager                               00:14:33 24-May-2004
                          Other GARP Port Parameters
1 - Display GVRP Counters
2 - Display GVRP Database
3 - Display GIP Connected Ports Ring
4 - Display GVRP State Machine

R - Return to Previous Menu
Enter your selection?
```

Figure 144 Other GARP Port Parameters Menu

Each option is reviewed in a separate subsection below.

GVRP Counters Option 1 - Display GVRP Counters in the Other GARP Port Parameters displays the GVRP Counters Menu (page 1) as shown in Figure 145.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Production Switch 4

User: Manager                                00:14:33 24-May-2004

                                GVRP Counters

Receive:                                Transmit:
-----                                -
Total GARP Packets                    41      Total GARP Packets                    166
Invalid GARP Packets                   0

Discarded:
-----
GARP Disabled                          0      GARP Disabled                          0
Port Not Listening                       0      Port Not Sending                       3117
Invalid Port                            0
Invalid Protocol                        0
Invalid Format                           0
Database Full                           0

N - Next Page
U - Updated Display
R - Return to Previous Menu

Enter your selection?

```

Figure 145 GVRP Counters Menu (page 1)

The statistics span two menus. To display the second menu, type **N** to select Next Page. The second menu is shown in Figure 146. The information in both menus is for display purposes only.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Production Switch 4

User: Manager                                00:14:33 24-May-2004

                                GVRP Counters

Receive:                                     Transmit:
-----                                     -
GARP Messages:
-----
LeaveAll              7          LeaveAll              77
JoinEmpty            0          JoinEmpty             58
JoinIn               68         JoinIn                285
LeaveEmpty            0          LeaveEmpty            1
LeaveIn               0          LeaveIn               0
Empty                5          Empty                 21
Bad Message          0
Bad Attribute        0

P - Previous Page
U - Updated Display
R - Return to Previous Menu

Enter your selection?
    
```

Figure 146 GVRP Counters Menu (page 2)

The GVRP counters in the menus are defined in Table 14.

Table 14 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.

Table 14 GVRP Counters

Parameter	Meaning
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.
Receive GARP Messages: JoinEmpty	Total number of GARP JoinEmpty messages received for all attributes in the GARP application.

Table 14 GVRP Counters

Parameter	Meaning
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: Leaveln	Total number of GARP Leaveln messages received for all attributes in the GARP application.
Transmit GARP Messages: Leaveln	Total number of GARP Leaveln 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.

GVRP Database Option 2 - Display GVRP Database in the Other GARP Port Parameters displays the GVRP Database Menu as shown in Figure 147.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Production Switch 4

User: Manager                                00:14:33 24-May-2004

                                GVRP Database

GARP Application: GVRP
GID index  VLAN ID                Used   GID index  VLAN ID  Used
-----
    0         1                   Yes     1         3       Yes
    2         2                   Yes

U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 147 GVRP Database Menu

The columns in the menu are defined in Table 15. The information is for viewing purposes only.

Table 15 GARP Database Parameters

Parameter	Meaning
GARP Application	Identifies the GARP application, that is, "GVRP".
GID index	Value of the GID index corresponding to the attribute. GID indexes begin at 0. If the GARP application has no attributes presently registered, "No attributes have been registered" is displayed.
VLAN ID	Value of the attribute.
Used	Indicates whether the GID index is currently being used by any port in the GARP application. The definition of "used" is whether the Applicant and Registrar state machine for the GID index are in a non-initialized state, that is, not in {Vo, Mt} state. The value of this parameter is either "Yes" or "No".

GIP Connected Ports Ring

Option 3 - Display GIP Connected Ports Ring in the Other GARP Port Parameters displays the GIP Connected Ports Ring Menu as shown in Figure 148.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Production Switch 4

User: Manager                                00:14:33 24-May-2004

GIP Connected Ports Ring

GARP Application: GVRP
GIP Context ID: 0, STP ID: 0
-----

1.2 -> 1.8 -> 4.4

U - Update Display
R - Return to Previous Menu

Enter your selection?
    
```

Figure 148 GIP Connected Ports Ring Menu

The information in the menu is defined in Table 16. This information is for viewing purposes only.

Table 16 GIP Connected Ports Ring Parameters

Parameter	Meaning
GARP Application	Identifies the GARP application, that is, "GVRP."
GIP Context Index ID	A number assigned to the instance for the GIP context.
STP ID	Present if the GARP application is GVRP; identifies the STP that has these ports connected in the GIP connected ring.
Connected Ring	Ring of connected ports. Only ports presently in the STP Forwarding state are eligible for membership to 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.

GVRP State Machine

Option 4 - Display GVRP State Machine in the Other GARP Port Parameters displays the GVRP State Machine Menu (page 1) as shown in Figure 149.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Production Switch 4

User: Manager                                00:14:33 24-May-2004

GVRP State Machine

Enter a VLAN ID for displaying the state machine: [1 to 4094] -> 1
    
```

Figure 149 GVRP State Machine Menu (page 1)

Entering a VLAN ID displays the GVRP State Machine Menu (page 2) as shown in Figure 150.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Production Switch 4

User: Manager                                00:14:33 24-May-2004

GVRP State Machine

State Machine for VLAN: 1
Port  App  Reg | Port  App  Reg | Port  App  Reg | Port  App  Reg |
-----|-----|-----|-----|
2.1   Qa   Fix | 2.2   Qa   Fix | 2.3   Qa   Fix | 2.4   Qa   Fix |
2.5   Qa   Fix | 2.6   Qa   Fix | 2.7   Qa   Fix | 2.8   Qa   Fix |
3.1   Qa   Fix | 3.2   Qa   Fix | 3.3   Qa   Fix | 3.4   Qa   Fix |
8.1   Qa   Fix | 8.2   Qa   Fix | 8.3   Qa   Fix | 8.4   Qa   Fix |
8.5   Qa   Fix | 8.6   Qa   Fix | 8.7   Qa   Fix | 8.8   Qa   Fix |

U - Update Display
R - Return to Previous Menu

Enter your selection?
    
```

Figure 150 Display GVRP State Machine Menu (page 2)

The information in the menu is defined in Table 17. This information is for viewing purposes only.

Table 17 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 17 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

Table 17 GVRP State Machine Parameters (Continued)

Parameter	Meaning
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.
	Reg
"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.	

Section V

Security Features

The chapters in Section V explain how to configure an AT-8400 switch with security features. The chapters include:

- Chapter 21: Port Security on page 469
- Chapter 22: Web Server on page 477
- Chapter 23: Encryption on page 484
- Chapter 24: Public Key Infrastructure (PKI) on page 501
- Chapter 25: Secure Sockets Layer (SSL) on page 523
- Chapter 26: Secure Shell (SSH) on page 529
- Chapter 27: TACACS+ and RADIUS Protocols on page 540
- Chapter 28: 802.1x Port-based Network Access Control on page 549

Chapter 21

Port Security

This chapter describes port security and provides the procedures for setting port security with a local or Telnet management session. It contains the following sections:

- ❑ Port Security Overview on page 470
- ❑ Configuring Port Security on page 473

Port Security Overview

The port security feature can enhance the security of your network. You can use the feature to control which end nodes can forward frames through the switch.

Note

The port security feature cannot be used on a port that is configured as a supplicant or an authenticator of the port-based network access feature, described in 802.1x Port-based Access Network Control Overview on page 550. When you configure a port as a supplicant or an authenticator, the security level changes to PA (Port Access) Controlled.

There are four levels of port security:

- Automatic
- Limited
- Secured
- Locked

You can set port security on a per port basis. Only one security level can be active on a port at a time.

Automatic The Automatic security mode disables port security on a port. This is the default security level for a port. In this mode, a switch can learn up to 8192 dynamic MAC addresses.

A dynamic MAC address learned by a port operating with this security level is deleted from the MAC address table if the end node becomes inactive. This prevents the table from becoming full of MAC addresses of inactive nodes. The length of time an inactive dynamic MAC address can remain in the table is determined by the MAC aging time.

If you want to include a port in a MAC-Based VLAN, you must set the port security setting to the Automatic security mode. For more information about MAC-Based VLANs, see Chapter 19: Port Security on page 469.

Limited The Limited security level allows you to specify the maximum number of dynamic MAC addresses a port can learn. Once a port has learned its maximum number of addresses, it discards all ingress frames with source MAC addresses not already learned.

When the Limited security mode is activated on a port, all dynamic MAC addresses learned by the port are deleted from the MAC address table. The port then begins to learn new addresses, up to the maximum allowed.

A dynamic MAC address learned on a port operating in the Limited security mode is never timed out from the MAC address table, even when the corresponding end node is inactive. Once the port has learned its maximum number of addresses, it does not learn any new addresses, even when end nodes are inactive.

Static MAC addresses are retained by the port and are not included in the count of maximum dynamic addresses. You can add more static MAC addresses to a port even if the port has already learned its maximum number of dynamic MAC addresses.

Secured The Secured security level instructs a port to forward frames using only static MAC address. The port does not learn any dynamic MAC addresses and deletes any dynamic addressees that it has already learned. Only those end nodes whose MAC addresses have been entered as static addresses can forward frames through the port.

You must enter, either before or after you activate this security level, the static MAC addresses of the end nodes that are allowed to forward frames through the port.

Locked The Lock security level causes a port to immediately stop learning new dynamic MAC addresses. Frames are forwarded using the dynamic MAC addresses that the port has already learned and any static MAC addresses assigned to the port.

Dynamic MAC addresses learned by the port prior to the activation of this security level are never timed out from the MAC address table, even when the corresponding end nodes are inactive. However, the port does not learn new dynamic addresses.

You can add new static MAC addresses to a port operating with this security level.

Note

For background information on MAC addresses and the MAC aging time, refer to MAC Address Overview on page 116.

Security Violations and Intrusion Actions

When you set a port's security level, you can also set the action a port performs in the event it receives an invalid frame. This is referred to as intrusion (intruder) action.

Before defining the intrusion actions, it can help to understand first what constitutes an invalid frame. This differs for each security level, as explained here:

- Limited Security Level - This security level works by setting a maximum number of MAC addresses that a port can learn. An invalid frame for the limited security level is an ingress frame with a new source MAC address after the port has reached its maximum number of dynamic MAC addresses. (A new source MAC address is a MAC address that has not been previously learned by the port.) Also, a MAC address that was not assigned to the port as a static address is considered an invalid frame.
- Secured Security Level - An invalid frame for this security level is an ingress frame with a source MAC address that was not entered as a static address on the port.
- Locked - An invalid frame for this security level is an ingress frame with a source MAC address that the port has not already learned or that was not assigned as a static address.

You can configure what a port does if it receives an invalid frame. Here are the options:

- Discard the invalid frame.
- Discard the invalid frame and send a trap.
- Discard the invalid frame, send a trap, and disable the port.

Configuring Port Security

To configure port security, do the following:

To set a switch's port security level, perform the following procedure:

1. From the Main Menu, type **6** to select Security Menu.

The Security Menu is shown in Figure 151.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142
User: Manager                                00:14:33 22-Mar-2004
Security Menu
1 - Keys/Certificates Configuration
2 - Local Port Security
3 - Port Access Control
4 - Secure Socket Layer (SSL)
5 - Secure Shell (SSH)
6 - Server Based Authentication

R - Return to Previous Menu
Enter your selection?

```

Figure 151 Security Menu

Note

Options 1, 4, and 5 in the Security Menu shown in Figure 151 are not available in all versions of the AT-S60 management software.

2. From the Security Menu, select Local Port Security.

The Local Port Security Menu is shown in Figure 152.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142
User: Manager                                00:14:33 15-Jan-2004
Local Port Security
1 - Configure Port Security
2 - Display Port Security

R - Return to Previous Menu
Enter your selection?

```

Figure 152 Local Port Security Menu

3. Type **1** to select Configure Port Security.

The following prompt is shown:

```
Enter port-list:
```

4. Enter the port(s) you want to configure. Then press Return.

For information about how to specify ports, see *Specifying Ports* on page 34.

The Configure Port Security Menu is shown in Figure 153.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142

User: Manager                                00:14:33 15-Jan-2004

          Configure Port Security
Configuring Port Security 3.1-2
1 - Security Mode ..... Automatic

D - Set Default Port Security
R - Return to Previous Menu

Enter your selection?
```

Figure 153 Configure Port Security Menu

Note

A security mode of PA Controlled for a port means that the port is functioning as a supplicant or authenticator of the port-based network access feature, described in 802.1x Port-based Access Network Control Overview on page 550. You cannot change the security mode of a port if its security mode is PA Controlled with the Port Security feature. To change the PA Controlled setting, you need to change the configuration of a port-- removing its supplicant or authenticator status.

5. Press **1** to change the port security on your specified port list.

The following prompt appears:

```
Enter new mode (A-Automatic, L-Limited, S-Secured,
K-locKed) :
```

6. Select the desired security level by typing the corresponding letter and then pressing Return. For definitions of the security levels, refer to *Port Security Overview* on page 470.

If you selected Automatic, which disables port security, return to the Main Menu to save your changes.

If you selected one of the other security levels, several new menu options are added to the Configure Port Security menu, as shown in Figure 154.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142

User: Manager                                00:14:33 15-Jan-2004

Configure Port Security 3.1-2
1 - Security Mode ..... Limited
2 - Intrusion Action ..... Discard
3 - Port Participating ..... No
4 - MAC Limit ..... 100

D - Set Default Port Security
R - Return to Previous Menu

Enter your selection?

```

Figure 154 Configure Port Security Menu

Note

Option **4** - MAC Limit appears only for the Limited security level.

7. To set the intrusion action for the port, do the following:

- a. Type **2** to select Intrusion Action.

The following prompt appears:

```
Enter intrusion action: (N-No Action(Discard),
T-Trap, D-Disable):
```

- b. Select the desired intrusion action:

N - No Action (Discard): The port discards an invalid frame. This is the default.

T - Trap: The port discards an invalid frame and sends a trap.

D - Disable: The port discards an invalid frame, sends a trap, and disables the port.

8. If you set the Intrusion Action parameter to trap or disable, type **3** to toggle the Port Participating option to Yes. This parameter allows the switch to send traps (if Intrusion Action is set to trap) or disables the port (if Intrusion Action is set to disable).

If you set Port Participating to No, the switch will not send traps (if Intrusion Action is set to trap) or it will allow the port to be enabled (if Intrusion Action is set to disable).

9. If you selected the Limited security mode for the port, do the following to specify the maximum number of dynamic MAC addresses you want the port to be able to learn:

- a. Type **4** to select MAC Limit.

The following prompt appears:

```
Enter port security threshold: [1 to 256] -> 100
```

- b. Enter the maximum number of dynamic MAC addresses you want the port to learn. The range is 1 to 256. The default is 100.

Note

The **D** - Select Default Port Security option in the menu sets the security mode for the port to the default value of Automatic.

10. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.
11. If you configured a port with the Secure security level, you must enter the static MAC addresses of the end nodes that can send packets through the port. For instructions on how to add static MAC addresses, refer to Adding Static Unicast and Multicast MAC Addresses on page 122.

Chapter 22

Web Server

The chapter provides an overview of the web server feature. In addition, it describes how to configure the switch as a secure web server as well as how to create self-signed and Certificate Authority (CA) certificates. It contains the following sections:

- ❑ Web Server Overview on page 478
- ❑ Configuring the Web Server for Security Features on page 479
- ❑ Configuring SSL Certificates on page 481

Web Server Overview

By default, the switch is configured as a non-secure web server. The web server feature allows you to configure the switch as a web server with advanced SSL security. In addition, you can use the web server feature to create self-signed and CA certificates. You create self-signed certificates for use within an organization. CA certificates are used between organizations, often over the Internet.

This chapter contains two sections:

- ❑ Configuring the Web Server for Security Features on page 479 provides a procedure to enable and configure the web server.
- ❑ Configuring SSL Certificates on page 481 for provides an overview of the procedures required to create self-signed and CA certificates.

Protocols Supported

The switch supports both several protocols. The switch supports the following HTTP and HTTPs protocols:

- ❑ HTTP v1.0 and v1.1 protocols
- ❑ HTTPS v1.0 and v1.1 protocols running over SSL (HTTPS)

The switch supports the following SSL protocols:

- ❑ SSL version 1.0
- ❑ SSL version 2.0
- ❑ TLS (Transmission Layer Security) version 1.0

Configuring the Web Server for Security Features

This procedure allows you to enable, disable, and configure the web server feature using a local or Telnet management session. In addition, you can enable the SSL protocol on the web server using this procedure. The default configuration for the switch is as a non-secure web server.

Note

Before you can configure the web server, you must disable it. Then configure the web server settings and, finally, enable the web server.

To configure the web server, perform the following procedure:

1. From the Main Menu, type **5** to select System Menu.
The System Menu is shown in Figure 5 on page 51.
2. From the System Menu, type **1** to select Configure System.
The Configure System Menu is shown in Figure 11 on page 59.
3. From the Configure System menu, type **1** to select Configure System Software.
The Configure System Software Menu is shown in Figure 12 on page 60.
4. From the Configure System Software menu, type **5** to select Configure Web Server.

The Web Server Configuration Menu is shown in Figure 155.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142

User: Manager                                00:14:33 15-Jan-2004

Web Server Configuration

1 - Status ..... Enabled
2 - Mode ..... HTTP
3 - Port Number ..... 80
4 - SSL Key ID

R - Return to Previous Menu

Enter your selection?

```

Figure 155 Web Server Configuration Menu

5. Type **1** to select Status to enable or disable the web server. To configure the web server, you need to first disable it.

Toggle between the following values:

Enabled - enables the web server. This is the default setting.

Disabled - disables the web server.

6. Type **2** to select Mode to determine the mode of the web server.

The following prompt appears:

```
Enter Web Server Mode (1 - HTTP, 2 - HTTPS):
[1 to 2] ->
```

Choose from the following selections:

1 - HTTP to select the HTTP mode for the web server. This is the default value.

2 - HTTPS to select the HTTPS secure mode web server. By selecting this value, you are enabling the SSL protocol on the web server.

Note

The SSL Key ID field only appears when you configure the Mode field as HTTPS.

The following prompt appears:

```
Enter Port Number [1 to 65531]-> 443
```

7. Enter a port number.

The default HTTPS web server port number is 443.

The following prompt appears:

```
Enter SSL Key ID ->
```

8. Enter an SSL Key ID.

Enter a Key Pair ID that you configured in the Configuring Keys for Encryption on page 491.

9. Type **1** to select Status to enable the web server

Select **Enabled** to enable the web server.

10. After making changes, type **R** to until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Configuring SSL Certificates

The high-level configuration procedures included in this section describe:

- ❑ Configuring Self-Signed Certificates on page 481
- ❑ Configuring CA Certificates on page 482

You configure self-signed certificates to create certificates that are used within your organization, often within your own network. You configure Certificate Authority (CA) certificates for use over the Internet.

Note

If you are learning to create certificates, Allied Telesyn recommends you first create a self-signed certificate.

Both of the procedures provided here are high-level procedures that reference several other chapters within this manual. Both procedures refer to sections in the following chapters:

- ❑ Chapter 23: Encryption on page 484
- ❑ Chapter 24: Public Key Infrastructure (PKI) on page 501
- ❑ Chapter 25: Secure Sockets Layer (SSL) on page 523

You may want to read the introductory material in the above chapters for definitions of pertinent terms.

Configuring Self-Signed Certificates

To configure a self-signed certificate, perform the following procedure:

1. Login with a Manager login id.
2. Create an RSA key pair for this switch.

To create an RSA key pair, see [Configuring Keys for Encryption](#) on page 491.

3. Set the switch's distinguished name.

To configure a distinguished name for a switch, see [Configuring Keys for Encryption](#) on page 491.

4. Set the Universal Coordinated Time (UTC).

To set the time, see [Setting the System Time](#) on page 59.

5. Create a self-signed certificate for the switch.

To create a PKI certificate without contacting a CA for browsing to the GUI, see [Configuring Certificates](#) on page 508.

**Warning**

Using this command creates a certificate that is only suitable for secure switch management via the GUI. A pop-up message appears in the browser window warning that the certificate is not issued by a trusted authority. For details, see Chapter 24: **Web Server** page 477.

6. Load self-signed switch certificate to the certificate database.

To load the signed switch certificate onto the switch, see Adding Certificates to the Database on page 513.

Note

Make sure you have a valid IP address for your web server.

7. Enable SSL on the HTTP Web server

To enable SSL on the HTTP server with a previously created SSL Key, use the procedure described in Configuring the Web Server for Security Features on page 479.

Configuring CA Certificates

To create a CA certificate, you perform many of the same steps as you did when you created a self-signed certificate. Then you generate an enrollment request. After you upload the enrollment request, you apply for a certificate from a known certificate authority such as VeriSign (www.verisign.com). Then, you use this certificate to deploy an AT-8400 Series switch on a commercial network.

To configure a CA Certificate on your switch, perform the following procedure:

1. Login with a Manager login id.
2. Create an RSA key pair for this switch.

To create an RSA key pair, see Configuring Keys for Encryption on page 491.

3. Set the switch's distinguished name.

To configure a distinguished name for a switch, see Configuring Keys for Encryption on page 491.

4. Set the Universal Coordinated Time (UTC).

To set the time, see the procedure in Setting the System Time on page 59.

5. Generate an enrollment request.

See the procedure in Generating Enrollment Requests on page 521.

6. Use TFTP to upload an enrollment request.
See [Downloading Files](#) on page 172.
7. Email enrollment request file to a Certificate Authority such as VeriSign.
8. Certificate Authority issues a CA certificate for your switch.
9. Add certificate to the certificate database on the switch.
See [Adding Certificates to the Database](#) on page 513.
10. Repeat steps 7 through 9 as needed, depending on the certificate chain for your switch.

Chapter 23

Encryption

This chapter contains a description of encryption and procedures for creating keys for encryption on a local or Telnet management session on an AT-8400 Series switch. It contains the following sections:

- ❑ Encryption Overview on page 485
- ❑ Data Encryption on page 486
- ❑ Data Authentication on page 489
- ❑ Key Exchange Algorithms on page 490
- ❑ Configuring Keys for Encryption on page 491

Note

The Encryption feature appears in the AT-S60 version 2.1.0 software only.

Encryption Overview

This chapter describes the data security services available on the switch, how the services are provided, the switch network functions which use these services, and how to monitor the services.

The encryption, or ENCO, feature provides encryption to other switch software modules (referred to as user modules).

The ENCO feature provides the following data security services:

- data encryption
- data authentication
- key exchange algorithms
- key creation and storage

The procedures in this chapter discuss how to configure a distinguish name and keys for encryption. To configure SSL, there are additional procedures you need to configure. For an comprehensive procedure that describes all the steps necessary for configuring SSL, see [Configuring SSL Certificates](#) on page 481.

Data Encryption

Data encryption for switches is driven by the need for organizations to keep sensitive data private and secure. Data encryption operates by applying an encryption algorithm and key to the original data (the plaintext) to convert it into an encrypted form (the ciphertext). The ciphertext produced by encryption is a function of the algorithm used and the key. Since it is easy to discover what type of algorithm is being used, the security of an encryption system relies on the secrecy of its key information. When the ciphertext is received by the remote router, the decryption algorithm and key are used to recover the original plaintext. Often, a checksum is added to the data before encryption. The checksum allows the validity of the data to be checked on decryption.

There are two main classes of encryption algorithm in use—symmetrical encryption and asymmetrical encryption.

Symmetrical Encryption

Symmetrical encryption refers to algorithms in which a single key is used for both the encryption and decryption processes. Anyone who has access to the key used to encrypt the plaintext can decrypt the ciphertext. Because the encryption key must be kept secret to protect the data, these algorithms are also called private, or secret key algorithms. The key can be any value of the appropriate length.

DES Encryption Algorithms

The most common symmetrical encryption system is the *Data Encryption Standard* (DES) algorithm (FIPS PUB 46). The DES algorithm has withstood the test of time and proved itself to be a highly secure encryption algorithm. To fully conform to the DES standard, the actual data encryption operations must be carried out in hardware. Software implementations can only be DES-compatible, not DES-compliant. The DES algorithm has a key length of 56 bits and operates on 64-bit blocks of data. DES can be used in the following modes:

- ❑ **Electronic Code Book (ECB)** is the fundamental DES function. Plaintext is divided into 64-bit blocks which are encrypted with the DES algorithm and key. For a given input block of plaintext ECB always produces the same block of ciphertext.
- ❑ **Cipher Block Chaining (CBC)** is the most popular form of DES encryption. CBC also operates on 64-bit blocks of data, but includes a feedback step which chains consecutive blocks so that repetitive plaintext data, such as ASCII blanks, does not yield identical ciphertext. CBC also introduces a dependency between data blocks which protects against fraudulent data insertion and replay attacks. The feedback for the first block of data is provided

by a 64-bit Initialization Vector (IV). This is the DES mode used for the switch's data encryption process.

- ❑ **Cipher FeedBack (CFB)** is an additive-stream-cipher method which uses DES to generate a pseudo-random binary stream that is combined with the plaintext to produce the ciphertext. The ciphertext is then fed back to form a portion of the next DES input block.
- ❑ **Output FeedBack (OFB)** combines the first IV with the plaintext to form ciphertext. The ciphertext is then used as the next IV.

The DES algorithm has been optimized to produce very high speed hardware implementations, making it ideal for networks where high throughput and low latency are essential.

Triple DES Encryption Algorithms

The Triple DES (3DES) encryption algorithm is a simple variant on the DES CBC algorithm. The DES function is replaced by three rounds of that function, an encryption followed by a decryption followed by an encryption. This can be done by using either two DES keys (112-bit key) or three DES keys (168-bit key).

The two-key algorithm encrypts the data with the first key, decrypts it with the second key and then encrypts the data again with the first key. The three-key algorithm uses a different key for each step. The three-key algorithm is the most secure algorithm due to the long key length.

There are several modes in which Triple DES encryption can be performed. The two most common modes are:

- ❑ **Inner CBC mode** encrypts the entire packet in CBC mode three times and requires three different initial is at ion vectors (IV's).
- ❑ **Outer CBC mode** triple encrypts each 8-byte block of a packet in CBC mode three times and requires one IV.

Asymmetrical (Public Key) Encryption

Asymmetrical encryption algorithms use two keys—one for encryption and one for decryption. The encryption key is called the public key because it cannot be used to decrypt a message and therefore does not have to be kept secret. Only the decryption, or private key, needs to be kept secret. The other name for this type of algorithm is public key encryption. The public and private key pair cannot be randomly assigned, but must be generated together. In a typical scenario, a decryption station generates a key pair and then distributes the public key to encrypting stations. This distribution does not to be kept secret, but it must be protected against the substitution of the public key by a malicious third party. Another use for asymmetrical encryption is as a

digital signature. The signature station publishes its public key, and then signs its messages by encrypting them with its private key. To verify the source of a message, the receiver decrypts the messages with the published public key. If the message that results is valid, then the signing station is authenticated as the source of the message.

The most common asymmetrical encryption algorithm is RSA. This algorithm uses mathematical operations which are relatively easy to calculate in one direction, but which have no known reverse solution. The security of RSA relies on the difficulty of factoring the modulus of the RSA key. Because typical key lengths of 512 bits or greater are used in public key encryption systems, decrypting RSA encrypted messages is almost impossible using current technology.

Asymmetrical encryption algorithms require enormous computational resources, making them very slow when compared to symmetrical algorithms. For this reason they are normally only used on small blocks of data (for example, exchanging symmetrical algorithm keys), and not for entire data streams.

Data Authentication

Data authentication for switches is driven by the need for organizations to verify that sensitive data has not been altered.

Data authentication operates by calculating a Message Authentication Code (MAC), commonly referred to as a *hash*, of the original data and appending it to the message. The MAC produced is a function of the algorithm used and the key. Since it is easy to discover what type of algorithm is being used, the security of an authentication system relies on the secrecy of its key information. When the message is received by the remote switch, another MAC is calculated and checked against the MAC appended to the message. If the two MACs are identical, the message is authentic.

Typically a MAC is calculated using a keyed one-way hash algorithm. A keyed one-way hash function operates on an arbitrary-length message and a key. It returns a fixed length hash. The properties which make the hash function one-way are:

- it is easy to calculate the hash from the message and the key
- it is very hard to compute the message and the key from the hash
- it is very hard to find another message and key which give the same hash

The two most commonly used one-way hash algorithms are MD5 (Message Digest 5, defined in RFC 1321) and SHA-1 (Secure Hash Algorithm, defined in FIPS-180-1). MD5 returns a 128-bit hash and SHA-1 returns a 160-bit hash. MD5 is faster in software than SHA-1, but SHA-1 is generally regarded to be slightly more secure.

HMAC is a mechanism for calculating a keyed Message Authentication Code which can use any one-way hash function. It allows for keys to be handled the same way for all hash functions and it allows for different sized hashes to be returned.

Another method of calculating a MAC is to use a symmetric block cypher such as DES in CBC mode. This is done by encrypting the message and using the last encrypted block as the MAC and appending this to the original message (plain-text). Using CBC mode ensures that the whole message affects the resulting MAC.

Key Exchange Algorithms

Key exchange algorithms are used by switches to securely generate and exchange encryption and authentication keys with other switches. Without key exchange algorithms, encryption and authentication session keys must be manually changed by the system administrator. Often, it is not practical to change the session keys manually. Key exchange algorithms enable switches to re-generate session keys automatically and on a frequent basis.

The most important property of any key exchange algorithm is that only the negotiating parties are able to decode, or generate, the shared secret. Because of this requirement, public key cryptography plays an important role in key exchange algorithms. Public key cryptography provides a method of encrypting a message which can only be decrypted by one party. A switch can generate a session key, encrypt the key using public key cryptography, transmit the key over an insecure channel, and be certain that the key can only be decrypted by the intended recipient. Symmetrical encryption algorithms can also be used for key exchange, but commonly require an initial shared secret to be manually entered into all switches in the secure network.

The *Diffie-Hellman* algorithm is one of the more commonly used key exchange algorithms. It is not an encryption algorithm because messages cannot be encrypted using Diffie-Hellman. Instead, it provides a method for two parties to generate the same shared secret with the knowledge that no other party can generate that same value. It uses public key cryptography and is commonly known as the first public key algorithm. Its security is based on the difficulty of solving the *discrete logarithm problem*, which can be compared to the difficulty of factoring very large integers.

A Diffie-Hellman algorithm requires more processing overhead than RSA-based key exchange schemes, but it does not need the initial exchange of public keys. Instead, it uses published and well tested public key values. The security of the Diffie-Hellman algorithm depends on these values. Public key values less than 768 bits in length are considered to be insecure.

A Diffie-Hellman exchange starts with both parties generating a large random number. These values are kept secret, while the result of a public key operation on the random number is transmitted to the other party. A second public key operation, this time using the random number and the exchanged value, results in the shared secret. As long as no other party knows either of the random values, the secret is safe.

Configuring Keys for Encryption

Use the following procedures to configure, modify, export, and import keys for encryption.

- Configuring a Distinguished Name and Keys on page 491
- Modifying and Deleting Keys on page 495
- Exporting Keys on page 497
- Importing Keys on page 498

For an comprehensive procedure that describes all the procedures necessary for configuring keys for encryption, see Configuring SSL Certificates on page 481.

Configuring a Distinguished Name and Keys

The following procedure describes how to configure a distinguished name and a key. After you create a key, you need to generate it. Key generation is a CPU-intensive process.



Caution

Key generation is a CPU-intensive process. Allied Telesyn International recommends you create keys when the switch is not connected to a network because this process may affect switch behavior

A *distinguished name* specifies the physical address of the subject of a certificate, much like a street address. It consists of a list of values that uniquely identifies the subject of a certificate. The Certification Authority may require that a particular distinguished name is used. Otherwise, use a logical distinguished name.

To assign a distinguished name and create keys for encryption, perform the following procedure:

1. From the Main Menu, type **6** to select Security Menu.
The Security Menu is shown in Figure 151 on page 473.
2. From the Security menu, select the Keys/Certificate Configuration menu.

The Keys/Certificate Configuration Menu is shown in Figure 156.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142
User: Manager                                00:14:33 30-Apr-2004
Keys/Certificate Configuration

1 - Distinguished Name .....
2 - Key Management
3 - Public Key Infrastructure (PKI) Configuration
R - Return to Previous Menu

Enter your selection?
```

Figure 156 Keys/Certificate Configuration Menu

3. To configure a distinguished name, select **1 - Distinguished Name**

The list of values that specify a distinguished name are:

- common name (cn), organization name(ou), organization (o), locality (l), and state-or-province-name (st) are all strings consisting of printable characters with the exception of quotation marks. To use the following special characters {,=,+<>#;\<CR>} type a\ before the character.
- country-name (c) is a string consisting of any printable characters. Country names are generally given in the form of the two-letter ISO 3166 code for the country, for example, us, de, or nz.

An example of a distinguished name for Janet Bloggs who works in Operations at Arctic Company in Fairbanks, Alaska is:

cn=Janet Bloggs, ou=Operations, o=Arctic Company,
l=Fairbanks, s=Alaska, c=us

4. To configure keys, select **2 - Key Management**.

The Key Management Menu is shown in Figure 157.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142
User: Manager                                00:14:33 30-Apr-2004
Key Management

ID      Algorithm  Length  Digest      Description
-----
150     RSA-Public  512     E3D1221D   atiwebserver150
200     RSA-Public  512     E3D1351D   atiwebserver250
250     RSA-Private 512     E3D1561D   atiwebserver350
300     RSA-Private 512     E3D1745D   atiwebserver450

1 - Create Key
2 - Delete Key
3 - Modify Key
4 - Export Key To File
5 - Import Key To File

N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 157 Key Management Menu

Note

The Digest field indicates the CRC32 value of the MD5 digest of the public key.

5. To create an RSA- private key, type **1** - Create Key.

The Create Key Menu is shown in Figure 158.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142

User: Manager                                00:14:33 30-Apr-2004

                                Create Key

1 - Key ID ..... 0
2 - Key Type ..... RSA - Private
3 - Key Length ..... 512
4 - Key Description .... WebServer214
5 - Generate Key

U- Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 158 Create Key Menu

Note

Once you have configured values for one or more of the parameters on the Create Key menu, type **5** - Generate Key to save your configuration. If you do not generate a key after you configure the Create Key parameters, your configuration is lost.

6. Type **1** to specify a key ID.

The following prompt is displayed:

```
Enter Key Id -> [0 to 65535] -> 0
```

7. Enter a key id.

Note

Menu item **2** - Key Type is for display purposes only. You cannot change this field.

8. Type **3** to change the key length.

The following message is displayed:

```
Enter Key Length ->[512 to 1536] -> 512
```

9. Enter a key length in increments of 256.

To configure host and server keys for SSH, there are guidelines regarding the length of the keys. The bit size of the host and server keys must differ by 128 bits. The recommended bit size for a server key is 768 bits. While the minimum bit size of the server key is 512 bits. The recommended size for the host key is 1024 bits.

10. Type **4** to create a key description.

The following prompt is displayed:

```
Enter new Description ->
```

11. Enter a description of the web server the key is used to protect, such as webserver46. You can enter up to 127 alphanumeric values including spaces. Control characters are not permitted.

12. Type **5** to generate a key.

To save the data you configured in the above steps, you must generate a key. The following message is displayed:

```
Key generation will take some time. Please wait...
```

Modifying and Deleting Keys

Use this procedure to modify the Key Description field and delete keys for encryption:

1. From the Main Menu, type **6** to select Security Menu.

The Security Menu is shown in Figure 151 on page 473.

2. From the Security menu, select the Keys/Certificate Configuration menu.

The Keys/Certificate Configuration Menu is shown in Figure 156 on page 492.

3. From the Keys/Certificate Configuration Menu, type **2** to select Key Management.

The Key Management menu is shown in Figure 157 on page 493.

4. From the Key Management Menu, type **3** to select Modify Key.

The following prompt is displayed:

```
Enter Key Id to modify -> [0 to 65535] -> 0
```

5. Enter the Key ID of the key you want to modify.

The following message is displayed.

```
Enter new Description ->
```

6. Enter a description of the web server the key is used to protect, such as webserver46. You can enter up to 127 alphanumeric values including spaces. Control characters are not permitted.

The following message appears:

```
Please wait while the information is being updated...Done!
```

7. To delete a key, select **2** - Delete Key from the Key Management menu.

The following message is displayed:

```
Enter Key Id to delete -> [0 to 65535] -> 0
```

8. Enter the Key Id that you want to delete.

The following message appears:

```
Key deletion will take some time. Please wait...
```


Exporting Keys

The following procedure allows you to export a key to a file. When you export RSA-Private keys, only the public key is output to a file.

Use the following procedure to export RSA- Public keys:

Note

You cannot export RSA-Private keys.

1. From the Main Menu, type **6** to select Security Menu.
The Security Menu is shown in Figure 151 on page 473.
2. From the Security menu, select the Keys/Certificate Configuration menu.
The Keys/Certificate Configuration menu is shown in Figure 156 on page 492.
3. From the Key Management Menu, type **4** to select Export Key to File to export an RSA - private key.

The Export Key to File Menu is shown in Figure 159.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142

User: Manager                                00:14:33 30-Apr-2004

Export Key to File Menu

1 - Key ID ..... 0
2 - Key Type ..... RSA-Public
3 - Key File Format ... HEX
4 - Key File Name
5 - Export Key To File
R - Return to Previous Menu

Enter your selection?

```

Figure 159 Export Key to File Menu

4. Type **1** to select Key ID to specify the key to be exported to a file.
5. The following prompt is displayed:

```
Enter Key ID -> [0 to 65535] ->
```

6. Enter a Key ID.

The Key ID must be a Key Pair ID that you configured in the Key Management Menu. See Figure 157 on page 493.

Note

Key Type is a read-only field. You cannot change this value.

7. To specify the format of the key, type **3** to select Key File Format.
8. Chose one of the following options by pressing **3** repeatedly:
 - HEX** - Indicates an internal format for storing files. Select this value for SSL configuration. This is the default.
 - SSH** - Indicates a format for a Secure Shell (SSH) environment. Select this value for a SSH server or client.
 - SSH2** - Indicates a format for a Secure Shell 2 environment. Select this value for a SSH2 server or client.
9. Type **4** to select Key File Name to specify the filename of the key. The key filename must have a .key extension.
10. Type **5** to select Export Key to File to export the key to a file. The following message is displayed:


```
Key Export in Progress. Please wait...Done
To view the list of key files, see the File Menu.
```

Importing Keys

Use the following procedure to import RSA-Public keys. If you have a file that contains both RSA-Public and RSA-Private keys, you can use this procedure to import the RSA-Public key; however, the RSA-Private key information is ignored.

To import RSA- Public keys, perform the following procedure:

1. From the Main Menu, type **6** to select Security Menu. The Security Menu is shown in Figure 151 on page 473.
2. From the Security menu, select the Keys/Certificate Configuration menu. The Keys/Certificate Configuration Menu is shown in Figure 156 on page 492.
3. From the Key Management Menu, type **5** to select Import Key From File to import a RSA - Public key.

The Import Key From File Menu is shown in Figure 160.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142
User: Manager                                00:14:33 30-Apr-2004

Import Key From File Menu

1 - Key ID ..... 0
2 - Key Type ..... RSA-Public
3 - Key File Format ... HEX
4 - Key File Name .....
5 - Export Key To File

R - Return to Previous Menu

Enter your selection?

```

Figure 160 Import Key From File Menu

4. Type **1** to select Key ID to specify the filename of the key to be added to the key database.

5. The following prompt is displayed:

```
Enter Key ID -> [0 to 65535] ->
```

6. Enter a Key ID.

This must be a new Key ID. It cannot match any of the Key Pair IDs that you configured in the Key Management Menu in Figure 157 on page 493.

Note

Key Type is a read-only field. You cannot change this value.

7. Type **3** to select Key File Format to specify the format of the key.
8. Press **3** to toggle between the following options:
 - HEX** - Indicates an internal format for storing files. Select this value for SSL configuration. This is the default.
 - SSH** - Indicates a format for a Secure Shell (SSH) environment. Select this value for a SSH server or client.
 - SSH2** - Indicates a format for a Secure Shell 2 environment. Select this value for a SSH2 server or client.
9. Type **4** to select Key File Name to specify the name of the key file. The key filename must have a .key extension. The key file must reside in the same directory as the AT-S60 software.

10. Type **5** to select Import Key From File to import a key to the switch from an external file.

The following message is displayed:

```
Key Import in Progress. Please wait...Done
```

After you receive this message, the key is added to the Key Management database. See the Key Management Menu in Figure 157 on page 493.

Chapter 24

Public Key Infrastructure (PKI)

This chapter describes the Public Key Infrastructure (PKI) feature and provides procedures for configuring certificates for web server security. This chapter contains the following sections:

- ❑ Public Key Infrastructure Overview on page 502
- ❑ PKI Implementation on page 507
- ❑ Configuring Certificates on page 508
- ❑ Generating Enrollment Requests on page 521

Note

The PKI feature appears in the AT-S60 version 2.1.0 software only.

Public Key Infrastructure Overview

This chapter describes the Public Key Infrastructure (PKI) feature, Allied Telesyn's implementation of the feature, and how to configure PKI for web server security. The PKI feature is part of the switch's suite of security modules, and consists of a set of tools for managing and using certificates.

The tools that make up the Public Key Infrastructure allow the switch to securely exchange public keys, while being sure of the identity of the keyholder.

The switch acts as an End Entity (EE) in an X.509 certificate-based PKI. More specifically, the switch can communicate with Certification Authorities (CAs) and Certificate Repositories to request, retrieve and verify X.509 certificates. The switch allows protocols running on the switch, such as ISAKMP, access to these certificates. The following sections of this chapter summarize these concepts and describe the switch's implementation of them.

This chapter contains the following procedures for creating and modifying certificates:

- ❑ Creating Certificates on page 508
- ❑ Adding Certificates to the Database on page 513
- ❑ Deleting and Modifying Certificates on page 515
- ❑ Viewing Certificates on page 518
- ❑ Generating Enrollment Requests on page 521

These procedures are part of a comprehensive procedure to create certificates on the switch. See *Configuring SSL Certificates* on page 481 for a list of all the procedures you must complete to create certificates on the switch.

Public Keys

Public key encryption involves the generation of two keys for each user, one private and one public. Material encrypted with a private key can only be decrypted with the corresponding public key, and vice versa. An individual's private key must be kept secret, but the public key may be distributed as widely as desired, because it is impossible to calculate the private key from the public key. The advantage of public key encryption is that the private key need never be exchanged, and so can be kept secure more easily than a shared secret key.

Message Encryption

One of the two main services provided by public key encryption is the exchange of encrypted messages. For example, user 1 can send a secure message to user 2 by encrypting it with user 2's public key. Only user 2 can decrypt it, because only user 2 has access to the corresponding private key.

Digital Signatures

The second main service provided by public key encryption is digital signing. Digital signatures both confirm the identity of the message's supposed sender and protect the message from tampering. Therefore they provide message authentication and non-repudiation. It is very difficult for the signer of a message to claim that the message was corrupted, or to deny that it was sent.

Both the exchange of encrypted messages and digital signatures are secure only if the public key used for encryption or decryption belongs to the message's expected recipient. If a public key is insecurely distributed, it is possible a malicious agent could intercept it and replace it with the malicious agent's public key (the Man-in-the-Middle attack). To prevent this, and other attacks, PKI provides a means for secure transfer of public keys by linking an identity and that identity's public key in a secure certificate.



Caution

Although a certificate binds a public key to a subject to ensure the public key's security, it does not guarantee that the security of the associated private key has not been breached. A secure system is dependent upon private keys being kept secret, by protecting them from malicious physical and virtual access.

Certificates

A *certificate* is an electronic identity document. To create a certificate for a subject, a trusted third party (known as the Certification Authority) verifies the subject's identity, binds a public key to that identity, and digitally signs the certificate. A person receiving a copy of the certificate can verify the Certification Authority's digital signature and be sure that the public key is owned by the identity in it.

The switch can generate a self-signed certificate but this should only be used with an SSL enabled HTTP server, or where third party trust is not required.

X.509 Certificates

The X.509 specification specifies a format for certificates. Almost all certificates use the X.509 version 3 format, described in RFC 2459, *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*. This is the format which is supported by the switch.

An X.509 v3 certificate consists of:

- A serial number, which distinguishes the certificate from all others issued by that issuer. This serial number is used to identify the certificate in a Certificate Revocation List, if necessary.
- The owner's identity details, such as name, company and address.
- The owner's public key, and information about the algorithm with which it was produced.
- The identity details of the organization which issued the certificate.
- The issuer's digital signature and the algorithm used to produce it.
- The period for which the certificate is valid.
- Optional information is included, such as the type of application with which the certificate is intended to be used.

The issuing organization's digital signature is included in order to authenticate the certificate. As a result, if a certificate is tampered with during transmission, the tampering is detected.

Elements of a Public Key Infrastructure

A Public Key Infrastructure is a set of applications which manage the creation, retrieval, validation and storage of certificates. A PKI consists of the following key elements:

- At least one Certification Authority (CA), which issues and revokes certificates.
- At least one publicly accessible repository, which stores certificates and Certificate Revocation Lists.
- At least one End Entity (EE), which retrieves certificates from the repository, validates them and uses them.

End Entities (EE)

End Entities own public keys and may use them for encryption and digital signing. The switch acts as an End Entity.

An entity which uses its private key to digitally sign certificates is not considered an End Entity. Instead, it is a Certification Authority.

Certification Authorities

A Certification Authority is an entity which issues, updates, revokes and otherwise manages public keys and their certificates. A CA receives requests for certification, validates the requester's identity according to the CA's requirements, and issues the certificate, signed with one of the CA's keys. CAs may also perform the functions of End Entities, in that they may make use of other CAs' certificates for message encryption and verification of digital signatures.

An organization may own a Certification Authority and issue certificates for use within its own networks. In addition, an organization's certificates may be accepted by another network, after an exchange of certificates has validated a certificate for use by both parties. As an alternative, an outside CA may be used. The switch can interact with the CA, whether a CA is part of the organization or not, by sending the CA requests for certification.

The usefulness of certificates depends on how much you trust the source of the certificate. You must be able to trust the issuing CA to verify identities reliably. The level of verification required in a given situation depends on the organization's security needs.

Certificate Validation

To validate a certificate, the End Entity verifies the signature in the certificate, using the public key of the CA who issued the certificate.

CA Hierarchies and Certificate Chains

It may not be practical for every individual certificate in an organization to be signed by one Certification Authority. A certification hierarchy may be formed, in which one CA (for example, national headquarters) is declared to be the root CA. This CA issues certificates to the next level down in the hierarchy (for example, regional headquarters), who become subordinate CAs and issue certificates to the next level down, and so on. A hierarchy may have as many levels as needed.

Certificate hierarchies allow validation of certificates through certificate chains and cross-certification. If a switch X, which holds a certificate signed by CA X, wishes to communicate securely with a switch Y, which holds a certificate signed by CA Y, there are two ways in which the switches can validate each other's certificates. Cross-certification occurs when switch X validates switch Y's CA (CA Y) by obtaining a certificate for switch Y's CA which has been issued by its own CA (CA X). A certificate chain is formed if both CA X and CA Y hold a certificate signed by a root CA Z, which the switches have verified out of band. Switch X can validate switch Y's certificate (and vice versa) by following the chain up to CA Z.

Root CA Certificates

A root CA must sign its own certificate. The root CA is the most critical link in the certification chain, because the validity of all certificates issued by any CA in the hierarchy depends on the root CA's validity. Therefore, every device which uses the root CA's certificate must verify it out of band.

Out-of-band verification involves both the owner of a certificate and the user who wishes to verify that certificate generating a one-way hash (a fingerprint) of the certificate. These two hashes must then be compared using at least one non-network-based communication method. Examples of suitable communication methods are mail, telephone, fax, or transfer by hand from a storage device such as a smart card or floppy disk. If the two hashes are the same, the certificate can be considered valid.

Certificate Revocation Lists (CRLs)

A certificate may become invalid because some of the details in it change (for example, the address changes), because the relationship between the Certification Authority and the subject changes (for example, an employee leaves a company) or because the associated private key is compromised. Every CA is required to keep a publicly accessible list of its certificates which have been revoked.

PKI Implementation

The following sections discuss Allied Telesyn's implementation of PKI for the AT-8400 Series Switch. The following topics are covered:

- PKI Standards
- Certificate Retrieval and Storage
- Certificate Validation
- Root CA Certificates

PKI Standards

The following standards are supported by the switch:

- draft-ietf-pkix-roadmap-05 — *PKIX Roadmap*
- RFC 1779 — *A String Representation of Distinguished Names*
- RFC 2459 — *PKIX Certificate and CRL Profile*
- RFC 2511 — *PKIX Certificate Request Message Format*
- PKCS #10 v1.7 — *Certification Request Syntax Standard*

Certificate Retrieval and Storage

Certificates are stored by CAs in publicly accessible repositories for retrieval by end entities. The following repositories used in PKI are commonly accessed via the following protocols: *Hypertext Transfer Protocol (HTTP)*, *File Transfer Protocol (FTP)*.

Before the switch can use a certificate, it must be retrieved and manually added to the switch's Certificate Database, which is stored in RAM memory. The switch attempts to validate the certificate, and if validation is successful the certificate's public key is available for use.

Root CA Certificate Validation

Root CA certificates are verified out of band by comparing the certificate's *fingerprint* (the encrypted one-way hash with which the issuing CA signs the certificate) with the fingerprint which the CA has supplied by a non-network-based method. To view a certificate's fingerprint, use the procedure described in *Creating Certificates* on page 508.

To manually set a verified root certificate to trusted, see *Viewing Certificates* on page 518.

Configuring Certificates

Use the procedures in this section to create a certificate, add it to a certificate database, delete a certificate, modify a certificate or view a certificate. The following procedures are provided:

- Creating Certificates on page 508
- Adding Certificates to the Database on page 513
- Deleting and Modifying Certificates on page 515
- Viewing Certificates on page 518

There are two ways of obtaining certificates. You can create a certificate using the procedure described below in the Creating Certificates section or you can download a certificate from the Internet. In either case, once you have a certificate, you need to add it to the database so it can become active. After you add a certificate to the certificate database, it is displayed on the X509 Certificate Management Menu.

Creating Certificates

To create a self-signed certificate, perform the following procedure:

Note

Before you create a certificate, you need to record the Key Pair IDs you have assigned using the Key Management Menu. See [Configuring Keys for Encryption on page 491](#).

1. From the Main Menu, type **6** to select Security Menu.
The Security Menu is shown in Figure 151 on page 473.
2. From the Security menu, select the Keys/Certificate Configuration menu.

The Keys/Certificate Configuration Menu is shown in Figure 156 on page 492.
3. From the Keys/Certificate menu, select **3** - Public Key Infrastructure (PKI) Configuration.

The Public Key Infrastructure (PKI) Certification Menu is shown in Figure 161.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142

User: Manager                                00:14:33 30-Apr-2004

Public Key Infrastructure (PKI) Configuration

1 - Maximum Number of Certificates..... 256
2 - X509 Certificate Management
3 - Generate Enrollment Request

R - Return to Previous Menu

Enter your selection?
```

Figure 161 Public Key Infrastructure (PKI) Configuration Menu

4. Type **1** - Maximum Number of Certificates to change the maximum number of certificates.

The following message is displayed:

```
Enter certificate limit -> [12 to 256] -> 256
```

Enter a value between 12 and 256. This value represents the maximum number of certificates that you can add to the certificate database. The certificates that are in the certificate database are listed in the X509 Certificate Management menu. See Figure 162.

5. Type **2** - X509 Certificate Management to create a certificate.

The X509 Certificate Management Menu is shown in Figure 162.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142
User: Manager                                00:14:33 30-Apr-2004
X509 Certificate Management
Certificate Database:
Name           State           MTrust  Type   Source
-----
testcert12     Untrusted        False   Self   Command
webserver43    Trusted          False   CA     Command
1 - Create Self-Signed Certificate
2 - Add Certificate
3 - Delete Certificate
4 - Modify Certificate
5 - View Certificate Details
U - Update Display
R - Return to Previous Menu
Enter your selection?
```

Figure 162 X509 Certificate Management Menu

Note
In the X509 Certificate Management Menu, MTrust means manually trusted. This field indicates that you verified the certificate. The Source field indicates the certificate was generated on the switch. Both MTrust and Source are read-only fields.

6. Type **1** - Create Self-Signed Certificate to create a certificate.

The Create Self-Signed Certificate Menu is shown in Figure 163.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142

User: Manager                                00:14:33 30-Apr-2004

Create Self-Signed Certificate

1 - Certificate Name.....
2 - Key Pair ID..... 0
3 - Format..... DER
4 - Serial Number..... 0
5 - Subject DN.....
6 - Create Self-Signed Certificate

R - Return to Previous Menu

Enter your selection?

```

Figure 163 Create Self-Signed Certificate Menu

7. Type **1** - Certificate Name to create an alphanumeric name for a certificate.

The following message is displayed:

```
Enter certificate name (24 chars max) ->
```

Enter a certificate name of up to 24 alphanumeric characters. The name you enter here is the filename of the certificate followed by the .cer extension. The Certificate Name does not appear within the certificate file.

8. Type **2** - Key Pair ID to associate a Key Pair ID with the certificate name.

The following message is displayed:

```
Enter certificate Key Pair ID -> [0 to 65535] ->
```

9. Enter a value from 0 to 65,535 and press Return.

You must enter a Key Pair ID value that you configured in the Key Management menus. See Configuring Keys for Encryption on page 491.

10. Type **3** - Format to select the type of encoding format the certificate is to use.

You can toggle between the following values:

DER - Indicates the certificate contents are in a binary format. This is the default.

PEM - Indicates the certificate are in the Privacy Enhanced Mail (PEM) format which is an ASCII format.

11. Type **4** - Serial Number to assign a certificate a serial number.

The following message is displayed:

```
Enter certificate serial number -> [0 to 2147483647]
-> 0
```

12. Enter a value between 0 and 2,147,483,647 and press Return.

Usually, self-signed certificates are assigned a serial number of 0.

13. Type **5** - Subject DN to assign a certificate a Distinguished Name (DN).

The default of the Subject DN field is the value you configured in the Switch Distinguished Name field on the Keys/Certificate Configuration Menu.(See Configuring a Distinguished Name and Keys on page 491.)

If you configured the Switch Distinguished Name, you do not have to configure the Subject DN. In other words, you can use the default value. However, if you want to change the DN for the certificate, enter a value for the Subject DN. If you did not configure a Switch Distinguished Name, you **must** configure the Subject DN.

Note

The value you configure for the Subject DN does not become the DN for the switch.

A distinguished name specifies the physical address of the subject of a certificate, much like a street address. It consists of a list of values that uniquely identifies the subject of a certificate. The Certification Authority may require that a particular distinguished name is used. Otherwise, use a logical distinguished name. The list of values that specify a distinguished name are:

- common name (cn), organization name(ou), organization (o), locality (l), and state-or-province-name (st) are all strings consisting of printable characters with the exception of quotation marks. To use the following special characters {,=,+<>#;\<CR>} type a \ before the character.
- country-name (c) is a string consisting of any printable characters.

Country names are generally given in the form of the two-letter ISO 3166 code for the country, for example, us, de, or nz.

An example of a distinguished name for Janet Bloggs who works in Operations at Arctic Company in Fairbanks, Alaska is:

cn=Janet Bloggs, ou=Operations, o=Arctic Company,
l=Fairbanks, s=Alaska, c=us

14. Type **6** to create the certificate you have defined in the previous steps.

Note

If you do not select **6** - Create Self-Signed Certificate the values you configured in the above fields are lost.

The following message is displayed:

```
Please wait while certificate is generated...Done!
```

Adding Certificates to the Database

Once you have created a certificate, you need to load, or add, it into the certificate database to make it available for use by the HTTPS Web Server. There are two ways of creating certificates. You can create a certificate using the procedure described in Creating Certificates on page 508 or you can download a certificate from the Internet using the Uploading and Downloading Menus. See **Chapter 11: File Downloads and Uploads** on page 167. After you add a certificate to the certificate database, it appears on the X509 Certificate Management Menu.

To add a certificate to the certificate database, perform the following procedure:

1. From the Main Menu, type **6** to select Security Menu.
The Security Menu is shown in Figure 151 on page 473.
2. From the Security menu, select the Keys/Certificate Configuration menu.
The Keys/Certificate Configuration Menu is shown in Figure 156 on page 492.
3. From the Keys/Certificate menu, type **3** to select Public Key Infrastructure (PKI) Configuration.
The Public Key Infrastructure (PKI) Configuration Menu is shown in Figure 161 on page 509
4. Type **2** to select X509 Certificate Management to add a certificate to the certificate database.

The X509 Certificate Management Menu is shown in Figure 162 on page 510.

5. From the X509 Certificate Management menu, type **2** to select Add Certificate.

The Add Certificate Menu is shown in Figure 164.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142
User: Manager                                00:14:33 30-Apr-2004
Add Certificate Menu
1 - Certificate Name .....
2 - State ..... Trusted
3 - Type ..... EE
4 - File Name .....
5 - Add Certificate

R - Return to Previous Menu

Enter your selection?
```

Figure 164 Add Certificate Menu

6. Type **1** - Certificate Name to type in the name of a certificate.
This is the name that appears in the certificate database list. You can enter up to 40 alphanumeric characters.
7. Type **2** - State to specify if a certificate is trusted or untrusted.
Trusted - This value indicates you have verified that the certificate is from a trusted CA. This is the default.
Untrusted - This value indicates the certificate is from an untrusted CA either because you have not verified the CA or you have verified the CA is untrusted.
8. Type **3** to specify the type of certificate. There are 3 types to choose from:
EE - Indicates the certificate was issued by a CA, such as VeriSign. This is the default.
CA - Indicates the certificate belongs to a CA.
Self - This value is a self-signed certificate. Use this value when you are creating a self-signed certificate. The switch treats this type of certificate as its own.
9. Type **4** - File Name to specify the filename of the certificate.

The filename is the Certificate Name with the *.cer extension. For example, if you assign the Certificate Name as webserver127, the filename of the certificate is webserver127.cer.

Note

To display the filenames of the certificates, see Displaying System Configuration Files on page 159.

10. Type **5** - Add Certificate to add the certificate to the certificate database.

A wait message is displayed.

Deleting and Modifying Certificates

To delete or modify a certificate that is in the certificate database, perform the following procedure:

1. From the Main Menu, type **6** to select Security Menu.
The Security Menu is shown in Figure 151 on page 473.
2. From the Security menu, select the Keys/Certificate Configuration menu.

The Keys/Certificate Configuration Menu is shown in Figure 156 on page 492.

3. From the Keys/Certificate menu, select **3** - Public Key Infrastructure (PKI) Configuration.

The Public Key Infrastructure (PKI) Configuration Menu is shown in Figure 161 on page 509

4. From the Public Key Infrastructure (PKI) Configuration Menu, type **2** - X509 Certificate Management.

The X509 Certificate Management Menu is shown in Figure 162 on page 510.

5. From the X509 Certificate Management menu, type **3** to delete a certificate.

The following message is displayed:

```
Enter certificate name (ALL - delete all) ->
```

6. Enter the name of the certificate you want to delete.

Enter **ALL** to delete all the current certificates.

You have completed the delete certificate procedure. To modify a certificate, continue with the next step.

7. From the X509 Certificate Management menu, type **4** to Modify a Certificate.

The following message is displayed:

Enter a certificate name ->

8. Enter the name of the certificate you want to modify. Then press Return.

The Modify Certificate Menu is shown in Figure 165.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142
User: Manager                                00:14:33 30-Apr-2004
Modify Certificate Menu
1 - Certificate Name..... testcertificate
2 - State ..... Trusted
3 - Type ..... Self
4 - Modify Certificate

R - Return to Previous Menu

Enter your selection?
```

Figure 165 Modify Certificate Menu

Note

The Certificate Name cannot be changed.

9. Type **2** - State to specify if a certificate is trusted or untrusted.
Trusted - This value indicates you have verified that the certificate is from a trusted CA. This is the default.
Untrusted - This value indicates the certificate is from an untrusted CA either because you have not verified the CA or you have verified the CA is untrusted.
10. Type **3** to specify the type assigned to the certificate. There are 3 types to choose from:
EE - This value indicates the End Entity type. When you specify this type, the switch tags the certificate to indicate that it belongs to another end entity. This is the default.
CA - This value indicates the certificate has been approved by a Certificate Authority (CA) such as VeriSign.
Self - This value is a self-signed certificate. Use this value when you are creating a dummy certificate during your initial configuration. The switch treats this type of certificate as its own.

11. Type **4** - Modify Certificate to update your changes in the certificate database.

The following message is displayed:

```
Please wait while certificate is updated...Done.
```

12. After making changes, type **R** to until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Viewing Certificates

To view the details of a certificate, perform the following procedure:

1. From the Main Menu, type **6** to select Security Menu.
The Security Menu is shown in Figure 151 on page 473.
2. From the Security menu, select the Keys/Certificate Configuration menu.
The Keys/Certificate Configuration Menu is shown in Figure 156 on page 492.
3. From the Keys/Certificate menu, select **3** - Public Key Infrastructure (PKI) Configuration.
The Public Key Infrastructure (PKI) Configuration Menu is shown in Figure 161 on page 509
4. From the Public Key Infrastructure (PKI) Configuration Menu, type **2** - X509 Certificate Management.
The X509 Certificate Management menu is shown in Figure 162 on page 510.
5. From the X509 Certificate Management menu, type **5** to view the details of a certificate.
The following message is displayed:

```
Enter certificate name ->
```
6. Enter a name of the certificate you want to view.

The View Certificate Details Menu (page 1) is shown in Figure 166.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142

User: Manager                                00:14:33 15-Jan-2004

View Certificate Details

Certificate Details:
Name ..... testcertificate
State ..... Trusted
Manually Trusted ... True
Type ..... EE
Source ..... Command

Version ..... V3 (0X2)
Serial Number ..... 5000 (0X1388)
Signature Alg ..... md5WithRSAEncryption
Public Key Alg ..... rsaEncryption
Not Valid Before ... Oct 9 01:28:18 2003 GMT
Not Valid After .... Oct 8 01:28:18 2005 GMT

N - Next Page
R - Return to Previous Menu

Enter your selection?

```

Figure 166 View Certificate Details Menu (page 1)

Type **N** to see the second page of certificate details. The View Certificate Details menu (page 2) is shown in Figure 167.

```

Allied Telesyn Ethernet AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142

User: Manager                                00:14:35 15-Jan-2004

View Certificate Details

Subject ..... CN=149.44.44.44
Issuer ..... CN=149.44.44.44
MD5 Fingerprint...4E:76:06:FA:F6:C1:DA:FF:4D:E9:76:02:1D:8F:DA:CB
SHA1 Fingerprint..F8:43:CB:E2:0A:BF:4A:02:CA:C6:B0:47:DF:74:1E:D3:A8:A3:F0:00

N - Previous Page
R - Return to Previous Menu

Enter your selection?

```

Figure 167 View Certificate Details Menu (page 2)

7. The following fields are displayed:
 - Name** - lists the name of the certificate.
 - State** - Indicates the certificate is Trusted or Untrusted.
 - Manually Trusted** - Indicates you verified the certificate is from a trusted or untrusted authority.
 - Type** - Indicates the type of the certificate. The options are EE, SELF, and CA.
 - Source** - Indicates the certificate was created on the switch.
 - Version** - Indicates the version number of the software.
 - Serial Number** - Indicates the serial number of the certificate.
 - Signature Alg** - Indicates the signature algorithm of the certificate.
 - Public Key Alg** - Indicates the public key algorithm.
 - Not Valid Before** - Indicates the date the certificate became active.
 - Not Valid After** - Indicates the date the certificate expires. Self-signed certificates are valid for two years.
 - Subject** - Lists the Subject Distinguished Name.
 - Issuer** - Lists the Distinguished Name of the issuer of the certificate.
 - MD5 Fingerprint** - Indicates the MD5 algorithm. This value provides a unique sequence for each certificate consisting of 16 bytes.
 - SHA1 Fingerprint** - Indicates the Secure Hash Algorithm. This value provides a unique sequence for each certificate consisting of 20 bytes.

Generating Enrollment Requests

To request a certificate from a Certificate Authority, you need to generate an enrollment request. By generating an enrollment request, you create a file with a .csr extension. After you have generated an enrollment request file, upload the file to a CA. For a complete list of all the steps to configure the switch to obtain a CA certificate, see *Configuring CA Certificates* on page 482.

To generate an enrollment request, perform the following procedure:

1. From the Main Menu, type **6** to select Security Menu.
The Security Menu is shown in Figure 151 on page 473.
2. From the Security menu, select the Keys/Certificate Configuration menu.

The Keys/Certificate Configuration Menu is shown in Figure 156 on page 492.

3. From the Keys/Certificate menu, select **3** - Public Key Infrastructure (PKI) Configuration.

The Public Key Infrastructure (PKI) Configuration menu is shown in Figure 161 on page 509.

4. From the Public Key Infrastructure (PKI) Configuration Menu, type **3** to generate an enrollment request.

The Generate Enrollment Request Menu is shown in Figure 168.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142
User: Manager                                00:14:33 30-Apr-2004
Generate Enrollment Request Menu
1 - Request Name.....
2 - KeyPair ID ..... 0
3 - Format ..... PEM
4 - Type ..... PKCS10
5 - Generate Enrollment Request

R - Return to Previous Menu

Enter your selection?

```

Figure 168 Generate Enrollment Request Menu

5. Type **1** - Request Name.

The following message is displayed:

```
Enter Enrollment Request Name ->
```

6. Enter up to 127 alphanumeric characters for an enrollment request name.

The name you enter is used to create the filename of the enrollment request. The full filename consists of the enrollment request name followed by .csr extension. For example, if you enter certificate75 as the enrollment request name, the filename is certificate75.csr.

7. Type **2** - KeyPair ID.

The following message is displayed:

```
Enter KeyPair ID [0 to 65535] -> 0
```

8. Enter a KeyPair ID between 0 and 65,535.

9. Type **3** - Format.

You can toggle between the following values:

DER - Indicates the certificate is in a binary format. This is the default.

PEM - Indicates the certificate is in the Privacy Enhanced Mail (PEM) format which is an ASCII format.

Note

The type of certificate is a read-only field. The value, PKCS10, indicates the internal format of an enrollment request.

10. Type **5** - Generate Enrollment Request

```
Enrollment request is being generated. Please  
wait...Done
```

Chapter 25

Secure Sockets Layer (SSL)

The chapter contains information about Secure Sockets Layer (SSL) as well as a procedure for configuring this protocol on a switch using a local or Telnet management session. It contains the following sections:

- Secure Sockets Layer Overview on page 524
- Configuring SSL on page 528

Note

The SSL feature appears in the AT-S60 version 2.1.0 software only.

Secure Sockets Layer Overview

This chapter describes the Secure Sockets Layer (SSL) feature, a security protocol that provides a secure and private TCP connection between a client and server. You can configure the SSL feature using a local or Telnet management session.

SSL can be used with many higher layer protocols including HTTP, File Transfer Protocol (FTP) and Net News Transfer Protocol (NNTP). Most web browsers and servers support SSL. The most common deployment of SSL is for secure connections between a client and server over the Internet. The switch supports SSL versions 2.0 (client hello only) and 3.0 which were developed by Netscape, and the Internet Engineering Task Force (IETF) standard for SSL, known as SSL version 3.1 or Transport Layer Security (TLS).

Within the Ethernet protocol stack, SSL is a layer 4 protocol that lies in between the HTTP and TCP protocol layers. HTTP communicates with SSL in the same way as with TCP. In other words, TCP processes SSL requests like any other protocol requesting its services.

SSL provides a secure connection over which web pages can be accessed from an HTTP server. The operation of SSL is transparent to the end user who is accessing a web site with the following exceptions:

- ❑ the site's URL changes from http to https
- ❑ the browser displays a padlock icon.

By default, HTTP and HTTPS use the separate well-known ports 80 and 443 respectively. Secure connections over the Internet are important when transmitting confidential data such as credit card details or passwords. In addition, SSL allows the client to verify the server's identity before either side sends any sensitive information. SSL also prevents a third party from interfering with the message because only trusted devices have access to the unprotected data.

The SSL feature is described in more detail in the following sections:

- ❑ SSL Encryption on page 525
- ❑ User Verification on page 525
- ❑ Authentication on page 526
- ❑ Support for SSL on page 526
- ❑ SSL and Enhanced Stacking on page 527

SSL Encryption

SSL uses *encryption* to ensure the security of data transmission. Encryption is a process that uses an algorithm to encode data so it can only be accessed by a trusted device. An encrypted message remains confidential.

All application data messages are authenticated by SSL with a *message authentication code* (MAC). The MAC is a checksum that is created by the sender and is sent as part of the encrypted message. The recipient recalculates the MAC, and if the values match, the sender's identity is verified. The MAC also ensures that the message has not been tampered with by a third party because any change to the message changes the MAC.

SSL uses *asymmetrical* (Public Key) encryption to establish a connection between client and server, and *symmetrical* (Secret Key) encryption for the data transfer phase. For more information about public keys and encryption, see **Chapter 25**, Public Key Infrastructure (PKI) on page 501 and **Chapter 23**, Encryption on page 484.

User Verification

An SSL connection has two phases: *handshake* and *data transfer*. The *handshake* initiates the SSL *session*, during which data is securely transmitted between a client and server. During the handshake, the following occurs:

1. The client and server establish the SSL version they are to use.
2. The client and server negotiate the *cipher suite* for the session, which includes encryption, authentication, and key exchange algorithms.
3. The *symmetrical key* is exchanged.
4. The client authenticates the server (optionally, the server authenticates the client).

SSL messages are encapsulated by the *Record Layer* before being passed to TCP for transmission. Four types of SSL messages exist, they are:

- Handshake
- Change Cipher Spec
- Alert
- Application data (HTTP, FTP or NNTP)

As discussed previously, the *Handshake* message initiates the SSL session.

The *Change Cipher Spec* message informs the receiving party that all subsequent messages are encrypted using previously negotiated security options. The parties use the strongest cryptographic systems that they both support.

The *Alert* message is used if the client or server detects an error. Alert messages also inform the other end that the session is about to close. In addition, the Alert message contains a severity rating and a description of the alert. For example, an alert message is sent if either party receives an invalid certificate or an unexpected message.

The *Application data* message encapsulates the encrypted application data.

Authentication

Authentication is the process of ensuring both the web site and the end user are genuine. In other words, they are not imposters. Both the server and an individual users need to be authenticated. This is especially important when transmitting secure data over the Internet.

To verify the authenticity of a server, the server has a public and private key. The public key is given to the user.

SSL uses *certificates* for authentication. A certificate binds a public key to a server name. A Certification Authority issues certificates after checking that a public key belongs to its claimed owner. There are several agencies that are trusted to issue certificates. Individual browsers have approved Root CAs that are built in to the browser.

Note

See Public Key Infrastructure Overview on page 502 for detailed information about certificates.

Support for SSL

The AT-8400 switch implements the following versions of SSL:

- Mandatory parts of RFC 2246 (TLSv1), except for DSS encryption
- Mandatory parts of SSLv3
- SSLv2 client hello
- SHA1 for MAC

SSL and Enhanced Stacking

Secure Sockets Layer (SSL) is supported in an enhanced stack, but only when all switches in the stack are using the feature.

A web server can operate in one of two modes— HTTP or HTTPS. When a switch's web server is operating in HTTP, management packets are transmitted in plaintext. When it operates in HTTPS, management packets are sent encrypted.

The web server on the AT-8400 Series switch and an AT-8524M switch, can operate in either HTTP or HTTPS. Enhanced stacking switches that do not support SSL, such as the AT-8000 Series switches, use HTTP exclusively.

A web browser management session of the switches in an enhanced stack cannot alternate between the different security modes during a session. The management session assumes that the web server mode that the master switch is using is the same for all the switches in the stack.

As an example, if the master switch is using HTTPS, a web browser management session assumes that all the other switches in the stack are also using HTTPS, and it will not allow you to manage any switches running HTTP.

For those networks that consist of enhanced stacking switches where some switches support SSL and others do not, there are two approaches you can take. One is to create different enhanced stacks for the different switches. You could create one enhanced stack for those switches that support SSL and another stack for those that do not. You create different enhanced stacks by assigning switches to different Management VLANs.

Another approach is to leave the switches in one enhanced stack, but designate two master switches. One master switch could be using HTTP and the other HTTPS. When you want to use your web browser to manage those switches that support SSL, you would start the management session on the master switch whose server mode is set to HTTPS. To manage those switch not supporting SSL, you would start the management session on the master switch whose web server is set to HTTP.

In order to implement SSL in an enhanced stack, each switch in the stack must be given its own encryption key pair and certificate. Switches cannot share keys and certificates. When you start a web browser management session on the master switch of an enhanced stack, the management session uses the certificate and key pair on the master switch. When you change to another switch in the stack, the management session starts to use the certificate and key pair on that switch, and so forth.

Configuring SSL

This section describes how to configure SSL. This procedure is part of a comprehensive procedure to create certificates on the switch. See *Configuring SSL Certificates* on page 481 for a list of all the procedures you must complete to create certificates on the switch.

To configure the SSL protocol, perform the following procedure:

1. From the Main Menu, type **6** to select Security Menu.
The Security Menu is shown in Figure 151 on page 473.
2. From the Security menu, select the Secure Socket Layer (SSL) menu.
The Secure Socket Layer (SSL) Menu is shown in Figure 169.

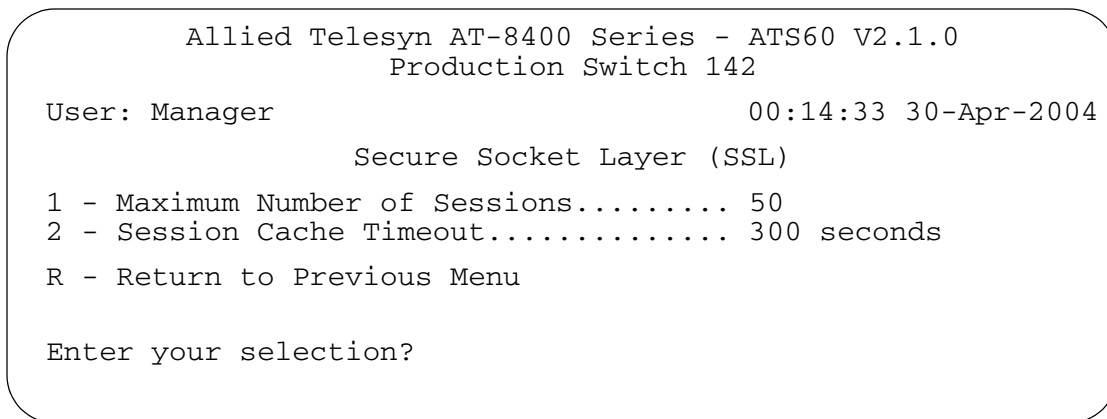


Figure 169 Secure Socket Layer (SSL) Menu

3. Select **1** - Maximum number of Sessions to increase the number of sessions.
Enter a value from 1 to 100. The maximum number of sessions is used to speed up a connection. By increasing the number of sessions, you increase HTTPS performance. However, increasing the number of sessions also increases the memory requirements. The default is 50.
4. Select **2** - Session Cache Timeout to increase or decrease the timer that determines when the session cache times out.
Enter a value, in seconds, from 1 to 600. The default is 300 seconds.

Chapter 26

Secure Shell (SSH)

The chapter contains overview information about the Secure Shell (SSH) protocol as well a procedure for configuring this protocol on a switch using a local or Telnet management session. It contains the following sections:

- SSH Overview on page 530
- SSH Overall Configuration on page 534
- Configuring SSH on page 535
- Displaying SSH Information on page 538

Note

The SSH feature appears in the AT-S60 version 2.1.0 software only.

SSH Overview

This chapter describes the Secure Shell (SSH) protocol, including:

- ❑ Support for Secure Shell on the switch
- ❑ How to configure the switch to act as a SSH server
- ❑ How to use Secure Shell to manage the switch.

To implement SSH on your switch, you need to configure the switch as an SSH server, install a SSH client on a management PC, and login to the client.

Secure management is increasingly important in modern networks, as the ability to easily and effectively manage switches and the requirement for security are two universal requirements. Traditionally, switches are managed using either remote terminal sessions via the Telnet protocol or SNMP. Both of these methods have serious security problems—they are only protected by cleartext reusable passwords which are vulnerable to wiretapping and password guessing.

The Secure Shell (SSH) protocol provides encrypted and strongly authenticated remote login sessions, similar to the Telnet and rlogin protocols, between a host running a Secure Shell server and a machine with a Secure Shell client.

The AT-8400 switch implements a Secure Shell server to enable network managers to securely manage the switches over an insecure network. It offers the benefit of cryptographic authentication and encryption. Secure Shell is strongly authenticated and encrypted. Secure Shell replaces Telnet for remote terminal sessions.

Support for SSH

The AT-8400 switch implementation of the SSH protocol is compliant with the SSH protocol versions 1.3, 1.5, and 2.0.

In addition, the following SSH options and features are supported:

- ❑ Inbound SSH connections (server mode) is supported.
- ❑ The following security algorithms are supported:
 - 128-bit Advanced Encryption Standard (AES), 192-bit AES, and 256-bit AES
 - Arcfour (RC4) security algorithm is supported.
 - Triple-DES (3DES) encryption for SSH sessions is supported.

- RSA public keys with lengths of 512 to 1536 bits are supported. Keys are stored in a format compatible with other Secure Shell implementations, and mechanisms are provided to copy keys to and from the switch.
- Compression of SSH traffic.

Note

DES is not supported by SSH 2.0.

The following SSH options and features are **not** supported:

- IDEA or Blowfish encryption
- Nonencrypted Secure Shell sessions
- Tunnelling of TCP/IP traffic

Note

Non-encrypted Secure Shell sessions serve no purpose.

SSH Server

When the SSH server is enabled, connections from SSH clients can be accepted. When the SSH server is disabled, connections from SSH clients are rejected by the switch. Within the switch, the AT-S60 software uses well-known port 22 as the SSH default port.

Note

If your switch is in a network that is protected by a firewall, you may need to configure the firewall to permit SSH connections.

The SSH server accepts connections from configured users only. Acceptable users are those with a Manager or Operator login as well as users configured with the RADIUS and TACACS+ protocols. You can add, delete, and modify users with the RADIUS and TACACS+ feature. For information about how to configure RADIUS and TACACS+, see Enabling TACACS+ or RADIUS on page 544.

SSH encryption key management is implemented by the Encryption (ENCO) protocol. RSA public keys can be imported and exported to and from the single-line ASCII format used by all SSH implementations. For information on how to configure the Encryption protocol, see Configuring Keys for Encryption on page 491.

SSH Clients

The SSH protocol provides a secure connection between the switch and SSH clients. Once you have configured the SSH server, you need to install SSH client software on your management PC. The AT-S60 software supports both SSH1 and SSH2 clients.

You can download client software from the Internet. Two popular SSH clients are PuTTY and CYGWIN. To install SSH client software, follow the directions from the vendor.

Once you have configured the SSH client software, you can use the client software to login to the SSH server as a manager, operator, or as RADIUS/TACACS+ users. The SSH server supports multiple client connections. The maximum number of SSH clients allowed is 10 users with one manager login.

SSH and Enhanced Stacking

The AT-S60 management software allows for encrypted SSH management sessions between a management workstation and a master switch of an enhanced stack, but not with slave switches, as explained in this section.

When you remotely manage a slave switch, all management communications are conducted through the master switch using the enhanced stacking feature. Management packets from your workstation are first directed to the master switch before being forwarded to the slave switch. The reverse is true as well. Management packets from a slave switch first pass through the master switch before reaching your management workstation.

Enhanced stacking uses a proprietary protocol that does not provide for encryption between a master switch and a slave switch. The result is that SSH encryption only occurs between your workstation and the master switch, not between your workstation and a slave switch.

This is shown in Figure 170. The figure shows an SSH management workstation that is managing a slave switch of an enhanced stack. The packets exchanged between the slave switch and the master switch are transmitted in plain text and those exchanged between the master switch and the SSH management workstation are encrypted.

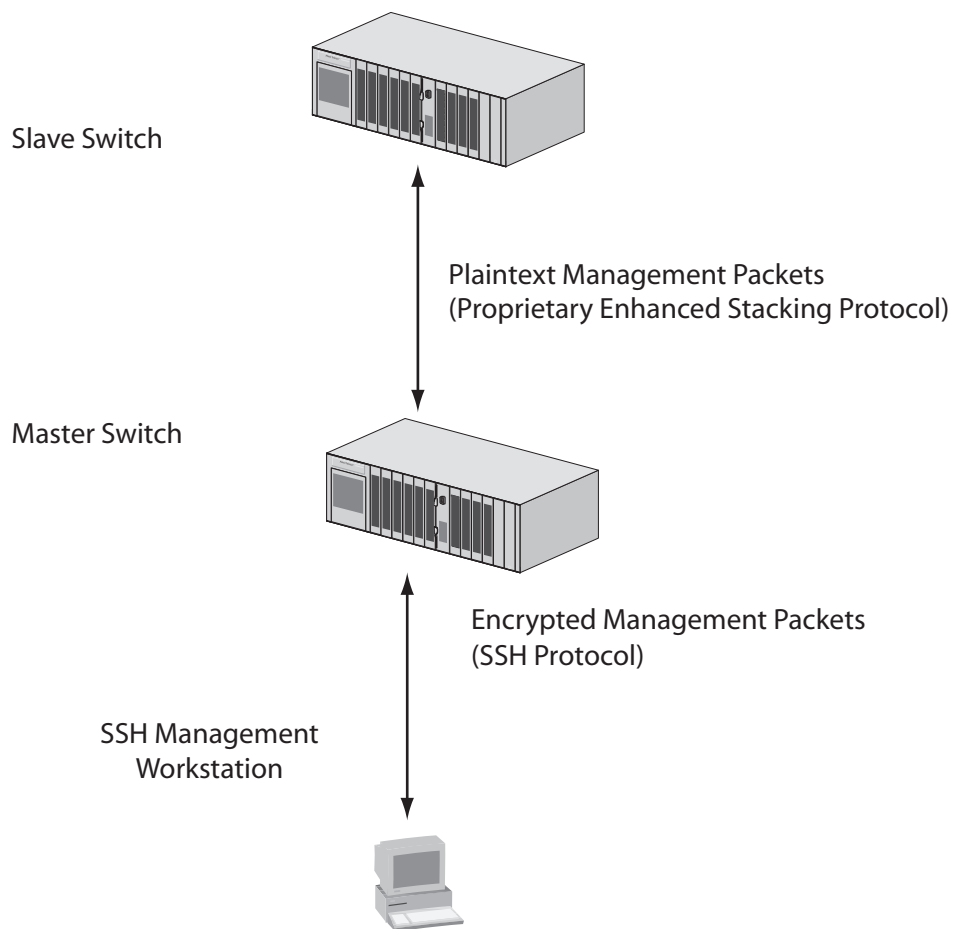


Figure 170 SSH Remote Management of a Slave Switch

Since enhanced stacking does not allow SSH encrypted management sessions between a management station and a slave switch, you configure SSH only on the master switch of a stack. Activating SSH on a slave switch has no affect.

SSH Overall Configuration

Configuring the SSH server requires you to perform several procedures. The information in this section lists the procedures you need to complete to configure the SSH feature, including the server and client configuration. Since SSH is a complex feature, you need to perform all the steps in the following procedure.

To configure the switch as an SSH server and configure SSH clients, perform the following procedure:

1. Log on to the switch with the Manager login id.
You can only configure the SSH server when you are logged in as Manager.
2. Create a host and server encryption keys.
Two RSA private keys are required to enable the Secure Shell server. The first, called the *host key*, is the switch's own RSA key. The recommended length of this key is 1024 bits. The second key, the *server key*, is a randomly created key, which is re-generated after the specified timeout. The server key must be 128 bits greater or less than the host key, but the server key should be at least 512 bits. For procedures for creating a RSA private key, see *Configuring Keys for Encryption* on page 491.
3. Configure and Enable the Secure Shell server.
See *Configuring SSH* on page 535.
4. Install SSH client software on your PC.
Follow the directions provided with the client software. You can download SSH client software from the Internet. Two popular SSH clients are PuTTY and CYGWIN.
5. Disable the Telnet server.
Although the software allows the SSH and Telenet servers to be enabled simultaneously, allowing Telnet to be enabled negates the security of the SSH feature. To disable the Telnet server, see *Configuring Management Access* on page 66.
6. Logon to the SSH server from the SSH client.
Acceptable users are those with a Manager or Operator login as well as users configured with the RADIUS and TACACS+ protocols. You can add, delete, and modify users with the RADIUS and TACACS+ feature. For information about how to configure RADIUS and TACACS+, see *Enabling TACACS+ or RADIUS* on page 544.

Configuring SSH

This section describes how to configure the switch as an SSH server. For a description of all the steps required to configure an SSH server, see SSH Overall Configuration on page 534.

Before you begin this procedure, you need to configure a host and server keys for SSH. See Configuring Keys for Encryption on page 491. The minimum bit size of the server key is 512 bits. The recommended bit size for a server key is 768 bits. The recommended size for the host key is 1024 bits. In addition, the bit size of the host and server keys must differ by 128 bits.

While you are configuring the SSH feature, you must disable the SSH server. When you have completed your configuration changes, enable the SSH server to permit SSH client connections.

Note

Allied Telesyn recommends disabling the Telnet server before you enable SSH. Otherwise, the security functions provided by SSH are lost. See Chapter 3, Basic Switch Parameters on page 45.

To configure the SSH protocol, perform the following procedure:

1. From the Main Menu, type **6** to select Security Menu.
The Security Menu is shown in Figure 151 on page 473.
2. From the Security Menu, select the Secure Shell (SSH) menu.

The Secure Shell (SSH) Menu is shown in Figure 171.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142

User: Manager                                00:14:33 30-Apr-2004

                Secure Shell (SSH)

1 - SSH Server Status ..... Disabled
2 - Host Key ID..... <Not Defined>
3 - Server Key ID ..... <Not Defined>
4 - Server Key Expiry Time .. 0 hours
5 - Login Timeout ..... 180 seconds

6 - Show Server Information
R - Return to Previous Menu

Enter your selection?
```

Figure 171 Secure Shell (SSH) Menu

- 3. Select **1** - SSH Server Status to enable or disable the SSH server.
- 4. Choose from one of the following:

Disabled - While you are configuring SSH, you must set this field to Disabled. This is the default.

Enabled - Select this value to enable the SSH server. Select this value after you have finished configuring SSH and want to log on to the server.

Note

When there are active SSH connections, you cannot disable the SSH server. If you attempt to disable the SSH server when it is in this state, you receive a warning message.

- 5. Select **2** - Host Key ID.
Enter a host key ID. The default is Not Defined. Enter a value that you configured in the Encryption Menus. See Configuring Keys for Encryption on page 491.
- 6. Select **3** - Server Key ID.
Enter a server key ID. The default is Not Defined. Enter a value that you configured in the Encryption Menus. See Configuring Keys for Encryption on page 491.
- 7. Select **4** - Server Key Expiry Time to set the time, in hours, for the server key to expire.

This timer determines how often the server key is regenerated. Naturally, 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 International recommends you set this field to 1. With this setting, a new key is generated every hour.

The default is 0 hours which means the server key never expires. The range is 0 to 5 hours.

8. Select **5** - Login Timeout.

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.

9. Select **1** - SSH Server Status to Enable the SSH server.

10. Select **Enable** to enable the SSH server.

Note

Allied Telesyn International recommends disabling the Telnet server before you enable SSH. Otherwise, the security provided by SSH is lost.

11. After making changes, type **R** to until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Displaying SSH Information

To display SSH server information, perform the following procedure:

1. From the Main Menu, type **6** to select Security Menu.
The Security Menu is shown in Figure 151 on page 473.
2. From the Security menu, select the Secure Shell (SSH) menu.
The Secure Shell (SSH) Menu is shown in Figure 171 on page 536.
3. From the Secure Shell (SSH) menu, type **6** to select Show Server information to display the SSH Server data.

The Show Server Information Menu is shown in Figure 172.

```

Allied Telesyn AT-8400 Series - AT560 V2.1.0
Engineering Switch 142

User: Manager                                00:15:42 30-Apr-2004

                Show Server Information Menu

Versions Supported ..... 1.3, 1.5, 2.0
Server Status ..... Enabled
Server Port ..... 22
Host Key ID ..... 200
Host Key Bits ..... 1024
Server Key ID ..... 250
Server Key Bits ..... 768
Server Key Expiry ..... 0 hours
Login Timeout ..... 180 seconds
Authentication Available . Password
Ciphers Available ..... DES, 3DES, 128 bit AES, 192 bit AES, 256 bit
AES, Arcfour (RC4)
MACs Available ..... hmac-sha1, hmac-md5
Data Compression ..... Available

R - Return to Previous Menu

Enter your selection?
```

Figure 172 Show Server Information Menu

The following information is displayed:

- Versions Supported:** Indicates the versions of SSH which are supported by the AT-S60 software.
- Server Status:** Indicates whether or not the SSH server is enabled or disabled.

- Server Port:** Indicates the well-known port for SSH. The default is port 22.
- Host Key ID:** Indicates the host key ID defined for SSH.
- Host Key Bits:** Indicates the number of bits in the host key.
- Server Key ID:** Indicates the server key ID defined for SSH.
- Server Key Bits:** Indicates the number of bits in the server key.
- Server Key Expiry:** Indicates the 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:** Indicates the time, in seconds, until a SSH server is released from an incomplete connection with a SSH client.
- Authentication Available:** Indicates the authentication method available. Currently, password authentication is the only supported method.
- Ciphers Available:** Indicates the SSH ciphers that are available on the switch. The ciphers that a client can access depends upon the SSH software that is installed on the client. For example, only a client running SSH 1.5 can access DES on the switch.
- MACs Available:** Indicates the Message Authorization Code (MAC) that is used to validate incoming SSH messages to the server. Two algorithms are supported.
- Data Compression:** Indicates whether or not data compression is available on the switch. Data compression is useful for networks that have a slow throughput speed.

Chapter 27

TACACS+ and RADIUS Protocols

This chapter explains how you can use the two authentication protocols TACACS+ and RADIUS to control who can log onto a switch to manage it. This chapter includes the following sections:

- ❑ TACACS+ and RADIUS Overview on page 541
- ❑ Enabling TACACS+ or RADIUS on page 544
- ❑ Configuring TACACS+ on page 545
- ❑ Configuring RADIUS on page 547

TACACS+ and RADIUS Overview

The AT-S60 software has two standard management login accounts: Manager and Operator. The Manager account lets you change a switch's parameter settings while the Operator account only lets you view the settings. Each account has its own password. The Manager account has a default password of "friend" and the Operator account has a default password "operator."

For those networks that are managed by one or two network managers, the standard accounts may be all you need. However, for larger networks managed by several network managers, you might want to give each manager his or her own management login account rather than have them share an account.

This is where TACACS+ and RADIUS can be useful. (TACACS+ is an acronym for Terminal Access Controller Access Control System. RADIUS is an acronym for Remote Authentication Dial In User Services.) These are authentication protocols. They can be used to transfer the task of validating management access from an AT-8400 Series switch to an authentication protocol server.

With the protocols, you can create a series of user name and password combinations that define who can manage an AT-8400 Series switch.

There are three basic functions an authentication protocol provides:

- Authentication
- Authorization
- Accounting

When a network manager logs in to a switch, the switch passes the user name and password entered by the manager to the authentication protocol server. The server checks to see if the user name and password are valid for that switch. This is referred to as authentication.

If the combination is valid, the authentication protocol server notifies the switch and the switch completes the login process, allowing the manager to manage the switch.

If the user name and password combination is invalid, the authentication protocol server notifies the switch and the switch cancels the login.

Authorization defines what a user can do once logged in to a switch. You assign an authorization level to each user name and password combination that you create on the server software. The access level is either Manager or Operator.

The final function of the TACACS+ protocol is accounting, which is used to keep track of user activity on network devices. The AT-8400 Series switch does not support this function.

Note

The AT-S60 management software does not support the two earlier versions of the TACACS+ protocol, TACACS and XTACACS.

So what does it take to use the TACACS+ and RADIUS protocols on an AT-8400 Series switch? Here are the main points.

- ❑ First, you need to install TACACS+ or RADIUS server software on one or more of your network servers or management stations. Authentication protocol server software is not available from Allied Telesyn.
- ❑ The authentication protocol server can be on the same subnet or a different subnet as the AT-8400 Series switch. If the server and switch are on different subnets, be sure to specify a default gateway in the Administration Menu so that the switch and server can communicate with each other.
- ❑ You need to configure the TACACS+ or RADIUS server software. This involves the following:
 - Specifying the user name and password combinations.
 - Assigning each combination an authorization level. This differs depending on the server software you are using. TACACS+ controls this through the sixteen (0 to 15) different levels of the Privilege attribute. A privilege level of "0" gives the combination Operator status. Any value from 1 to 15 gives the combination Manager status.

For RADIUS, management level is controlled by the Service Type attribute. This attribute has 11 different values, of which two are functional with an AT-8400 Series switch. A value of Administrative for this attribute gives the user name and password combination Manager access. A value of NAS Prompt assigns the combination Operator status.

Note

This manual does not explain how to configure TACACS+ or RADIUS server software. For server configuration, refer to the documentation that came with the software.

By default, authentication protocol is disabled on an AT-8400 Series switch. Once you activate it, you need to provide the following information:

- Which authentication protocol you want to use. Only one authentication protocol can be active on a switch at a time.
- IP addresses of up to three authentication servers.
- The encryption key used by the authentication servers.

Note

For more information on TACACS+, refer to the RFC 1492 standard. For more information on RADIUS, refer to the IEEE draft for the TACACS+ Protocol, Version 1.78.

Enabling TACACS+ or RADIUS

To enable or disable the server-based authentication feature on the switch and to configure the TACACS+ and RADIUS settings, perform the following procedure:

1. From the Main Menu, type **6** to select Security Menu.
The Security Menu is shown in Figure 151 on page 473.
2. From the Security Menu, select Server Based Authentication.
The Authentication Menu is shown in Figure 173.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142
User: Manager                                00:14:33 01-Jan-2004
Authentication Menu

1 - Server-based Authentication ..... Disabled
2 - Authentication Method ..... TACACS+
3 - TACACS+ Configuration
4 - RADIUS Configuration

R - Return to Previous Menu

Enter your selection?
    
```

Figure 173 Authentication Menu

3. To enable or disable the authentication feature on the switch, type **1** to select Server-based Authentication. The following prompt is displayed:

```
Server Based User Authentication (E-Enabled,
D-Disabled) ->
```

4. Type **E** to enable the TACACS+ and RADIUS protocols on the switch or **D** to disable them. The default is disabled.

If you enable the authentication feature, continue to the next step. If you disabled authentication, press **R** twice to return to the Main Menu. Then select **S** - Save Configuration Changes.

5. To select an authentication protocol, type **2** to select Authentication Method. The following prompt is displayed:

```
Enter T-TACACS+, R-RADIUS ->
```

6. Type **T** to select TACACS+ or **R** for RADIUS. The default is TACACS+. Only one protocol can be active at a time.

Configuring TACACS+

To configure TACACS+, perform the following procedure:

1. From the Main Menu, type **6** to select Security Menu.
The Security Menu is shown in Figure 151 on page 473.
2. From the Security Menu, select Server Based Authentication.
The Authentication Menu is shown in Figure 173 on page 544.
3. Type **3** to select TACACS+ Configuration.

The TACACS+ Client Configuration Menu is shown in Figure 174.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142
User: Manager                                00:14:36 01-Jan-2004
TACACS+ Client Configuration

1 - TAC Server 1 ..... 0.0.0.0
2 - TAC Server 2 ..... 0.0.0.0
3 - TAC Server 3 ..... 0.0.0.0
4 - TAC Server Order ..... 1 2 3
5 - TAC Global Secret .....
6 - TAC Timeout ..... 30 seconds

R - Return to Previous Menu

Enter your selection?

```

Figure 174 TACACS+ Client Configuration Menu

4. Configure the settings as needed. The settings are described below:

1 - TAC Server 1

2 - TAC Server 2

3 - TAC Server 3

Use these parameters to specify the IP addresses of up to three network servers containing TACACS+ server software. After you have entered an IP address, the following prompt is displayed:

```
Use per-server secret [Y/N] ->
```

If you are specifying more than one TACACS+ server and if all of the servers use the same encryption secret, you can answer No to this prompt and enter the encryption secret by typing **5** to select TAC Global Secret parameter.

However, if you are specifying only one TACACS+ server or if the servers have difference encryption secrets, then respond with Yes to this prompt. The following prompt is displayed:

```
Enter per-server secret [max 40 characters] ->
```

Use this prompt to enter the encryption secret for the TACACS+ server whose IP address you are specifying.

4 - TAC Server Order

You use this selection to indicate the order in which you want the switch to query the TACACS+ servers for logon authentication. Of course, you can skip this option if you specified only one IP address. The default is 1, 2, and 3, in that order.

5 - TAC Global Secret

If all of the TACACS+ servers have the same encryption secret, you can use this option to enter the secret once rather than entering the same secret each time you enter an IP addresses.

3 - TAC 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 aren't any more servers, the switch defaults to the standard Manager and Operator accounts. The default is 30 seconds. The range is 1 to 300 seconds.

5. After configuring the parameters, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Configuring RADIUS

To configure RADIUS, perform the following procedure:

1. From the Main Menu, type **6** to select Security Menu.
The Security Menu is shown in Figure 151 on page 473.
2. From the Security Menu, select Server Based Authentication.
The Authentication Menu is shown in Figure 173 on page 544.
3. Type **4** to select RADIUS Configuration.

The RADIUS Client Configuration Menu is shown in Figure 175.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142

User: Manager                                00:14:38 01-Jan-2004

RADIUS Client Configuration

1 - Global Encryption Key ..... ATI
2 - Global Server Timeout period..... 30 seconds
3 - RADIUS Server 1 Configuration ..... 0.0.0.0
4 - RADIUS Server 2 Configuration ..... 0.0.0.0
5 - RADIUS Server 3 Configuration ..... 0.0.0.0
6 - Show Status

R - Return to Previous Menu

Enter your selection?

```

Figure 175 RADIUS Client Configuration Menu

4. Configure the parameters as needed. The parameters are defined below:

Global Encryption Key

This parameter specifies the encryption key for the RADIUS servers. This option is useful if you are entering more than one RADIUS server and all the servers share the same encryption key. If the servers use different encryption keys, leave this option blank. Once you enter a key and press Return, the RADIUS Client Configuration menu is updated with the key.

Global Server Timeout period

This parameter specifies the maximum amount of time the switch waits for a response from a RADIUS server before assuming that

the server cannot respond. If the timeout expires and the server hasn't responded, the switch queries the next RADIUS server in the list. If there aren't any more servers in the list, then the switch defaults to the standard Manager and Operator accounts. The default is 30 seconds. The range is 1 to 60 seconds.

3 - RADIUS Server 1 Configuration

4 - RADIUS Server 2 Configuration

5 - RADIUS Server 3 Configuration

Use these parameters to specify the IP addresses of up to three network servers containing the RADIUS server software. Selecting one of the above options displays the RADIUS Server Configuration Menu as shown in Figure 176.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Engineering Switch 142
User: Manager                                00:14:39 01-Jan-2004
RADIUS Server 1 Configuration
1 - Server IP Address ..... 0.0.0.0
2 - Server Authentication UDP Port .... 1812
3 - Server Encryption Key ..... <Not Defined>
R - Return to Previous Menu
Enter your selection?
```

Figure 176 RADIUS Server Configuration Menu

The options are described below:

1 - Server IP Address

Use this option to specify the IP address of the RADIUS server.

2 - Server Authentication UDP Port

Use this option to specify the UDP port of the RADIUS protocol. This is an internal port number used by the TCP/IP stack to determine which application an incoming message is sent to.

3 - Server Encryption Key

Use this option to specify the encryption key for the RADIUS server. This is an alphanumeric value with a maximum length of 24 characters.

- 5. After configuring the parameters, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Chapter 28

802.1x Port-based Network Access Control

This chapter explains 802.1x Port-based Network Access Control and how you can use this feature to restrict access to the network ports on the switch. The following sections are provided:

- ❑ 802.1x Port-based Access Network Control Overview on page 550
- ❑ Enabling and Disabling Port-based Access Control on page 557
- ❑ Setting the Port Access Role on page 559
- ❑ Configuring Authenticator Parameters on page 561
- ❑ Configuring Supplicant Parameters on page 565
- ❑ Configuring RADIUS Accounting on page 568
- ❑ Displaying Port-based Access Control Status on page 571

802.1x Port-based Access Network Control Overview

The AT-S60 management software has several different methods for protecting your network and its resources from unauthorized access. This chapter explains yet another method of securing your network using the port-based access control (IEEE 802.1x) feature. This feature uses the RADIUS protocol to control who can send traffic through and receive traffic from a port. With this feature, the switch does not allow an end node to send or receive traffic through a port until the user of the node has logged on by entering a username and password that the RADIUS server validates.

The benefit to this type of network security is obvious. This feature can prevent an unauthorized individual from connecting a computer to a port or using an unattended workstation to access your network resources. Only those users to whom you have assigned valid user names and passwords are able to use the switch to access the network.

This port security method uses the RADIUS authentication protocol. The AT-S60 software comes with RADIUS client software. If you have already read Chapter 27, TACACS+ and RADIUS Protocols on page 540, then you know that you can also use the RADIUS client software on the switch, along with a RADIUS server on your network, to create new manager accounts that control who can manage and change the AT-S60 parameter on the switch.

Note

RADIUS with Extensible Authentication Protocol (EAP) extensions is the only supported authentication server for this feature. The port-based access control feature is not supported with the TACACS+ authentication protocol. The switch can support only one authentication protocol at a time. Consequently, to implement IEEE 802.1 port-based access control as explained in this chapter, and create new manager accounts as explained in Chapter 27, you must use the RADIUS protocol.

Here are a few terms to keep in mind when using this feature.

- ❑ **Supplicant** - A supplicant is an end user or end node that wants to access the network through a port. A supplicant is also referred to as a client.
- ❑ **Authenticator** - The authenticator is a port on the switch that prohibits network access by a supplicant until the network user has entered a valid username and password.

- ❑ Authentication server - The authentication server is the network device that has the RADIUS server software. This is the device that does the actual authenticating of the user names and password from the supplicants.

The AT-8400 switch does not authenticate the username and passwords from the clients. Instead, the switch acts as an intermediary between a supplicant and the authentication server during the authentication process.

Note

Ports under 802.1x control do not support trunking, STP, or static and dynamic learning. In addition, ports under 802.1x control must be a member of a only one VLAN.

Authentication Process

Below is a brief overview of the authentication process that occurs between a supplicant, authenticator, and authentication server. For further details, refer to the IEEE 802.1x standard.

1. An authentication message exchange can be initiated by either the authenticator port or the supplicant port. The switch initiates an exchange when it detects a change in the status of a port (such as when the port transitions from no link to valid link), or if it receives a packet on the port with a source MAC address not in the MAC address table.

An authenticator starts the exchange by sending an EAP-Request/Identity packet. A supplicant starts the exchange with an EAPOL-Start packet, to which the authenticator responds with a EAP-Request/Identity packet.

2. The supplicant responds with an EAP-Response/Identity packet to the authentication server via the authenticator.
3. The authentication server responds with an EAP-Request packet to the supplicant via the authenticator.
4. The supplicant responds with an EAP-Response/MD5 packet containing a username and password. This packet is sent to the authentication server via the authenticator.
5. The authentication server sends either an EAP-Success packet or an EAP-Reject packet to the supplicant via the authenticator.
6. Upon successful authorization of the supplicant by the authentication server, the switch adds the supplicant's MAC address to the MAC address table as an authorized address and begins forwarding network traffic to and from the port.

7. When the supplicant sends an EAPOL-Logoff message, the switch removes the supplicant's MAC address from the MAC address table, preventing the supplicant from sending or receiving any further traffic from the port.

Port Roles

In order to implement this feature, you need to specify the roles of the ports on the switch. You can assign a port one of the following roles:

- None
- Authenticator
- Supplicant

None Role

A port in the none role does not participate in port-based access control. Any device can connect to the port and send traffic through it and receive traffic from it without having to authenticate by providing a username and password. This is the default setting for a port.

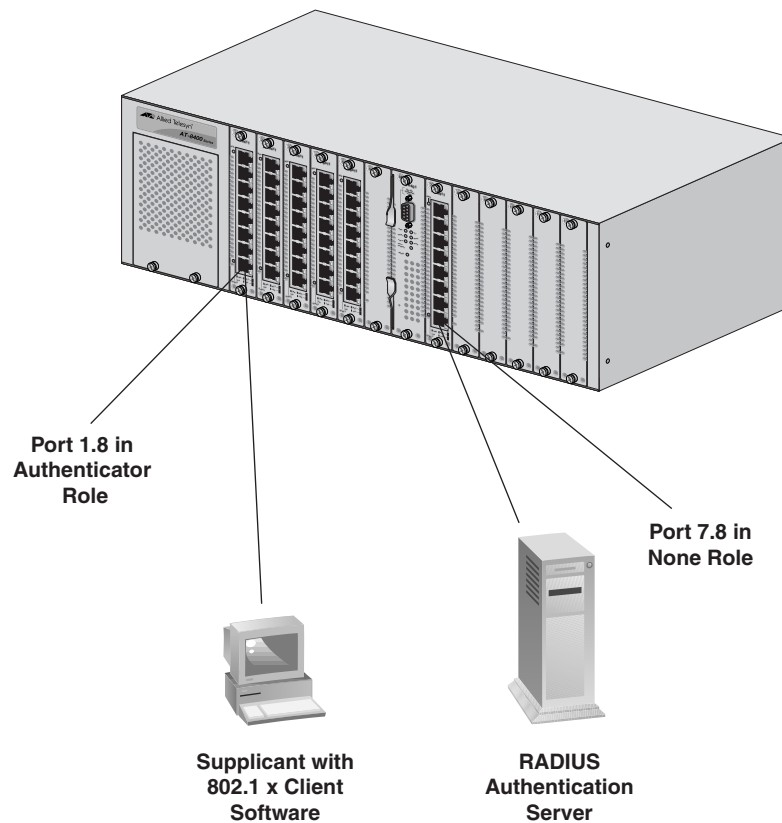
Set a port to this role if you do not want its client to have to authenticate to use the network. This also happens to be the correct role for a port that's connected to an authentication server. Since an authentication server cannot authenticate itself, the port to which it is connected must be set to this role.

Authenticator Role

Placing a port in the authenticator role activates port-based access control on the port. A port in the role of authenticator does not forward network traffic to or from the client until the client has entered a username and password and the authentication server has validated them.

Determining whether a port should be set to the authenticator role is straightforward. If you want the user of the client connected to the port to log in before using the network, then you set the port to the authenticator role.

The authenticator role is shown in Figure 177 on page 553. Port 1.8 on the switch is set to the authenticator role because it is connected to a client with 802.1x client software. The end user at the workstation must log on to use the network.



109

Figure 177 Example of Authenticator Role

As mentioned earlier, the switch does not authenticate the user names and passwords from the clients. That is the responsibility of the authentication server, which contains the RADIUS server software. Instead, the switch acts as an intermediary for the authentication server by denying access to the network by the client until the client has provided a valid username and password, which the authentication server validates.

Supplicant Role

On the AT-8400 switch, a port in the supplicant role acts as a client. The port assumes it must log in by providing a valid user name and password to whatever device it is connected to, typically another port.

The supplicant role is shown in Figure 178 on page 554. Port 3.2 on Switch B has been set to the supplicant role. Now, whenever Switch B is power cycled or reset and initiates a link with Switch A it will have to log on by providing a username and password. (You enter this information when you configure the port for the supplicant role.)

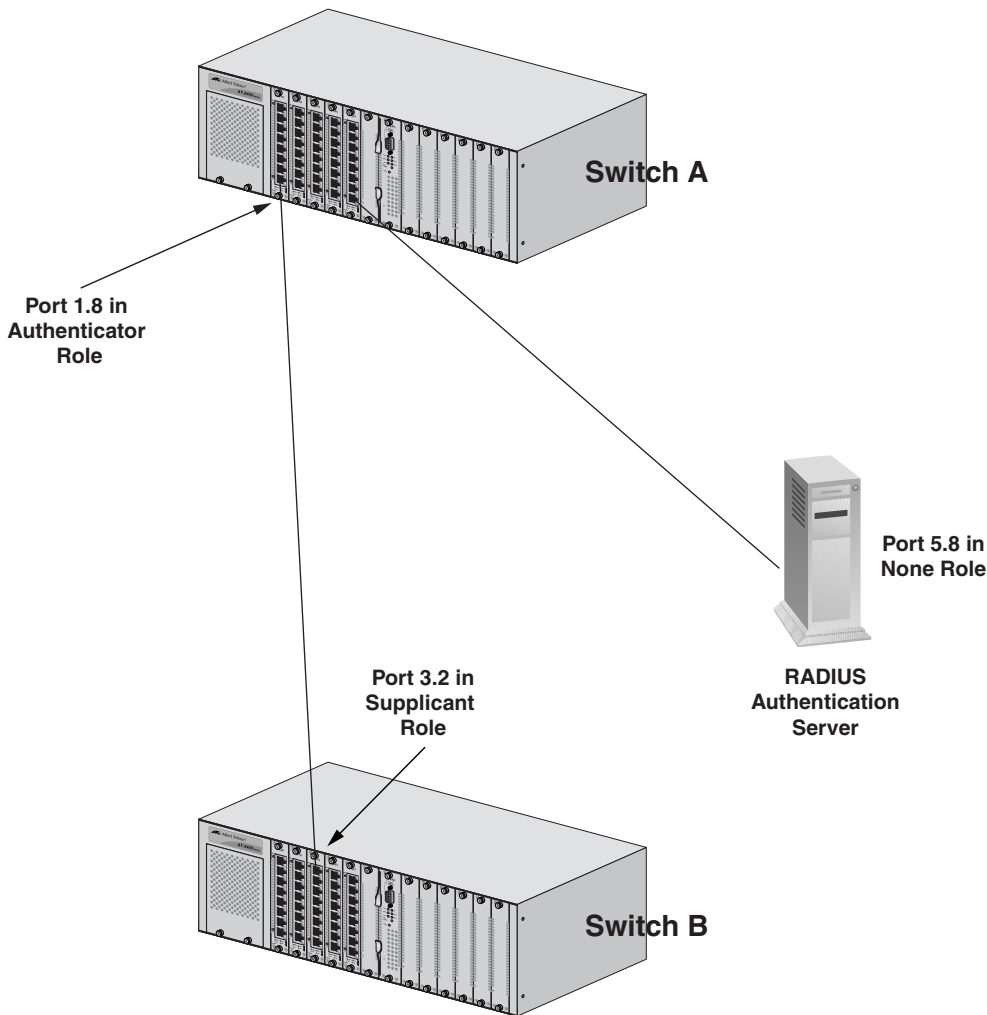


Figure 178 Example of the Supplicant Role

Note
Allied Telesyn International recommends that you limit the use of the supplicant role. Otherwise, undesirable switch operation may occur. Configure a port with the supplicant port role when the link carries traffic from one client or when the link carries only management traffic. Typically, you set ports used to interconnect switches to the none role.

Authentication Server

The authentication server verifies the supplicant's details passed to it by the authenticator. This implementation of 802.1x control requires that a port acting as an authenticator must communicate with a RADIUS authentication server. The RADIUS server must be capable of receiving and deciphering EAP in RADIUS packets. See Figure 179.

The supported encryption mechanisms for communication with the RADIUS server are EAP-MD5.

For more information on RADIUS, refer to TACACS+ and RADIUS Overview on page 541.

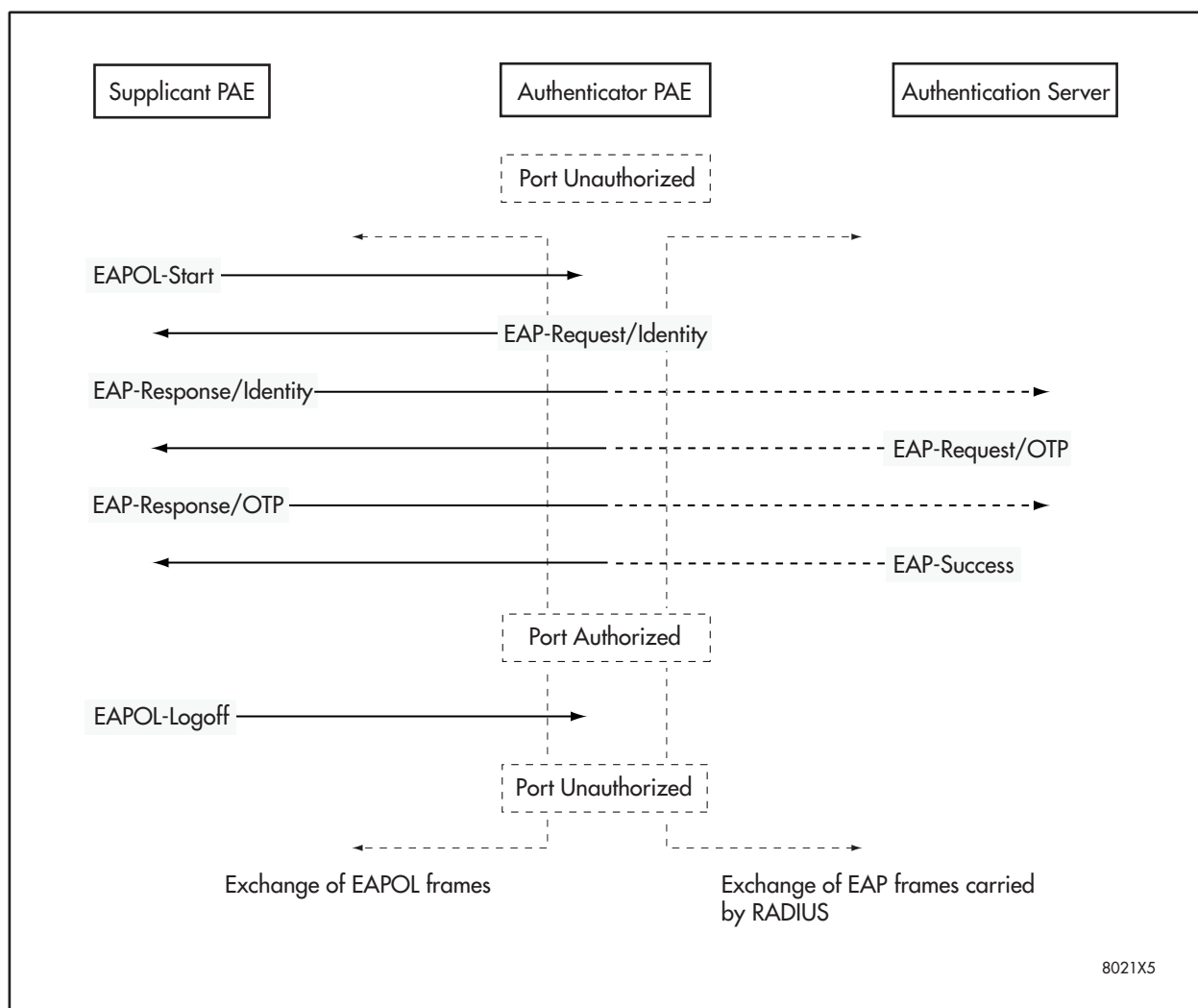


Figure 179 Authentication Messaging Exchange

RADIUS Accounting

The AT-S60 management software supports RADIUS accounting for ports set to the Authenticator role. This feature allows the switch to send information to the RADIUS server about the status of its supplicants. You can view this information on the RADIUS server to monitor network activity and use.

The switch sends accounting information to the RADIUS server when one of the following events occur:

- Supplicant logs on
- Supplicant logs off
- A change in the status of an Authenticator port during an active Supplicant session (for example, the port is reset or is changed from the Authenticator role to the none role while a Supplicant is logged on)

The information sent by the switch to the RADIUS server for an event includes:

- Port number where the event occurred
- The date and time when the event occurred
- The number of packets transmitted and received by the port during a supplicant's session. (This information is sent only when the client logs off.)

You can also configure the accounting feature to send interim updates so you can monitor which clients are still active.

Here are a few guidelines to using the accounting feature:

- The AT-S60 management software supports the Network level of accounting, but not the System or Exec.
- This feature is available for ports operating in the Authenticator role. Accounting is not supported for ports operating in the Supplicant or None role.
- You must configure 802.1x Port-based Access Control as explained in this chapter and designate the Authenticator ports.
- You must also specify from one to three RADIUS servers. The instructions for this are in Configuring RADIUS on page 547.

For instructions on configuring this feature, refer to Configuring RADIUS Accounting on page 568.

Enabling and Disabling Port-based Access Control

To globally enable or disable port-based access control, perform the following procedure.

Note

Enabling or disabling port-based access control can only be performed in a local management session.

Note

Before activating this feature, you must have the RADIUS EAP specified and enabled as the authentication method. This is discussed in Enabling TACACS+ or RADIUS on page 544.

1. From the Main Menu, type **6** to select Security Menu.

The Security Menu is shown in Figure 151 on page 473.

2. From the Security Menu, select Port Access Control.

The Port Access Control Menu is shown in Figure 180.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Production Switch 142

User: Manager                                00:14:33 25-Jan-2004

Port Access Control

1 - Port Access Control ..... Enabled
2 - Authentication Method ..... RADIUS EAP
3 - Configure Port Access Role
4 - Configure Authenticator
5 - Configure Supplicant
6 - Display Port Access Status

R - Return to Previous Menu

Enter your selection?

```

Figure 180 Port Access Control Menu

3. Type **1** to select Port Access Control. The following prompt is displayed:

```
Port Access Control (E-Enable, D-Disable) ->
```

4. Type **E** to enable port-based access control, or **D** to disable port-based access control.

If you select **E**, the following message appears:

```
This change has an impact on port security limited  
mode and MAC address table!
```

5. Press any key to continue.
6. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Setting the Port Access Role

Use this procedure to configure a port with an access role of authenticator or supplicant. For information about authenticators and supplicants, see the 802.1x Port-based Access Network Control Overview on page 550.

The number of ports you assign as authenticators and supplicants is only limited by the number of ports on a card. In addition, you can assign both authenticators and supplicants to one line card. For example, there are 8 ports on an AT-8411 line card. You can assign 4 ports with the role of authenticators and 4 ports with the role of supplicants.

Note

When you configure a port as an authenticator or supplicant, the port security level is automatically changed to PA (Port Access). It cannot be changed as long as the port is functioning as an authenticator or supplicant. For more information about port security levels, see Port Security Overview on page 470.

To configure port-based access control, perform the following procedure:

1. From the Main Menu, type **6** to select Security Menu.

The Security Menu is shown in Figure 151 on page 473.

2. From the Security Menu, select Port Access Control.

The Port Access Control Menu is shown in Figure 180 on page 557.

3. To configure a port or a list of ports with a port access role, type **3** to select Configure Port Access Role.

The following prompt is displayed:

```
Enter port-list:
```

4. Enter a port or a range of ports that you want to configure.

For information about how to specify ports, see Specifying Ports on page 34.

The Port Access Control Menu is shown in Figure 181.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Production Switch 142
User: Manager                                00:14:33 25-Jan-2004
Configure Port Access Role

Configuring Port 3.1
1 - Port Role ..... None
R - Return to Previous Menu

Enter your selection?
```

Figure 181 Configure Port Access Role Menu

- 5. Type **1** to select Port Role.

The following prompt is displayed:

```
Enter new Port Role [N=None, A=Authenticator,
S=Supplicant] ->
```

- 6. Choose from the following:

A - Select A to choose Authenticator. With this selection, the port performs the role of authenticating the supplicants that are connected to the port.

S - Select S to choose Supplicant. With this selection, the port becomes a Supplicant to the Authenticator port.

N - Select N to choose None. If you select None, the port does not participate in port-based access control. The default for this parameter is None.

- 7. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Configuring Authenticator Parameters

After you have enabled port-based access control and configured a port as an authenticator, use this procedure to configure the authenticator parameters. The procedure in [Setting the Port Access Role](#) on page 559 describes how to configure a port as an authenticator. For information about the role of an authenticator, see the [802.1x Port-based Access Network Control Overview](#) on page 550.

To display the authenticator parameters, see [Displaying Authenticator Ports](#) on page 573.

Note

When you configure a port as an authenticator or supplicant, the port's security level is automatically changed to PA (Port Access). The Port Access value cannot be changed as long as the port is functioning as an authenticator or supplicant. For more information about port security, see [Port Security Overview](#) on page 470.

To configure authenticator parameters, perform the following procedure:

1. From the Main Menu, type **6** to select Security Menu.

The Security Menu is shown in [Figure 151](#) on page 473.

2. From the Security Menu, select Port Access Control.

The Port Access Control Menu is shown in [Figure 180](#) on page 557.

3. From the Port Access Control menu, type **4** to select Configure Authenticator.

The Configure Authenticator Menu is shown in Figure 182.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Production Switch 142
User: Manager                                00:14:33 25-Jan-2004
Configure Authenticator
1 - Configure Authenticator Port Access Parameters
2 - Display Authenticator Port Access Parameters
R - Return to Previous Menu
Enter your selection?
```

Figure 182 Configure Authenticator Menu

4. To configure parameters for a port configured with an authenticator port role, type **1** to select Configure Authenticator Port Access Parameters.

The following prompt is displayed:

```
Enter port-list:
```

5. Enter a port or a list of ports. Then press Return.

For information about how to specify ports, see Specifying Ports on page 34.

The Configure Authenticator Port Access Parameters menu is shown. See Figure 183.

Note

If you configure a port as an authenticator using a Telnet session, it is possible to lose the telnet session.

The authenticator port access parameters are listed as menu items with default ranges set at the factory.

The Configure Authenticator Port Access Parameters Menu is shown in Figure 183.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Production Switch 142

User: Manager                                00:14:37 25-Jan-2004
Configure Authenticator Port Access Parameters

Configuring Port 1.3
1 - Port Control ..... Auto
2 - Quiet Period ..... 60   Seconds
3 - Tx Period ..... 30    Seconds
4 - Reauth Period ..... 3600 Seconds
5 - Supplicant Timeout .. 30   Seconds
6 - Server Timeout ..... 30   Seconds
7 - Max Requests ..... 2

R - Return to Previous Menu

Enter your selection?

```

Figure 183 Configure Authenticator Port Access Parameters Menu

6. Select the parameter that you want to modify. They are described below:

1 - Port Control

Choose from the following values:

- 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. The switch requests the identity of the client and begins relaying authentication messages between the client and the authentication server. The switch identifies each client that attempts to access the network by the client's MAC address. This is the default value.
- Force-authorized:** Disables 802.1X port-based authentication and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client.

- ❑ **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

2 - Quiet Period

Sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. The default value is 60 seconds. The range is 0 to 65,535 seconds.

3 - Tx Period

Sets the number of seconds the switch waits for the EAP-request/identity frame response from the supplicant before retransmitting the request. The default value is 30 seconds. The range is 1 to 65,535 seconds.

4 - Reauth Period

Enables periodic re-authentication of the client, which is disabled by default. The default value is 3,600 seconds. The range is 1 to 65,535 seconds.

5 - Supplicant Timeout

Sets the switch-to-client retransmission time for the EAP-request frame. The default value is 30 seconds. The range is 1 to 600 seconds.

6 - Server Timeout

This is the timer used by the switch to determine authentication server timeout conditions. The default value is 30 seconds. The range is 1 to 65,535 seconds.

7 - Max Requests

This parameter 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 is 2 retransmissions. The range is 1 to 10 retransmissions.

7. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Configuring Supplicant Parameters

After you have enabled port-based access control and configured a port as a supplicant, use this procedure in this section to configure the supplicant parameters. The procedure in *Setting the Port Access Role* on page 559 describes how to configure a port as a supplicant. For information about the role of a supplicant, see the *802.1x Port-based Access Network Control Overview* on page 550.

To display supplicant ports and parameters, see *Displaying Supplicant Ports* on page 574.

To configure the supplicant parameters on a port, you need to create a user name and password for the port. The user name and password for a port can be any value as long as the information is present on a RADIUS server.

Before you configure the user name and password for a supplicant, decide if you want to use the same user name and password for all supplicants or individual user names and passwords for each supplicant.

To configure supplicant parameters on a port, perform the following procedure:

1. From the Main Menu, type **6** to select Security Menu.

The Security Menu is shown in Figure 151 on page 473.

2. From the Security Menu, select Port Access Control.

The Port Access Control Menu is shown in Figure 180 on page 557.

3. From the Port Access Control Menu, type **5** to select Configure Supplicant.

The Configure Supplicant Menu is shown in Figure 184.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Production Switch 142
User: Manager                                00:14:33 25-Jan-2004
Configure Supplicant
1 - Configure Supplicant Port Access Parameters
2 - Display Supplicant Port Access Parameters
R - Return to Previous Menu
Enter your selection?
```

Figure 184 Configure Supplicant Menu

- 4. Type **1** to select Configure Supplicant Port Access Parameters to configure supplicant parameters.

The following prompt is displayed:

Enter port-list:

- 5. Enter a port or a list of ports.

For information about how to specify ports, see Specifying Ports on page 34.

The Configure Supplicant Port Access Parameters menu is shown in Figure 185. The supplicant port access parameters are listed as menu items with factory set default ranges.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Production Switch 142
User: Manager                                00:14:33 25-Jan-2004
Configure Supplicant Port Access Parameters
Configuring Ports 2.7
1 - Auth Period ..... 30 Seconds
2 - Held Period ..... 60 Seconds
3 - Max Start ..... 3
4 - Start Period ..... 30 Seconds
5 - User Name: .....
6 - User Password: .....
R - Return to Previous Menu
Enter your selection?
```

Figure 185 Configure Supplicant Port Access Parameters Menu

6. Select the parameter that you want to modify. They are described below:
 - 1 - Auth Period:** This is the initialization time used by the authentication timer. The value is in seconds. The default is 30 seconds. The range is 1 to 300 seconds.
 - 2 - Held Period:** This is the initialization value for the supplicant held timer. The value is in seconds. The default is 60 seconds. The range is 0 to 65,535 seconds.
 - 3 - Max Start:** This parameter determines the maximum number of successive EAPoL Start messages that are sent before the Supplicant assumes there is no Authenticator. The value is in whole numbers. The default is 3 messages. The range is 1 to 10 messages.
 - 4 - Start Period:** This parameter provides the initialization value for the timer that determines when EAPoL Start messages are sent. The value is in seconds. The default is 30 seconds. The range is 1 to 60 seconds.
 - 5 - User Name:** Enter a user name to access the supplicant port. The values of Manager and Operator are not permitted. There is no default value. This is an alphanumeric value of up to 40 characters.
 - 6 - User Password:** Enter a password to access the supplicant port. There is no default value. This is an alphanumeric value of up to 40 characters.
7. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Configuring RADIUS Accounting

The AT-S60 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 port during a client session. For background information on this feature, refer to RADIUS Accounting on page 556. This feature is disabled by default on the switch.

To configure this feature, perform the following procedure:

1. From the Main Menu, type **6** to select Security Menu.
The Security Menu is shown in Figure 151 on page 473.
2. From the Security Menu, type **3** to select Port Access Control.
The Port Access Control Menu is shown in Figure 180 on page 557.
3. From the Port Access Control Menu, type **7** to select Configuring Accounting.

The RADIUS Accounting Menu is shown in Figure 186.

```
Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Production Switch 142
User: Manager                                00:14:33 25-Jan-2004
                                Radius Accounting
1 - Radius Accounting Status..... Disabled
2 - Radius Accounting Port..... 1813
3 - Radius Accounting Type..... Network
4 - Radius Accounting Trigger Type..... Start_Stop
5 - Radius Accounting Update Status..... Disabled
6 - Radius Accounting Update Interval... 60
R - Return to Previous Menu
Enter your selection?
```

Figure 186 Radius Accounting Menu

4. To activate or deactivate RADIUS accounting on the switch, type **1** to select Radius Accounting Status.

The following prompt is displayed:

```
RADIUS Accounting (E-Enable, D-Disable):
```


5. Select a status for the RADIUS Accounting feature.

Choose from the following options:

E - Enables RADIUS accounting on the switch.

D - Disables RADIUS accounting on the switch. The default is Disable.

6. To specify the UDP port for RADIUS accounting, type **2** to select Radius Accounting Port.

The following prompt is displayed:

```
Enter new value: [1 to 65535] -> 1813
```

7. Enter a new value for the UDP for RADIUS accounting. The default is port 1813.

Note

The type of RADIUS accounting is specified by option **3** - RADIUS Accounting Type parameter. This is a read-only parameter. The default value is Network.

8. To specify the action that causes the switch to sending accounting information to the RADIUS server, type **4** to select Radius Accounting Trigger Type.

The following prompt is displayed:

```
RADIUS Accounting Trigger (1-Start Stop 2-Stop Only)-> [1 to 2]-> 1
```

9. Select the action that causes the switch to send accounting information to the RADIUS server.

Choose from the following selections:

1 - Select 1 to choose Start Stop. With this selection, the switch sends accounting information whenever a client logs on or logs off the network. This is the default.

2 - Select 2 to choose Stop Only. With this selection, the switch sends accounting information only when a client logs off.

10. To control whether or not the switch sends interim accounting updates to the RADIUS server, type **5** to select Radius Accounting Update Status.

The following prompt is displayed:

```
RADIUS Accounting Update (E-Enable, D-Disable)->
```

11. Enter the RADIUS Accounting update status.

Choose from the following selections:

E - Select E to enable the switch to send interim accounting updates to the RADIUS server. If you enable this feature, use the next option in the menu, RADIUS Accounting Update Interval, to specify the intervals at which the switch is to send the accounting updates.

D - Select D to disable the interim accounting updates from being sent to the RADIUS server. The default is disabled.

12. To specify the intervals at which the switch is to send interim accounting updates to the RADIUS server, type **6** to select RADIUS Accounting Update Interval.

The following prompt is displayed:

```
Enter new update interval in Second(s)
[30 to 300]-> 60
```

13. Enter a new update interval.

The range is 30 to 300 seconds. The default is 60 seconds.

14. After making changes, type **R** until you return to the Main Menu. Then type **S** to select Save Configuration Changes.

Displaying Port-based Access Control Status

There are three ways to display port-based access control status. You can display:

- Port roles assigned to all ports
- All Authenticator ports and their associated parameters
- All Supplicant ports and their associated parameters

Each type of display provides different parameters. The advantage of displaying the individual authenticator and supplicant port information is that more information is given.

Displaying Port Access Status

To display the port access status of all the ports on the switch as None, Authenticator, or Supplicant, perform the following procedure:

1. From the Main Menu, type **6** to select Security Menu.
The Security Menu is shown in Figure 151 on page 473.
2. From the Security Menu, select Port Access Control.
The Port Access Control Menu is shown in Figure 180 on page 557.
3. From the Port Access Control Menu, type **6** to select Display Port Access Status.

The Display Port Access Status menu is shown in Figure 187.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Production Switch 142
User: Manager                                00:14:33 22-Mar-2004
Display Port Access Status

Port      PortRole      State      Additional Info
-----
6.1      None          -----
6.2      Authenticator Connecting
6.3      Authenticator Authenticated 00:a0:d2:18:1a:c8
6.4      Authenticator Connecting
6.5      None          -----
6.6      None          -----
6.7      None          -----
6.8      Supplicant   -----

N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection?
    
```

Figure 187 Display Port Access Status Menu

4. The Display Port Access Status menu has the following parameters:

Port - lists the port number of the line card.

PortRole - lists the port access role configured for the port. Values can be None, Authenticator, or Supplicant.

State - lists the status of the port. The status field is dependent on whether a port is configured as an authenticator or a supplicant.

When you configure a port with an Authenticator Role, the Status field can have the following values:

- Aborting
- Authenticated
- Authenticating
- Connecting
- Disconnected
- Force_Auth
- Force_Unauth
- Held
- Initialize

When you configure a port with a Supplicant role, the Status field can have the following values:

Acquired
 Authenticated
 Authenticating
 Connecting
 Disconnected
 Held
 Logoff

Note

Consult IEEE std 8021X-2001 for Port-Based Network Access Control for detailed information regarding the above mentioned values in the Status field.

Additional Info - When you assign a port the role of Authenticator and it has a status of Authenticated, this field also displays the MAC address of the Authenticator.

Displaying Authenticator Ports

To display information about authenticator ports and parameters, perform the following procedure:

1. From the Main Menu, type **6** to select Security Menu.
 The Security Menu is shown in Figure 151 on page 473.
2. From the Security Menu, select Port Access Control.
 The Port Access Control Menu is shown in Figure 180 on page 557.
3. From the Port Access Control Menu, type **4** to select Configure Authenticator.
 The Configure Authenticator menu is shown in Figure 182 on page 562.
4. Type **2** to select Display Authenticator Port Access Parameters.

The Display Authenticator Port Access Parameters Menu is shown in Figure 188.

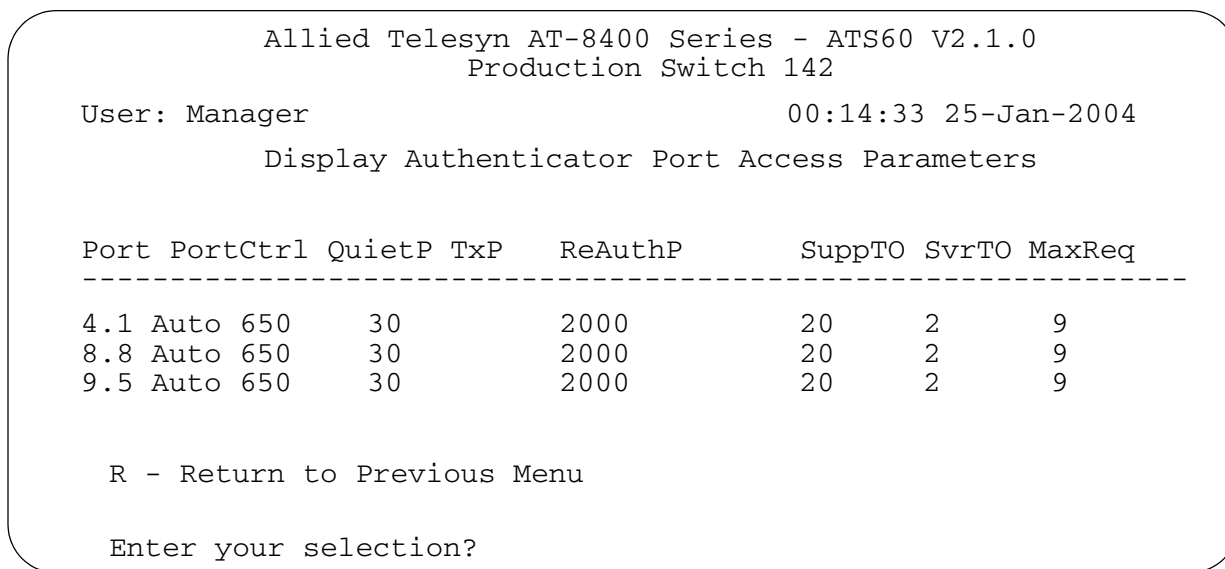


Figure 188 Display Authentication Port Access Parameters

For information about the fields in the Display Authenticator Port Access Parameters menu, see the parameter descriptions in Configuring Authenticator Parameters on page 561.

**Displaying
Supplicant
Ports**

To display information about supplicant ports and parameters, perform the following procedure:

1. From the Main Menu, type **6** to select Security Menu.
The Security Menu is shown in Figure 151 on page 473.
2. From the Security Menu, select Port Access Control.
The Port Access Control Menu is shown in Figure 180 on page 557.
3. From the Port Access Control menu, type **5** to select Configure Supplicant.
The Configure Supplicant menu is shown in Figure 184 on page 566.
4. Type **2** to select Display Supplicant Port Access Parameters.

The Display Supplicant Port Access Parameters Menu is shown in Figure 189.

```

Allied Telesyn AT-8400 Series - ATS60 V2.1.0
Production Switch 142

User: Manager                                00:14:33 22-Mar-2004

Display Supplicant Port Access Parameters

Port   Auth   Held   Max   Start   Supplicant   Supplicant
Period Period Start Period Name       Name         Password
-----
6.1    30     60     3     30     pizza57     pepperoni112
6.2    30     60     3     30     pizza57     pepperoni112
6.3    30     60     3     30     pizza57     pepperoni112
6.4    30     60     3     30     pizza57     pepperoni112
6.5    30     60     3     30     pizza57     pepperoni112
6.6    30     60     3     30     pizza57     pepperoni112
6.7    30     60     3     30     pizza57     pepperoni112
6.8    30     60     3     30     pizza57     pepperoni112

N - Next Page
U - Update Display
R - Return to Previous Menu

Enter your selection?

```

Figure 189 Display Supplicant Port Access Parameters Menu

For information about the fields in the Display Supplicant Port Access Parameters Menu, see the parameter descriptions in Configuring Supplicant Parameters on page 565.

Section VI

Web Browser Management

The chapters in Section IV explain how to manage an AT-8400 switch using a web browser. The chapters include:

- Chapter 29: Starting a Web Browser Management Session on page 578
- Chapter 30: Basic Switch Parameters on page 582
- Chapter 31: File Downloads and Uploads on page 608
- Chapter 32: Enhanced Stacking on page 614
- Chapter 33: Port Parameters on page 620
- Chapter 34: MAC Address Table on page 633
- Chapter 35: Port Trunking on page 641
- Chapter 36: Port Mirroring on page 648
- Chapter 37: Event Log on page 655
- Chapter 38: IGMP Snooping on page 662
- Chapter 39: STP, RSTP, and MSTP on page 669
- Chapter 40: SNMPv3 Protocol on page 694
- Chapter 41: Port-based VLANs on page 755
- Chapter 42: GARP VLAN Registration Protocol on page 766
- Chapter 43: Port Security on page 783
- Chapter 44: Web Server Security on page 787

- ❑ Chapter 45: TACACS+ and RADIUS Protocols on page 796
- ❑ Chapter 46: 802.1x Port-based Network Access Control on page 806

Chapter 29

Starting a Web Browser Management Session

This chapter contains the procedure for starting a management session on an AT-8400 Series switch using a web browser, such as Microsoft Internet Explorer or Netscape Navigator.

Starting a Web Browser Management Session

This section explains how to start a web browser management session, bookmark the IP address of the switch, and quit out of a web browser management session.

To start a web browser management session with the AT-S60 software, there must be at least one AT-8400 Series switch on your network that has been assigned an IP address. The switch with the IP address is referred to as the master switch. Once you have started a web browser management session on the master switch, you have management access to all other AT-8400 and AT-8000 Series Switches that reside in the same subnet.

Note

For optimal viewing of an AT-S60 Web Browser management session on your PC, Allied Telesyn recommends setting the screen resolution to 1024 x 768 pixels.

There are a total of 14 login sessions available using the console, Telnet, and web browser management sessions. However, you can have only one Manager session on the switch regardless of how you or others are accessing the switch. There are additional limitations for the different types of management sessions. The console and Telnet sessions allow a total of 10 active sessions, while a web browser management session allows four active login sessions.

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

1. Start your web browser.

Note

If your PC (where the web browser resides) is connected directly to the switch or is on the same side of a firewall as the switch, you must configure your browser's network options to not use proxies. Consult your web browser's documentation on how to configure the switch's web browser to not use proxies.

2. Enter the IP address of the switch in the URL field of the browser, as shown in Figure 190.

Switch's IP Address

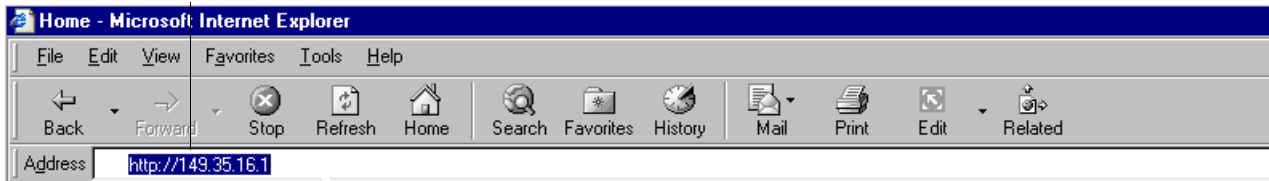


Figure 190 Entering a Switch's IP Address in the URL Field

3. When prompted, enter a user name and password. For information about login ids, see **Management Access Levels** on page 33.

You cannot change the user names. However, you can change the passwords, as explained in **Configuring the Management Passwords** on page 65.

The Home Page is shown in Figure 191.

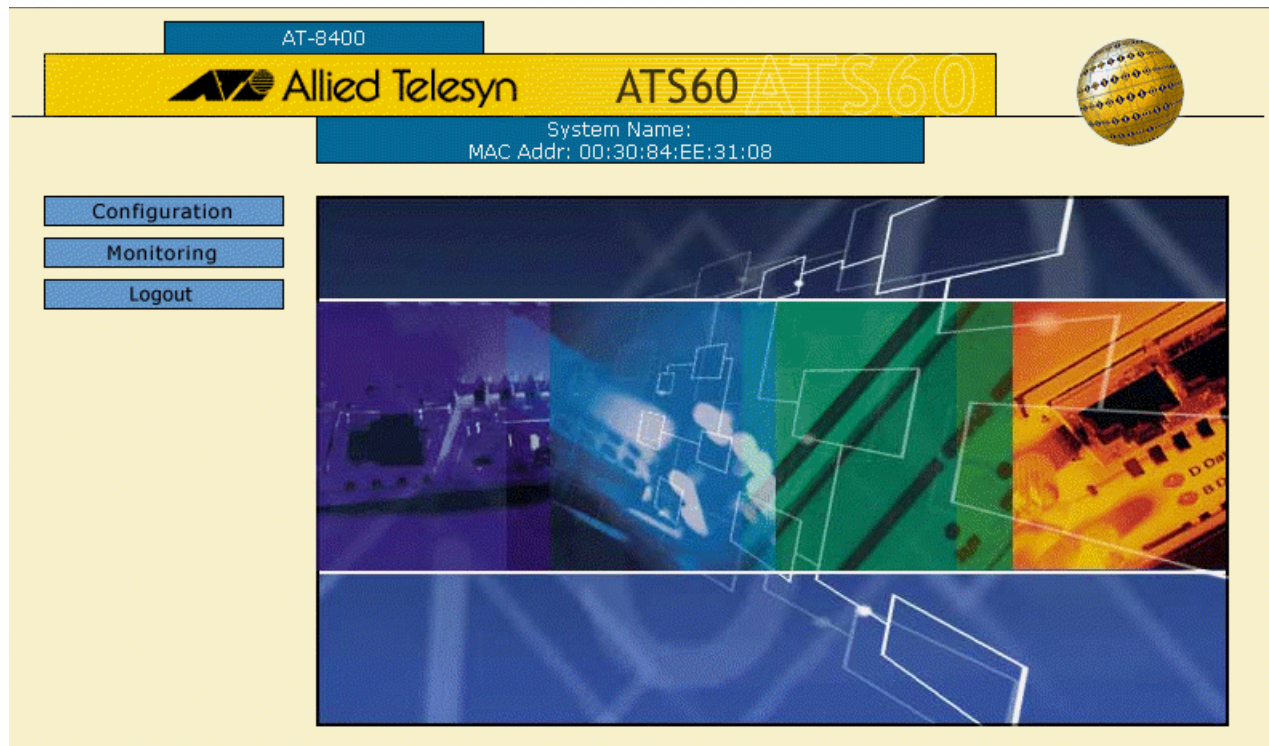


Figure 191 Home Page

The main menu is on the left side of the Home Page. It consists of the following menus:

- Configuration
- Monitoring
- Logout

Note

The main menu includes an Enhanced Stacking option when enhanced stacking is implemented.

Browser Tools

You can use the browser's bookmark feature to record the IP address of the switch.

Note

After 10 minutes of inactivity, a web browser management session times out.

**Quitting a Web
Browser
Management
Session**

To exit a web browser management session, select **Logout** from the Home Page which is shown in Figure 191 on page 580.

Chapter 30

Basic Switch Parameters

This chapter provides the following procedures for configuring basic switch parameters using a web browser management session:

- Configuring an IP Address and Switch Name on page 583
- Setting the System Time on page 588
- Activating the BOOTP and DHCP Services on page 591
- Displaying System Information on page 592
- Configuring SNMPv1 and SNMPv2c Protocols on page 595
- Resetting a Switch on page 604
- Pinging a Remote System on page 605
- Returning the AT-S60 Software to the Factory Default Values on page 606

Configuring an IP Address and Switch Name

This procedure describes the parameters in the Administration section of the Configuration Menu. Information about the Configuration and MAC Address Aging Time parameters are discussed later in this guide.

Note

For guidelines on when to assign an IP address, subnet address, and gateway address to an AT-8400 Series switch, refer to Assigning an IP Address to a Switch on page 46.

To set the basic switch parameters for an AT-8400 switch, 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 192.

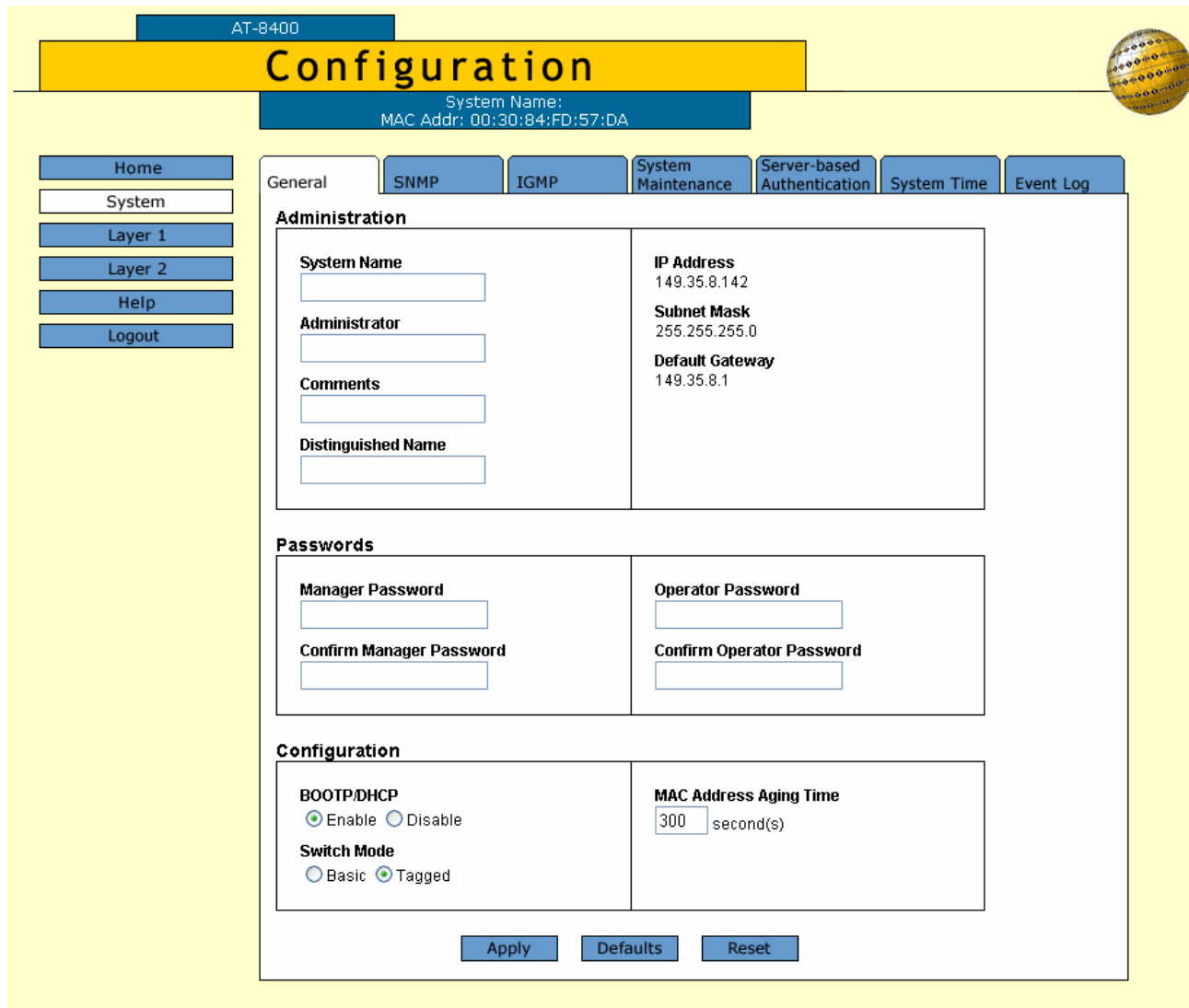


Figure 192 Configuration System Page, General Tab

Note
Save Changes is only displayed when you make a change to the default configuration.

2. Change the following parameters as desired:

System Name

This parameter specifies a name for the switch (for example, Sales Ethernet switch). Entering a value for this parameter is optional.

Note

Allied Telesyn International recommends that you assign a name to each switch because switch names help you identify the various switches in your network. Knowing a switch's name ensures you perform a configuration procedure on the correct switch.

Administrator

This parameter specifies the name of the network administrator responsible for managing the switch. Entering a value for this parameter is optional.

Comments

This parameter specifies additional information about the switch, such as its location (for example, Floor 4, Wiring closet 402B). Entering a value for this parameter is optional.

**Caution**

Changing the IP address of the switch may result in the loss of your management session.

Distinguished Name

This parameter specifies the physical address of the subject of a certificate. For more information about distinguished names refer to Creating Certificates on page 508.

IP Address

This parameter specifies the IP address of the switch. You must specify an IP address if you intend to remotely manage the switch using a web browser, a Telnet utility, or an SNMP management program. In addition, you must specify an IP address if you want to configure the switch as the master switch of an enhanced stack.

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.

Default Gateway

This parameter specifies the default router's IP address. You are required to enter a value for this parameter if you remotely manage the switch from a management station that is separated from the switch by a router.

Manager Password**Manager Confirm Password**

These parameters are used to change the administrator's login password for the switch. The password can be from 0 to 20 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."

**Caution**

Allied Telesyn International recommends that you do not use spaces or special characters, such as asterisks (*) and exclamation points (!), in either the Manager or Operator password if you are managing the switch from a web browser. Many web browsers do not permit special characters in passwords.

Operator Password**Operator Confirm Password**

These parameters are used to change the Operator's password for the switch. The password can be from 0 to 20 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 "operator."

BOOTP/DHCP

For information about these parameters, see Activating the BOOTP and DHCP Services on page 591.

Switch Mode

Defines the switch's current VLAN mode. If this parameter displays "Tagged," the switch supports port-based and tagged VLANs. If this parameter displays "Basic," the switch is operating in the Basic VLAN Mode. For information about VLANs, refer to the overview sections in Chapter 18, Tagged and Port-based Virtual LANs on page 401. For instructions on how to set the switch's VLAN mode from a web browser management session, refer to Setting the Switch's VLAN Mode on page 765.

MAC Address Aging Time

For information about this parameter, see Changing the Aging Time on page 640.

3. After you have set the parameters, click **Apply**.
Your changes are activated on the switch.
4. To save your changes, click **Save Changes**.

Note

Changing any of the above parameters, including the IP address and subnet mask, is immediately activated on the switch.

Changing the IP address of the switch can cause the loss of the remote management session. You can restart the management session using the switch's new IP address.

Setting the System Time

To set system time manually on the switch, 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 192 on page 584.

2. Select the **System Time** Tab.

The System Time Tab is shown in Figure 193.

The screenshot shows the 'Configuration' page for a switch (AT-8400). The 'System Time' tab is selected. The interface includes a navigation menu on the left with options: Home, System, Layer 1, Layer 2, Help, and Logout. The main content area has tabs for General, SNMP, IGMP, System Maintenance, Server-based Authentication, System Time, and Event Log. The 'System Time' section contains the following fields and controls:

- System Time:** A time selection field showing 18:27:45 on 2011-1970, with an 'Apply' button below it.
- Additional Time Parameters:**
 - UTC Offset:** A text input field containing '+0'.
 - Daylight Savings Time (DST):** Radio buttons for 'Disabled' and 'Enabled' (selected), with an 'Apply' button below.
- Simple Network Time Protocol (SNTP) Settings:**
 - Status:** Radio buttons for 'Disabled' (selected) and 'Enabled'.
 - Server IP Address:** A text input field containing '178.45.9.1'.
 - Poll Interval:** A text input field containing '600' with the unit 'seconds' next to it, and an 'Apply' button below.

Figure 193 Configuration System Page, System Time Tab

3. In the **System Time** section, specify the time and date for the switch.
For the time, use a 24 hour clock (or military time) and the following format: hours, minutes, and seconds.
For the date, use two numbers to specify the day and month. Use four numbers to specify the year. For example, enter September 5, 2003 as 05 09 2003.
4. Click **Apply**.

5. In the Additional Time Parameters section you can specify the UTC offset and enable or disable daylight savings time:

UTC Offset - Specify a difference between the UTC and local time. The default is 0 hours. The range is -12 to +12 hours.

Daylight Savings Time - Click Enabled to enable or Disabled to disable the switch's ability to adjust the system time to daylight savings time.

6. Click **Apply**.

Your changes are activated on the switch.

7. To save your changes, return to the General Tab and click **Save Changes**.

Setting Up SNTP

When you set up SNTP, the switch polls an SNTP or NTP server for the time. SNTP is a reduced version of the Network Time Protocol (NTP). However, it is important to note that SNTP servers and clients are interoperable with NTP servers and clients.

Note

For more information about SNTP, refer to Setting the System Time on page 59.

To set up SNTP, 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 192 on page 584.

2. Select the **System Time** Tab.

The System Time Tab is shown in Figure 193 on page 588.

3. In the Simple Network Time Protocol Settings section, select disable or enable and set up the switch to query a NTP or SNTP server:

Status - Click **Enabled** to allow the switch to query at the specified time interval for the current time and date. Click **Disabled** to prevent the switch from querying a NTP or SNTP server.

Server IP Address - Enter an IP address of your SNTP or NTP server in the standard IP format.

Note

If you have enabled DHCP on the switch, the switch attempts to retrieve the SNTP server IP address from the DHCP server automatically. The automatic determination of server IP occurs only if DHCP is enabled.

Poll Interval - Poll Interval to specify the time interval between two successive queries to the SNTP server. Enter the number of seconds the switch waits to poll the SNTP server. The default is 600 seconds. The range is from 60 to 1200 seconds.

4. Click **Apply**.

Your changes are activated on the switch.

5. To save your changes, return to the General Tab and click **Save Changes**.

Activating the BOOTP and DHCP Services

For background information on BOOTP and DHCP, refer to the section *Activating the BootP and DHCP Services* on page 57.

To activate or deactivate the BOOTP and DHCP protocols on the switch from a web browser management session, 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 192 on page 584.
2. In the Configuration section, BOOTP/DHCP item, click either **Enable** or **Disable**.

Note

If you activate BOOTP/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.

Displaying System Information

To view system information you access the Monitoring Page. The parameters on this page are strictly for viewing purposes only. You cannot change any of the values from this page.

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 194.

The screenshot shows the 'Monitoring' page for an AT-8400 switch. The page has a yellow background and a blue navigation bar at the top. The main content area is divided into several sections: General, System Software, and Hardware. The General section contains a table with system parameters. The System Software section contains a table with software versions. The Hardware section contains a table with hardware details.

System Name: AT-8400
System Name: [redacted]
MAC Addr: 00:30:84:FD:57:DA

General

System Name	149.35.8.105
Administrator	Subnet Mask 255.255.255.0
Comments	Default Gateway 149.35.8.1
Distinguished Name	Switch Mode Tagged
BOOTP/DHCP Disabled	System Up Time 2 Days 16 Hours 10 Minutes 16 Seconds
MAC Address Aging Time 300 second(s)	

System Software

Application Software	AT-S60 v2.1.0 (Dec 9 2004 12:25:59)
Bootloader	ATS60_LOADER v1.3.0 (Dec 29 2003 15:20:44)

Hardware

Slot #	Model Name	Serial Number	Temperature (Deg. C)	Upper/Lower Temp. Threshold (Deg. C)
M	AT-8401	A00501S030600027	26	80/25
2	AT-8411	S05525A023800012	27	80/-25
6	AT-8411	A00502S030600018	30	80/-25

Figure 194 Monitoring System Page, General Tab

The sections in the Tab are defined below.

General

This section displays the basic switch information. The values cannot be changed at this menu. For the procedure to change the values of the System Name, Administrator, Comments, IP Address, Subnet Mask, and Default Gateway parameters, see [Configuring an IP Address and Switch Name](#) on page 583.

This section contains the following items:

- System Name** - This parameter specifies a name for the switch (for example, Sales Ethernet switch).
- Administrator** - This parameter specifies the name of the network administrator responsible for managing the switch.
- Distinguished Name**
This parameter specifies the physical address of the subject of a certificate. For more information about distinguished names refer to [Creating Certificates](#) on page 508.
- Comments** - This parameter specifies additional information about the switch, such as its location.
- BOOTP/DHCP** - Defines whether the switch obtains its IP address from a BOOTP or DHCP server on your network. If this parameter is enabled, the switch obtains its IP address from BOOTP or DHCP server.
- MAC Address Aging Time** - Specifies how long an inactive dynamic MAC address can remain in the MAC address table before it is deleted. The default is 300 seconds (5 minutes). For background information about MAC addresses, refer to [MAC Address Overview](#) on page 116.
- IP Address** - This parameter specifies the IP address of the switch.
- Subnet Mask** - This parameter specifies the subnet mask for the switch.
- Default Gateway** - This parameter specifies the default router's IP address.

- ❑ **Switch Mode** - Defines the switch's current VLAN mode. If this parameter displays "Tagged," the switch supports port-based and tagged VLANs. If this parameter displays "Basic," the switch is operating in the Basic VLAN Mode. For information about VLANs, refer to the overview sections in Chapter 18, Tagged and Port-based Virtual LANs on page 401. For instructions on how to set the switch's VLAN mode from a web browser management session, refer to Setting the Switch's VLAN Mode on page 765.
- ❑ **System Up Time** - The number of days, hours, minutes, and seconds since the switch was rebooted.

System Software

This section contains information about the version of the AT-S60 software and the version of the bootloader.

This section contains the following items:

- ❑ **Application Software** - This parameter lists the current version of the AT-S60 software.
- ❑ **Bootloader** - This parameter lists the current version of the bootloader software.

Hardware

This section contains information about the current line cards and management card installed in the AT-8400 switch.

This section contains a table with the following headings:

- ❑ **Slot#** - This heading indicates which slot number the line card or management card installed in the chassis. For example, in Figure 194 on page 592 under the heading Slot#, 1 indicates an AT-8411 line card installed in slot 1 of the chassis.
- ❑ **Model Name** - This heading indicates the name of the line card or management card.
- ❑ **Serial Number** - This heading indicates the serial number that is printed on the line card or management card.
- ❑ **Temperature (Deg. C)** - This heading indicates the current temperature, in Celsius, of the line card or management card.
- ❑ **Upper/Lower Temp. Threshold (Deg. C)** - This heading indicates the current upper and lower temperature thresholds, in Celsius, for the line card.

Configuring SNMPv1 and SNMPv2c Protocols

This section provides instructions on how to create SNMPv1 and SNMPv2c communities that have access to the switch. In addition, a procedure that permits you to modify current SNMPv1 and SNMPv2c community parameters is provided as well as a procedure to delete SNMPv1 and SNMPv2c community access.

See the following procedures:

- Creating an SNMPv1 and SNMPv2c Community on page 595
- Modifying an SNMPv1 and SNMPv2c Community on page 599
- Deleting an SNMPv1 and SNMPv2c Community on page 601
- Displaying the SNMPv1 and SNMPv2c Communities on page 601

For reference information about SNMPv1 and SNMPv2c, see Chapter 5: SNMPv1 and SNMPv2c Configuration on page 84.

Creating an SNMPv1 and SNMPv2c Community

This procedure allows you to create up to eight SNMPv1 and SNMPv2c communities that have access to the switch. In creating an SNMPv1 and SNMPv2c community, you can specify up to eight IP addresses of management stations that can access the switch. In addition, you can specify up to eight trap receiver IP addresses of trap receivers that can receive trap messages from the switch.

To create an SNMP community, 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 192 on page 584.
2. Select the **SNMP** Tab.

The SNMP Tab is shown in Figure 195.

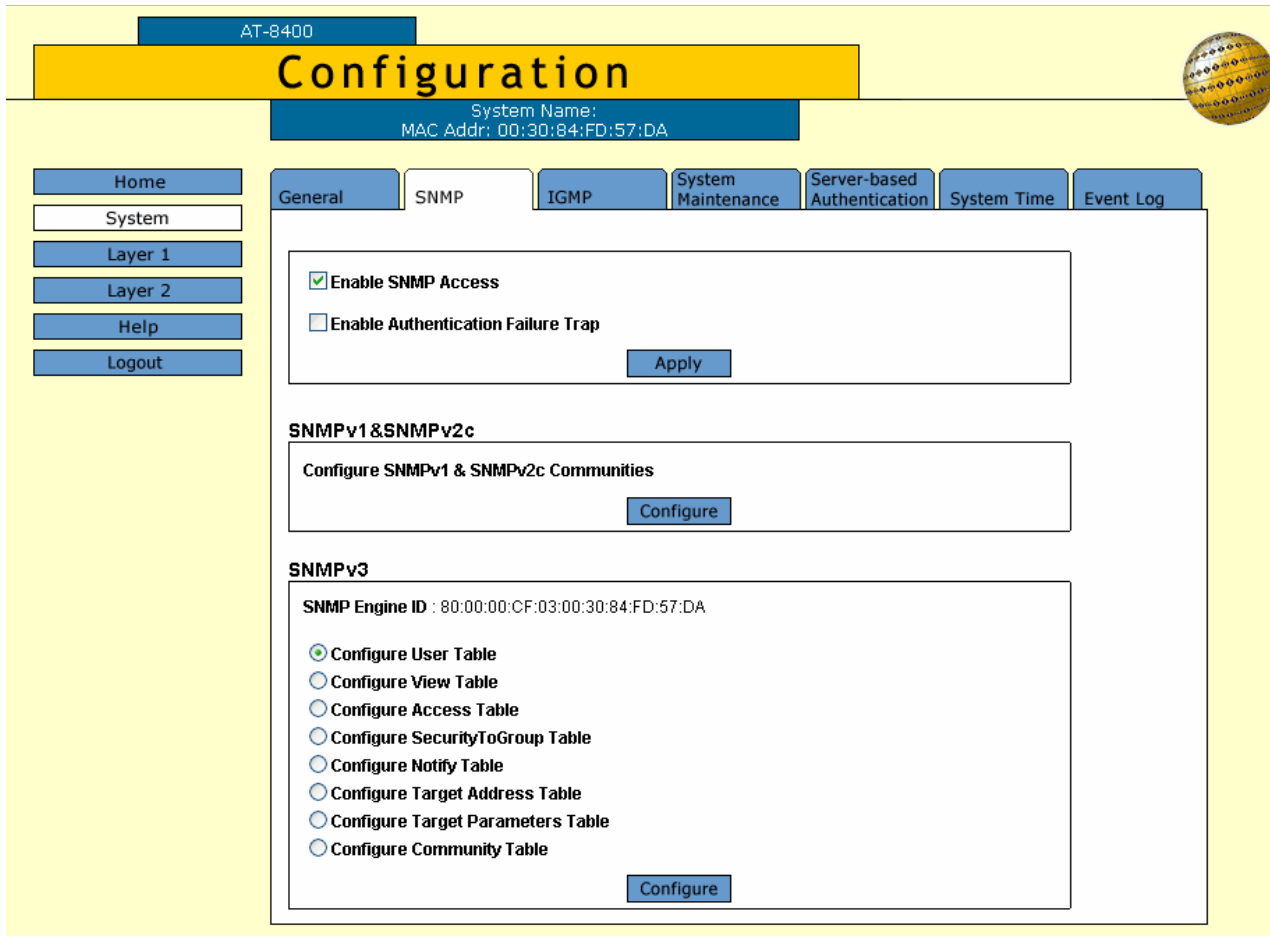


Figure 195 Configuration System Page, SNMP Tab

3. To enable SNMP Access for the SNMPv1 and SNMPv2c protocols, click the box next to Enable SNMP Access.

Use this parameter to enable the switch to be remotely managed with an SNMP application program.

Note

If the check box in the Enable SNMP Access box is empty, the switch cannot be managed through SNMP. This is the default.

4. To enable authentication failure traps to be sent, click the box next to Enable Authentication Failure Trap.

When this field is selected and the switch receives an unauthenticated request, an authentication failure trap is sent to the trap receivers configured on the switch.

5. Click **Apply** to update the SNMP Tab.

- To configure SNMPv1 and SNMPv2 communities, click **Configure** in the SNMPv1 & SNMPv2c section of the web page.

The SNMPv1 & SNMPv2c Communities Page is shown in Figure 196.

AT-8400

Configuration

System Name:
MAC Addr: 00:30:84:FD:57:DA

Home
System
Layer 1
Layer 2
Help
Logout

General | **SNMP** | IGMP | System Maintenance | Server-based Authentication | System Time | Event Log

SNMPv1 & SNMPv2c Communities

Total Entries: 5. Page 1 of 1

	Community Name	Access Mode	Manager Stations	Trap Receivers	Open Access	Status
<input checked="" type="radio"/>	colorado	Read Only	198.1.20.11	198.1.20.11	No	Enabled
<input type="radio"/>	guadalupe	ReadWrite	198.1.20.1, 198.1.20.5, 198.1.20.7	198.1.20.1, 198.1.20.5, 198.1.20.7	No	Enabled
<input type="radio"/>	private	ReadWrite			Yes	Enabled
<input type="radio"/>	public	Read Only			Yes	Enabled
<input type="radio"/>	sacramento	Read Only	198.1.1.9	198.1.1.9	No	Enabled

Figure 196 SNMPv1 & SNMPv2c Communities Page

- To create a SNMPv1 and SNMPv2c community, click **Add**.

The Add New SNMPv1 & SNMPv2c Community Page is shown in Figure 197.

Add New SNMPv1 & SNMPv2c Community

Community Name :

Status : Enable Disable

Access Mode : Read Only Read-Write

Managers	Trap Receivers
<input type="checkbox"/> Open Access	
Manager IP Address 1 <input type="text" value="198.1.1.1"/>	Trap Receiver IP Address 1 <input type="text" value="198.1.1.1"/>
Manager IP Address 2 <input type="text" value="198.20.2.2"/>	Trap Receiver IP Address 2 <input type="text" value="198.20.2.2"/>
Manager IP Address 3 <input type="text" value="198.30.3.3"/>	Trap Receiver IP Address 3 <input type="text" value="198.30.3.3"/>
Manager IP Address 4 <input type="text"/>	Trap Receiver IP Address 4 <input type="text"/>
Manager IP Address 5 <input type="text"/>	Trap Receiver IP Address 5 <input type="text"/>
Manager IP Address 6 <input type="text"/>	Trap Receiver IP Address 6 <input type="text"/>
Manager IP Address 7 <input type="text"/>	Trap Receiver IP Address 7 <input type="text"/>
Manager IP Address 8 <input type="text"/>	Trap Receiver IP Address 8 <input type="text"/>

Figure 197 Add New SNMPv1 & SNMPv2c Community Page

8. 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.

Open Access

Click this option to allow any SNMP manager to access the switch.

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 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.

9. Click **Apply** to update the SNMP Page.
10. To save your changes, return to the General Tab and click **Save Changes**.

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 Configuration System Page is displayed with the General Tab selected by default, as shown in Figure 192 on page 584.
2. Select the **SNMP** Tab.
The SNMP Tab is shown in Figure 195 on page 596.
3. To configure SNMPv1 and SNMPv2 communities, select **Configure** in the SNMPv1 & SNMPv2c section of the SNMP Tab.
The SNMPv1 & SNMPv2c Communities Page is shown in Figure 196 on page 597.
4. To change an SNMP community, click the circle next to the community name. Then click **Modify**.
The Modify SNMPv1 & SNMPv2c Community Page is shown in Figure 198.

Modify SNMPv1 & SNMPv2c Community

Community Name : sassafras12

Status : Enable Disable

Access Mode : Read Only Read-Write

Managers	Trap Receivers
<input type="checkbox"/> Allow Any Station	
Manager IP Address 1 <input type="text" value="198.1.1.1"/>	Trap Receiver IP Address 1 <input type="text" value="198.1.1.1"/>
Manager IP Address 2 <input type="text" value="198.20.2.2"/>	Trap Receiver IP Address 2 <input type="text" value="198.20.2.2"/>
Manager IP Address 3 <input type="text" value="198.30.3.3"/>	Trap Receiver IP Address 3 <input type="text" value="198.30.3.3"/>
Manager IP Address 4 <input type="text"/>	Trap Receiver IP Address 4 <input type="text"/>
Manager IP Address 5 <input type="text"/>	Trap Receiver IP Address 5 <input type="text"/>
Manager IP Address 6 <input type="text"/>	Trap Receiver IP Address 6 <input type="text"/>
Manager IP Address 7 <input type="text"/>	Trap Receiver IP Address 7 <input type="text"/>
Manager IP Address 8 <input type="text"/>	Trap Receiver IP Address 8 <input type="text"/>

Figure 198 Modify SNMPv1 & SNMPv2c Community Page

5. Modify the following parameters:

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.

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.

6. Click **Apply** to update the SNMPv1 and SNMPv2c Modify Web Page.
7. To save your changes, return to the General Tab and click **Save Changes**.

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 Configuration System Page is displayed with the General Tab selected by default, as shown in Figure 192 on page 584.
2. Select the SNMP Tab.
The SNMP Tab is shown in Figure 195 on page 596.
3. Select **Configure** in the SNMPv1 & SNMPv2c section of the SNMP Tab.
The SNMPv1 & SNMPv2c Communities Page is shown in Figure 196 on page 597.
4. To remove an SNMPv1 & SNMPv2c community, click the circle next to the community name and click **Remove**.
A warning message is displayed. Click OK to remove the SNMP community.
5. To save your changes, return to the General Tab and click **Save Changes**.

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 194 on page 592.
2. Select the **SNMP** Tab.

The SNMP Monitoring Tab is shown in Figure 199.

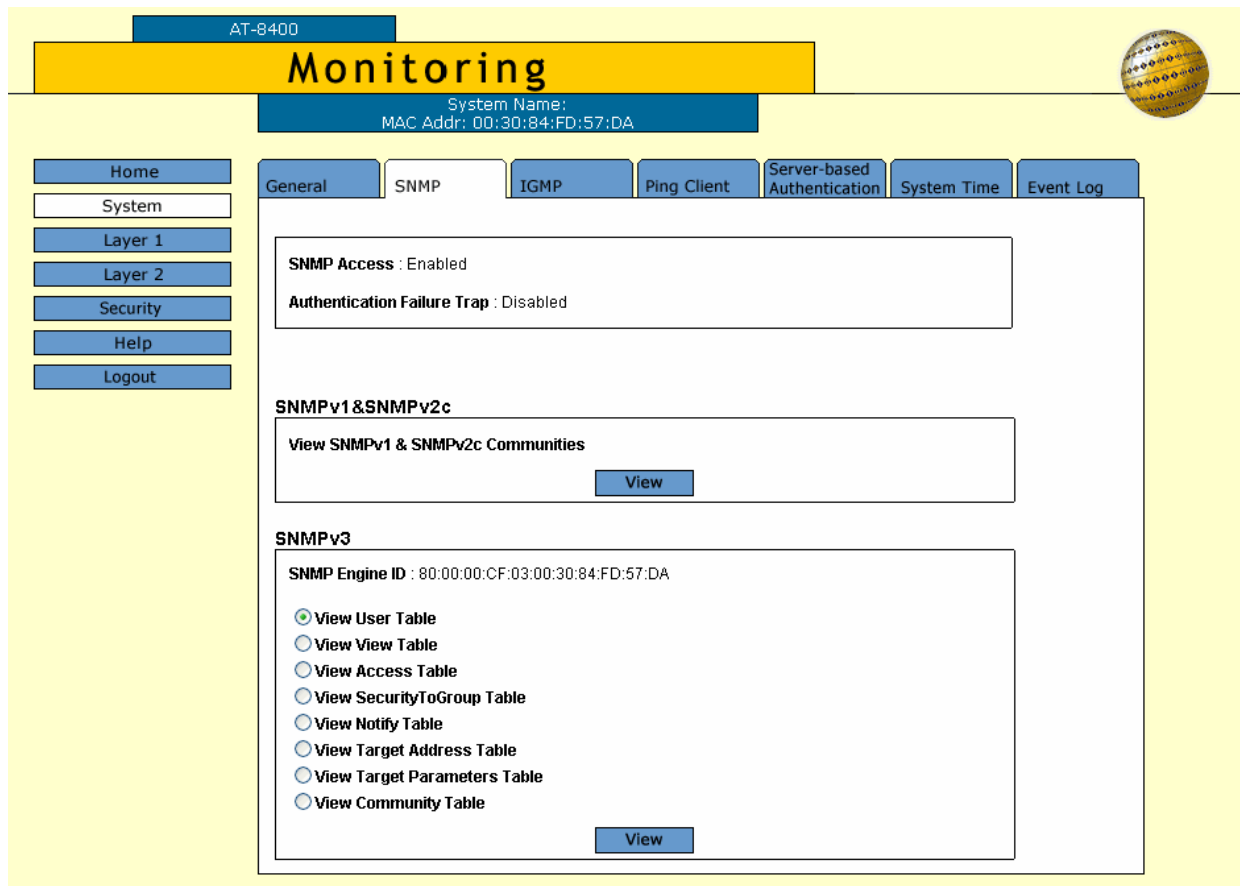


Figure 199 SNMP Monitoring Tab

3. Click **View** in the SNMPv1 & SNMPv2c section of the SNMP Monitoring Tab.

The Monitoring, SNMPv1 & SNMPv2c Communities Page is shown in Figure 200.

The screenshot displays the 'Monitoring' page for device AT-8400. The system name is 'AT-8400' and the MAC address is '00:30:84:FD:57:DA'. The page is titled 'Monitoring' and includes a navigation menu with options: Home, System, Layer 1, Layer 2, Security, Help, and Logout. The main content area is divided into tabs: General, SNMP (selected), IGMP, Ping Client, Server-based Authentication, System Time, and Event Log. The 'SNMPv1 & SNMPv2c Communities' section shows a table with 5 entries. Below the table are 'Refresh' and 'Back' buttons.

Community Name	Access Mode	Manager Stations	Trap Receivers	Open Access	Status
colorado	Read Only	198.1.20.11	198.1.20.11	No	Enabled
guadalupe	Read Write	198.1.20.1, 198.1.20.5, 198.1.20.7	198.1.20.1, 198.1.20.5, 198.1.20.7	No	Enabled
private	Read Write			Yes	Enabled
public	Read Only			Yes	Enabled
sacramento	Read Only	198.1.1.9	198.1.1.9	No	Enabled

Figure 200 Monitoring, SNMPv1 & SNMPv2c Communities Page

Resetting a Switch

To reset a switch, 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 192 on page 584.

2. Click the **Reset** button at the bottom of the page.

A confirmation prompt is displayed.

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

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

Note

The switch does not forward traffic while it reloads the AT-S60 management software. This takes approximately 30 seconds to complete.

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 194 on page 592.

2. Select the **Ping Client** Tab.

The Ping Client Tab is shown in Figure 201.

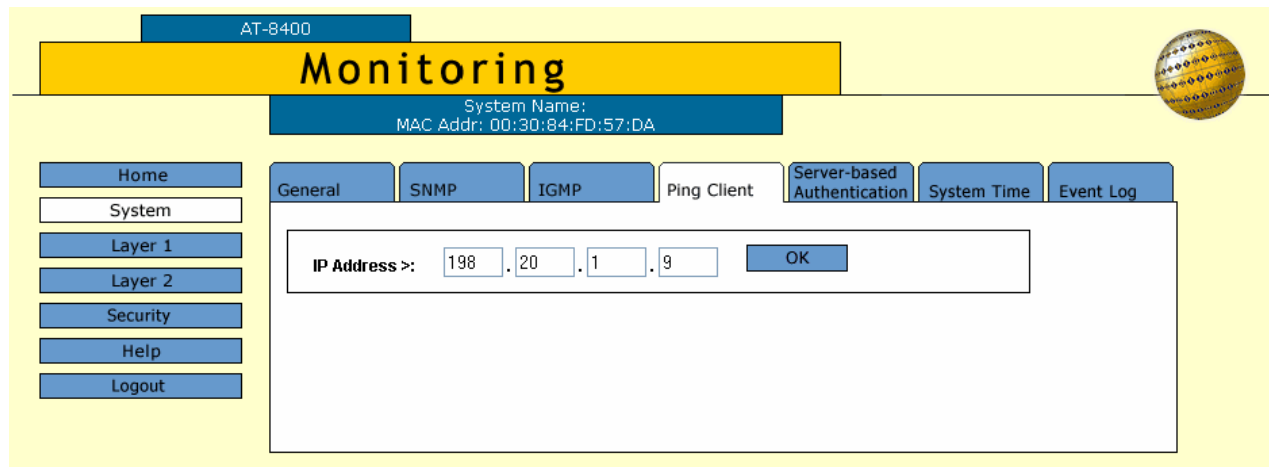


Figure 201 Monitoring System Page, Ping Client Tab

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

The results of the ping are displayed in a new page.

5. To stop the pinging, click **OK**.

Returning the AT-S60 Software to the Factory Default Values

The procedure in this section returns all AT-S60 software parameters, except the IP address, subnet mask, and gateway address, to their default values. This procedure also deletes any VLANs that you have created on the switch.

Note

The AT-S60 software default values are described in **Appendix A**, AT-S60 Default Settings on page 820.

To return the AT-S60 management software to its 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 192 on page 584.

2. Select the **System Maintenance** Tab.

The System Maintenance Tab is shown in Figure 202.

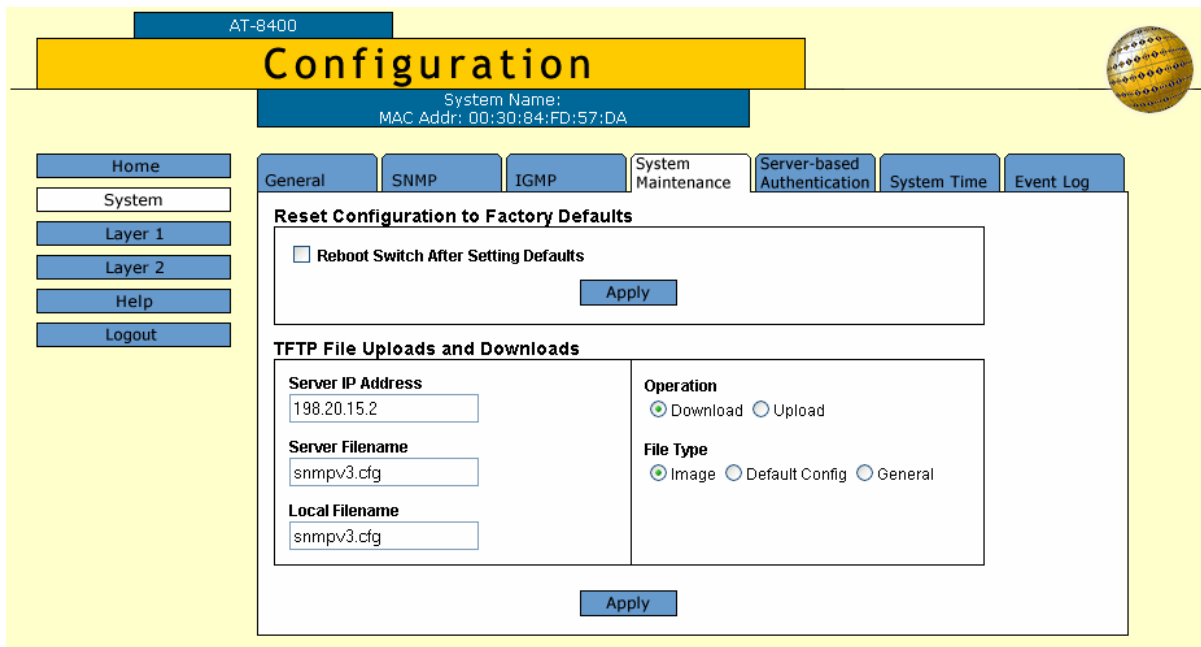


Figure 202 Configuration System Page, System Maintenance Tab

3. Click the **Reboot Switch After Setting Defaults** checkbox.
4. Click **Apply**.
5. Follow the online prompts.

Note

For information about TFTP file uploads and downloads, see Chapter 31: File Downloads and Uploads on page 608.

Chapter 31

File Downloads and Uploads

This chapter contains the procedure for downloading a new AT-S60 image file onto the switch using a web browser management session. In addition, it contains procedures for uploading and downloading system files. This chapter contains the following sections:

- ❑ Downloading a File on page 609
- ❑ Uploading a File on page 612

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-S60 image file
- Configuration file
- Public key
- CA certificate
- Certificate enrollment request

Note

The public key and CA certificate are only supported on the version of AT-S60 management software that features SSL, PKI, and SSH security.

To list the current files stored on the switch, use the Local or Telnet management interface. See *Setting, Creating, Editing, and Displaying System Configuration Files* on page 156 and *Displaying System Files* on page 165.

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.
- 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-S60 image file contains the bootloader for the switch. You cannot load the image file and bootloader separately.

- ❑ Installing a new AT-S60 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, see Returning the AT-S60 Software to the Factory Default Values on page 606.

**Caution**

The switch will stop forwarding Ethernet traffic after it has downloaded an AT-S60 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.

2. Select the **System Maintenance** Tab.

The System Maintenance Tab is shown in Figure 203.

Figure 203 System Maintenance Tab

Note

The top portion of the tab is used to return the switch to its factory default settings. For instructions, see Returning the AT-S60 Software to the Factory Default Values on page 606.

3. In the Server IP Address field, enter the IP address of the network node that contains the TFTP server software.
4. In the Operation field, click **Download**.
5. In the Server Filename field, enter the name of the file that resides on the TFTP server.

This file is downloaded to the switch.

6. In the Local Filename field, enter a name for the file.

This is the filename that appears on the switch. If you are downloading the AT-S60 image file, enter "ats60.img" as the filename.

7. In the File Type, select one of the following:

- Image - Select this option if you are downloading the AT-S60 image file.
- Default 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.
- General - 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 will notify you once the download is complete.

**Caution**

Once you download an AT-S60 switch image file, the switch writes it to flash. During this process, do not reset or power off the unit. Then you must restart the switch in order to load the new image. To continue managing the switch via the Web, 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:

- AT-S60 Image file
- Configuration file
- Public encryption key
- CA certificate
- CA enrollment request

Note

The public key, CA certificate, and CA enrollment request are only supported on the version of AT-S60 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.
- 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.

2. Select the **System Maintenance** Tab.

Note

The System Maintenance Tab is shown in Figure 203 on page 610. The top portion of the tab is used to return the switch to its factory default settings. For instructions, see Returning the AT-S60 Software to the Factory Default Values on page 606.

3. In the Server IP Address field, enter the IP address of the network node that contains the TFTP server software.

4. In the Operation field, click **Upload**.
5. In the Server Filename field, enter a name for the file.
This is the name of the file on the TFTP server.
6. In the 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 File Type options are not used when uploading a file.

7. Click **Apply**.

The management software will notify you once the upload is complete.

Chapter 32

Enhanced Stacking

This chapter introduces enhanced stacking, describes how to assign enhanced stacking status to an AT-8400 Series Switch, and describes how to select a remote switch using a web browser management session.

This chapter contains the following sections:

- Overview on page 615
- Setting a Switch's Enhanced Stacking Status on page 616
- Selecting a Switch in an Enhanced Stack on page 617

Note

For background information on enhanced stacking, refer to Enhanced Stacking Overview on page 76.

Overview

Using a web browser management session, you can view and set the enhanced stacking status of the switch. In addition, you can view and manage other switches in an enhanced stack. For detailed information about enhanced stacking, see Enhanced Stacking Overview on page 76.

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

- ❑ **Master:** An AT-8400 switch configured as “master” can be used to manage other AT-8400 and AT-8000 Series Switches in the same 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 services on the switch.

- ❑ **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.

Note

The default setting for a switch is slave.

Setting a Switch's Enhanced Stacking Status

To adjust a switch's enhanced stacking status, 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 192 on page 584.
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 212 on page 634.
3. Select the **Enhanced Stacking** Tab.
The Enhanced Stacking Tab is shown in Figure 204.

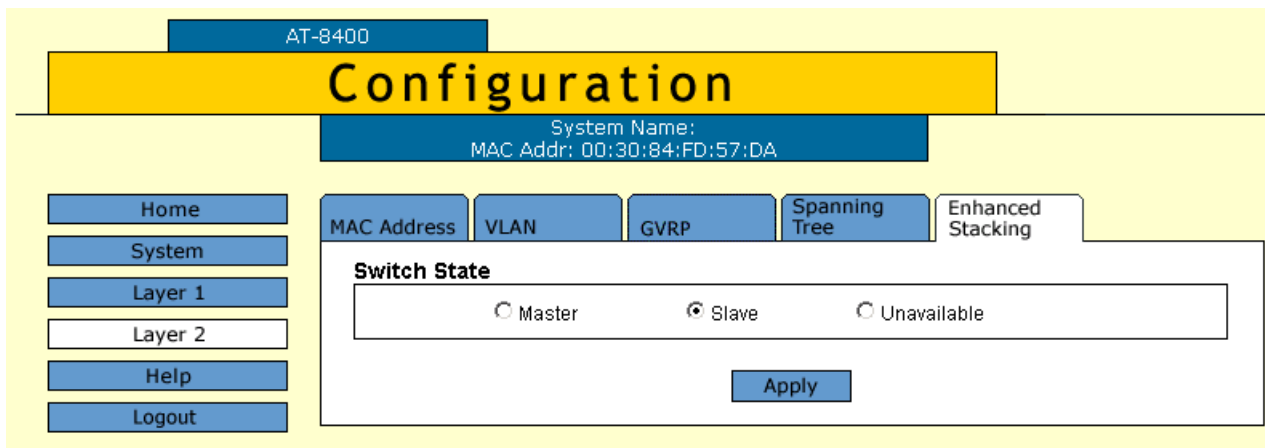


Figure 204 Configuration Layer 2 Page, Enhanced Stacking Tab

4. Click the desired enhanced stacking status for the switch.
5. Click **Apply**.
The new enhanced stacking status is immediately activated on the switch.
6. From the Configuration menu, select the **System** option.
The System Page is displayed with the General Tab shown by default.
7. Click **Save Changes**.
The changes you made are saved on the switch.

Selecting a Switch in an Enhanced Stack

You can use the AT-S60 software to access a remote switch from a master switch. The remote switch can be either a slave or a master.

When you start a web browser management session on the master switch, you are addressing only the master switch. Consequently, the management tasks that you perform only affect the master switch. To manage a remote switch in the same subnet, you need to select it from the master switch.

Each switch in a subnet has a unique MAC address. To quickly differentiate between switches in a subnet, Allied Telesyn suggests configuring system names. For example, using system names helps you determine the difference between two AT-8400 switches within the same subnet. For information about how to assign a system name to an AT-8400 switch, see *Configuring an IP Address and Switch Name* on page 583.

Use this procedure to select a remote switch from a master switch. You must configure the AT-8400 switch as a master switch to view the Enhanced Stacking button.

1. From the Home Page, click the **Enhanced Stacking** button.

Note

If the Home Page does not have an Enhanced Stacking button, 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 all remote switches in the same subnet and displays a list of the switches in the Enhanced Stacking Page. See Figure 205.

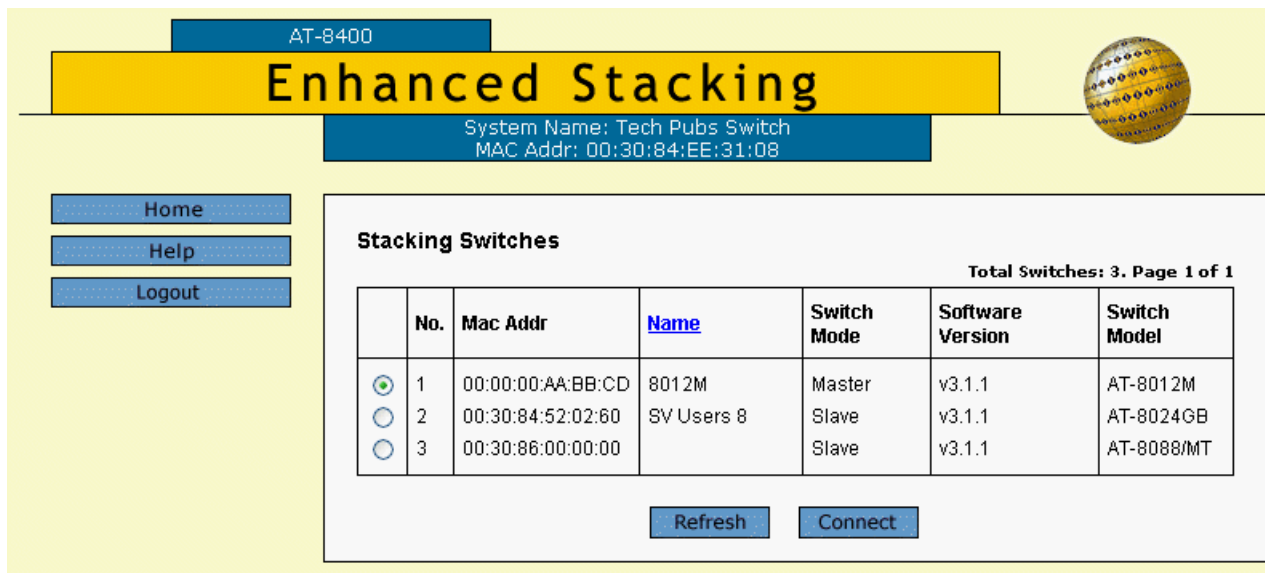


Figure 205 Enhanced Stacking Page

To sort the switches in the list by switch name or MAC address, click on the column headers. By default, the list is sorted by MAC addresses.

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

2. Click the green button next the switch you want to manage and click **Connect**.

You are prompted to enter the user name and password for the remote switch.

3. Enter the user name and password for the remote switch and click **OK**.

The Home Page for the remote switch you selected is displayed. An example is shown in Figure 206. You can now manage the remote switch.

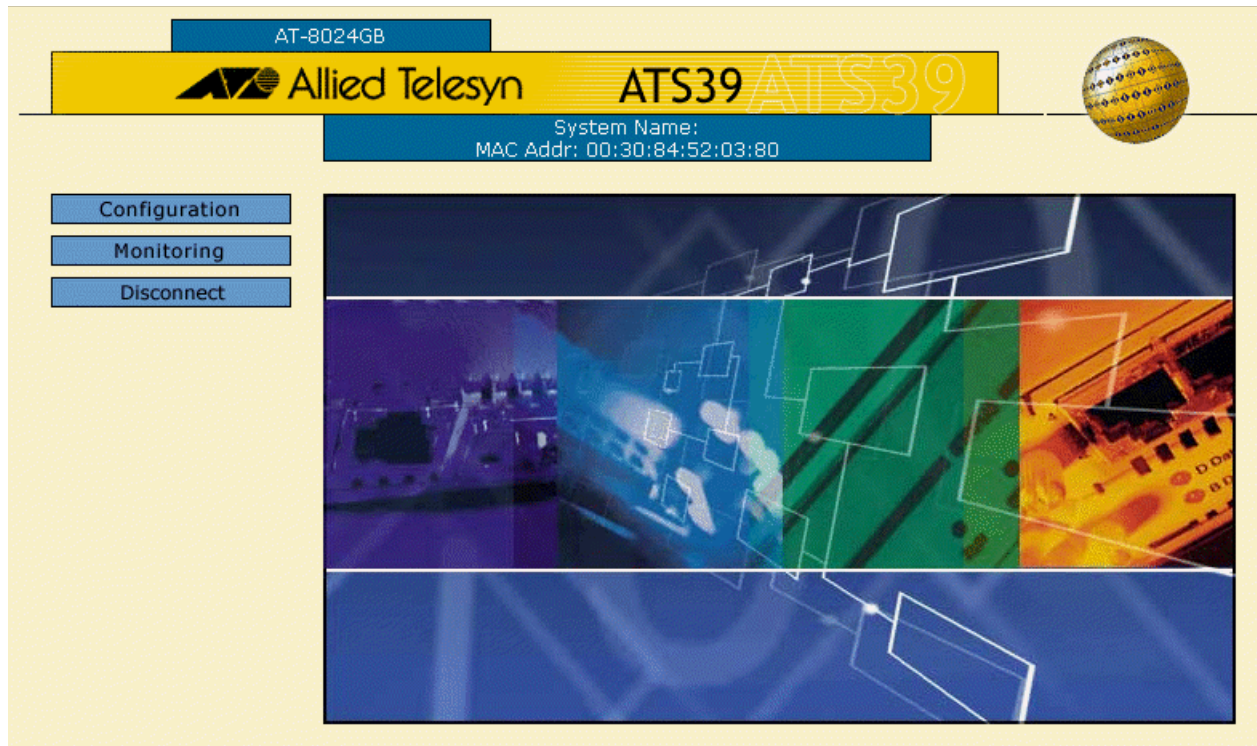


Figure 206 AT-S39 Home Page

For information about the remote switch you selected, consult the appropriate Allied Telesyn documentation.

Returning to the Master Switch

When you have finished managing a remote switch, select the **Disconnect** option on the Home Page of the remote switch. This returns you to the Enhanced Stacking Page in Figure 205 on page 618. When you see that page, you are addressing the master switch again.

You can either select another switch in the list to manage or, to manage the master switch, return to the master switch's Home Page by selecting Home.

Chapter 33

Port Parameters

The procedures in this chapter allow you to view and change the parameter settings for the individual ports on a switch using a web browser management session. The duplex mode and port speed are examples of port parameters that you can modify.

This chapter contains the following procedures:

- ❑ [Configuring Port Parameters on page 621](#)
- ❑ [Displaying Port Status and Statistics on page 626](#)

Configuring Port Parameters

This procedure describes how to configure one or more ports on an AT-8400 switch. It is important to note that when you select multiple ports for configuration, you are making the same configuration changes on all of the ports.

To configure the parameter settings for a port or ports on a switch, 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 192 on page 584.

2. Select the **Layer 1** option.

The Layer 1 Page is displayed with the Port Settings Tab selected by default, as shown in Figure 207.

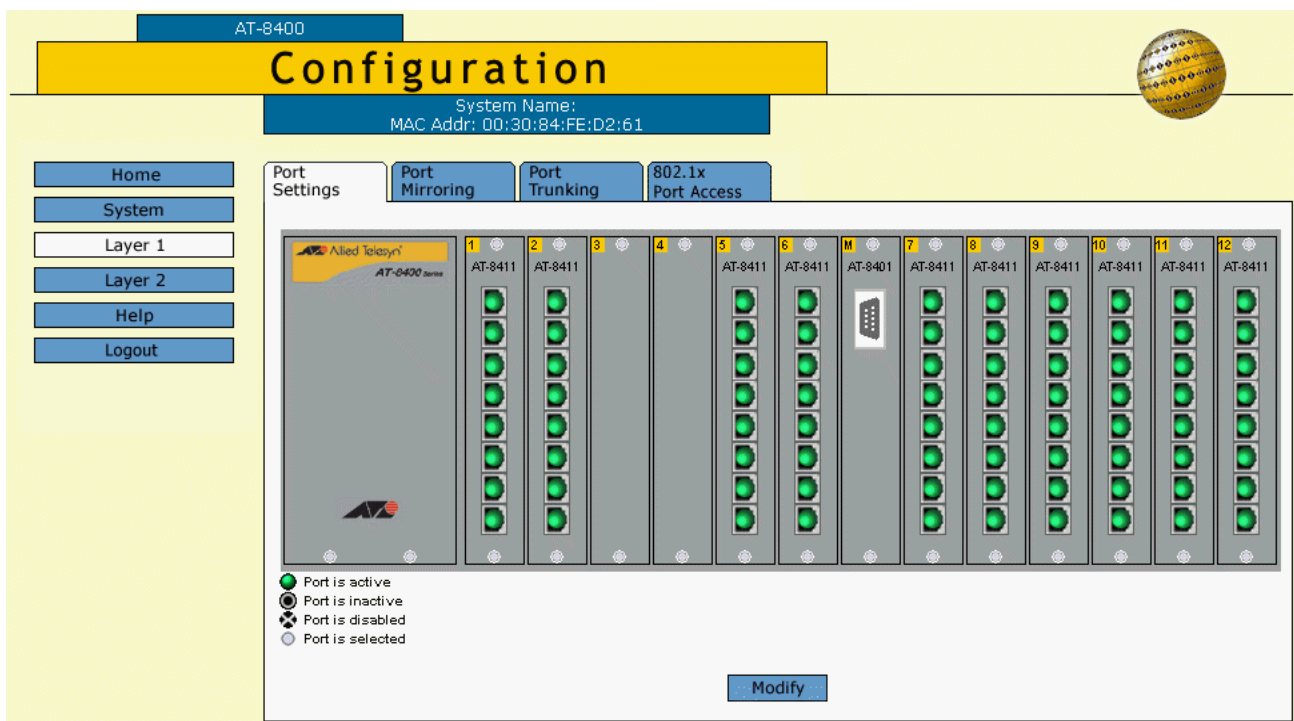


Figure 207 Configuration Layer 1 Page, Port Settings Tab

This page displays a graphical image of the front of the switch. Ports with a valid link to an end node are green.

3. Click on the port or ports that you want to configure. After you click on a port, it turns white. (To deselect a port, click it again.)

**Caution**

Use caution when you update the port that is connected to your management workstation and is communicating with the switch. When you make changes to this port, you could inadvertently lose your management session.

4. Click **Modify**.

The Port Configuration Page is shown in Figure 208.

The screenshot shows a web-based configuration interface for a port. At the top, a yellow header bar contains the text "Port Configuration - 2.1". Below this is a white-bordered box containing various configuration options, each with radio buttons or a dropdown menu. The options are:

- Port Name :** A text input field containing "Port_2.1".
- Speed and Duplex:** A dropdown menu showing "1GB - Full Duplex".
- HOL Blocking:** Radio buttons for "Disabled" (selected) and "Enabled".
- Override Priority:** Radio buttons for "None" (selected), "Low", and "High".
- Media Type:** Radio buttons for "GBIC" and "TP" (selected).
- Status:** Radio buttons for "Disabled" and "Enabled" (selected).
- Broadcast Filter:** Radio buttons for "Disabled" (selected) and "Enabled".
- Back Pressure:** Radio buttons for "Disabled" (selected) and "Enabled".
- Flow Control:** Radio buttons for "Auto" (selected), "Disabled", and "Enabled".
- MDI/MDIX Crossover:** Radio buttons for "Auto", "MDI", and "MDIX" (selected).

At the bottom of the configuration box are three buttons: "Apply", "Defaults", and "Close".

Figure 208 Port Configuration Page

Note

Clicking the **Defaults** button returns the port settings to the default values which are listed in **Appendix A**, AT-S60 Default Settings on page 820.

5. Adjust the port parameters as desired.

The parameters are described below.

Port Name:

This is the name of the port or ports you selected for configuration in Step 5. If you selected one port, you can change the port name in this field. However, if you selected more than one port, you cannot change this value. The port(s) you selected appear at the top of the page. In Figure 208, the port 2.1 was selected.

Speed and Duplex

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

To select a value, click the circle next it. Possible values are:

- Auto-Negotiate: Select Auto-Negotiation to set both speed and duplex mode for the port automatically. This is the default setting.
- 10 Mbps - Half Duplex: Select this value to set the port or ports to a speed of 10 Mbps and half-duplex mode.
- 10 Mbps - Full Duplex: Select this value to set the port or ports to a speed of 10 Mbps and full-duplex mode.
- 100 Mbps - Half Duplex: Select this value to set the port or ports to a speed of 100 Mbps and half-duplex mode.
- 100 Mbps - Full Duplex: Select this value to set the port or ports to a speed of 100 Mbps and full-duplex mode.
- 1 GB - Full Duplex: Select this value to set the port or ports to a speed of 1 Gigabit and full-duplex mode.

HOL Blocking

You use this selection to prevent a packet from being forwarded to a blocking or blocked port. For example, a blocking or blocked port can be one that is receiving too many packets.

To select a value, click the circle next it. Possible values are:

- Enabled - Indicates HOL blocking is turned on. Packets sent from this port are not forwarded to a blocked port. This is the default.
- Disabled - Indicated HOL blocking is turned off. Packets sent from this port are forwarded to a blocked port.

Override Priority

You use this selection to determine packet priority.

For more information about this feature, refer to Class of Service Overview on page 215.

To select a value, click the circle next it. Possible values are:

- None - Indicated that no override priority is assigned to incoming packets. Instead, the port forwards packets according to the priority embedded in the packet. This is the default.
- Low - Indicates low priority has been assigned to the port. As a result, all tagged and untagged packets are sent to the low priority queue.

- High - Indicates high priority has been assigned to the port. As a result, all tagged and untagged packets are sent to the high priority queue.

Media Type

Use this parameter to select the media type on an AT-8413 line card. The Media Type parameter is only available when you configure the Speed and Duplex parameter with one of the following settings: 10_Half, 10_Full, 100_Half, 100_Full, or 1GB_Full.

Choose from the following settings to configure the Media Type parameter:

- Type GBIC (for GBIC port) to indicate only the GBIC port is available for connectivity.
- Type TP (for twisted pair) to indicate only the twisted pair port is available for connectivity.

Status

You use this selection to enable or disable a port. When disabled, a port does not receive or transmit frames.

For example, you may want to disable a port and prevent packets from being forwarded if a problem occurs with the node or cable connected to the port. Once the problem has been fixed, you can enable the port again to resume normal operation. You can also disable an unused port to secure it from unauthorized connections.

To select a value, click the circle next it. Possible values are:

- Enabled - The port receives and forwards packets. This is the default setting.
- Disabled - The port does not receive or forward packets.

Broadcast Filter

You use this selection to protect a port from a deluge of packets caused by a broadcast storm. Enabling the broadcast filter parameter on a port causes the port to discard all ingress broadcast frames.

To select a value, click the circle next it. Possible values are:

- Enabled - The port discards all ingress broadcast frames.
- Disabled - The port accepts all ingress broadcast frames. This is the default setting.

Back Pressure

You can use this selection only if the port or ports you specified are operating at half-duplex mode. When you specify that a port is in this mode and it has a packet that is pending transmission, then the software suspends the JAM pattern before sending the packet. After the packet is sent, the JAM pattern resumes.

To select a value, click the circle next it. Possible values are:

- Enabled - Indicates back pressure is activated on this port. When the port is receiving too many packets, the port sends a signal to the end node to stop sending information.
- Disabled - Indicates back pressure is not activated on this port. When the port is receiving too many packets, the port does not send a signal to the end node to stop sending information. This is the default.

Flow Control

Flow control applies only to ports operating in full-duplex mode. The switch uses 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.

To select a value, click the circle next it. Possible values are:

- Auto - Indicates the port conforms to the flow control setting of the end node. For example, if flow control is active on the end node then flow control is active on this port. Also, if flow control is not active on the end node, then flow control is not active on this port. This is the default.
- Disabled - Indicates that no flow control occurs on the port.
- Enabled - Indicates that flow control occurs on the port.

MDI/MDIX Crossover

The operating configuration of the port. Auto indicates that the port automatically determines the appropriate MDI or MDI-X setting.

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

You are returned to the Port Settings Tab as shown in Figure 207 on page 621.

7. After you have set the parameters, click **Apply**.

Your changes are activated on the switch.

To save your changes, return to the General Tab and click **Save Changes**. The changes you made are saved on the switch.

Displaying Port Status and Statistics

The procedures in this section display the operating status of the ports on a switch and port statistics. You can view a port’s operating speed, duplex mode, MDI/MDI-X configuration, and more. You can also view the operating status of any GBIC modules installed.

Displaying Port Status

To display the status 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 194 on page 592.

2. Select the **Layer 1** option.

The Layer 1 Page is displayed with the Port Settings Tab selected by default, as shown in Figure 209.

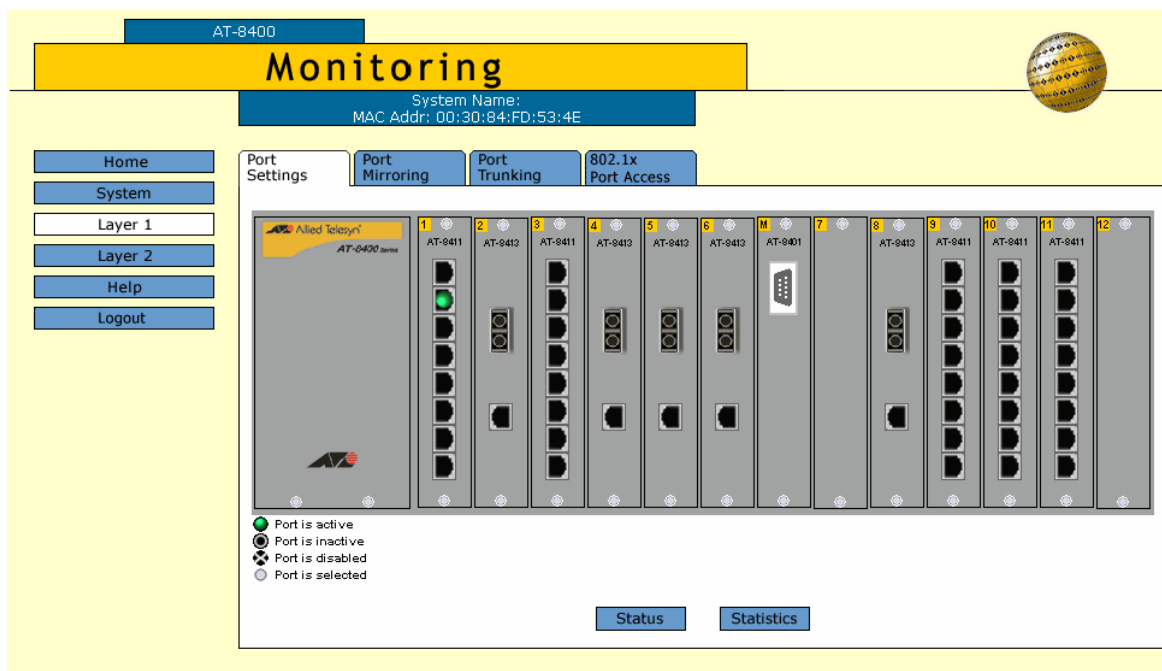


Figure 209 Monitoring Layer 1 Page, Port Settings Tab

This page displays a graphical image of the front of the switch. Ports with a valid link to an end node are green.

3. Click on 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. After you select a port, it turns white. (To deselect a port, click it again.)

4. Click **Status** to display the port's operating status.

The Port Status Page is shown in Figure 210.

Port Status - 2.2-8,6.1-8

Total Ports Selected: 15. Page 1 of 2

Port	Name	Media	Link	Neg	MDI/X	Speed	Duplex	PVID	Flow Ctl	STP State	Priority
2.2	Port_2.2	Auto	Down	Auto	---	---	---	1	----	Disabled	No
2.3	Port_2.3	Auto	Down	Auto	---	---	---	1	----	Disabled	No
2.4	Port_2.4	Auto	Down	Auto	---	---	---	1	----	Disabled	No
2.5	Port_2.5	Auto	Down	Auto	---	---	---	1	----	Disabled	No
2.6	Port_2.6	Auto	Down	Auto	---	---	---	1	----	Disabled	No
2.7	Port_2.7	Auto	Down	Auto	---	---	---	1	----	Disabled	No
2.8	Port_2.8	Auto	Down	Auto	---	---	---	1	----	Disabled	No
6.1	Port_6.1	Auto	Down	Auto	---	---	---	1	----	Disabled	No
6.2	Port_6.2	Auto	Down	Auto	---	---	---	1	----	Disabled	No
6.3	Port_6.3	Auto	Down	Auto	---	---	---	1	----	Disabled	No

Figure 210 Port Status Page

The information on this page is for viewing purposes only. To adjust port parameters, refer to Configuring Port Parameters on page 621.

Note

To view the statistics after you view the status, click **Statistics**.

The columns on the page are described below:

Port

Indicates the port number in the following format:
slot number. port number

Name

Indicates the name of the port. The default name is the port number.

Media

Indicates the type of port. See the following:

- TP (for twisted pair) indicates one of the following:
 - An RJ-45 port on an AT-8411 line card.
 - An RJ-45 port an AT-8413 line card when the Negotiation parameter on the Port Configuration Menu is set to Auto and the port is connected to another RJ-45 port. For more information about the Port Configuration Menu, see Configuring Port Parameters on page 621.
 - An RJ-45 port an AT-8413 line card when the Negotiation parameter on the Port Configuration Menu is set to Manual and the Media Selection parameter on the Port Configuration Menu is set to TP. For more information about the Port Configuration Menu, see Configuring Port Parameters on page 621.
- Fiber indicates a fiber optic port on an AT-8412 or AT-8414 line card.
- GBIC (for GBIC port) indicates one of the following:
 - A GBIC port on an AT-8413 line card when Negotiation is set to Auto and the port is connected to another GBIC port.
 - A GBIC port on an AT-8413 line card when Negotiation is set to Manual and the Media Selection is set to GBIC.
- Auto indicates a port on an AT-8413 line card with Auto-negotiation enabled when the port is not connected to another port.

Link

The status of the link between the port and the end node connected to the port. The possible values are:

- Up - indicates that a valid link exists between the port and the end node.

- Down - indicates that the port and the end node have not established a valid link.

Neg

The status of Auto-Negotiation on the port. Possible values are:

- Auto - Indicates that the port is using Auto-Negotiation to set operating speed and duplex mode.
- Manual - Indicates that the operating speed and duplex mode have been set manually.

MDI/X

The operating configuration of the port. Possible values are Auto, MDI, MDI-X. The status Auto indicates that the port is automatically determining the appropriate MDI or MDI-X setting.

Speed

The operating speed of the port. Depending on the port you specified, possible values are:

- 0010 - Indicates 10 Mbps.
- 0100 - Indicates 100 Mbps.
- 1000 - Indicates 1000 Mbps.

Duplex

The duplex mode of the port. Possible values are half-duplex and full-duplex.

PVID

The port VLAN identifier currently assigned to the port.

Flow Ctrl

The flow control setting for the port. Possible values are:

- Disabled - No flow control occurs on the port.
- Enabled - Flow control occurs on the port.

STP State

The current operating status of the port. Possible values are:

- Forwarding - The port is sending and receiving Ethernet frames. This is the normal state for a switch port.
- Disabled - STP operations have been disabled on the port.
- Blocking - This is the standby mode. The port does not participate in frame relay. The forwarding process discards received frames and does not submit forwarded frames for transmission.
- Listening - The port is enabled for receiving frames only. The port is preparing to participate in frame relay.
- Learning - The port is enabled for receiving frames only. The learning process can add new source address information to the forwarding database.

Priority

The priority assigned to packets that are received by the port. Possible values are:

- No - Indicates no override priority has been assigned to the port. Untagged packets are forwarded to the low priority queue. Tagged packets are forwarded to either the high or low queue, depending on the priority embedded in the packets.
- Low - Indicates low priority has been assigned to the port. As a result, all tagged and untagged packets are sent to the low priority queue.
- High - Indicates high priority has been assigned to the port. As a result, all tagged and untagged packets are sent to the high priority queue.

For more information, see [Class of Service Overview](#) on page 215.

Displaying Port Statistics

To display the statistics 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 194](#) on page 592.

2. Select the **Layer 1** option.

The Layer 1 Page is displayed with the Port Settings Tab selected by default, as shown in [Figure 209](#) on page 626.

3. Click on a port.

You can select only one port when displaying statistics. After you select a port, it turns white. (To deselect a port, click it again.)

4. Click **Statistics**.

The Port Statistics Page is shown in Figure 211.

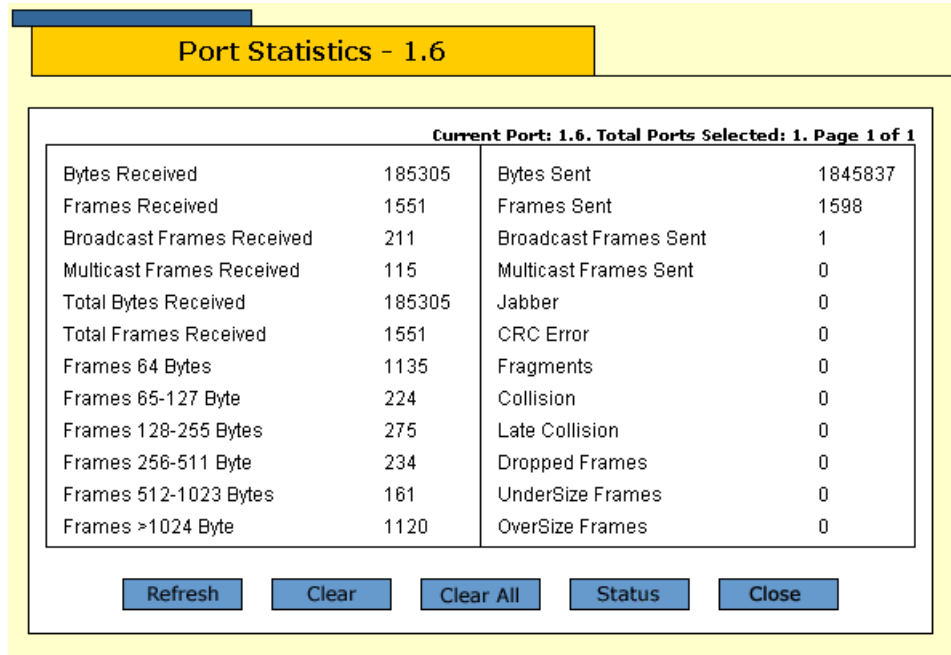


Figure 211 Port Statistics Page

Note

To view the status of the port, click **Status**.

The information on this page is described below:

Bytes Received

Number of bytes received on the port.

Frames Received

Number of frames received on the port.

Broadcast Frames Received

Number of broadcast frames received on the port.

Frames 64 Bytes

Frames 65-127 Bytes

Frames 128-255 Bytes

Frames 256-511 Bytes

Frames 512-1023 Bytes

Frames >1024 Bytes

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

Bytes Sent

Number of bytes transmitted from the port.

Frames Sent

Number of frames transmitted from the port.

Broadcast Frames Sent

Number of broadcast frames transmitted from the port.

Multicast Frames Sent

Number of multicast frames transmitted from the port.

Jabber

Number of received packets in which the packet data is greater than MAXFRAMESIZE and the packet has an invalid CRC.

CRC Error

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

Collision

Number of collisions that have occurred on the port.

Late Collision

Number of received packets in which a late collision event has been detected.

Dropped Frames

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

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.

5. Click **Clear** to clear the port statistics information for the port on the current page, or click **Clear All** to clear the port statistics information for all the ports listed at the top of the Statistics page.

Chapter 34

MAC Address Table

This chapter describes how to display the dynamic and static addresses in the MAC address table using a web browser management session. It contains the following procedures:

- Displaying the MAC Address Table on page 634
- Adding Static Unicast and Multicast MAC Addresses on page 637
- Deleting MAC Addresses on page 639
- Changing the Aging Time on page 640

Note

For background information on MAC addresses, refer to MAC Address Overview on page 116.

Displaying the MAC Address Table

To view the MAC address table, perform the following procedure:

1. From the Home Page, select either **Configuration** or **Monitoring**.

If you select Configuration, the Configuration System Page is displayed with the General Tab displayed by default, as shown in Figure 192 on page 584.

2. Select the **Layer 2** option.

The Layer 2 Page is displayed with the MAC Address Tab shown by default. Figure 212 shows how this page appears when you display it through the Configuration main menu selection.

If you display the **MAC Address Tab** through the Monitoring main menu selection, the **Add** button is not included. This button is used to add static and multicast addresses to the switch. (For instructions on how to add static and multicast MAC addresses, refer to the next procedure.)

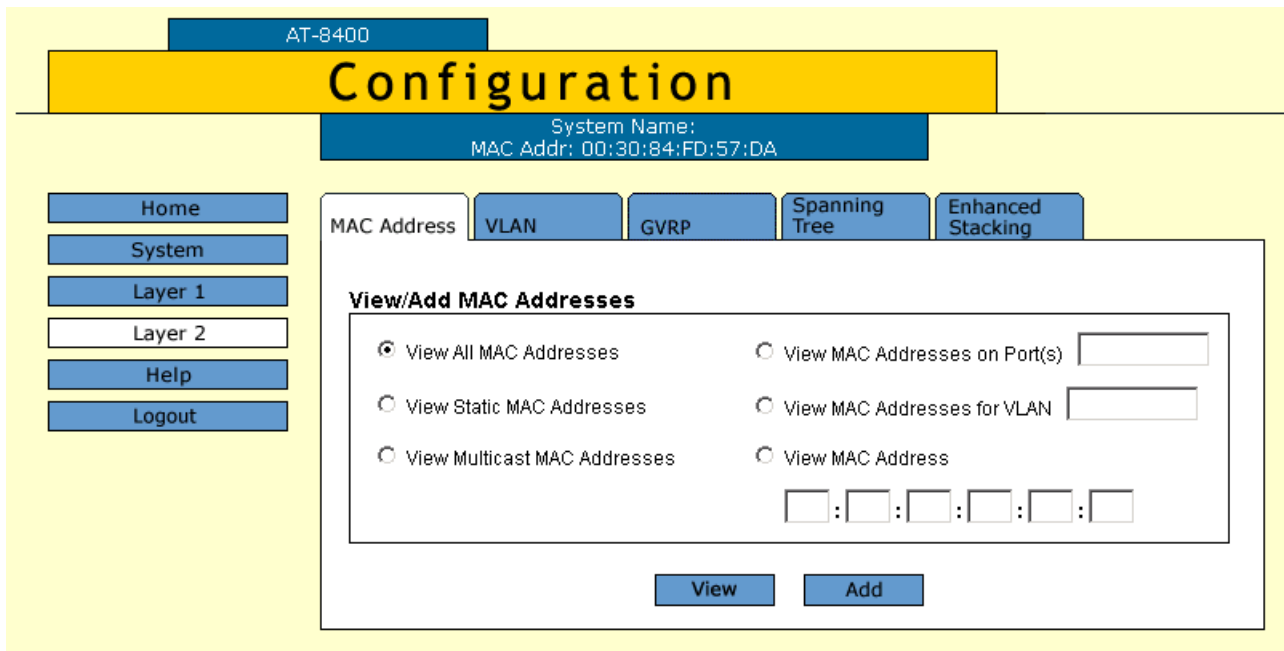


Figure 212 Configuration Layer 2 Page, MAC Address Tab

The options for displaying MAC addresses are described below.

View All MAC Addresses

This option displays both static and dynamic MAC addresses. This is the default setting.

View Static MAC Addresses

This option displays only the static MAC addresses. Static MAC addresses are addresses that you entered manually into the MAC address table.

View IP Multicast Addresses

This option displays the multicast MAC addresses.

View MAC Addresses on Port(s)

This option is used to display the MAC addresses learned on a particular port. For information about how to specify ports, see **Specifying Ports on page 34**.

View MAC Addresses for VLAN

This option displays the MAC addresses learned by a particular VLAN on the switch. You specify the VLAN by its VID.

View MAC Addresses

This option is used to locate the port on the switch where a MAC address was learned or assigned. To use this option, enter the MAC address of the node in the field.

- Once you have selected one of the options, click **View**.

See Figure 213 for an example of the MAC Address Table Page that is displayed when you click on the **View MAC addresses on Port(s)**.

MAC Address Table

Total MAC Addresses: 131. Page 1 of 14

	VLAN ID	MAC ADDRESS	PORT	TYPE
<input checked="" type="radio"/>	1	00:00:CD:01:6B:5D	1.1	Dynamic
<input type="radio"/>	1	00:00:CD:01:D3:4B	1.1	Dynamic
<input type="radio"/>	1	00:00:F4:A3:AA:23	1.1	Dynamic
<input type="radio"/>	1	00:00:F4:A4:12:44	1.1	Dynamic
<input type="radio"/>	1	00:00:F4:DD:29:31	1.1	Dynamic
<input type="radio"/>	1	00:01:A5:00:07:8D	1.1	Dynamic
<input type="radio"/>	1	00:02:72:00:22:62	1.1	Dynamic
<input type="radio"/>	1	00:02:DD:30:41:6B	1.1	Dynamic
<input type="radio"/>	1	00:04:5A:65:25:60	1.1	Dynamic
<input type="radio"/>	1	00:06:5B:23:0F:7E	1.1	Dynamic

Refresh
Remove
Next
Close

Figure 213 MAC Address Table Page

The MAC addresses are displayed in a table. The columns in the table are:

VLAN ID

The VID of the VLAN to which the port is an untagged member.

MAC ADDRESS

The MAC addresses of the nodes connected to the port.

PORT

The port on the switch where the MAC address was learned or assigned. See Specifying Ports on page 34.

TYPE

The MAC address type. The type can be either static or dynamic.

4. Click **Close**.

The MAC Addresses Table Page is displayed as shown in Figure 212 on page 634. Your changes are immediately activated on the switch.

5. To save your changes, return to the General Tab and click **Save Changes**. Your changes are saved on the switch.

Adding Static Unicast and Multicast MAC Addresses

This section contains the procedure for assigning a static unicast or multicast address to ports on the switch. You can assign up to 255 static MAC addresses per port.

Note

When you add a static multicast address you must assign the address to all ports on the switch that belong to the multicast group. This includes the ports connected to the multicast application server and the host nodes. Failure to assign the address to all ports in the group prevents the multicast packets from reaching all appropriate nodes.

To add a static unicast or multicast address to the MAC 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 192 on page 584.

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 212 on page 634.

3. Click **Add**.

The Add MAC Address Page is shown in Figure 214.

The screenshot shows the 'Add MAC Address' configuration page. The page has a yellow header with the title 'Add MAC Address'. Below the header is a form with three fields: 'MAC Address' (a six-digit hexadecimal input field), 'Port Number' (a text input field), and 'VLAN ID' (a text input field with the value '1'). At the bottom of the form are two buttons: 'Apply' and 'Cancel'.

Figure 214 Add MAC Address Page

4. In the MAC Address field, enter the new static unicast or multicast MAC address.

5. In the Port Number field, enter the port number that is to be assigned the MAC address. You can specify more than one port.
For information about specifying ports, see Specifying Ports on page 34.
6. In the VLAN ID field, enter the VLAN ID for the specified port.
The range of VLAN IDs is 1 to 4094, with 1 as the default VLAN ID.
7. Click **Apply**.
The MAC Addresses Table Page is displayed as shown in Figure 212 on page 634.
8. Repeat this procedure to add other static or multicast addresses to the switch.
9. Click **Close**.
The MAC Address Tab is redisplayed. Your changes are immediately activated on the switch.
10. To save your changes, return to the General Tab and click **Save Changes**. Your changes are saved on the switch.

Deleting MAC Addresses

To delete a static, dynamic, or multicast MAC address from the switch, 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 192 on page 584.
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 212 on page 634.
3. Select one of the MAC address options.
For instructions, refer to Displaying the MAC Address Table on page 634.
4. Click **View**.
The MAC Address Table is displayed as shown in Figure 213 on page 635.
5. Click the circle next to the MAC address that you want to delete from the switch.
6. Click **Remove**.
The address is removed from the MAC address table.
7. Click **Close**.
The MAC Addresses Table Page is displayed as shown in Figure 212 on page 634.
8. Click **Close**.
The MAC Address Tab is redisplayed. Your changes are immediately activated on the switch.
9. To save your changes, return to the General Tab and click **Save Changes**. Your changes are saved on the switch.

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 node addresses that are inactive.

The default setting for the aging time is 300 seconds (5 minutes).

To adjust the aging time, 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 192 on page 584.
2. In the Configuration section, enter a new value, in seconds, in the **MAC Address Aging Time** field.
The range for this field is from 8 to 512 seconds.
3. Click **Apply**.
Your changes are immediately activated on the switch.
4. Click **Save Changes**.
The changes you made are saved on the switch.

Chapter 35

Port Trunking

This chapter explains how to configure a port trunk using a web browser management session.

This chapter contains the following procedures:

- Creating or Deleting a Port Trunk on page 642
- Modifying a Port Trunk on page 645
- Displaying the Port Trunks on page 647

Note

For background information on port trunking, refer to Port Trunking Overview on page 128.

Creating or Deleting a Port Trunk

The following procedures allow you to create or delete a port trunk using the web browser management session.

Creating a Port Trunk

To create a port trunk, perform the following procedure:



Caution

Configure the software for ports on the switch and the end node before you connect the cables of a port trunk. Connecting the cables prior to configuring the ports can create loops in your network topology. Loops can result in broadcast storms. This can adversely effect the operations of your network.

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

The Configuration System Page is displayed with the General Tab selected by default, as shown in Figure 192 on page 584.

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

The Layer 1 Page is displayed with the Port Settings Tab shown by default, as shown in Figure 207 on page 621.

3. Select the Port Trunking Tab.

The Port Trunking Tab is shown in Figure 215.

AT-8400

Configuration

System Name: Middle School
MAC Addr: 00:30:84:EE:31:08

Home System Layer 1 Layer 2 Help

Port Settings Port Mirroring Port Trunking 802.1x Port Access

Total Trunks : 2. Page 1 of 1

	ID	Name	Type	Ports
<input checked="" type="radio"/>	1	highschool	10/100MB	1.2-4
<input type="radio"/>	2	elementaryschool	10/100MB	4.1-2

Refresh Modify Remove Add

Figure 215 Configuration Layer 1 Page, Port Trunking Tab

4. Click **Add**.

The Add New Trunk Page is shown in Figure 216.

Figure 216 Add New Trunk Page

5. Enter the name of the trunk in the Trunk Name box.
6. Click on the ports you want to include in the trunk.
Selected ports turn white. To deselect a port, click it again.
7. Scroll down the page.
8. Click **Apply**.
You are returned to the Port Trunking Page. It is updated with the new trunk port information. The new port trunk is immediately activated on the switch.
9. To save your changes, return to the General Tab and click **Save Changes**. Your changes are saved on the switch.

10. Configure the ports on the remote switch for port trunking.

You can now connect the data cables to the ports of the trunk on the switch.

Deleting a Port Trunk

To delete a port trunk, perform the following procedure:



Caution

Before you delete a trunk in software, disconnect the cables from the ports. Deleting the trunk without disconnecting the data cables can create a loop in your network topology. This situation can result in broadcast storms.

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

The Configuration System Page is displayed with the General Tab selected by default, as shown in Figure 192 on page 584.

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

The Layer 1 Page is displayed with the Port Settings Tab shown by default, as shown in Figure 207 on page 621.

3. Select the Port Trunking Tab.

The Port Trunking Tab is displayed as shown in Figure 215 on page 642.

4. Select a trunk.

A green light appears next to the selected trunk.

5. Click **Remove**.

The port is deleted from the switch. The Port Trunking Page is updated to reflect your changes.

To save your changes, return to the General Tab and click **Save Changes**. Your changes are saved on the switch.

Modifying a Port Trunk

This procedure allows you to modify a port trunk using a web browser management session.

To modify a port trunk, 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 192 on page 584.

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

The Layer 1 Page is displayed with the Port Settings Tab shown by default, as shown in Figure 207 on page 621.

3. Select the Port Trunking Tab.

The Port Trunking Tab is shown in Figure 215 on page 642.

4. Select **Modify**.

The Modify Trunk Page is shown in Figure 217.

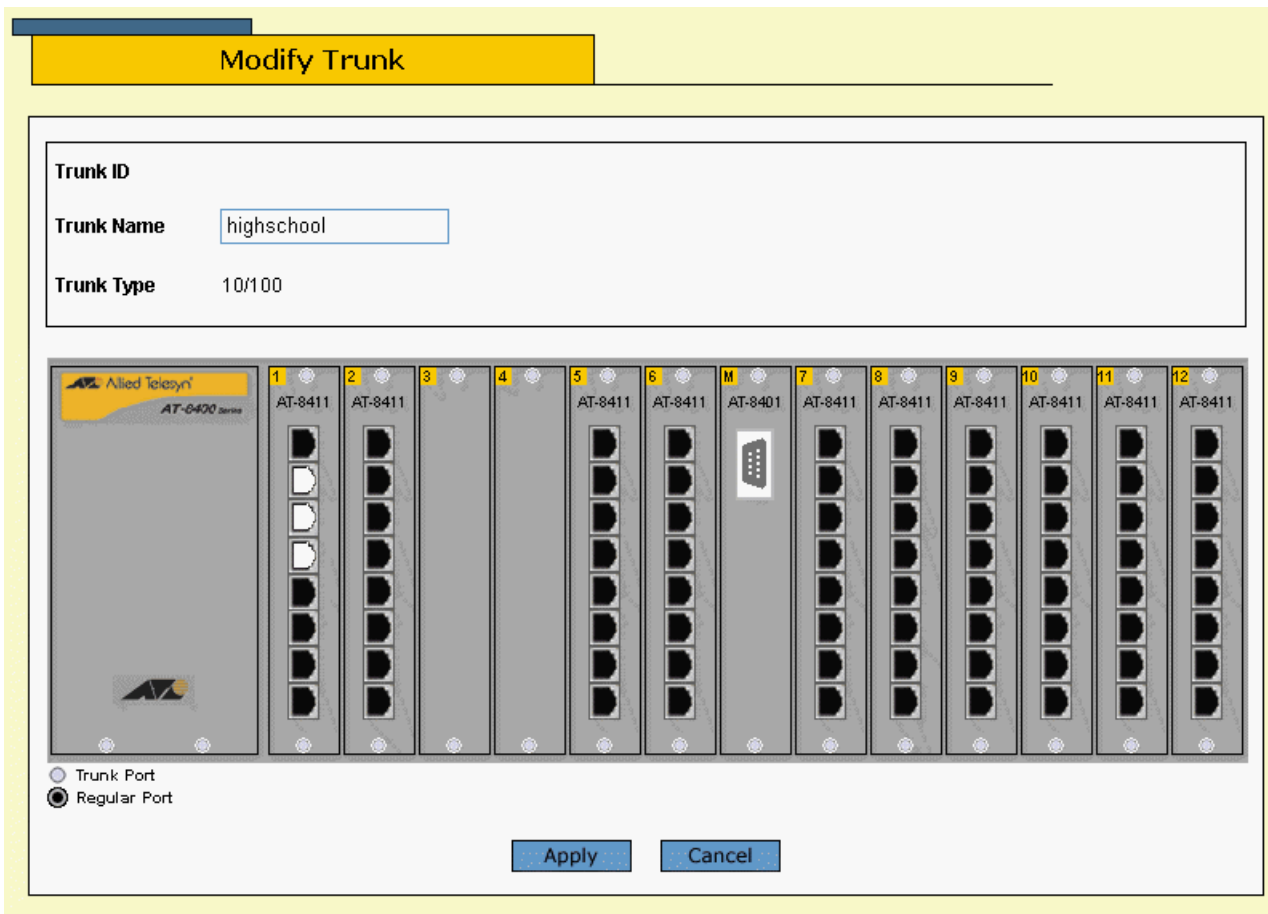


Figure 217 Modify Trunk Page

5. Click on the ports to select them for port trunking. Selected ports turn white. Click again to deselect a port.
6. Scroll down the page and click **Apply**.
7. The Port Trunking Page opens as shown in Figure 215 on page 642. Your changes are immediately activated on the switch.
8. To save your changes, return to the General Tab and click **Save Changes**. Your changes are saved on the switch.

Displaying the Port Trunks

This procedure allows you to view the port trunk settings using a web browser management session.

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 194 on page 592.

2. Select the **Layer 1** option.

The Layer 1 Page is displayed with the Port Settings Tab selected by default, as shown in Figure 209 on page 626.

3. Select the Port Trunking Tab.

The Port Trunking Tab is shown in Figure 218.

The screenshot shows the AT-S60 Management Software web interface. At the top, there is a blue bar with 'AT-8400' and a yellow bar with 'Monitoring'. Below this, a blue bar displays 'System Name:' and 'MAC Addr: 00:30:84:FD:57:DA'. A navigation menu on the left includes buttons for Home, System, Layer 1, Layer 2, Security, Help, and Logout. The main content area has tabs for Port Settings, Port Mirroring, Port Trunking, and 802.1x Port Access. The Port Trunking tab is active, showing a table of port trunks. The table has columns for ID, Name, Type, and Ports. There are two rows of data. A 'Refresh' button is located below the table. The text 'Total Trunks : 2. Page 1 of 1' is displayed in the top right corner of the table area.

ID	Name	Type	Ports
1	marketingTrunk1	10/100MB	2.6-8
2	engTrunk14	10/100MB	6.2-3

Figure 218 Monitoring Layer 1 Page, Port Trunking Tab

Chapter 36

Port Mirroring

This chapter explains how to configure a port mirror using a web browser management session.

This chapter contains the following procedures:

- Creating a Port Mirror on page 649
- Deleting a Port Mirror on page 651
- Modifying a Port Mirror on page 652
- Displaying the Port Mirror List on page 654

Note

For background information on port mirroring, refer to Port Mirroring Overview on page 143.

Creating or Deleting a Port Mirror

Use the following procedures to create, delete, or modify a port mirror. For information about how ports are specified, see *Specifying Ports* on page 34. After you have made your changes, you need to save them on the Configuration System Page.

Creating a Port Mirror

To create a port mirror, 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 192 on page 584.

2. Select the **Layer 1** option.

The Layer 1 Page is displayed with the Port Settings Tab selected by default, as shown in Figure 207 on page 621.

3. Select the Port Mirroring Tab.

The Port Mirroring Tab is shown in Figure 219.

AT-8400

Configuration

System Name: Middle School
MAC Addr: 00:30:84:EE:31:08

Home System Layer 1 Layer 2 Help

Port Settings Port Mirroring Port Trunking 802.1x Port Access

Total Mirrors: 1. Page 1 of 1

	Destination Port	Source Port(s)	Status
	1.7	4.1	Enabled

Refresh Modify Remove Add

Figure 219 Configuration Layer 1 Page, Port Mirroring Tab

4. Click **Add**.

The Add New Mirror Page is displayed as shown in Figure 220.

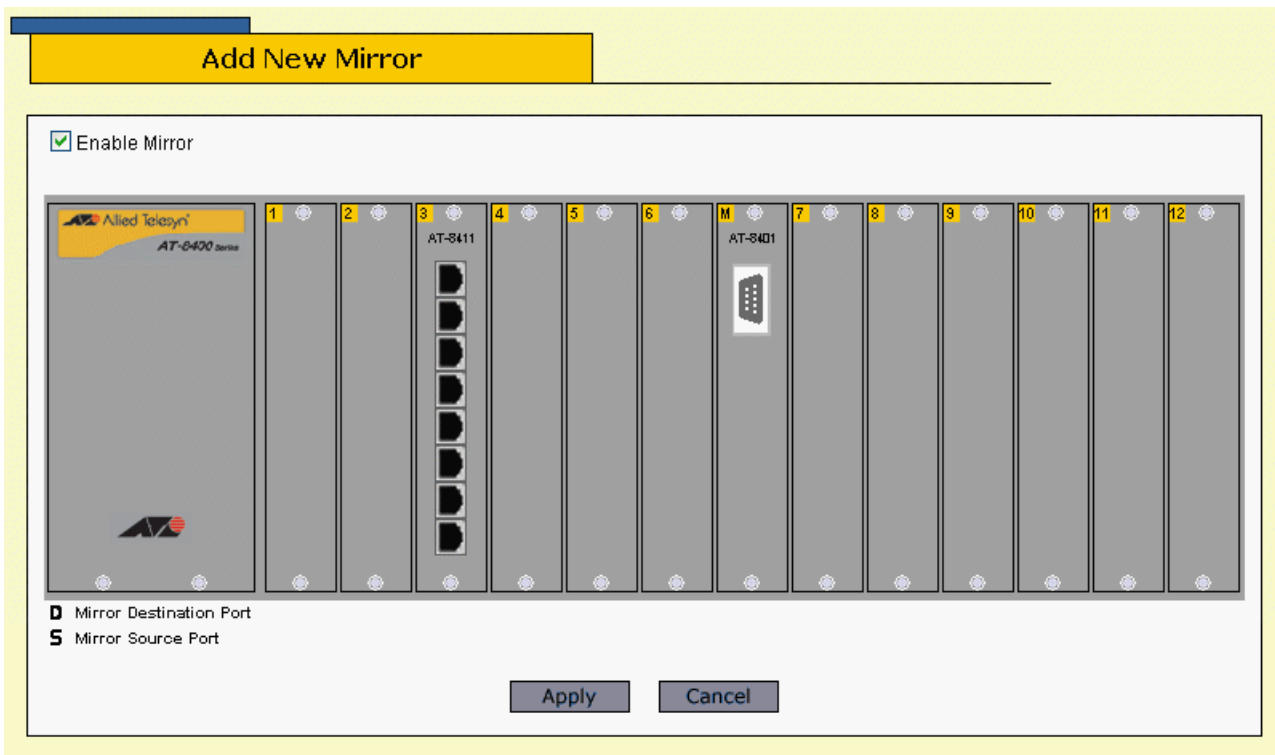


Figure 220 Add New Mirror Page

5. Click the ports in the graphical switch image.
Click once for S, which stands for the source mirror port. Click twice for D, which stands for destination mirror port. Click three times to deselect a port.
6. Click **Apply**.
The Port Mirroring Tab is displayed. It reflects the changes you made in Step 6. The port mirror is immediately activated on the switch.
To save your changes, return to the General Tab and click **Save Changes**
You can connect a data analyzer to the destination mirror port to monitor the traffic on the selected ports.

Deleting a Port Mirror

Use this procedure to delete a port mirror using a web browser management session.

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

The Configuration System Page is displayed with the General Tab selected by default, as shown in Figure 192 on page 584.

2. Select the **Layer 1** option.

The Layer 1 Page is displayed with the Port Settings Tab selected by default, as shown in Figure 207 on page 621.

3. Select the Port Mirroring Tab.

The Port Mirroring Tab is shown in Figure 219 on page 649.

4. Click on the port mirror you want the remove.

The circle next to the port mirror turns green.

5. Click **Remove** to delete a port mirror.

The port mirror is deleted. The Port Mirroring Tab is updated to reflect your changes.

To save your changes, return to the General Tab and click **Save Changes**.

Modifying a Port Mirror

To change the source mirror port or the destination mirror port on an existing port mirror, 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 192 on page 584.

2. Select the **Layer 1** option.

The Layer 1 Page is displayed with the Port Settings Tab selected by default, as shown in Figure 207 on page 621.

3. Select the Port Mirroring Tab.

The Port Mirroring Tab is shown in Figure 219 on page 649.

4. Click **Modify** to modify a port mirror.

The Modify Mirror Page is shown in Figure 221.

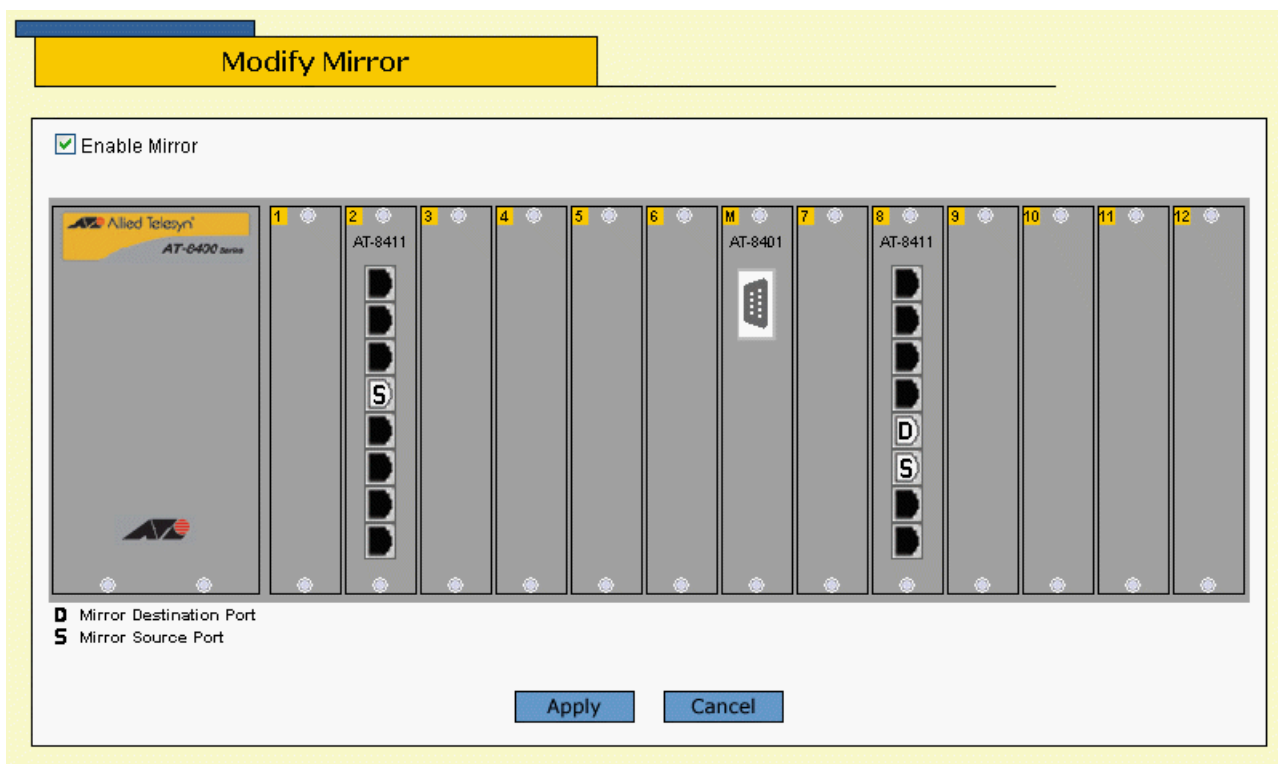


Figure 221 Modify Mirror Page

5. Configure the mirror ports:

- Click once to select **S** for source mirror port.
- Click twice to select **D** for destination mirror port.

To change the destination mirror port to another port, deselect the current destination port mirror by clicking it off. Then you can select a new destination port mirror.

6. Click **Apply**.

Your changes are activated on the switch. The Port Mirroring Page opens with the new ports.

To save your changes, return to the General Tab and click **Save Changes**.

Your modifications to the port mirror or port mirrors are saved to the switch.

Displaying the Port Mirror List

This procedure allows you to view the list of port mirrors using a web browser management session.

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

The Monitoring System Page is displayed with the General Tab selected by default, as shown in Figure 194 on page 592.

2. Select the **Layer 1** option.

The Layer 1 Page is displayed with the Port Settings Tab selected by default, as shown in Figure 209 on page 626.

3. Select the Port Mirroring Tab.

The Port Mirroring Tab is shown in Figure 222.

AT-8400

Monitoring

System Name:
MAC Addr: 00:30:84:FE:D3:23

Home System Layer 1 Layer 2 Security Help Logout

Port Settings Port Mirroring Port Trunking 802.1x Port Access

Total Mirrors: 2. Page 1 of 1

	Destination Port	Source Port(s)	Status
<input checked="" type="radio"/>	2.8	2.5	Enabled
<input type="radio"/>	4.1	3.1	Enabled

Refresh View

Figure 222 Monitoring Layer 1 Page, Port Mirroring Tab

Chapter 37

Event Log

This chapter describes how to configure the Event Log using a web browser management session. It includes the following procedures:

- Enabling or Disabling the Event Log on page 656
- Displaying Events on page 658
- Saving the Event Log on page 660
- Clearing the Event Log on page 661

Note

For background information on this feature, refer to Event Log Overview on page 204.

Enabling or Disabling the Event Log

Allied Telesyn recommends setting the switch's date and time if you intend to use the Event Log. If you do not set the switch's date and time, the switch does not log the entries with the correct date and time. For instructions, see *Setting the System Time* on page 59.

To enable or disable 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 192 on page 584.

2. From the System page, select the **Event Log** tab.

The Event Log tab is shown in Figure 223.

The screenshot shows the AT-8400 Configuration page with the Event Log tab selected. The page header includes the system name 'Jenny's Switch' and MAC address '00:30:84:FD:57:DA'. The left sidebar contains navigation links: Home, System, Layer 1, Layer 2, Help, and Logout. The main content area is divided into two sections: Log Settings and Filter Settings and Actions.

Log Settings

Status <input checked="" type="radio"/> Disabled <input type="radio"/> Enabled	Log Full Action <input checked="" type="radio"/> Wrap <input type="radio"/> Halt
Clear Log <input type="checkbox"/> Clear Log	

Filter Settings and Actions

Log Location Temporary (RAM)	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"/>

Buttons: Apply, View, Save

Figure 223 Event Log Tab

3. For Status in Log Settings, click either **Disable** or **Enable**.

If you enable the log, the system immediately begins to add events to the log. The default is enabled.

4. For Log Full Action, click either **Wrap** or **Halt**.

Wrap: Indicates the log deletes old entries as it adds new entries once it reaches its maximum capacity of 4,000 events. The default is Wrap.

Halt: Indicates the log stops adding new entries once it reaches maximum capacity.

5. Click **Apply**.
6. To save your changes, return to the General Tab and click **Save Changes**.

To display the events in the log, go to the next procedure.

Displaying Events

To view the Event Log, do the following:

1. From the Home Page, click either **Configuration** or **Monitoring**.

The System page is displayed with the General tab selected by default, as shown in Figure 192 on page 584.

2. From the System page, select the **Event Log** tab.

The Event Log tab is shown in Figure 223 on page 656.

3. Configure the following options which are located at the bottom of the web page:

Severity Selections

Displays events of a selected severity. Choose from the following:

I-Informational: Indicates informational messages.

E-Error: Indicates error messages.

W-Warning: Indicates warning messages.

D-Debug: Indicates debug messages.

ALL: Indicates all of the above message types.

The default display is a combination of informational, error, and warning messages. You can display more than one severity at a time by holding down the Shift key when making a selection.

Display Order

Controls the order of the events in the log. Choices are Chronological, which displays the events in the order of oldest to newest, and Reverse Chronological, which displays the events in the order of newest to oldest. The default is Chronological.

Mode

Controls the format of the Event Log. Choices are Normal, which displays the time, module, severity, and description for each event, and Full, which displays the same information as Normal, plus filename, line number, and event ID. The default is Normal.

Module Selections

Displays events of a selected AT-S60 module. For a list of the modules, refer to Software Modules on page 210. The default is ALL, which displays the events for all modules. You can display more than one module at a time by holding down the Shift key when making a selection.

4. Once you have set the log filters, click **View**.

Figure 224 shows an example of the Event Log in the Full display mode. The Normal display mode does not include the Filename, Line Number, and Event ID items.

Events View - FullMode				
Severity	Date and Time	EventID	Filename:Line	Event
I	01/01/80 00:00:00	183001	fileapp.c:131	file: File System initialized
I	01/01/80 00:00:00	243004	websevr.c:79	http: Server reset to defaults
I	01/01/80 00:00:00	323003	atisssh.c:535	ssh: SSH server disabled
I	01/01/80 00:00:00	363001	cfgmain.c:159	cfg: Configuration initialized
I	01/01/80 00:00:00	283001	tacacs.c:830	tacacs: TACACS+ initialized
I	01/01/80 00:00:00	273001	radiusclient.c:1280	radius: RADIUS initialized
I	01/01/80 00:00:00	073001	garpmain.c:259	garp: GARP initialized
I	01/01/80 00:00:03	083001	portconfig.c:998	pcfg: PortConfig initialized
I	01/01/80 00:00:04	203002	qosapp.c:711	qos: Number of Egress Queues set to 4
I	01/01/80 00:00:04	203003	qosapp.c:787	qos: Priority 0 mapped to Egress Queue 0

[Close](#)

Figure 224 Event Log Example

The columns in the log are described below:

- S (Severity) - The event's severity. Table 7 on page 209 defines the different severity levels.
- Date/Time - The date and time the event occurred.
- Event ID - A unique number that identifies the event. (Displayed only in the Full display mode.)
- Filename: Line - The subpart of the AT-S60 module and the line number that generated the event. (Displayed only in the Full display mode.)
- Event - The module within the AT-S60 software that generated the event followed by a brief description of the event. For a list of the AT-S60 modules, see Software Modules on page 210.

Saving the Event Log

You can save the Event Log as a file in the file system. Once you save the Event Log as a file, you can view it or download it to your management workstation. For information about the AT-S60 file system, refer to Chapter 10, File System Configuration.

To save the Event Log, do the following:

1. Perform steps 1 to 3 in Displaying Events on page 658 using the Configuration tab and not the Monitoring tab.
2. In the Save Filename field, enter a name for the file.

The name can be up to 16 alphanumeric characters, followed by a 3 letter extension. Use “.log” as the extension.

3. Click **Save**.

The Event Log is immediately saved to the file system.

Clearing the Event Log

To clear all events from the log, perform the following procedure:

1. From the Home Page, click **Configuration**.

The System page is displayed with the General tab selected by default, as shown in Figure 192 on page 584.

2. From the System page, select the **Event Log** tab.

The Event Log tab is shown in Figure 223 on page 656.

3. In Log Settings, click **Clear Log**.

4. Click **Apply**.

The log, if enabled, learns new events immediately.

Chapter 38

IGMP Snooping

This chapter describes how to configure the IGMP snooping feature on the switch. It contains the following procedures:

- ❑ [Configuring IGMP Snooping on page 663](#)
- ❑ [Displaying a List of Host Nodes and Multicast Routers on page 666](#)

Note

For background information on this feature, refer to [IGMP Snooping Overview on page 219](#).

Configuring IGMP Snooping

To configure IGMP snooping from a web browser management session, 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 192 on page 584.

2. Select the IGMP Tab.

The Configuration IGMP Tab is shown in Figure 225.

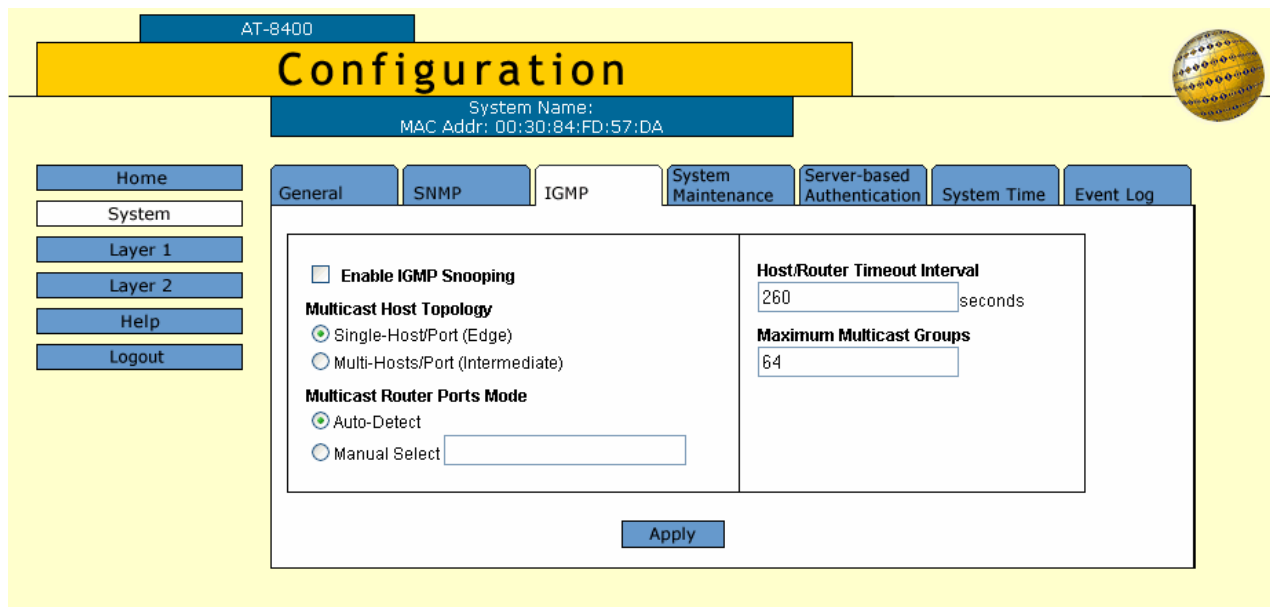


Figure 225 Configuration System Page, IGMP Tab

3. Adjust the IGMP parameters as necessary.

The parameters are explained below:

Enable IGMP Snooping

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 port or multiple host nodes per port. Possible settings are Single-Host/Port (Edge) and Multi-Hosts/Port (Intermediate).

Select the Single-Host/Port (Edge) setting 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 from a port under the following conditions:

- When a host node signals its desire to leave a multicast group by sending a leave request
- When the host node stops sending reports and times-out

The switch forwards the leave request to the router and simultaneously ceases transmission of multicast packets from the port where the host node is connected.

Select the Multi-Hosts/Port (Intermediate) setting if there is more than one host node connected to a 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 from 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 port have transmitted leave requests (or have timed out) does the switch stop sending multicast packets from 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, select Multi-Hosts/Port (Intermediate).

Multicast Router Ports Mode

Controls whether the detection of ports on the switch that are connected to multicast routers is made automatically or manually.

You use this selection to specify which of the ports on the switch are connected to multicast routers. You can allow the switch to determine this automatically by selecting Auto-Detect, which is the default setting. To specify the ports manually, click Manual Select and type the port numbers in the box.

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 256 groups. The default is 64 multicast groups.

This parameter 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 256 addresses. The default is 64 multicast addresses.

4. After setting the IGMP parameters, click **Apply**.
Your changes are activated on the switch.
5. To save your changes, return to the General Tab and click **Save Changes**. The changes you made are saved on the switch.

Displaying a List of Host Nodes and Multicast Routers

You can use the AT-S60 software to display a list of the multicast groups on a switch, as well as the host nodes. In addition, you can view the multicast routers. A multicast router receives multicast packets from a multicast application and transmits the packets to host nodes.

To view host nodes and 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 194 on page 592.
2. Select the IGMP Tab.
The IGMP Tab is shown in Figure 226.

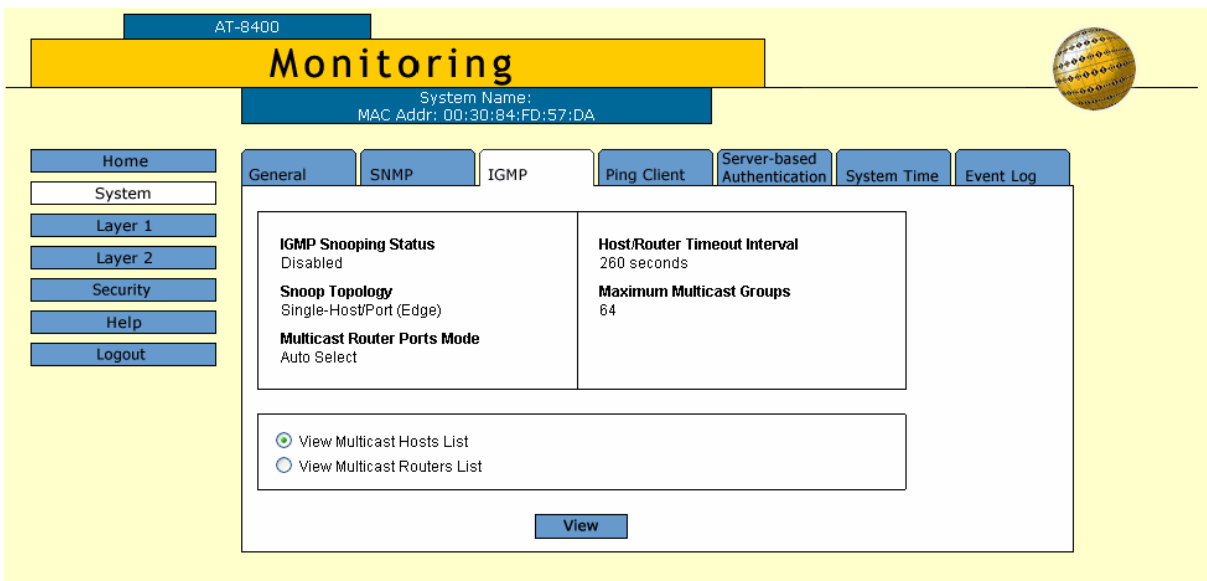


Figure 226 Monitoring System Page, IGMP Tab

3. To view the multicast addresses and the host nodes, click **View Multicast Host List** and then click **View**.

The View Multicast Hosts List Page is shown in Figure 227.

Total Multicast Groups: 4. Page 1 of 1				
Multicast Group	VLAN ID	Member Port/ Trunk ID	Host IP	Status
01:00:5E:00:01:01	1	-/13	172.16.10.51	Active
01:00:5E:7F:FF:FA	1	1.2/-	149.35.200.75	Active
			149.35.200.65	Active
01:00:5E:00:00:02	1	1.6/-	149.35.200.69	Active
01:00:5E:00:00:09	1	-/19	149.35.200.61	Active

Figure 227 View Multicast Hosts List Page

This page displays the following 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/Trunk ID

This column displays host members present on either a port or a trunk of the switch.

Host IP

The IP address(es) of the host node(s) connected to the port.

Status

Indicates IGMP group status of the port.

- Active indicates the port is active in the IGMP group.
- Left Group indicates the port is not active in the IGMP group.

4. To view the multicast routers, click **View Multicast Router List** and then click **View**.

The View Multicast Routers List Page is shown in Figure 228.

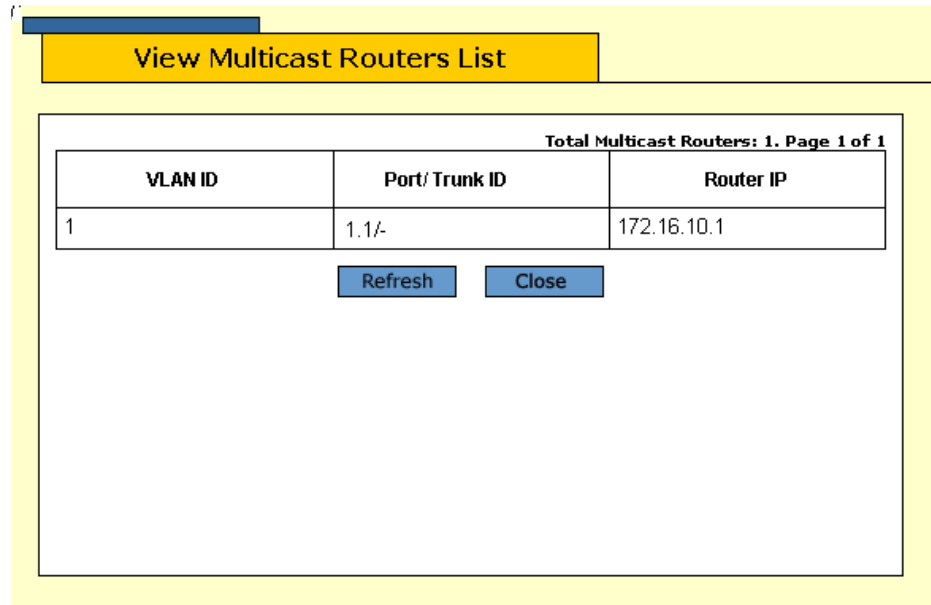


Figure 228 View Multicast Routers List Page

The page displays the following information:

Port/Trunk ID

This column displays router members present on either a port or a trunk of the switch.

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 a different page opens, as displayed in Figure 229.

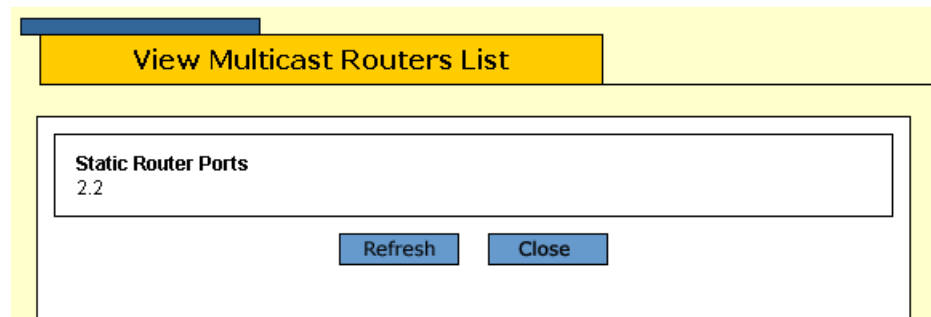


Figure 229 View (Static) Multicast Routers List Page

Chapter 39

STP, RSTP, and MSTP

This chapter explains how to configure STP, RSTP, and MSTP parameters on an AT-8400 chassis using a web browser management session. It contains the following procedures:

- Enabling STP, RSTP, or MSTP on page 670
- Configuring and Modifying STP on page 672
- Configuring and Modifying RSTP on page 676
- Configuring and Modifying MSTP on page 681
- Displaying STP, RSTP, or MSTP Settings on page 691

Note

For background information on STP and RSTP, refer to STP and RSTP Overview on page 229. For background information on MSTP, refer to on page 256.

Enabling STP, RSTP, or MSTP

The AT-8400 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. Once selected, you can then enable or disable it.

To select 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 Configuration System Page is displayed with the General Tab selected by default, as shown in Figure 192 on page 584.
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 212 on page 634.
3. Select the Spanning Tree Tab.
The Spanning Tree Tab is shown in Figure 230.

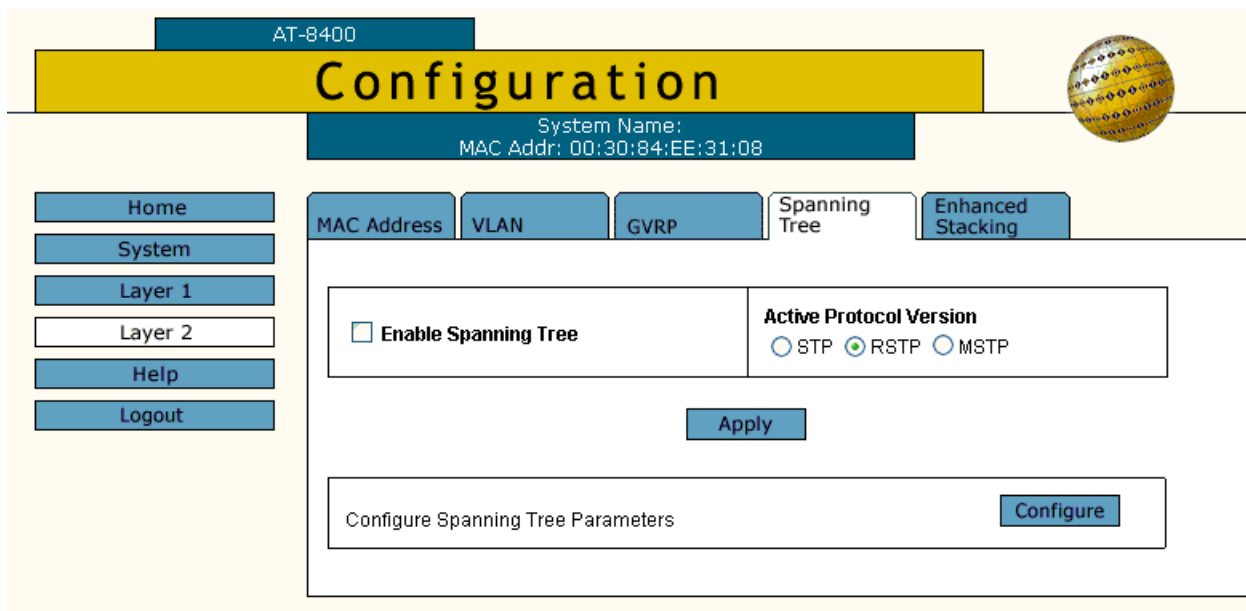


Figure 230 Configuration Layer 2 Page, Spanning Tree Tab

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-S60 management software.

7. If you activated STP, go to Configuring and Modifying STP on page 672. If you activated RSTP go to Configuring and Modifying RSTP on page 676. If you activated MSTP, go to Configuring and Modifying MSTP on page 681.

Configuring and Modifying STP

To configure and modify STP, perform the following procedure:



Caution

The bridge provides default STP parameters that are adequate for most networks. Changing the STP parameters without prior experience and an understanding of how STP works may have a negative effect on your network. Consult the IEEE 802.1d standard before changing any of the STP parameters.

1. Follow the steps in the procedure described in Enabling STP, RSTP, or MSTP on page 670, then select STP as your active protocol version.
2. On the Spanning Tree Tab, click **Configure**.

An expanded Spanning Tree Tab is shown in Figure 231 on page 673.

The screenshot displays the configuration interface for an AT-8400 device. At the top, the system name is "AT-8400" and the MAC address is "00:30:84:FE:D2:61". The main configuration area is titled "Configuration" and includes tabs for "MAC Address", "VLAN", "GVRP", "Spanning Tree", and "Enhanced Stacking". The "Spanning Tree" tab is active, showing the "Configure STP Parameters" section. This section contains the following fields:

- Bridge Priority [0-15]:** A text input field containing "8", with a calculation below it: $* 4096 = 32768$.
- Bridge Hello Time [1-10]:** A text input field containing "2".
- Bridge Forwarding [4-30]:** A text input field containing "15".
- Bridge Max Age [6-40]:** A text input field containing "20".
- Bridge Identifier:** A text input field containing "00:30:84:FE:D2:61".

Below the parameters are "Apply" and "Defaults" buttons. The bottom section shows a rack of 12 ports, labeled AT-8411 through AT-8411, with a "M" label above port 6. Each port has a selection radio button. A legend indicates that a selected radio button (filled) means "Port is selected" and an unselected one (empty) means "Port is not selected". Below the port selection are "Modify" and "Back" buttons.

Figure 231 Expanded STP Spanning Tree Tab

3. In the Configure STP Parameters section, adjust the bridge STP settings as needed. The parameters are described below.

Bridge Priority

The priority number for the bridge. This number is used in determining the root bridge for STP. The bridge with the lowest priority number is selected as the root bridge. If two or more bridges have the same priority value, the bridge with the numerically lowest MAC address becomes the root bridge. 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 15, with 0 having the highest priority. For a list of the increments, refer to **Table 9**, Bridge Priority Value Increments on page 231

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 adapted to the change, possibly resulting in a network loop. You can set this parameter from 4 to 30 seconds. The default is 30 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 of 20, all bridges delete current configuration messages after 20 seconds. You can set this parameter from 6 to 40 seconds. The default is 20 seconds.

In selecting a value for maximum age, you **must** observed the following equations:

$$\text{MaxAge} < (2 \times (\text{HelloTime} + 1))$$

$$\text{MaxAge} < (2 \times (\text{ForwardingDelay} - 1))$$

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.

4. After you have made the desired changes, click **Apply**.
If you are finished making changes, skip to step 9.
5. To adjust 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 Page is shown in Figure 232.

The screenshot shows a web interface for configuring STP settings. At the top, there is a yellow header bar with the text "STP Settings - Port(s) 4.2-3". Below this is a white form area. Inside the form, there are two side-by-side input fields. The left field is labeled "Port Priority [0-15]" and contains the number "8". To its right, the text "* 16 = 128" is displayed. The right field is labeled "Port Cost [0 - 200000000]" and contains the number "0". To its right, the text "(0 = Auto Update)" is displayed. Below these two fields, there are two blue buttons: "Apply" and "Cancel".

Figure 232 STP Settings Page

- Adjust the settings as desired. The parameters are described below.

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 default value for priority is 128. The range is 0-15, with 0 having the highest priority.

Port Cost

The spanning tree algorithm uses the cost parameter to decide which port provides the lowest-cost path to the root bridge for a particular LAN. Enter a value from 0 to 200,000,00. The default values are:

- 0 for Auto-detect
 - 4 for a 1 Gigabit port
 - 10 for a 10 Mbps port
 - 100 for a 100 Mbps port
- After you have configured the parameters, click **Apply**.
 - To save your changes, return to the General Tab and click **Save Changes**. The changes you made are saved on the switch.

Configuring and Modifying RSTP

To configure and modify RSTP, perform the following procedure:



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. Consult the IEEE 802.1w standard before changing any of the RSTP parameters.

1. Follow the steps in the procedure described in Enabling STP, RSTP, or MSTP on page 670.
2. On the Spanning Tree Tab, click **Configure**.
3. Select **RSTP** as your active protocol version.

The Configure RSTP Parameters Tab is displayed as shown in Figure 233.

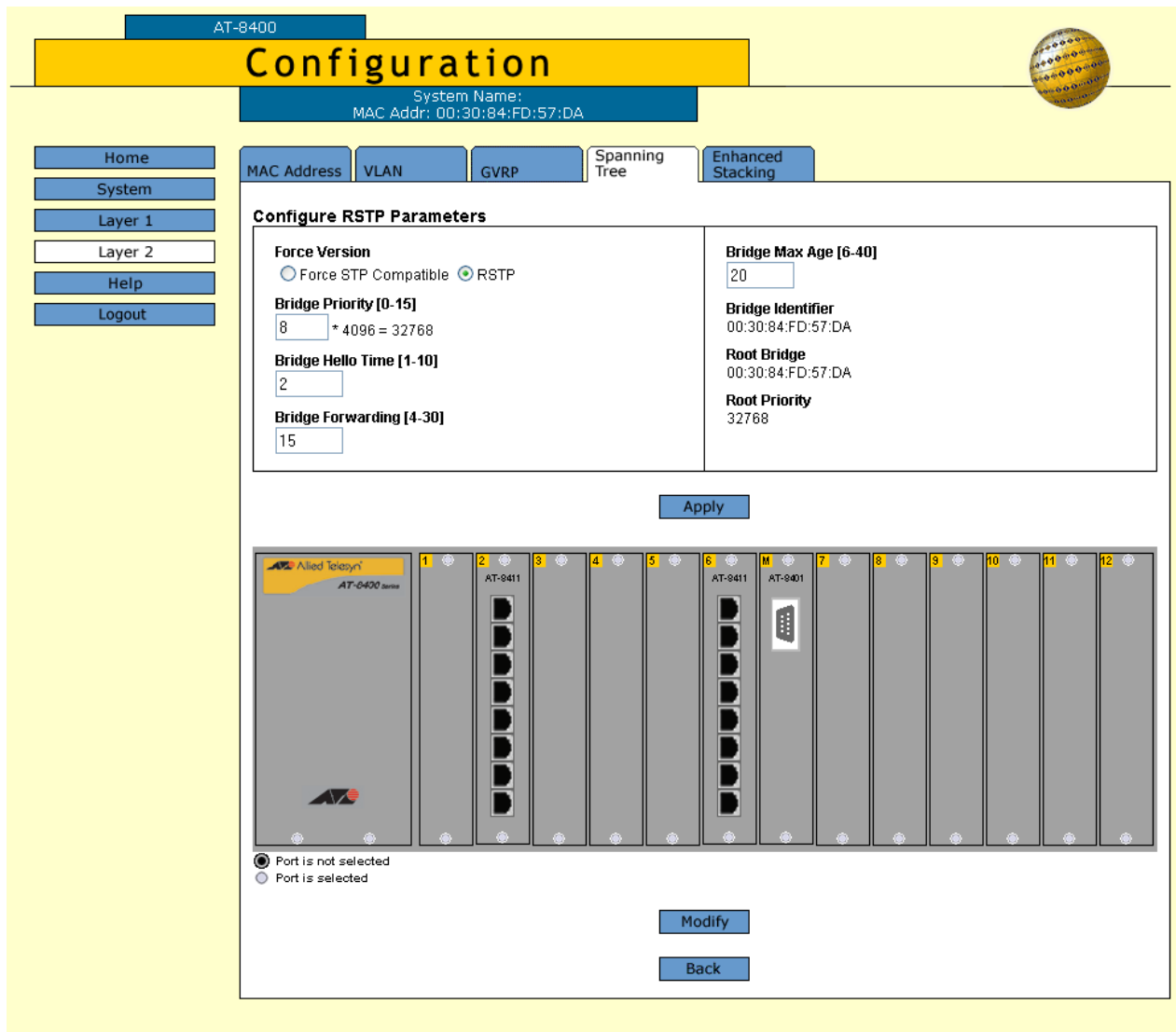


Figure 233 Expanded RSTP Spanning Tree Tab

4. In the Configure RSTP Parameters section, adjust the parameters as desired. The parameters are defined below.

Force Version

This selection determines whether the bridge operates with RSTP or in an STP-compatible mode. The default is RSTP. 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 all ports in STP.

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 15, with 0 having the highest priority. For a list of the increments, refer to **Table 9**, Bridge Priority Value Increments on page 231

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.

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 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, you **must** observe the following equations:

$$\text{MaxAge} < (2 \times (\text{HelloTime} + 1))$$

$$\text{MaxAge} < (2 \times (\text{ForwardingDelay} - 1))$$

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.

Root Bridge

Indicates the MAC address of the switch in the network that is currently functioning as the root bridge for all the switches in the spanning tree domain. The MAC address is determined by the spanning tree protocol. This parameter provides an easy way for a network manager to determine which switch in the network is functioning as the root bridge. This is a read-only parameter.

Root Priority

Indicates the bridge priority value on the root bridge. The bridge priority value is used by spanning tree to select the root bridge for the spanning tree domain. The bridge with the lowest value is assigned as the root bridge. This is a read-only parameter.

5. After you have made your changes, click **Apply**.
6. To adjust a port's RSTP 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 Page is shown in Figure 234.

Figure 234 RSTP Settings Page

7. Adjust the settings as desired. The parameters are described below.

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 of 128). For a list of the increments, refer to **Table 11**, Port Priority Value Increments on page 233.

Port Cost

The spanning tree algorithm uses the cost parameter to decide which port provides the lowest cost path to the root bridge for the specified LAN. The range is 0 to 200,000,000.

Enable Migration Check

This parameter (MCHECK) resets an RSTP port, allowing it to send RSTP BPDUs. When an RSTP bridge receives STP BPDUs on an RSTP port, the port transmits STP BPDUs. The RSTP port continues to transmit STP BPDUs indefinitely. Click to reset the RSTP port to transmit RSTP BPDUs.

Each time an RSTP port is reset by receiving STP BPDUs, you need to reset the RSTP port, allowing it to send RSTP BPDUs.

Note

MCHECK is only valid when the RSTP mode is enabled. This option does not apply when the switch is in STP mode.

Point-to-Point

This parameter defines whether the port is functioning as a point-to-point port. The default setting is Auto Detect, which sets port cost depending on the speed of the port. Default values are 100 for a 10 Mbps port, 10 for a 100 Mbps port, and 4 for a 1 Gbps port. For an explanation of this parameter, refer to Point-to-Point Ports and Edge Ports on page 234.

Edge Port

This parameter defines whether the port is functioning as an edge port. For an explanation of this parameter, refer to Point-to-Point Ports and Edge Ports on page 234.

8. Once you have configured the parameters, click **Apply**.

To save your changes, return to the General Tab and click **Save Changes**. The changes you made are saved on the switch.

Configuring and Modifying MSTP

The procedures for configuring and modifying MSTP are provided in this section. See the following procedures:

- Configuring MSTP Parameters on page 681
- Configuring the CIST Priority on page 684
- Creating, Deleting, or Modifying MSTI IDs on page 685
- Adding, Removing, or Modifying VLAN Associations to MSTIs on page 687
- Configuring MSTP Port Parameters on page 689

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 STP, RSTP, or MSTP on page 670.

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 in Figure 192 on page 584.
2. From the Configuration menu, select the **Layer 2** option.
The Layer 2 Page is displayed with the MAC Address Tab selected by default in Figure 212 on page 634.
3. Select the Spanning Tree Tab.
The Spanning Tree Tab is shown in Figure 230 on page 670.
4. Click on MSTP as the active protocol version.
5. Click **Apply**.

The following message is displayed:

```
The switch will be rebooted for this change. Do you
want to continue?
```

6. Click **Okay**.
7. Click **Configure**.

The expanded MSTP Spanning Tree Tab is displayed as shown in Figure 235.

Configuration
System Name:
MAC Addr: 00:30:84:FE:D2:61

Home System Layer 1 Layer 2 Help Logout

MAC Address VLAN GVRP Spanning Tree Enhanced Stacking

Configure MSTP Parameters

Force Version
 Force STP Compatible MSTP

Bridge Hello Time [1-10]

Bridge Forwarding [4-30]

Configuration Name

Bridge Max Age [6-40]

Bridge Max Hops [1-40]

Revision Level [0-255]

Apply Defaults

Configure CIST Parameters

CIST Priority [0-15]
 * 4096 = 32768

Apply

CIST/MSTI Table

Total CIST/MSTIs: 1. Page 1 of 1

CIST/MSTI ID	Priority	VLAN Associations
<input checked="" type="radio"/> 0	32768	1

Refresh Add

1	2	3	4	5	6	M	7	8	9	10	11	12
AT-8411	AT-8411			AT-8411	AT-8411	AT-8401	AT-8411	AT-8411	AT-8411	AT-8411	AT-8411	AT-8411

Port is not selected
 Port is selected

Modify Back

Figure 235 Expanded MSTP Spanning Tree Tab

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 687. The graphic image of the switch is described in Configuring MSTP Port Parameters on page 689.

8. In the Configure MSTP Parameters section, adjust the parameters as needed. The parameters are described below.

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 less 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. Once 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.

9. Click **Apply**.

To save your changes, return to the General Tab and click **Save Changes**. The changes you made are saved on the switch. 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. Display the Spanning Tree Expanded Page for MSTP by performing Steps 1 through 4 in the procedure Configuring MSTP Parameters on page 681.
2. 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.

3. Click **Apply**.

To save your changes, return to the General Tab and click **Save Changes**. The changes you made are saved on the switch.

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, do the following:

1. Display the Spanning Tree Expanded Page for MSTP by performing Steps 1 through 4 in the procedure Configuring MSTP Parameters on page 681.
2. In the CIST/MSTI Table section of the tab, click **Add**.
The Add New MSTI Page is displayed as shown in Figure 236.

Figure 236 Add New MSTI Page

3. In the MSTI ID field, enter a new MSTI ID. The range is 1 to 15.
4. 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 9**, Bridge Priority Value Increments on page 231. The default is 0.
5. Click **Apply**.
To save your changes, return to the General Tab and click **Save Changes**. The changes you made are saved on the switch.
6. Repeat this procedure to create more MSTI IDs.

Deleting an MSTI ID

To delete an MSTI ID, do the following:

1. Display the Spanning Tree Expanded Page for MSTP by performing Steps 1 through 4 in the procedure Configuring MSTP Parameters on page 681.
2. In the CIST/MSTI Table section of the tab, click the circle next to the MSTI ID you want to delete. You can select only one MSTI ID at a time.
3. Click **Remove**.
4. A confirmation prompt is displayed.
5. Click **OK** to delete the MSTI or **Cancel** to cancel the procedure.
6. 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, do the following:

1. Display the Spanning Tree Expanded Page for MSTP by performing Steps 1 through 4 in the procedure Configuring MSTP Parameters on page 681.
2. In the CIST/MSTI Table section of the tab, click the circle next to the MSTI ID you want to modify. You can select only one MSTI ID at a time. You cannot modify CIST.
3. Click **Modify**.

The Modify MSTI Page is displayed as shown in Figure 237.

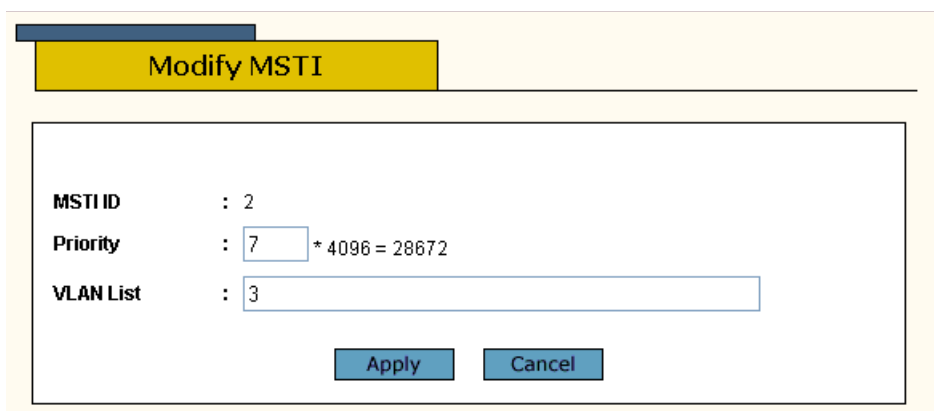


Figure 237 Modify MSTI Page

4. 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 9**, Bridge Priority Value Increments on page 231. The default is 0.
5. Click **Apply**.
To save your changes, return to the General Tab and click **Save Changes**. The changes you made are saved on the switch.
6. 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, do the following:

1. Display the Spanning Tree Expanded Page for MSTP by performing Steps 1 through 4 in the procedure Configuring MSTP Parameters on page 681.
2. 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).
3. Click Apply.

To save your changes, return to the General Tab and click **Save Changes**. The changes you made are saved on the switch. Or, proceed to the next procedure to configure the CIST priority.

Removing a VLAN Association

To remove a VLAN association, do the following:

1. Display the Spanning Tree Expanded Page for MSTP by performing Steps 1 through 4 in the procedure Configuring MSTP Parameters on page 681.
2. 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).
3. Click Apply.

To save your changes, return to the General Tab and click **Save Changes**. The changes you made are saved on the switch. Or, proceed to the next procedure to configure the CIST priority.

Modifying a VLAN Association

To modify a VLAN association, do the following:

1. Display the Spanning Tree Expanded Page for MSTP by performing Steps 1 through 4 in the procedure Configuring MSTP Parameters on page 681.
2. 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).
3. Click Apply.

To save your changes, return to the General Tab and click **Save Changes**. The changes you made are saved on the switch. Or, proceed to the next procedure to configure the CIST priority.

Configuring MSTP Port Parameters

To configure MSTP port parameters, perform the following procedure:

1. Perform Steps 1 through 4 in the procedure Configuring MSTP Parameters on page 681 to display the expanded Spanning Tree Page for MSTP.
2. 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.

3. Click **Modify**.

The MSTP Port Settings Page is displayed in Figure 238.

Figure 238 MSTP Port Settings Page

4. Adjust the parameters as needed. The parameters are described below.

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 11**, Port Priority Value Increments on page 233.

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. For an explanation of this parameter, refer to Point-to-Point Ports and Edge Ports on page 234.

Point-to-Point

This parameter defines whether the port is functioning as a point-to-point port. For an explanation of this parameter, refer to Point-to-Point Ports and Edge Ports on page 234.

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.

5. After adjusting the parameters, click **Apply**.

To save your changes, return to the General Tab and click **Save Changes**. The changes you made are saved on the switch.

6. Repeat this procedure to configure MSTP parameters for other switch ports.

Displaying STP, RSTP, or MSTP Settings

To display spanning tree 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 194 on page 592.

2. Select the **Layer 2** option.

The Monitoring Layer 2 Page is displayed with the MAC Address Tab selected by default, as shown Figure 212 on page 634.

3. Select the Spanning Tree Tab.

The Monitoring Spanning Tree Tab is shown in Figure 240. This tab displays whether spanning tree is enabled or disabled and which spanning tree protocol is active.

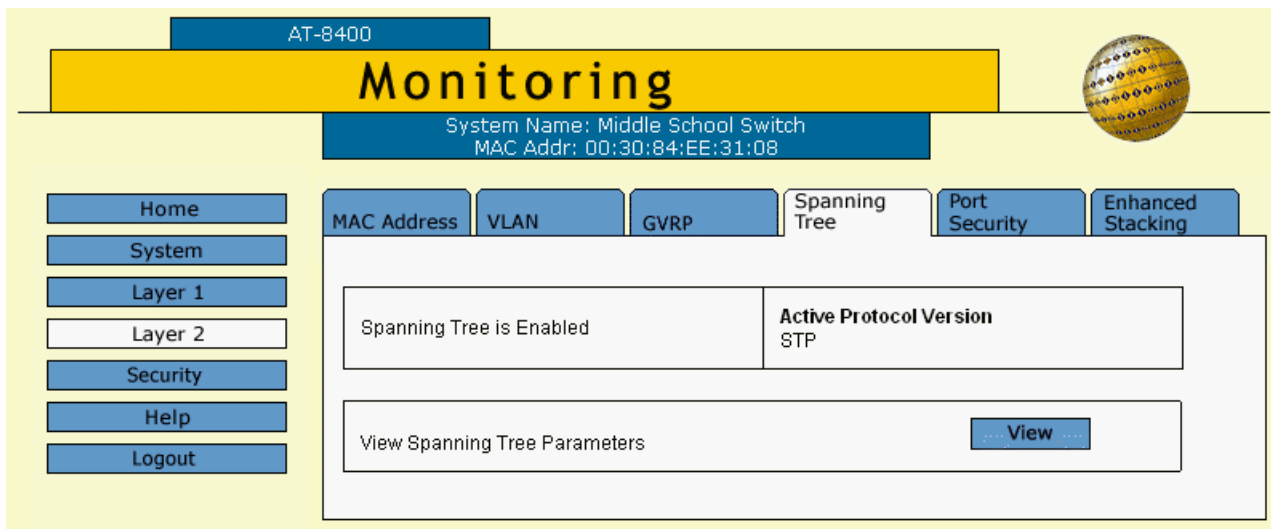


Figure 239 Monitoring Layer 2 Page, Spanning Tree Tab

4. To view the current settings for the active spanning tree protocol, click **View**.

Figure 240 shows an example of the Monitor STP Parameters Tab. The contents of this tab differs depending on which spanning tree protocol is active on the switch. The information in this page is for viewing purposes only.

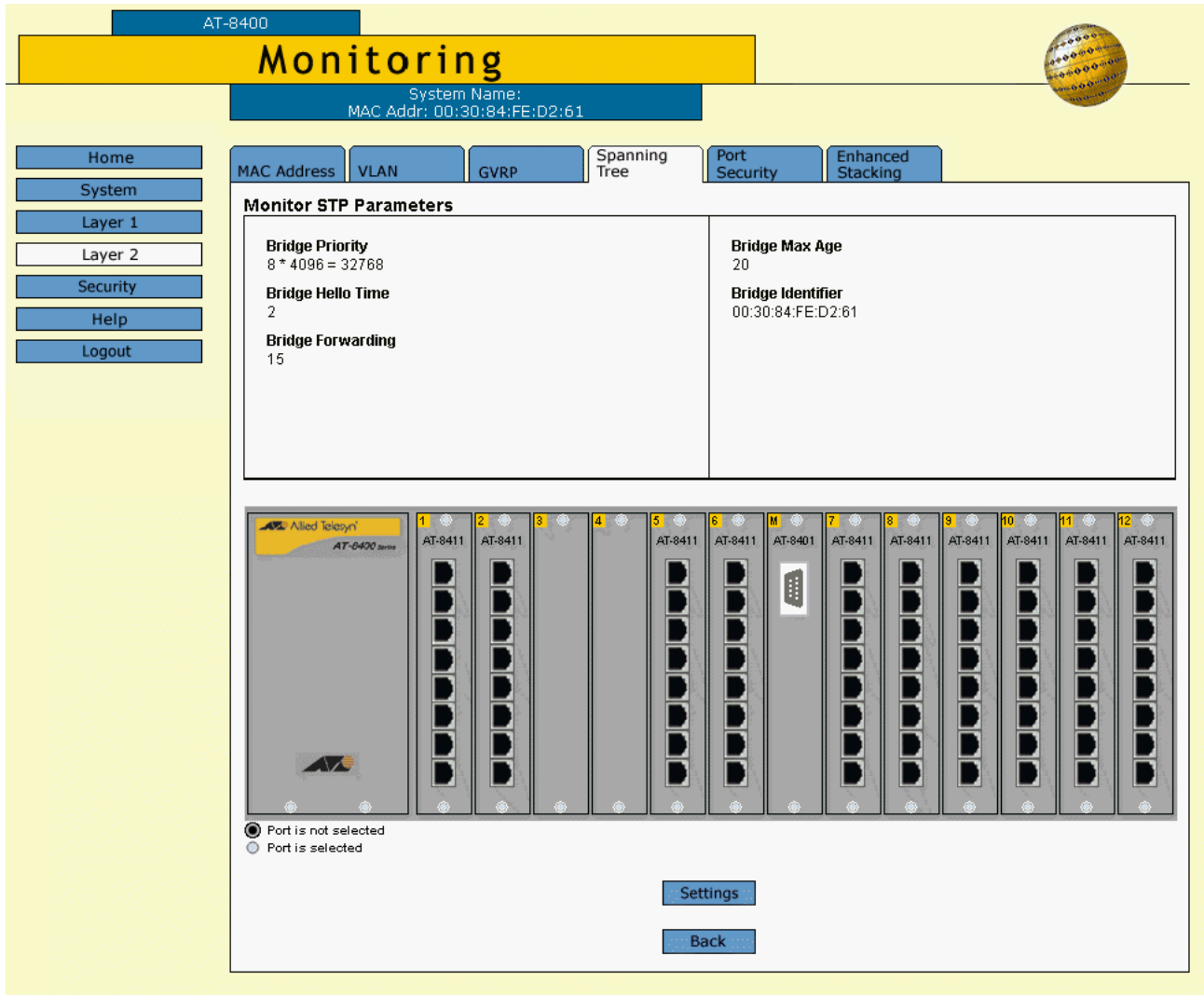
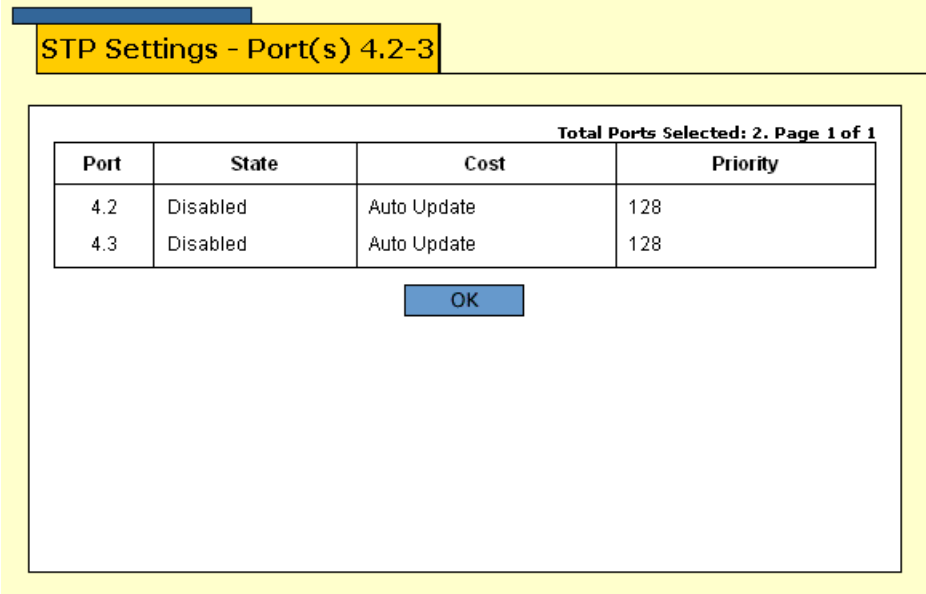


Figure 240 Monitoring Layer 2 Page, Spanning Tree Tab

- To view port settings, click a port on the switch and click **Settings**. You can select more than one port.

The STP Settings Page is shown in Figure 241.



The screenshot displays the 'STP Settings - Port(s) 4.2-3' window. At the top right, it indicates 'Total Ports Selected: 2. Page 1 of 1'. Below this is a table with four columns: Port, State, Cost, and Priority. The table contains two rows of data for ports 4.2 and 4.3. Both ports are in a 'Disabled' state with a 'Cost' of 'Auto Update' and a 'Priority' of '128'. Below the table is a blue 'OK' button.

Port	State	Cost	Priority
4.2	Disabled	Auto Update	128
4.3	Disabled	Auto Update	128

OK

Figure 241 STP Settings Page

6. Click **OK**.

Chapter 40

SNMPv3 Protocol

This chapter provides the following procedures for configuring basic switch parameters using a web browser management session:

- Configuring the SNMPv3 Protocol on page 695
- Enabling the SNMP Protocol on page 696
- Configuring the SNMPv3 User Table on page 698
- Configuring the SNMPv3 View Table on page 705
- Configuring the SNMPv3 Access Table on page 710
- Configuring the SNMPv3 SecurityToGroup Table on page 717
- Configuring the SNMPv3 Notify Table on page 722
- Configuring the SNMPv3 Target Address Table on page 727
- Configuring the SNMPv3 Target Parameters Table on page 733
- Configuring the SNMPv3 Community Table on page 740
- Displaying SNMPv3 Tables on page 746

Configuring the SNMPv3 Protocol

To configure the SNMPv3 protocol, you need to configure the SNMPv3 tables. To enable a manager to access the SNMPv3 protocol on the switch, you need to enable the SNMP protocol. See the following procedures:

- Enabling the SNMP Protocol on page 696
- Configuring the SNMPv3 User Table on page 698
- Configuring the SNMPv3 View Table on page 705
- Configuring the SNMPv3 Access Table on page 710
- Configuring the SNMPv3 SecurityToGroup Table on page 717
- Configuring the SNMPv3 Notify Table on page 722
- Configuring the SNMPv3 Target Address Table on page 727
- Configuring the SNMPv3 Target Parameters Table on page 733
- Configuring the SNMPv3 Community Table on page 740

Note

Use the SNMPv3 Community Table only if you are configuring the SNMPv3 protocol with the SNMPv1 or an SNMPv2c protocol. Allied Telesyn does not recommend this configuration.

For reference information about the SNMPv3 protocol, see Chapter 17: SNMPv3 Configuration on page 293.

Enabling the SNMP Protocol

In order to allow an NMS (an SNMP manager) to access the switch, you need to enable SNMP access. In addition, to allow the switch to send a trap when it receives a request message, 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 Configuration System Page is displayed with the General Tab selected by default, as shown in Figure 192 on page 584.

2. Select the SNMP Tab.

The SNMP Tab is shown in Figure 242.

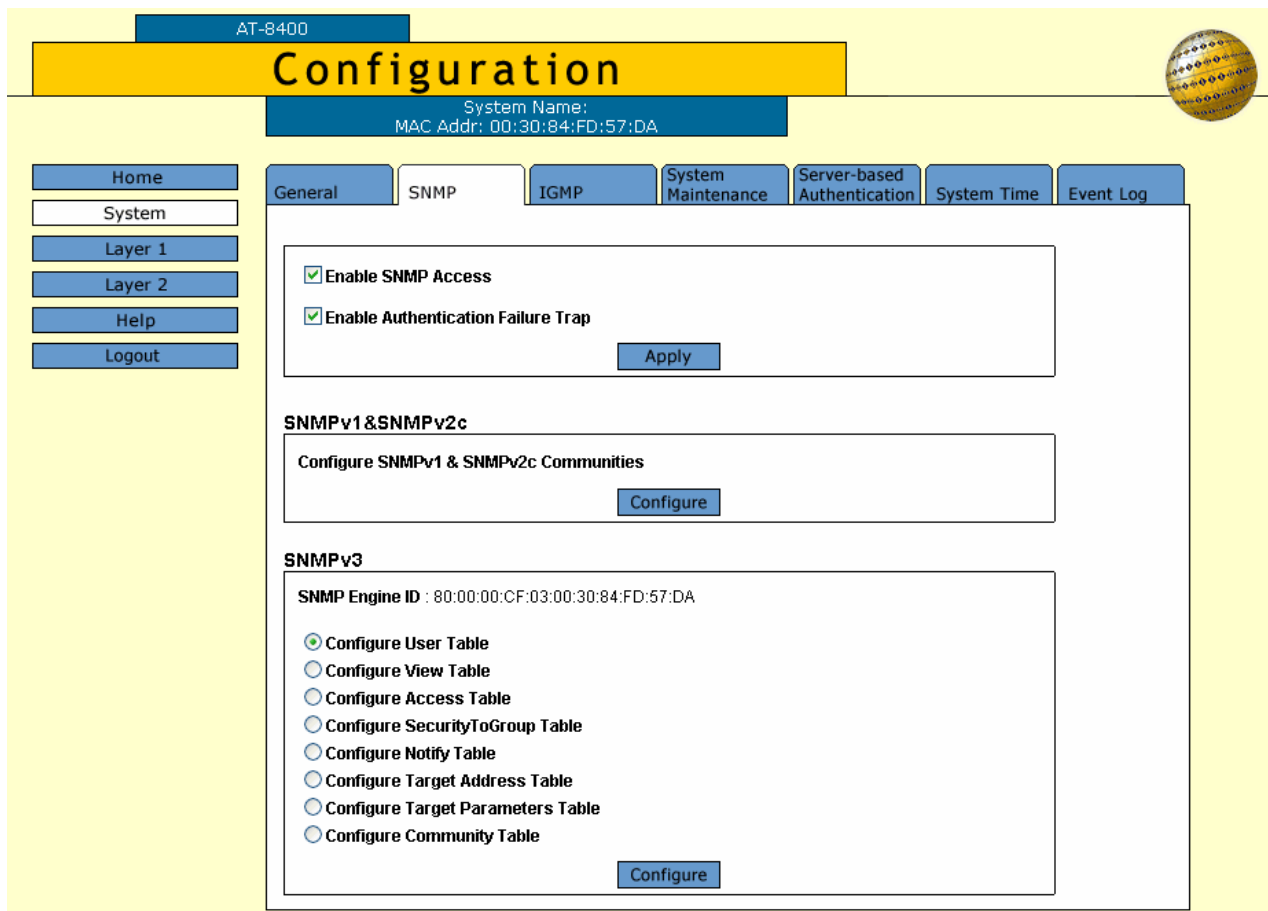


Figure 242 Configuration System Page, SNMP Tab

3. To enable SNMP Access, click the box next to Enable SNMP Access.

Use this parameter to enable the switch to be remotely managed with an SNMP application program.

Note

If the check box in the Enable SNMP Access box is empty, the switch cannot be managed through SNMP. This is the default.

4. To enable authentication failure traps to be sent on behalf of the switch, click the box next to Enable Authentication Failure Trap.
5. Click **Apply** to update the User Table.
6. To save your changes, return to the General Tab and click **Save Changes**.

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 698
- Deleting a User Table Entry on page 701
- Modifying a User Table Entry on page 702

For reference information about the SNMPv3 User Table, see [Configuring the SNMPv3 User Table on page 305](#).

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 192 on page 584](#).
2. Select the SNMP Tab.
The SNMP Tab is shown in [Figure 195 on page 596](#).
3. In the SNMPv3 section of the page, click the circle next to Configure User Table. Then click **Configure** at the bottom of the page.

The SNMPv3 User Table Page is shown in Figure 243.

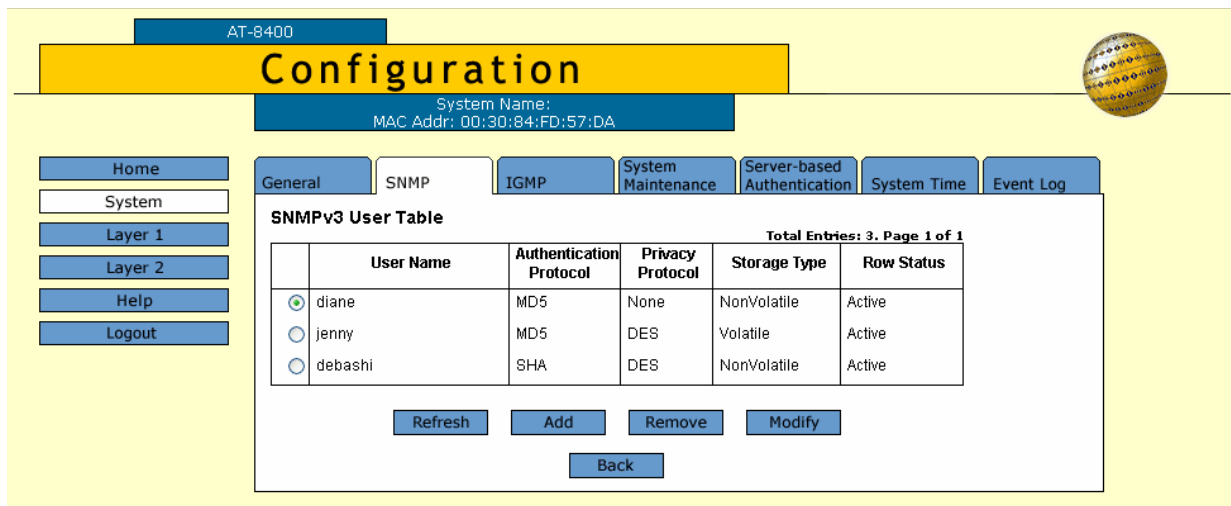


Figure 243 SNMPv3 User Table Page

- Click the **Add** button to add a new SNMPv3 User Table entry. The Add New SNMPv3 User Page is shown in Figure 244

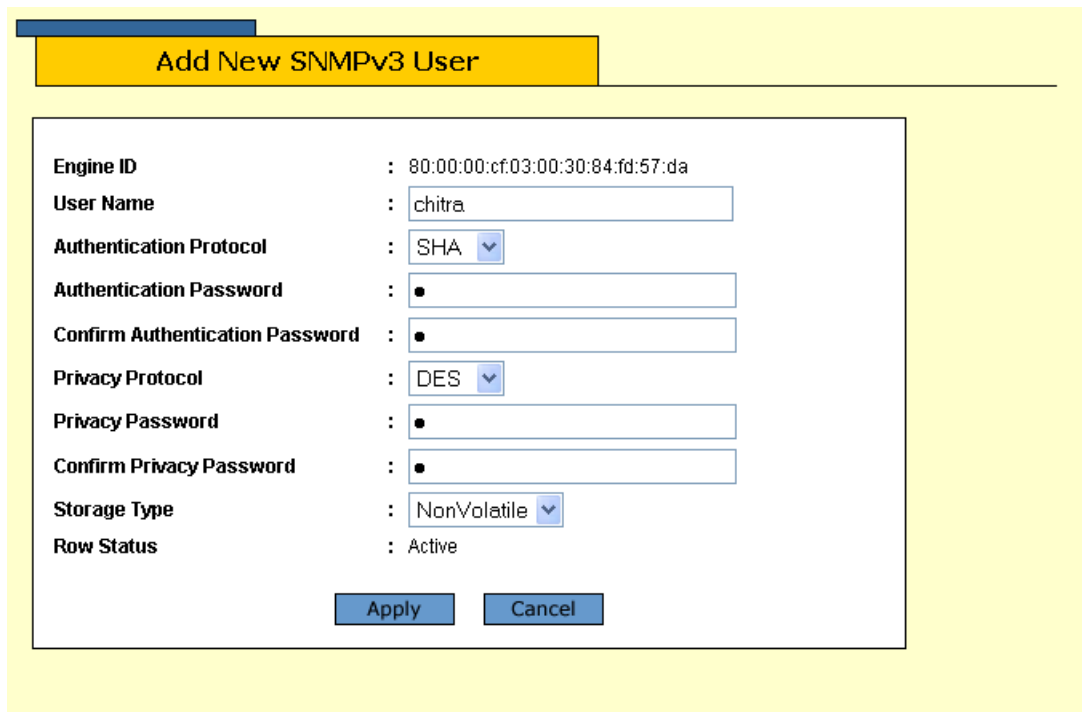


Figure 244 Add New SNMPv3 User Page

- 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:

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.

MD5

This value represents the MD5 authentication protocol. With this selection, users are authenticated with the MD5 authentication protocol after a message is received. With this 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. With this selection, you can configure a Privacy Protocol.

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 AT-S60 software version 2.1.0 that does not contain the encryption features, then the Privacy Protocol field is read-only field and it is set to None.

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:

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.

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.

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 to the configuration file. After making changes to an User Table entry with a Volatile storage type, **Save Changes** does not appear on the General Tab.

NonVolatile

Select this storage type if you want the ability to save an entry in the User Table to the configuration file. After making changes to an User Table entry with a NonVolatile storage type, **Save Changes** appears on the General Tab.

Note

The Row Status parameter is a read-only field in the Web interface. The Active value indicates the SNMPv3 User Table entry takes effect immediately.

13. Click **Apply** to update the SNMPv3 User Table.
14. To save your changes, return to the General Tab and click **Save Changes**.

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 192 on page 584.
2. Select the SNMP Tab.
The SNMP Tab is shown in Figure 195 on page 596.
3. In the SNMPv3 section of the page, click the circle next to Configure User Table. Then click **Configure**.
The SNMPv3 User Table Page is shown in Figure 243 on page 699.
4. Click the circle next to the User Table entry that you want to delete. Then click **Remove**.

A warning message is displayed. Click OK to remove the User Table entry.

- To save your changes, return to the General Tab and click **Save Changes**.

Modifying a User Table Entry

To modify an entry SNMPv3 User 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 192 on page 584.
- Select the SNMP Tab.
The SNMP Tab is shown in Figure 195 on page 596.
- In the SNMPv3 section of the page, click the circle next to Configure User Table. Then click **Configure**.
The SNMPv3 User Table Page is shown in Figure 243 on page 699.
- To modify an SNMPv3 User Table entry, click the circle next to the SNMPv3 user that you want to change. Then click **Modify**.
The Modify SNMPv3 User Page is shown in Figure 245.

Modify SNMPv3 User

Engine ID : 80:00:00:cf:03:00:30:84:fd:57:da

User Name : debashis

Authentication Protocol : MD5

Authentication Password :

Confirm Authentication Password :

Privacy Protocol : DES

Privacy Password :

Confirm Privacy Password :

Storage Type : NonVolatile

Row Status : Active

Figure 245 Modify SNMPv3 User Page

- In the Authentication Protocol field, enter an authentication protocol. This is an optional parameter.

Select one of the following:

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.

MD5

This value represents the MD5 authentication protocol. With this selection, users are authenticated with the MD5 authentication protocol after a message is received. With this 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. With this selection, you can configure a Privacy Protocol.

Note

When you change the Authentication Protocol field, you must reenter the authentication password. In addition, if the Privacy Protocol is set to DES and you change Authentication Protocol, then you must reenter the Privacy Password.

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 AT-S60 software version 2.1.0 that does not contain the encryption features, then the Privacy Protocol field is read-only field and it is set to None.

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:

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.

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.

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 to the configuration file. After making changes to an SNMPv3 User Table entry with a Volatile storage type, **Save Changes** does not appear on the General Tab.

NonVolatile

Select this storage type if you want the ability to save an entry in the SNMPv3 User Table to the configuration file. After making changes to an SNMPv3 User Table entry with a NonVolatile storage type, **Save Changes** appears on the General Tab.

Note

The Row Status parameter is a read-only field in the Web interface. The Active value indicates the SNMPv3 User Table entry takes effect immediately.

12. Click **Apply** to update the SNMPv3 User Table.
13. To save your changes, return to the General Tab and click **Save Changes**.

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 705
- Deleting a View Table Entry on page 707
- Modifying a View Table Entry on page 708

For reference information about the SNMPv3 View Table, see [Configuring the SNMPv3 View Table on page 705](#).

Creating a View Table Entry

To create an entry in the SNMPv3 View Table entry, 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 192 on page 584](#).
2. Select the SNMP Tab.
The SNMP Tab is shown in [Figure 195 on page 596](#).
3. In the SNMPv3 section of the page, click the circle next to Configure View Table. Then click **Configure** at the bottom of the page.
The SNMPv3 View Table Page is shown in [Figure 246](#).

AT-B400

Configuration

System Name: AT-B400
MAC Addr: 00:30:84:FD:57:DA

Home System Layer 1 Layer 2 Help Logout

General **SNMP** IGMP System Maintenance Server-based Authentication System Time Event Log

SNMPv3 View Table Total Entries: 6. Page 1 of 2

	View Name	SubTree OID	SubTree Mask	View Type	Storage Type	Row Status
<input checked="" type="radio"/>	mgmt	1.36.1.2		Excluded	NonVolatile	Active
<input type="radio"/>	private	1.3.6.1.4	FF:FF	Included	NonVolatile	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

Refresh Add Remove Modify Next

Back

Figure 246 SNMPv3 View Table Page

4. To create a new SNMPv3 View Table entry click **Add**.
The Add New SNMPv3 View Page is shown in Figure 247.

Figure 247 Add New SNMPv3 View Page

5. In the View Name field, enter a descriptive name of 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 in the View Subtree parameter. This parameter is in binary format.

The View Subtree parameter defines a MIB View and the Subtree Mask further restricts a user's view, for example, to a specific row of the MIB tree. The value of the Subnet Mask parameter is dependent on the subtree you select. See RFC 2575 for detailed information about defining a subnet mask.

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 to the configuration file. After making changes to a View Table entry with a Volatile storage type, **Save Changes** does not appear on the General Tab.

NonVolatile

Select this storage type if you want the ability to save an entry in the View Table to the configuration file. After making changes to a View Table entry with a NonVolatile storage type, **Save Changes** appears on the General Tab.

Note

The Row Status parameter is a read-only field in the Web interface. The Active value indicates the SNMPv3 View Table entry takes effect immediately.

10. Click **Apply** to update the SNMPv3 View Table.
11. To save your changes, return to the General Tab and click **Save Changes**.

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 192 on page 584.
2. Select the SNMP Tab.
The SNMP Tab is shown in Figure 195 on page 596.

3. In the SNMPv3 section of the page, click the circle next to Configure View Table. Then click **Configure**.
4. The SNMPv3 View Table Page is shown in Figure 246 on page 705.
5. Click the circle next to the View Table entry that you want to delete. Then click **Remove**.
A warning message is displayed. Click OK to remove the View Table entry.
6. To save your changes, return to the General Tab and click **Save Changes**.

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 192 on page 584.
2. Select the SNMP Tab.
The SNMP Tab is shown in Figure 195 on page 596.
3. In the SNMPv3 section of the page, click the circle next to Configure View Table. Then click **Configure** at the bottom of the page.
The SNMPv3 View Table Page is shown in Figure 246 on page 705.
4. To modify an SNMPv3 View Table entry, click the circle next to the SNMPv3 View Table entry that you want to change. Then click **Modify**.
The Modify SNMPv3 View Page is shown in Figure 248.

Modify SNMPv3 View	
View Name	: mgmt
Subtree OID	: 1.3.6.1.2
Subtree Mask	: <input type="text"/>
View Type	: Included ▼
Storage Type	: NonVolatile ▼
Row Status	: Active
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Figure 248 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 in the View Subtree parameter. This parameter is in binary format.

The View Subtree parameter defines a MIB View and the Subtree Mask further restricts a user's view, for example, to a specific row of the MIB tree. The value of the Subnet Mask parameter is dependent on the subtree you select. See RFC 2575 for detailed information about defining a subnet mask.

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 to the configuration file. After making changes to an Target Parameters Table entry with a Volatile storage type, **Save Changes** does not appear on the General Tab.

NonVolatile

Select this storage type if you want the ability to save an entry in the View Table to the configuration file. After making changes to a View Table entry with a NonVolatile storage type, **Save Changes** appears on the General Tab.

Note

The Row Status parameter is a read-only field in the web interface. The Active value indicates the SNMPv3 View Table entry takes effect immediately.

8. Click **Apply** to update the SNMPv3 View Table.
9. To save your changes, return to the General Tab and click **Save Changes**.

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 710
- Deleting an Access Table Entry on page 714
- Modifying an Access Table Entry on page 714

For reference information about the SNMPv3 Access Table, see *Configuring the SNMPv3 Access Table* on page 710.

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 192 on page 584.
2. Select the SNMP Tab.
The SNMP Tab is shown in Figure 195 on page 596.
3. In the SNMPv3 section of the page, click the circle next to Configure Access Table. Then click **Configure** at the bottom of the page.
The SNMPv3 Access Table Page is shown in Figure 249.

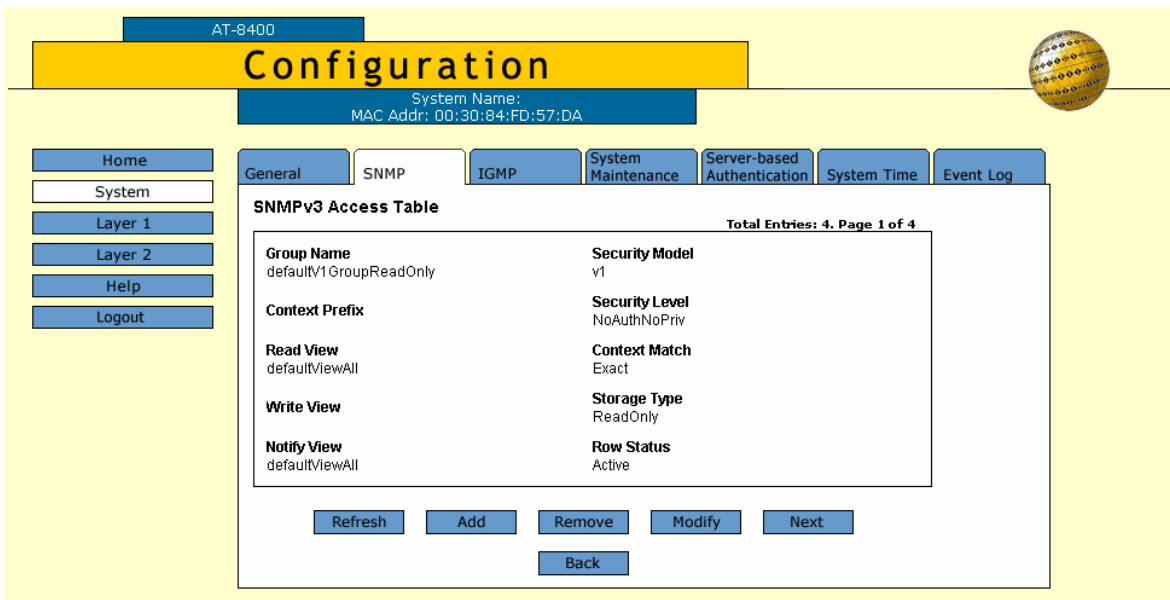


Figure 249 SNMPv3 Access Table Page

4. To create an SNMPv3 Access Table entry, click **Add**.

The Add New SNMPv3 Access Page is shown in Figure 250.

Figure 250 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 users 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, NoAuthenticationNoPrivacy 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 to the configuration file. After making changes to an Access Table entry with a Volatile storage type, **Save Changes** does not appear on the General Tab.

NonVolatile

Select this storage type if you want the ability to save an entry in the Access Table to the configuration file. After making changes to an Access Table entry with a NonVolatile storage type, **Save Changes** appears on the General Tab.

Note

The Row Status parameter is a read-only field in the Web interface. The Active value indicates the SNMPv3 Access Table entry will take effect immediately.

12. Click **Apply** to update the SNMPv3 Access Table.
13. To save your changes, return to the General Tab and click **Save Changes**.

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 192 on page 584.
2. Select the SNMP Tab.
The SNMP Tab is shown in Figure 195 on page 596.
3. In the SNMPv3 section of the page, click the circle next to Configure Access Table. Then click **Configure** at the bottom of the page.
The SNMPv3 Access Table Page is shown in Figure 249 on page 710.
4. Display the Access Table entry that you want to delete.
Click **Next** or **Previous** to display an entry.
5. Click **Remove**.
A warning message is displayed. Click OK to remove the Access Table entry.
6. To save your changes, return to the General Tab and click **Save Changes**.

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 192 on page 584.
2. Select the SNMP Tab.
The SNMP Tab is shown in Figure 195 on page 596.
3. In the SNMPv3 section of the page, click the circle next to Configure Access Table. Then click **Configure** at the bottom of the page.
The SNMPv3 Access Table Page is shown in Figure 249 on page 710.
4. Display the Access Table entry that you want to change.
Click **Next** or **Previous** to display an entry.
5. Click **Modify**.

The Modify SNMPv3 Access Page is shown in Figure 251.

Modify SNMPv3 Access

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

Apply Cancel

Figure 251 Modify SNMPv3 Access Page

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 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 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 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 to the configuration file. After making changes to an Access Table entry with a Volatile storage type, **Save Changes** does not appear on the General Tab.

NonVolatile

Select this storage type if you want the ability to save an entry in the Access Table to the configuration file. After making changes to an Access Table entry with a NonVolatile storage type, **Save Changes** appears on the General Tab.

Note

The Row Status parameter is a read-only field in the Web interface. The Active value indicates the Access Table entry takes effect immediately.

10. Click **Apply** to update the SNMPv3 Access Table.
11. To save your changes, return to the General Tab and click **Save Changes**.

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 717
- Deleting a SecurityToGroup Table Entry on page 719
- Modifying a SecurityToGroup Table Entry on page 720

For reference information about the SNMPv3 Configuring the SNMPv3 SecurityToGroup Table on page 717.

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 192 on page 584.

2. Select the SNMP Tab.

The SNMP Tab is shown in Figure 195 on page 596.

3. In the SNMPv3 section of the page, click the circle next to Configure SecurityToGroup Table. Then click **Configure** at the bottom of the page.

The SNMPv3 SecurityToGroup Table Page is shown in Figure 252.

AT-8400

Configuration

System Name:
MAC Addr: 00:30:84:FD:57:DA

Home System Layer 1 Layer 2 Help Logout

General **SNMP** IGMP System Maintenance Server-based Authentication System Time Event Log

SNMPv3 SecurityToGroup Table

Total Entries: 9. Page 2 of 2

	Security Model	Security Name	Group Name	Storage Type	Row Status
<input checked="" type="radio"/>	v3	diane	testengineering	NonVolatile	Active
<input type="radio"/>	v3	jenny	swengineering	NonVolatile	Active
<input type="radio"/>	v3	chitra	testengineering	NonVolatile	Active
<input type="radio"/>	v3	debashis	swengineering	NonVolatile	Active

Refresh Add Remove Modify Previous

Back

Figure 252 SNMPv3 SecurityToGroup Table Page

- To create an SNMPv3 SecurityToGroup Table entry, click **Add**.
The Add New SNMPv3 SecurityToGroup Page is shown in Figure 253.

Figure 253 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 User Name with the SNMPv1 protocol.
 - v2c**
Select this value to associate the User Name with the SNMPv2c protocol.
 - v3**
Select this value to associate the User Name with the SNMPv3 protocol.
- 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 698.
- In the Group Name field, enter a Group Name that you configured in the Access Table.
See Creating an Access Table on page 710.

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 to the configuration file. After making changes to a SecurityToGroup Table entry with a Volatile storage type, **Save Changes** does not appear on the General Tab.

NonVolatile

Select this storage type if you want the ability to save an entry in the SecurityToGroup Table to the configuration file. After making changes to a SecurityToGroup Table entry with a NonVolatile storage type, **Save Changes** appears on the General Tab.

Note

The Row Status parameter is a read-only field in the Web interface. The Active value indicates the SNMPv3 SecurityToGroup Table entry takes effect immediately.

9. Click **Apply** to update the SNMPv3 SecurityToGroup Table.
10. To save your changes, return to the General Tab and click **Save Changes**.

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 192 on page 584.
2. Select the SNMP Tab.
The SNMP Tab is shown in Figure 195 on page 596.
3. In the SNMPv3 section of the page, click the circle next to Configure SecurityToGroup Table. Then click **Configure** at the bottom of the page.

The SNMPv3 SecurityToGroup Table Page is shown in Figure 252 on page 717.

4. Click the circle next to the SecurityToGroup Table entry that you want to delete. Then click **Remove**.

A warning message is displayed. Click OK to remove the SNMPv3 SecurityToGroup Table entry.

5. To save your changes, return to the General Tab and click **Save Changes**.

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 192 on page 584.

2. Select the SNMP Tab.

The SNMP Tab is shown in Figure 195 on page 596.

3. In the SNMPv3 section of the page, click the circle next to Configure SecurityToGroup Table. Then click **Configure** at the bottom of the page.

The SNMPv3 SecurityToGroup Table Page is shown in Figure 252 on page 717.

4. Click the circle next to the SecurityToGroup Table entry that you want to change. Then click **Modify**.

The Modify SNMPv3 SecurityToGroup Page is shown in Figure 254.

The screenshot shows the 'Modify SNMPv3 SecurityToGroup' page. The page has a yellow header with the title 'Modify SNMPv3 SecurityToGroup'. Below the header is a white form box containing the following fields:

- Security Model** : v3
- Security Name** : hoa
- Group Name** : swengineering
- Storage Type** : NonVolatile
- Row Status** : Active

At the bottom of the form are two buttons: **Apply** and **Cancel**.

Figure 254 Modify SNMPv3 SecurityToGroup Page

5. In the Group Name field, enter a Group Name that you configured in the SNMPv3 Access Table.

See Creating an Access Table on page 710.

There are four default values for this field that are reserved for SNMPv1 and SNMPv2c implementations:

- defaultV1GroupReadOnly
- defaultV1GroupReadWrite
- defaultV2cGroupReadOnly
- defaultV2cGroupReadWrite

6. 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 to the configuration file. After making changes to a SecurityToGroup Table entry with a Volatile storage type, **Save Changes** does not appear on the General Tab.

NonVolatile

Select this storage type if you want the ability to save an entry in the SecurityToGroup Table to the configuration file. After making changes to a SecurityToGroup Table entry with a NonVolatile storage type, **Save Changes** appears on the General Tab.

Note

The Row Status parameter is a read-only field in the Web interface. The Active value indicates the SNMPv3 SecurityToGroup Table entry takes effect immediately.

7. Click **Apply** to update the SNMPv3 SecurityToGroup Table.
8. To save your changes, return to the General Tab and click **Save Changes**.

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 722
- Deleting a Notify Table Entry on page 724
- Modifying a Notify Table Entry on page 724

For reference information about the SNMPv3 Notify Table, see *Configuring the SNMPv3 Notify Table* on page 722.

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 192 on page 584.
2. Select the SNMP Tab.
The SNMP Tab is shown in Figure 195 on page 596.
3. In the SNMPv3 section of the page, click the circle next to Configure Notify Table. Then click **Configure** at the bottom of the page.
The SNMPv3 Notify Table Page is shown in Figure 255.

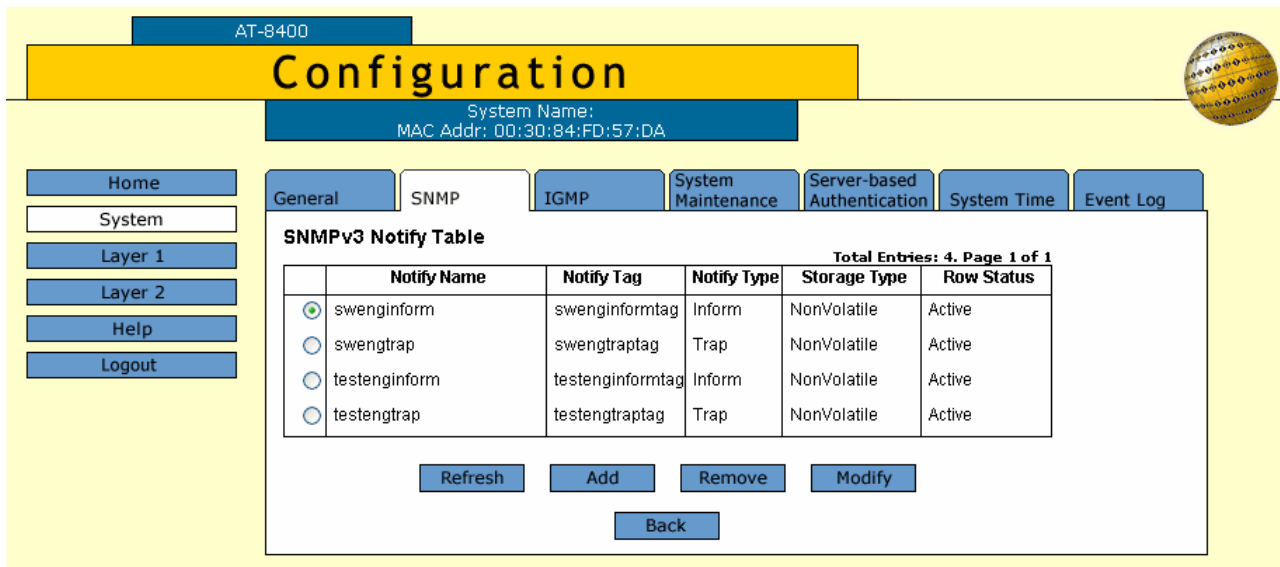


Figure 255 SNMPv3 Notify Table Page

- To create an SNMPv3 Notify Table entry, click **Add**.

The Add New SNMPv3 Notify Page is shown in Figure 256.

Figure 256 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.
- 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.

- 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 to the configuration file. After making changes to a Notify Table entry with a Volatile storage type, **Save Changes** does not appear on the General Tab.

NonVolatile

Select this storage type if you want the ability to save an entry in the Notify Table to the configuration file. After making changes to a Notify Table entry with a NonVolatile storage type, **Save Changes** appears on the General Tab.

Note

The Row Status parameter is a read-only field in the Web interface. The Active value indicates the SNMPv3 Notify Table entry takes effect immediately.

9. Click **Apply** to update the SNMPv3 Notify Table.
10. To save your changes, return to the General Tab and click **Save Changes**.

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 192 on page 584.
2. Select the SNMP Tab.
The SNMP Tab is shown in Figure 195 on page 596.
3. In the SNMPv3 section of the page, click the circle next to Configure Notify Table. Then click **Configure** at the bottom of the page.
The SNMPv3 Notify Table Page is shown in Figure 255 on page 722.
4. Click the circle next to the Notify Table entry that you want to delete. Then click **Remove**.
A warning message is displayed. Click OK to remove the SNMPv3 Notify Table entry.
5. To save your changes, return to the General Tab and click **Save Changes**.

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 192 on page 584.
2. Select the SNMP Tab.
The SNMP Tab is shown in Figure 195 on page 596.

3. In the SNMPv3 section of the page, click the circle next to Configure Notify Table. Then click **Configure** at the bottom of the page.

The SNMPv3 Notify Table Page is shown in Figure 255 on page 722.

4. Click the circle next to the table entry that you want to change. Then click **Modify**.

The Modify SNMPv3 Notify Page is shown in Figure 257

Figure 257 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 to the configuration file. After making changes to an Notify Table entry with a Volatile storage type, **Save Changes** does not appear on the Configuration Tab.

NonVolatile

Select this storage type if you want the ability to save an entry in the Notify Table to the configuration file. After making changes to an Notify Table entry with a NonVolatile storage type, **Save Changes** appears on the Configuration Tab.

Note

The Row Status parameter is a read-only field in the Web interface. The Active value indicates the SNMPv3 Notify Table entry takes effect immediately.

8. Click **Apply** to update the SNMPv3 Notify Table.
9. To save your changes, return to the General Tab and click **Save Changes**.

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 727
- Deleting a Target Address Table Entry on page 730
- Modifying Target Address Table Entry on page 730

For reference information about the SNMPv3 Target Address Table, see [Configuring the SNMPv3 Target Address Table on page 727](#).

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 192 on page 584](#).
2. Select the SNMP Tab.
The SNMP Tab is shown in [Figure 195 on page 596](#).
3. In the SNMPv3 section of the page, click the circle next to Configure Target Address Table. Then click **Configure** at the bottom of the page.
The SNMPv3 Target Address Table Page is shown in [Figure 258 on page 728](#).

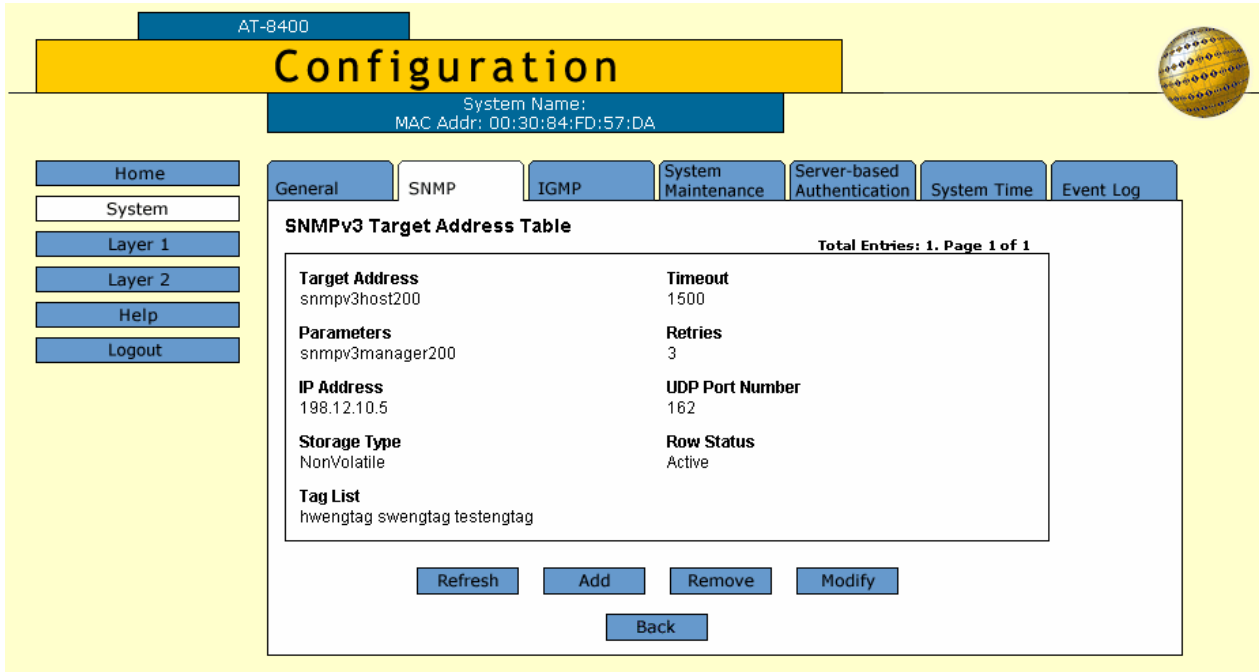


Figure 258 SNMPv3 Target Address Table Page

- To create an SNMPv3 Target Address Table entry, click **Add**. The Add New SNMPv3 Target Address Table Page is shown in Figure 259.

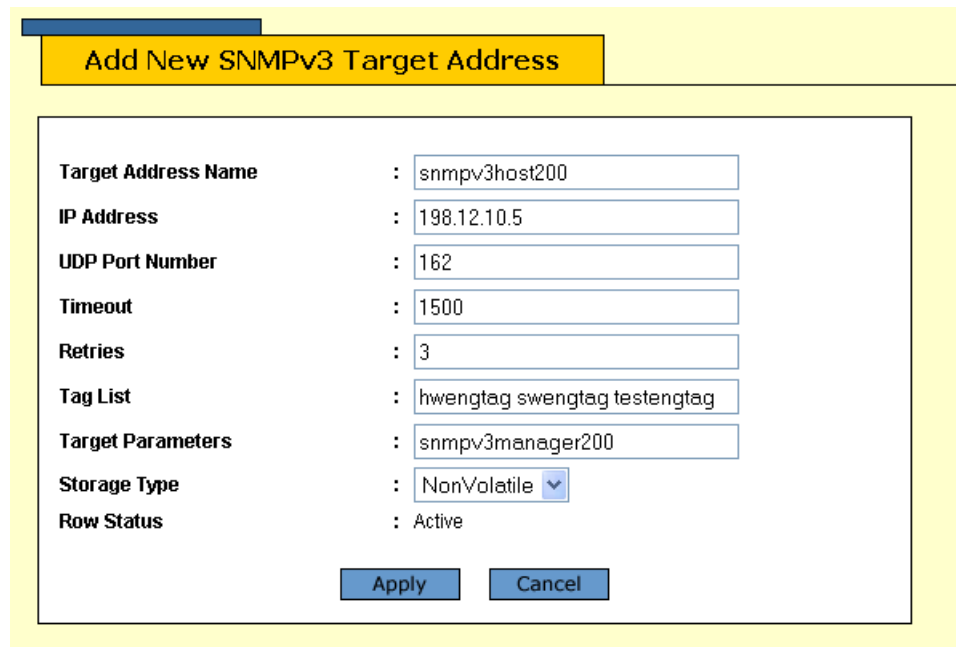


Figure 259 Add New SNMPv3 Target Address Table Page

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 722. 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 to the configuration file. After making changes to a Target Address Table entry with a Volatile storage type, **Save Changes** does not appear on the General Tab.

NonVolatile

Select this storage type if you want the ability to save an entry in the Target Address Table to the configuration file. After making changes to a Target Address Table entry with a NonVolatile storage type, **Save Changes** appears on the General Tab.

Note

The Row Status parameter is a read-only field in the Web 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. To save your changes, return to the General Tab and click **Save Changes**.

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 192 on page 584.
2. Select the SNMP Tab.
The SNMP Tab is shown in Figure 195 on page 596.
3. In the SNMPv3 section of the page, click the circle next to Configure Target Address Table. Then click **Configure** at the bottom of the page.
The SNMPv3 Target Address Table Page is shown in Figure 258 on page 728.
4. Display the SNMPv3 Target Address Table entry that you want to delete.
Click **Next** or **Previous** to display an entry.
5. Click **Remove**.
A warning message is displayed. Click OK to remove the Target Address Table entry.
6. To save your changes, return to the General Tab and click **Save Changes**.

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 192 on page 584.

2. Select the SNMP Tab.

The SNMP Tab is shown in Figure 195 on page 596.

3. In the SNMPv3 section of the page, click the circle next to Configure Target Address Table. Then click **Configure** at the bottom of the page.

The SNMPv3 Target Address Table Page is shown in Figure 258 on page 728.

4. Display the Target Address Table entry that you want to change. Click **Next** or **Previous** to display an entry.

5. Click **Modify**.

The Modify SNMPv3 Target Address Table Page is shown Figure 260.

Modify SNMPv3 Target Address	
Target Address Name	: snmpv3host200
IP Address	: <input type="text" value="198.12.10.5"/>
UDP Port Number	: <input type="text" value="162"/>
Timeout	: <input type="text" value="1500"/>
Retries	: <input type="text" value="3"/>
Tag List	: <input type="text" value="hwengtag"/>
Target Parameters	: <input type="text" value="snmpv3manager200"/>
Storage Type	: <input type="text" value="NonVolatile"/>
Row Status	: Active
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Figure 260 Modify SNMPv3 Target Address Table 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 722. 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 to the configuration file. After making changes to a Target Address Table entry with a Volatile storage type, **Save Changes** does not appear on the General Tab.

NonVolatile

Select this storage type if you want the ability to save an entry in the Target Address Table to the configuration file. After making changes to an Target Address Table entry with a NonVolatile storage type, **Save Changes** appears on the General Tab.

13. Click **Apply** to update the SNMPv3 Target Address Table.
14. To save your changes, return to the General Tab and click **Save Changes**.

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 727
- Deleting a Target Address Table Entry on page 730
- Modifying Target Address Table Entry on page 730

For reference information about the SNMPv3 Target Parameters Table, see Configuring the SNMPv3 Target Parameters Table on page 733.

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 192 on page 584.

2. Select the SNMP Tab.

The SNMP Tab is shown in Figure 195 on page 596.

3. In the SNMPv3 section of the page, click the circle next to Configure Target Parameters Table. Then click **Configure** at the bottom of the page.

The SNMPv3 Target Parameters Table Page is shown in Figure 261.

AT-8400

Configuration

System Name:
MAC Addr: 00:30:84:FD:57:DA

Home
System
Layer 1
Layer 2
Help
Logout

General | **SNMP** | IGMP | System Maintenance | Server-based Authentication | System Time | Event Log

SNMPv3 Target Parameters Table Total Entries: 8. Page 2 of 2

	Params Name	Message Processing Model	Security Model	Security Name	Security Level	Storage Type	Row Status
<input checked="" type="radio"/>	snmpv3manager250	v3	v3	diane	AuthPriv	NonVolatile	Active
<input type="radio"/>	snmpv3manager300	v3	v3	yiyu	AuthPriv	NonVolatile	Active
<input type="radio"/>	snmpv3manager50	v3	v3	debashis	AuthPriv	NonVolatile	Active

Refresh Add Remove Modify Previous
Back

Figure 261 SNMPv3 Target Parameters Table Page

- To create an SNMPv3 Target Parameters Table entry, click **Add**.
The Add New SNMPv3 Target Parameter Table Page is shown in Figure 262.

Figure 262 Add New SNMPv3 Target Parameters Table 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 an SNMP Protocol 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.

7. 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 698.

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 698.

No Authentication/Privacy

This option represents neither an authentication nor privacy protocol. Select this security level if you do not want to authenticate users 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.

10. 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 to the configuration file. After making changes to a Target Parameters Table entry with a Volatile storage type, then **Save Changes** does not appear on the Configuration Tab.

NonVolatile

Select this storage type if you want the ability to save an entry in the Target Parameters Table to the configuration file. After making changes to a Target Parameters Table entry with a NonVolatile storage type, then **Save Changes** appears on the Configuration Tab.

Note

The Row Status parameter is a read-only field in the Web interface. The Active value indicates the SNMPv3 Target Parameters Table entry takes effect immediately.

11. Click **Apply** to update the SNMPv3 Target Parameters Table.
12. To save your changes, return to the General Tab and click **Save Changes**.

Deleting a Target Parameters Table Entry

To delete an SNMPv3 Target Parameters Table entry, 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 192 on page 584.
2. Select the SNMP Tab.
The SNMP Tab is shown in Figure 195 on page 596.
3. In the SNMPv3 section of the page, click the circle next to Configure Target Parameters Table. Then click **Configure** at the bottom of the page.
The SNMPv3 Target Parameters Table Page is shown in Figure 261 on page 733.
4. Click the circle next to the Target Parameters Table entry that you want to delete. Then click **Remove**.

A warning message is displayed. Click OK to remove the Target Parameters Table entry.

5. To save your changes, return to the General Tab and click **Save Changes**.

Modifying a Target Parameters Table Entry

To modify an SNMPv3 Target Parameters Table entry, 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 192 on page 584.

2. Select the SNMP Tab.

The SNMP Tab is shown in Figure 195 on page 596.

3. In the SNMPv3 section of the page, click the circle next to Configure Target Parameters Table. Then click **Configure** at the bottom of the page.

The SNMPv3 Target Parameters Table Page is shown in Figure 261 on page 733.

4. Click the circle next to the Target Parameters Table entry that you want to change. Then click **Modify**.

The Modify SNMPv3 Target Parameter Table Page is shown in Figure 263 on page 737.

The screenshot shows a web-based configuration interface for modifying an SNMPv3 target parameter. The title bar reads "Modify SNMPv3 Target Parameter". The main content area contains several labeled fields:

- Target Parameters Name**: snmpv3manager100
- Message Processing Model**: v3 (dropdown menu)
- Security Model**: v3 (dropdown menu)
- Security Name**: chitra (text input field)
- Security Level**: Privacy (dropdown menu)
- Storage Type**: NonVolatile (dropdown menu)
- Row Status**: Active

At the bottom of the form, there are two buttons: "Apply" and "Cancel".

Figure 263 Modify SNMPv3 Target Parameters Table 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 698.

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 698.

No Authentication/Privacy

This option represents neither an authentication nor privacy protocol. Select this security level if you do not want to authenticate users 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 to the configuration file. After making changes to an Target Parameters Table entry with a Volatile storage type, **Save Changes** does not appear on the General Tab.

NonVolatile

Select this storage type if you want the ability to save an entry in the Target Parameters Table to the configuration file. After making changes to an Target Parameters Table entry with a NonVolatile storage type, **Save Changes** appears on the General Tab.

Note

The Row Status parameter is a read-only field in the Web 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. To save your changes, return to the General Tab and click **Save Changes**.

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 740
- Deleting an SNMPv3 Community Table Entry on page 743
- Modifying an SNMPv3 Community Table Entry on page 743

For reference information about the SNMPv3 Community Table, see [Configuring the SNMPv3 Community Table on page 740](#).

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 SNMPv3 Community Table entry, 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 192 on page 584.
2. Select the SNMP Tab.
The SNMP Tab is shown in Figure 195 on page 596.
3. In the SNMPv3 section of the page, click the circle next to Configure Community Table. Then click **Configure** at the bottom of the page.
The SNMPv3 Community Table Page is shown in Figure 264 on page 741.

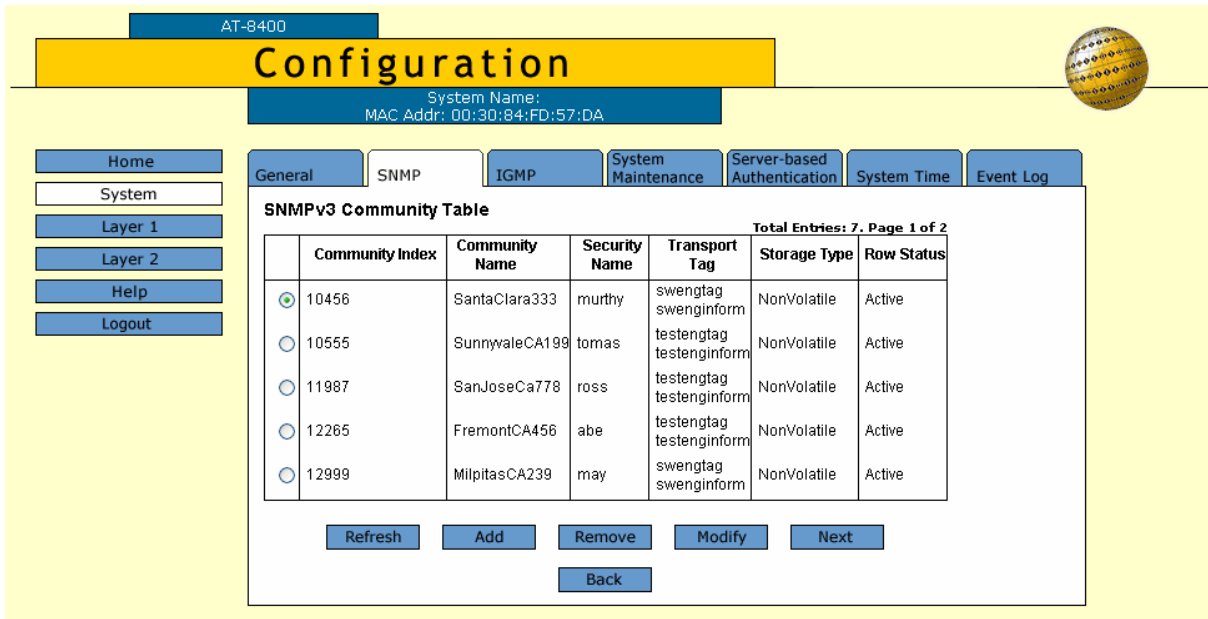


Figure 264 SNMPv3 Community Table Page

- To create an SNMPv3 Community Table entry, click **Add**.
The Add New SNMPv3 Community Table Page is shown in Figure 265.

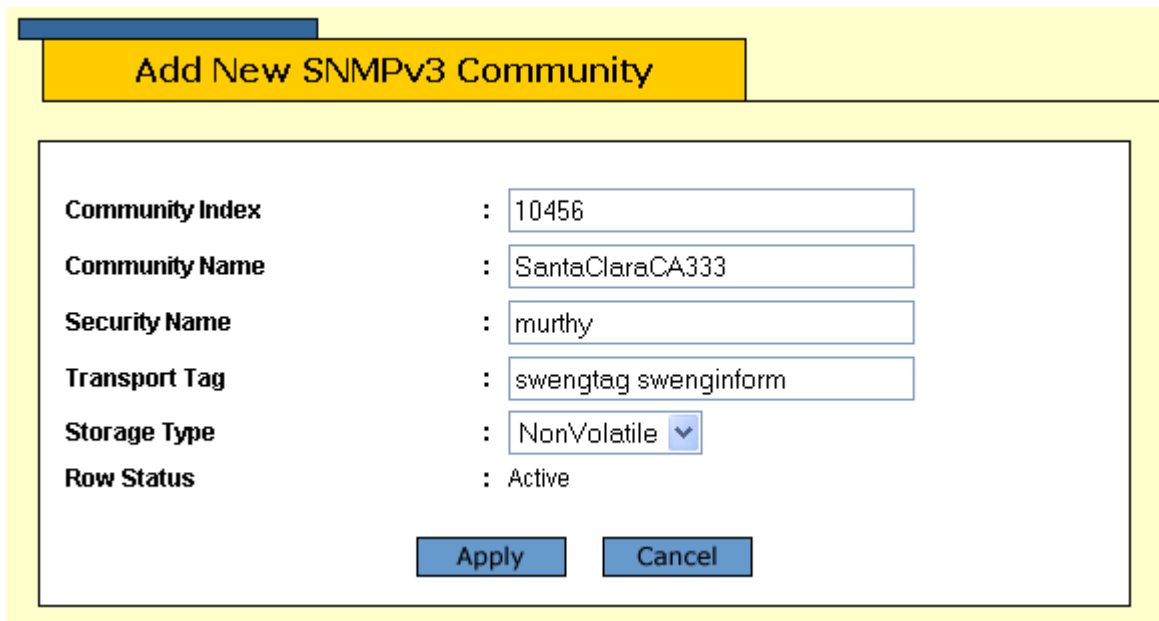


Figure 265 Add New SNMPv3 Community Table Page

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 727.

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 to the configuration file. After making changes to an SNMPv3 Community Table entry with a Volatile storage type, **Save Changes** does not appear on the General Tab.

NonVolatile

Select this storage type if you want the ability to save an entry in the SNMPv3 Community Table to the configuration file. After

making changes to an SNMPv3 Community Table entry with a NonVolatile storage type, **Save Changes** appears on the General Tab.

Note

The Row Status parameter is a read-only field in the Web interface. The Active value indicates the SNMPv3 Community Table entry takes effect immediately.

10. Click **Apply** to update the SNMPv3 Community Table.
11. To save your changes, return to the General Tab and click **Save Changes**.

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 192 on page 584.
2. Select the SNMP Tab.
The SNMP Tab is shown in Figure 195 on page 596.
3. In the SNMPv3 section of the page, click the circle next to Configure Community Table. Then click **Configure** at the bottom of the page.
The SNMPv3 Community Table Page is shown in Figure 264 on page 741.
4. Click the circle next to the SNMPv3 Community Table entry that you want to delete. Then click **Remove**.
A warning message is displayed. Click OK to remove the SNMPv3 Community Table entry.
5. To save your changes, return to the General Tab and click **Save Changes**.

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 192 on page 584.
2. Select the SNMP Tab.
The SNMP Tab is shown in Figure 195 on page 596.

3. In the SNMPv3 section of the page, click the circle next to Configure Community Table. Then click **Configure** at the bottom of the page.
The SNMPv3 Community Table Page is shown in Figure 264 on page 741.
4. Click the circle next to the SNMPv3 Community Table entry that you want to change. Then click **Modify**.
The Modify SNMPv3 Community Table Page is shown in Figure 266.

Modify SNMPv3 Community

Community Index	: 10456
Community Name	: <input type="text" value="SantaClaraCA333"/>
Security Name	: <input type="text" value="murthy"/>
Transport Tag	: <input type="text" value="swengtag swenginformat"/>
Storage Type	: <input type="text" value="NonVolatile"/>
Row Status	: Active

Figure 266 Modify SNMPv3 Community Table 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 727.

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 to the configuration file. After making changes to an SNMPv3 Community Table entry with a Volatile storage type, **Save Changes** does not appear on the General Tab.

NonVolatile

Select this storage type if you want the ability to save an entry in the SNMPv3 Community Table to the configuration file. After making changes to an SNMPv3 Community Table entry with a NonVolatile storage type, **Save Changes** appears on the General Tab, allowing you to save your changes.

Note

The Row Status parameter is a read-only field in the Web interface. The Active value indicates the SNMPv3 Community Table entry takes effect immediately.

9. Click **Apply** to update the SNMPv3 Community Table.
10. To save your changes, return to the General Tab and click **Save Changes**.

Displaying SNMPv3 Tables

This section contains procedures to display the SNMPv3 Tables. The following procedures are provided:

- [Displaying User Table Entries on page 747](#)
- [Displaying View Table Entries on page 748](#)
- [Displaying Access Table Entries on page 749](#)
- [Displaying SecurityToGroup Table Entries on page 750](#)
- [Displaying Notify Table Entries on page 751](#)
- [Displaying Target Address Table Entries on page 752](#)
- [Displaying Target Parameters Table Entries on page 753](#)
- [Displaying SNMPv3 Community Table Entries on page 754](#)

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 194 on page 592.
2. Select the SNMP Tab.
The SNMP Monitoring Tab is shown in Figure 199 on page 602.
3. From the SNMP Monitoring Tab, click the circle next to View User Table.
4. Click **View** at the bottom of the page.
The Monitoring, SNMPv3 User Table Page is shown in Figure 267.

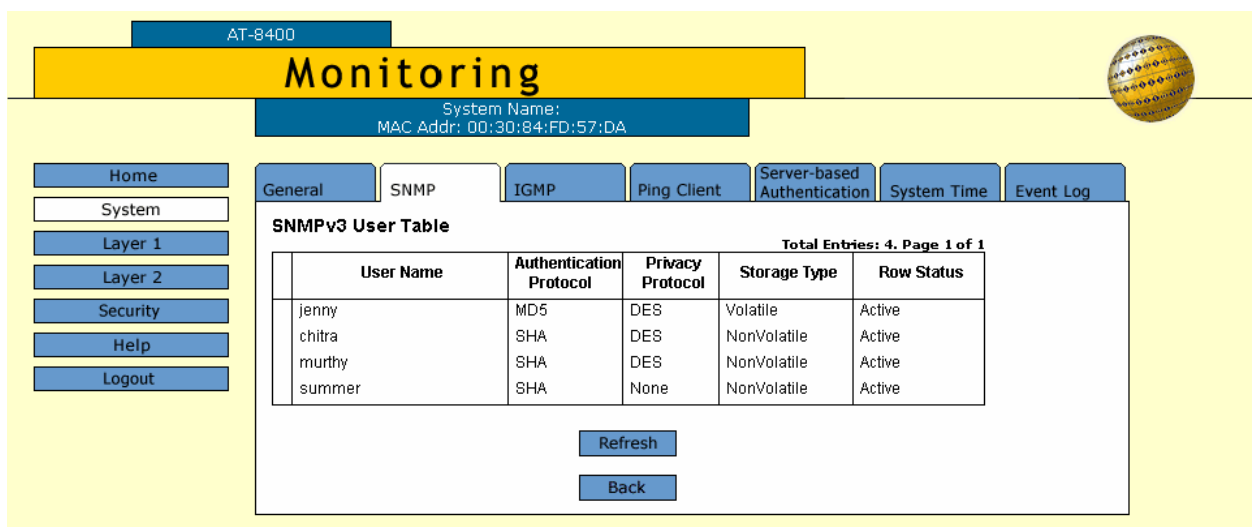


Figure 267 Monitoring, SNMPv3 User Table Page

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 194 on page 592.
2. Select the SNMP Tab.
The SNMP Monitoring Tab is shown in Figure 195 on page 596.
3. From the SNMP Monitoring Tab, click the circle next to View View Table.
4. Click **View** at the bottom of the page.
The Monitoring, SNMPv3 View Table Page is shown in Figure 268.

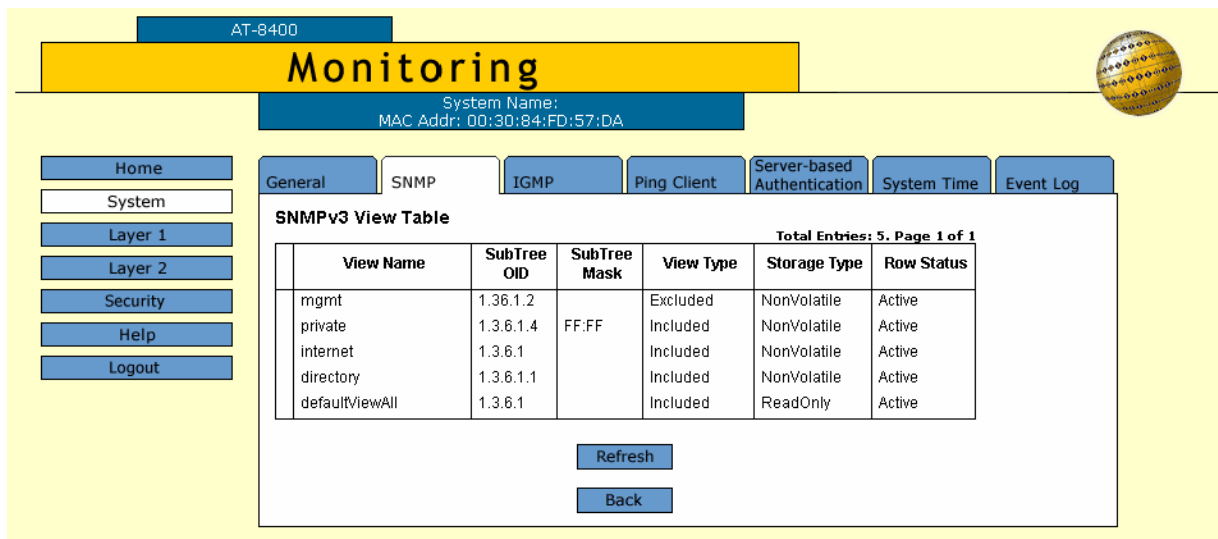


Figure 268 Monitoring, SNMPv3 View Table Page

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 194 on page 592.
2. Select the SNMP Tab.
The SNMP Monitoring Tab is shown in Figure 195 on page 596.
3. From the SNMP Monitoring Tab, click the circle next to View Access Table.
4. Click **View** at the bottom of the page.

The Monitoring, SNMPv3 Access Table Page is shown in Figure 269.

AT-8400

Monitoring

System Name:
MAC Addr: 00:30:84:FD:57:DA

Home System Layer 1 Layer 2 Security Help Logout

General **SNMP** IGMP Ping Client Server-based Authentication System Time Event Log

SNMPv3 Access Table

Total Entries: 5. Page 1 of 5

Group Name testengineering	Security Model v3
Context Prefix	Security Level AuthPriv
Read View internet	Context Match Exact
Write View private	Storage Type Volatile
Notify View internet	Row Status Active

Refresh Next Back

Figure 269 Monitoring, SNMPv3 Access Table Page

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 194 on page 592.

2. Select the SNMP Tab.

The SNMP Monitoring Tab is shown in Figure 195 on page 596.

3. From the SNMP Monitoring Tab, click the circle next to the View SecurityToGroup Table.

4. Click **View** at the bottom of the page.

The Monitoring, SNMPv3 SecurityToGroup Table Page is shown in Figure 270.

AT-8400

Monitoring

System Name:
MAC Addr: 00:30:84:FD:57:DA

Home System Layer 1 Layer 2 **Security** Help Logout

General **SNMP** IGMP Ping Client Server-based Authentication System Time Event Log

SNMPv3 SecurityToGroup Table Total Entries: 8. Page 2 of 2

	Security Model	Security Name	Group Name	Storage Type	Row Status
	v3	diane	testengineering	NonVolatile	Active
	v3	jenny	swengineering	NonVolatile	Active
	v3	debashis	swengineering	NonVolatile	Active

Refresh Previous Back

Figure 270 Monitoring, SNMPv3 SecurityToGroup Table Page

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 194 on page 592.

2. Select the SNMP Tab.

The SNMP Monitoring Tab is shown in Figure 195 on page 596.

3. From the SNMP Monitoring Tab, click the circle next to View Notify Table.

4. Click **View** at the bottom of the page.

The Monitoring, SNMPv3 Notify Table Page is shown in Figure 271.

The screenshot shows the AT-S60 Management Software interface. At the top, there is a blue header with 'AT-8400' and a yellow 'Monitoring' banner. Below the banner, the system name and MAC address are displayed. A navigation menu on the left includes Home, System, Layer 1, Layer 2, Security, Help, and Logout. The main content area has tabs for General, SNMP, IGMP, Ping Client, Server-based Authentication, System Time, and Event Log. The SNMP tab is active, showing the 'SNMPv3 Notify Table' with a table of entries. The table has columns for Notify Name, Notify Tag, Notify Type, Storage Type, and Row Status. Below the table are 'Refresh' and 'Back' buttons.

SNMPv3 Notify Table				
Total Entries: 4. Page 1 of 1				
Notify Name	Notify Tag	Notify Type	Storage Type	Row Status
swenginform	swenginformtag	Inform	NonVolatile	Active
swengtrap	swengtraptag	Trap	NonVolatile	Active
testenginform	testenginformtag	Inform	NonVolatile	Active
testengtrap	testengtraptag	Trap	NonVolatile	Active

Figure 271 Monitoring, SNMPv3 Notify Table Page

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 194 on page 592.
2. Select the SNMP Tab.
The SNMP Monitoring Tab is shown in Figure 195 on page 596.
3. From the SNMP Monitoring Tab, click the circle next to View Target Address Table.
4. Click **View** at the bottom of the page.

The Monitoring, SNMPv3 Target Address Table Page is shown in Figure 272.

AT-8400

Monitoring

System Name:
MAC Addr: 00:30:84:FD:57:DA

Home System Layer 1 Layer 2 Security Help Logout

General **SNMP** IGMP Ping Client Server-based Authentication System Time Event Log

SNMPv3 Target Address Table

Total Entries: 1. Page 1 of 1

Target Address snmpv3host200	Timeout 1500
Parameters snmpv3manager200	Retries 3
IP Address 198.12.10.5	UDP Port Number 162
Storage Type NonVolatile	Row Status Active
Tag List hwengtag swengtag testengtag	

Refresh Back

Figure 272 Monitoring, SNMPv3 Target Address Table Page

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 194 on page 592.

2. Select the SNMP Tab.

The SNMP Monitoring Tab is shown in Figure 195 on page 596.

3. From the SNMP Monitoring Tab, click the circle next to the View Target Parameters Table.

4. Click **View** at the bottom of the page.

The Monitoring, SNMPv3 Target Parameters Table Page is shown in Figure 272.

AT-8400

Monitoring

System Name:
MAC Addr: 00:30:84:FD:57:DA

Home System Layer 1 Layer 2 Security Help Logout

General **SNMP** IGMP Ping Client Server-based Authentication System Time Event Log

SNMPv3 Target Parameters Table Total Entries: 9. Page 2 of 2

Params Name	Message Processing Model	Security Model	Security Name	Security Level	Storage Type	Row Status
snmpv3manager220	v3	v3	luke	AuthNoPriv	NonVolatile	Active
snmpv3manager250	v3	v3	diane	AuthPriv	NonVolatile	Active
snmpv3manager300	v3	v3	yiYu	AuthPriv	NonVolatile	Active
snmpv3manager50	v3	v3	debashsis	AuthPriv	NonVolatile	Active

Refresh Previous Back

Figure 273 Monitoring, SNMPv3 Target Parameters Table Page

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 194 on page 592.

2. Select the SNMP Tab.

The SNMP Monitoring Tab is shown in Figure 195 on page 596.

3. From the SNMP Monitoring Tab, click the circle next to the View Community Table.

4. Click **View** at the bottom of the page.

The Monitoring, SNMPv3 Community Table Page is shown in Figure 274.

AT-8400

Monitoring

System Name:
MAC Addr: 00:30:84:FD:57:DA

Home System Layer 1 Layer 2 Security Help Logout

General **SNMP** IGMP Ping Client Server-based Authentication System Time Event Log

SNMPv3 Community Table Total Entries: 7, Page 1 of 2

Community Index	Community Name	Security Name	Transport Tag	Storage Type	Row Status
10456	SantaClara333	murthy	swengtag swenginform	NonVolatile	Active
10555	SunnyvaleCA199	tomas	testengtag testenginform	NonVolatile	Active
11987	SanJoseCa778	ross	testengtag testenginform	NonVolatile	Active
12265	FremontCA456	abe	testengtag testenginform	NonVolatile	Active
12999	MilpitasCA239	may	swengtag swenginform	NonVolatile	Active

Refresh Next Back

Figure 274 Monitoring, SNMPv3 Community Table Page

Chapter 41

Port-based VLANs

This chapter explains how to create, modify, and delete VLANs using a web browser management session. In addition, this chapter explains how to change a switch's VLAN operating mode.

This chapter contains the following procedures:

- Creating a Port Based VLAN on page 756
- Modifying a Port-Based VLAN on page 760
- Deleting a VLAN on page 762
- Displaying VLANs on page 763
- Setting the Switch's VLAN Mode on page 765

Note

For background information on VLANs and on the Basic VLAN mode, refer to Chapter 18, Tagged and Port-based Virtual LANs on page 401.

Creating a Port Based VLAN

To create a new port-based or tagged VLAN, perform the following procedure. Before you create a VLAN, you may want to set the VLAN mode for a switch. See Setting the Switch's VLAN Mode on page 765.

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

The Configuration System Page is displayed with the General Tab selected by default, as shown in Figure 192 on page 584.

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 212 on page 634.

3. Select the **VLAN** Tab.

The VLAN Tab is shown in Figure 275.

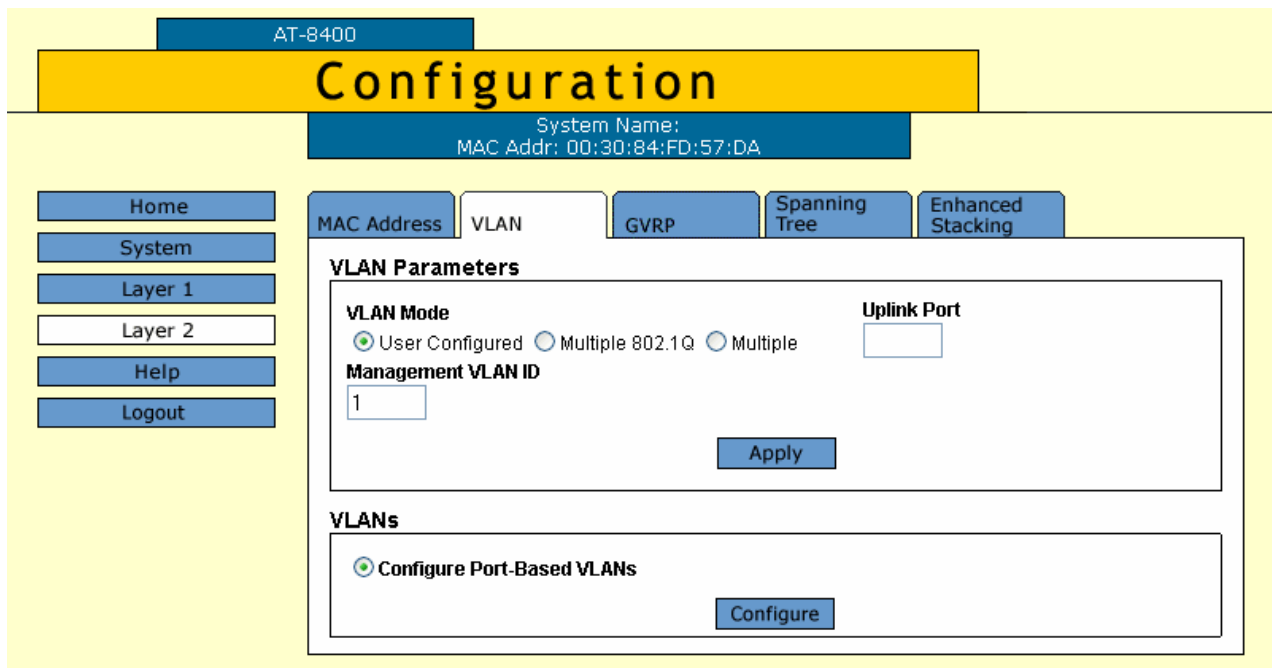


Figure 275 Configuration Layer 2 Page, VLAN Tab

4. In the VLANs section, click **Configure**.

The Port-Based VLANs Page is displayed in Figure 276 on page 757.

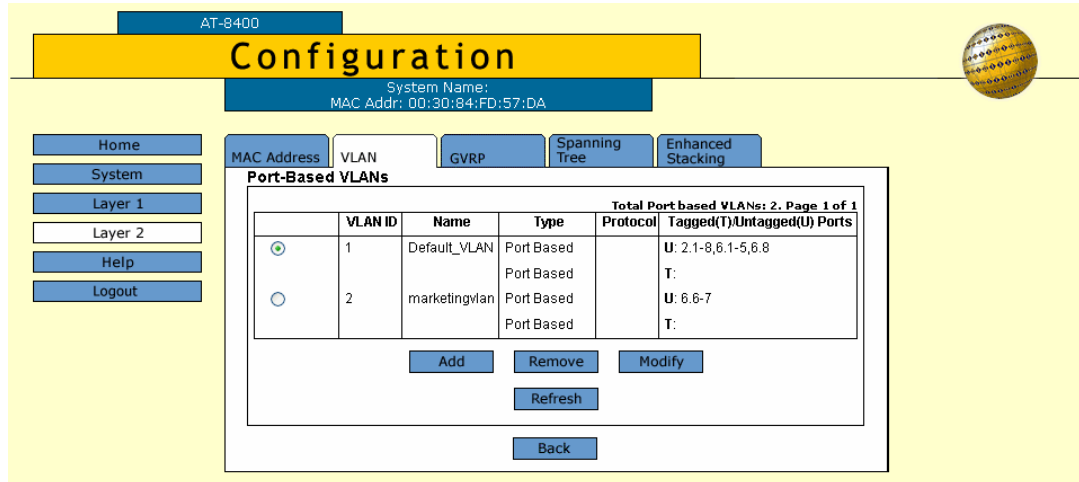


Figure 276 Port-Based VLANs Page

5. Click **Add**.

The Add New VLAN Page is shown in Figure 277.

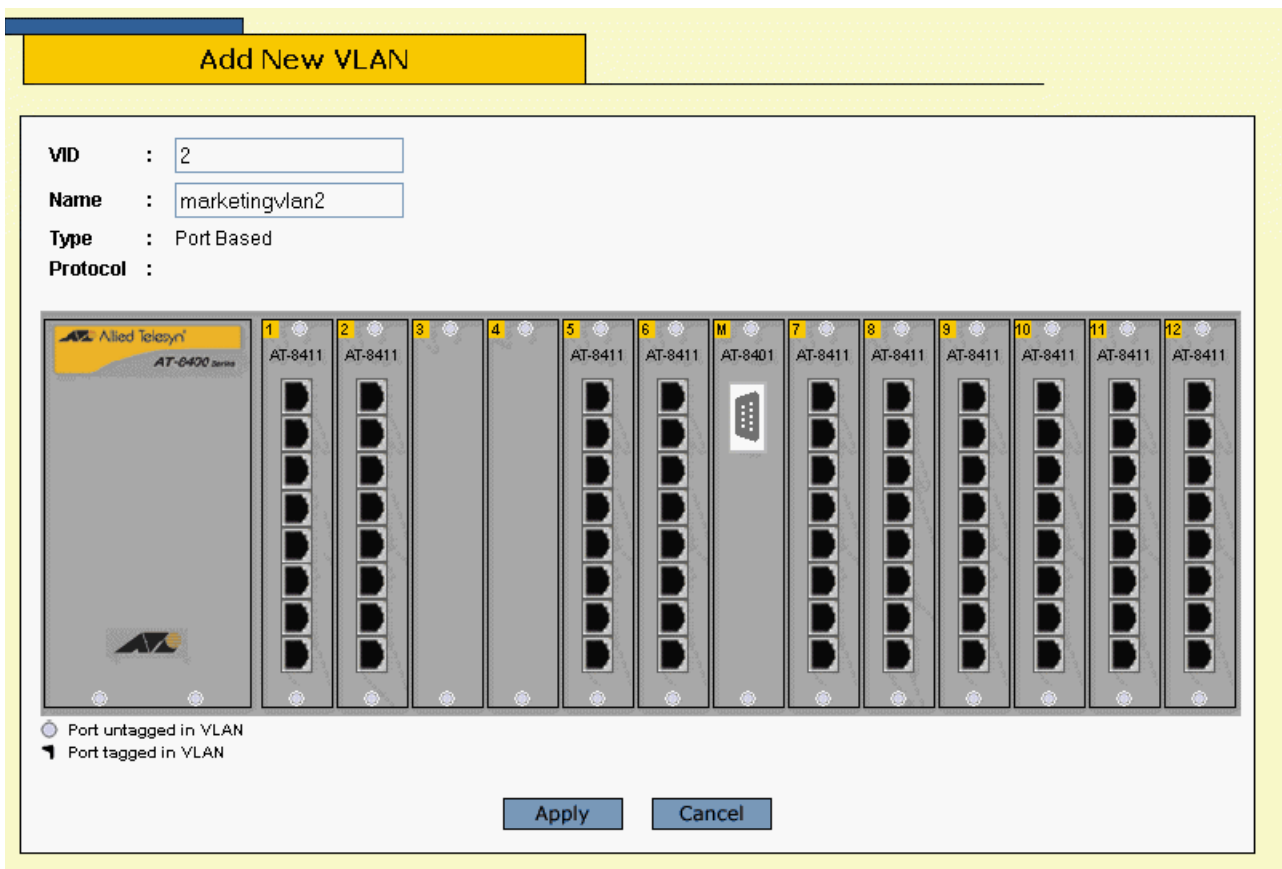


Figure 277 Add New VLAN Page

- In the **VID** field, enter a VID value for the new VLAN. The range of the VID value is 2 to 4094. The default is the next available VID number on the switch.

If this is a unique VLAN in your network, its VID must be unique as well. However, if the VLAN is to be part of a larger VLAN that spans multiple switches, assign the same VID value on each switch. For example, if you are creating a VLAN called Sales that spans three switches, you must assign the same VID value to each Sales VLAN on all three switches.

Note

You must assign a VID to a VLAN.

- In the **Name** field, enter a name for the new VLAN.

The name can be from one to 18 characters in length. The name should reflect the function of the nodes of the VLAN (for example, Sales or Accounting). The name can contain spaces but not special characters, such as asterisks (*) or exclamation points (!).

If the VLAN is to be unique in your network, the name should be unique as well. However, if the VLAN is to be part of a larger VLAN that spans multiple switches, the name for the VLAN needs to be the same on each switch. For example, if VLAN that is called Administration spans three switches, then the VLAN needs to have the same name on all three switches.

Note

You must assign a name to a VLAN.

- To select ports for the VLAN, click on the ports in the switch image. Clicking repeatedly on a port toggles the port through the following possible settings:

 Untagged port

 Tagged port

 Port not a member of the VLAN

- Click **Apply**.

The VLAN is created on the switch. The VLAN is now ready for network operations.

Note

The untagged ports that you assign to the new VLAN are automatically removed from their current VLAN assignment.

To save your changes, return to the General Tab and click **Save Changes**. The changes you made are saved on the switch.

Modifying a Port-Based VLAN

To modify a port-based or tagged VLAN, 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 194 on page 592.
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 212 on page 634.
3. Select the **VLAN** Tab.
The VLAN Tab is shown in Figure 275 on page 756.
4. In the VLANs section, click **Configure**.
The Port-Based VLANs Page is displayed in Figure 276 on page 757.
5. Click the circle next to the name of the VLAN you want to modify.
6. Click **Modify**.

The Modify VLAN Page is displayed as shown in Figure 278.

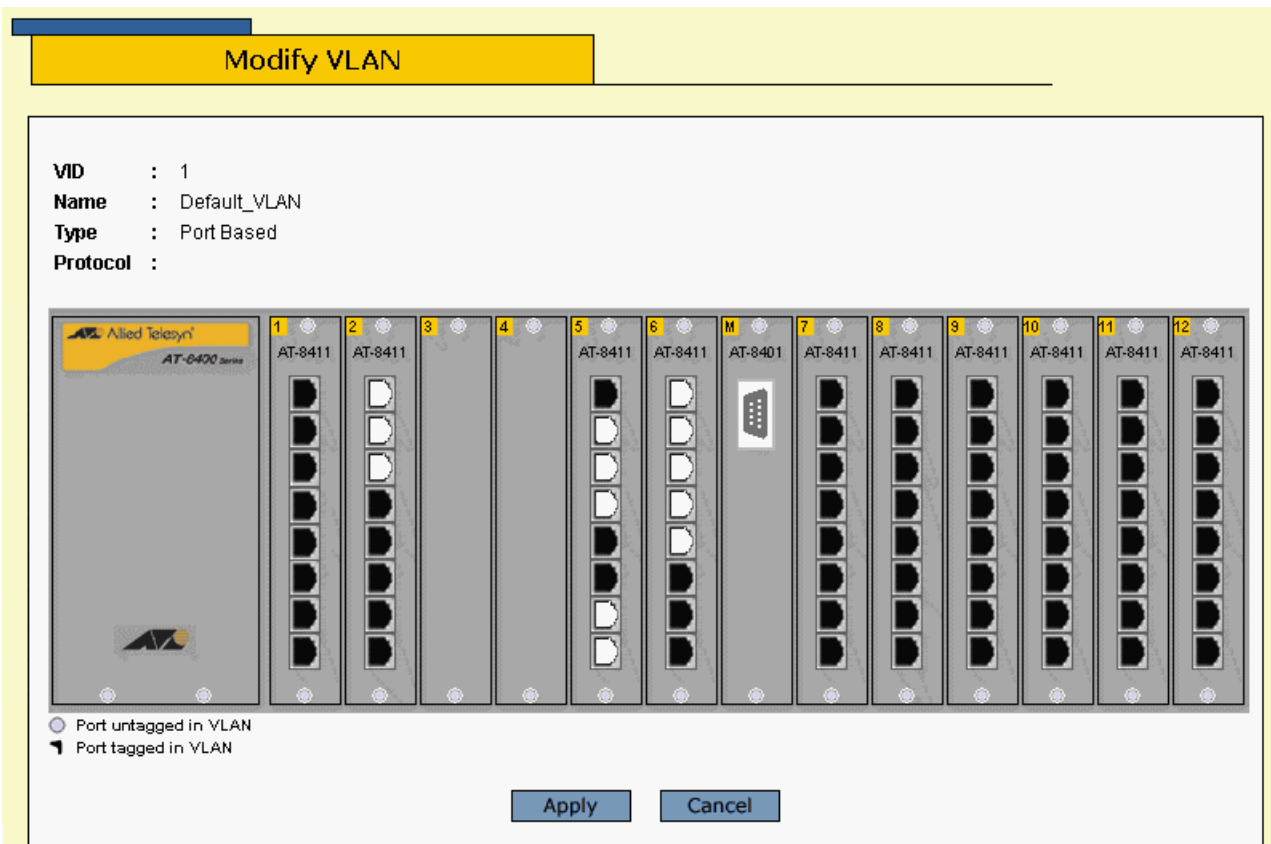


Figure 278 Modify VLAN Page

- Modify the VLAN parameters by referring to Step 7 through Step 8 in the previous procedure, Creating a Port Based VLAN on page 756.

When you modify a VLAN, observe the following guidelines:

- You cannot change the VID of a VLAN.
- You cannot change the name of any VLAN.

- After making the desired changes, click **Apply**.

The modified VLAN is now ready for network operations.

Note

Untagged ports that are added to a VLAN are automatically removed from their current VLAN assignment. Untagged ports that are removed from a VLAN are returned to the Default_VLAN.

- To save your changes, return to the General Tab and click **Save Changes**. The changes you made are saved on the switch.

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 Configuration System Page is displayed with the General Tab selected by default, as shown in Figure 192 on page 584.
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 212 on page 634.
3. Select the **VLAN** Tab.
The VLAN Tab is shown in Figure 275 on page 756.
4. In the VLANs section, click **Configure**.
The Port-Based VLANs Page is displayed in Figure 276 on page 757.
5. Click the circle next to the name of the VLAN you want to delete.
6. Click **Remove**.
A confirmation prompt is displayed.
7. 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.

Note

You cannot delete the Default_VLAN.

8. To save your changes, return to the General Tab and click **Save Changes**. The changes you made are saved on the switch.

Displaying VLANs

To display all the existing 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 194 on page 592.

2. Select the **Layer 2** option.

The Monitoring Layer 2 Page is displayed with the MAC Address Tab selected by default, as shown Figure 212 on page 634.

3. Select the **VLAN** Tab.

The Monitoring VLAN Tab is shown in Figure 279.

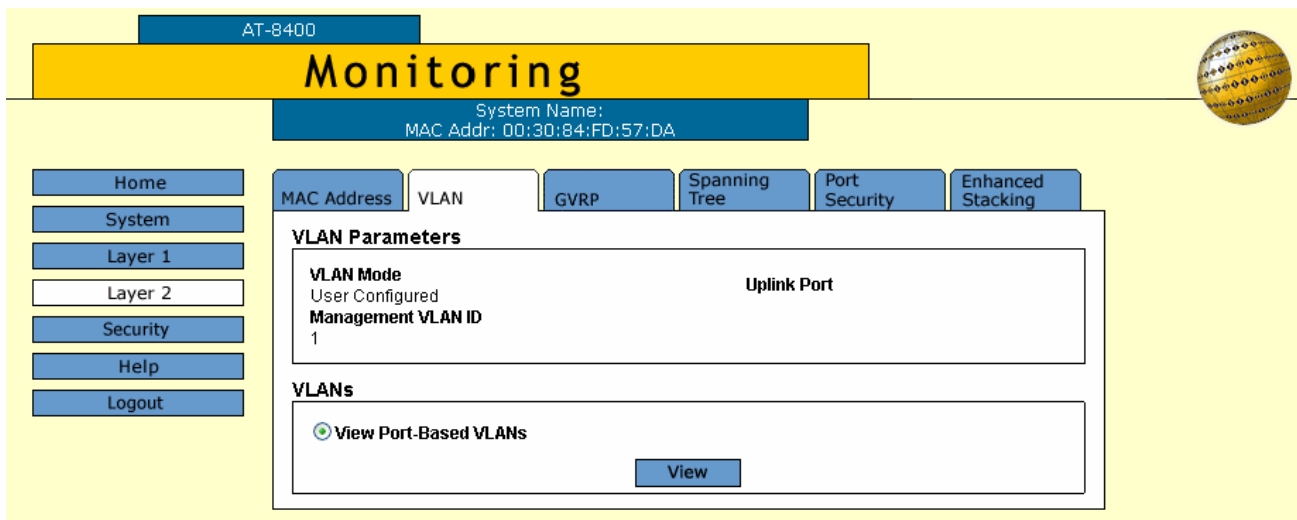


Figure 279 Monitoring Layer 2 Page, VLAN Tab

4. Click on View Port Based VLANs.

The Port-Based VLANs Page is shown in Figure 280.

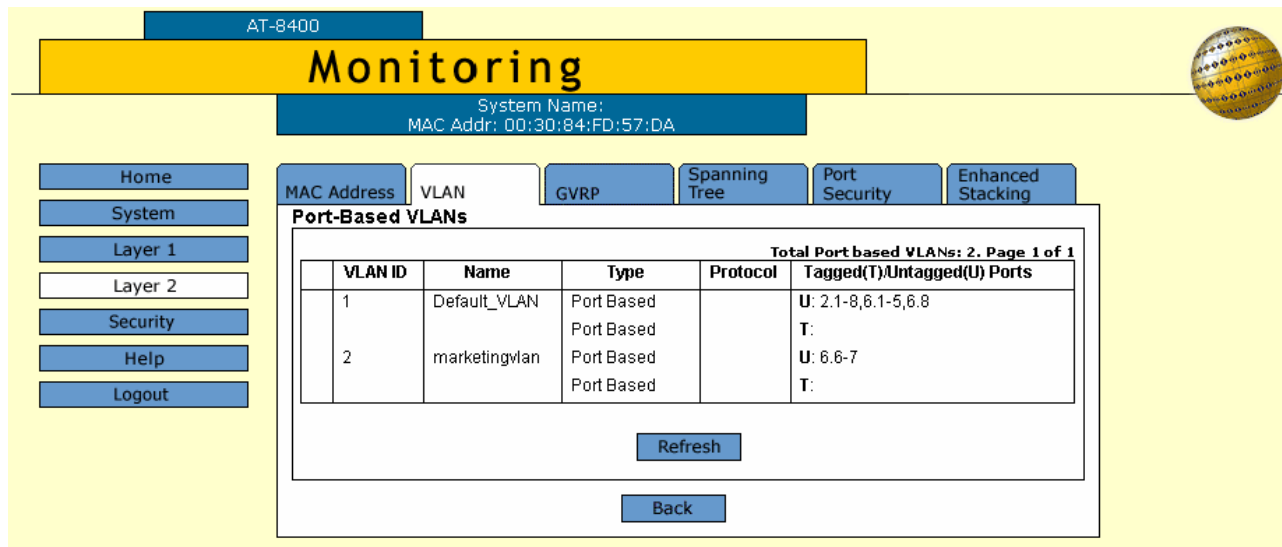


Figure 280 Monitoring, Port-Based VLANs Page

The VLANs are displayed in a table. The columns in the table are:

VLAN ID

VID value for the VLAN.

Name

Name of the VLAN.

Type

The VLAN type: port-based or tagged.

Protocol

The only option is GVRP.

Tagged(T)/Untagged(U) Ports

Which ports are tagged (T) and which are untagged (U).

Setting the Switch's VLAN Mode

This section contains the procedure for setting a switch's VLAN mode. You can configure a switch to support port-based and tagged VLANs or to operate in the Basic VLAN mode. A change to VLAN status is not activated until you reset the switch.

Note

Refer to Chapter 18, Tagged and Port-based Virtual LANs on page 401, for descriptions of port-based and tagged VLANs and the Basic VLAN mode.

To set the switch's VLAN mode, 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 192 on page 584.

2. Scroll down to the Configuration section of the Page.
3. In the circle next to the Switch Mode field, choose one of the following:
 - Click **Tagged** to permit the switch to support both port-based VLANs and tagged VLANs. This is the default.
 - Click **Basic** to permit the switch to operate in the Basic VLAN mode.
4. Click **Apply**.

The following confirmation message is displayed:

```
The switch will be rebooted for the change to take effect. This page will not be available while the switch reboots. Continue anyway?
```

5. Select **OK** to continue with the reboot. Select **Cancel** to cancel the reboot.

A change to VLAN status is not activated until you reset the switch. To reset the switch, refer to Resetting a Switch on page 604.

Chapter 42

GARP VLAN Registration Protocol

This chapter about web server security contains the following procedures:

- Configuring GVRP on page 767
- Resetting GVRP to the Defaults on page 769
- Modifying the GVRP Port Configuration on page 770
- Displaying the GVRP Settings on page 771

Note

For background information on GVRP, refer to Chapter 20: GARP VLAN Registration Protocol on page 766.

Configuring GVRP

To configure GVRP, 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 192 on page 584.

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 212 on page 634.

3. Select the **GVRP** Tab.

The GVRP Tab is shown in Figure 281.

The screenshot displays the configuration interface for GVRP on an AT-8400 device. The top navigation bar includes 'Home', 'System', 'Layer 1', 'Layer 2', 'Help', and 'Logout'. The 'Configuration' menu is open, showing tabs for 'MAC Address', 'VLAN', 'GVRP', 'Spanning Tree', and 'Enhanced Stacking'. The 'GVRP Parameters' section includes checkboxes for 'Enable GVRP' and 'Enable GIP', along with input fields for 'Leave Time' (60 CentiSeconds) and 'Join Time' (20 CentiSeconds). The 'GVRP Port Configuration' section shows a row of 12 ports, with port 2 labeled 'AT-8411' and port 7 labeled 'AT-8401'. A 'Modify' button is located at the bottom of the port configuration area.

Figure 281 Configuration Layer 2 Page, GVRP Tab

Note

When MSTP is enabled, the GVRP Tab is not shown.

4. Configure the following parameters:

Enable GVRP

Click in this box to enable GVRP.

Leave Time

Sets the duration of the Leave Period timer. The range is from 30 to 180 centiseconds and the default is 60.

Join Time

Sets the duration of the Join Period timer. The range is from 10 to 60 centiseconds and the default is 20.

Enable GIP

Enables the operation of GIP. If enabled, attribute registrations and de-registrations processed on a port are propagated to other ports in the GIP-connected ring.

Leave All Time

Sets the duration of the LeaveAll Period timer. The range is from 500 to 3000 centiseconds and the default is 1000.

5. Click **Apply**.

Resetting GVRP to the Defaults

To reset GVRP to the defaults:

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

The Configuration System Page is displayed with the General Tab selected by default, as shown in Figure 192 on page 584.

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 212 on page 634.

3. Select the **GVRP** Tab.

The GVRP Tab is shown in Figure 281 on page 767.

4. Click **Defaults**.

Modifying the GVRP Port Configuration

To modify the GVRP port configuration:

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

The Configuration System Page is displayed with the General Tab selected by default, as shown in Figure 192 on page 584.

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 212 on page 634.

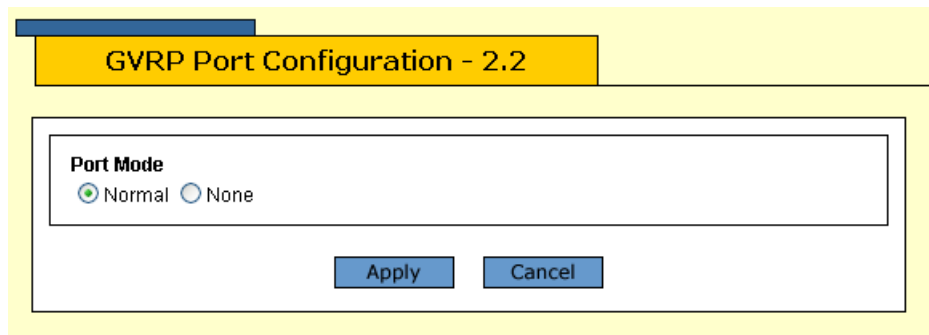
3. Select the **GVRP** Tab.

The GVRP Tab is shown in Figure 281 on page 767.

4. Select a port.

5. Click **Modify**.

The GVRP Port Configuration Page is shown in Figure 282.



The screenshot shows a web interface for GVRP Port Configuration. At the top, there is a yellow header bar with the text "GVRP Port Configuration - 2.2". Below this, there is a white box containing the "Port Mode" section. This section has two radio buttons: "Normal" (which is selected) and "None". At the bottom of the white box, there are two blue buttons: "Apply" and "Cancel".

Figure 282 GVRP Port Configuration Page

6. Change the port mode if desired.
7. Click **Apply**.

Displaying the GVRP Settings

The procedures in this section allow you to display the various GVRP settings. See the following procedures:

- Displaying GVRP Port Configuration on page 771
- Displaying the GVRP Counters on page 773
- Displaying GVRP Database on page 776
- Displaying GIP Connected Ports Ring on page 778
- Displaying GVRP State Machine on page 779

Displaying 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 194 on page 592.
2. Select the **Layer 2** option.
The Monitoring Layer 2 Page is displayed with the MAC Address Tab selected by default, as shown Figure 212 on page 634.
3. Select the **GVRP** Tab.

The GVRP Tab is shown in Figure 283.

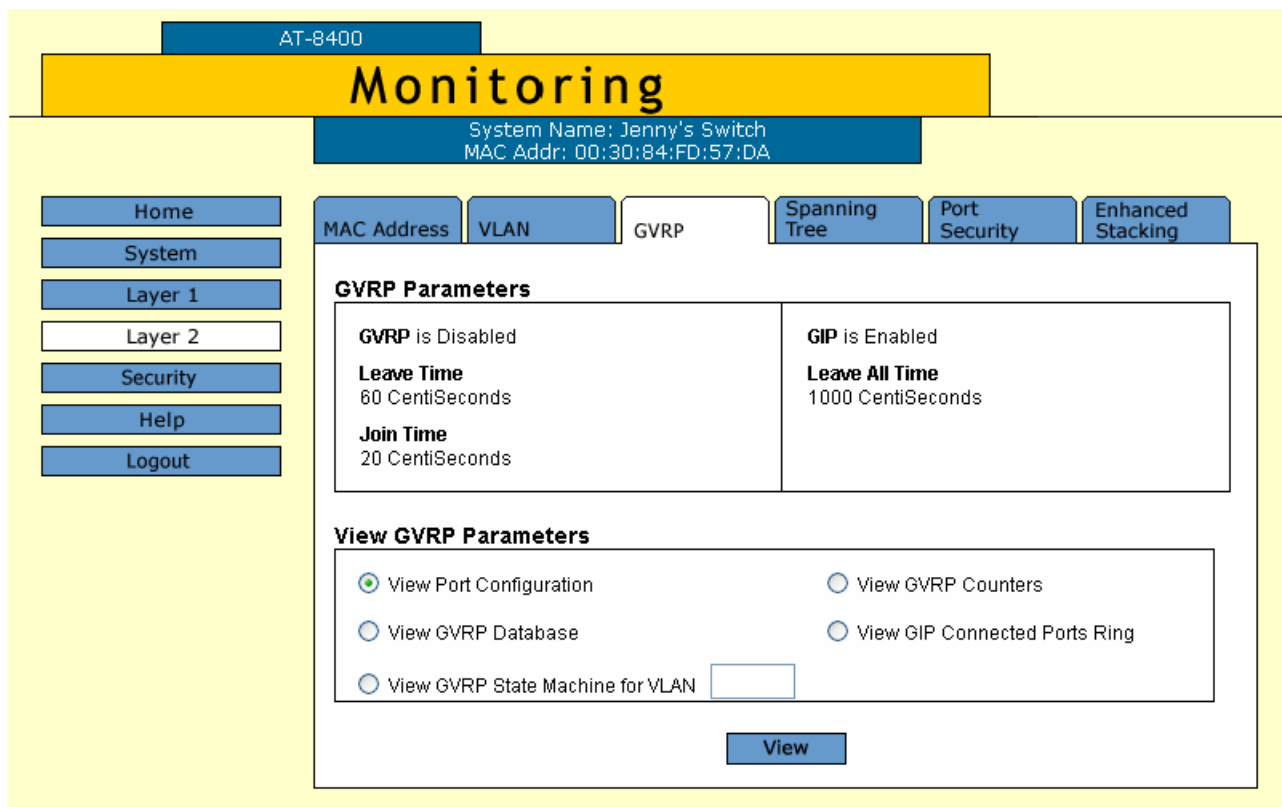


Figure 283 Monitoring Layer 2 Page, GVRP Tab

4. To view the port configuration, click the circle next to **View Port Configuration** in the View GVRP Parameters section of the page. Then click **View**.

The GVRP Port Configuration Page is shown in Figure 284.

The screenshot shows a web interface titled "GVRP Port Configuration". It contains a table with two columns: "Port Number" and "Mode". The table lists seven ports (3.1 to 3.7), all with a "Normal" mode. Below the table are two buttons: "Refresh" and "Close". The page is labeled "Page 1 of 1" in the top right corner.

Port Number	Mode
3.1	Normal
3.2	Normal
3.3	Normal
3.4	Normal
3.5	Normal
3.6	Normal
3.7	Normal

Figure 284 GVRP Port Configuration Page

Displaying the GVRP Counters

To display the GVRP Port 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 194 on page 592.

2. Select the **Layer 2** option.

The Monitoring Layer 2 Page is displayed with the MAC Address Tab selected by default, as shown Figure 212 on page 634.

3. Select the **GVRP** Tab.

The GVRP Tab is shown in Figure 283 on page 772.

4. To display the GVRP counters, click the circle next to **View GVRP Counters** in the View GVRP Parameters section of the page. Then click **View**.

The GVRP Counters Page is shown in Figure 285.

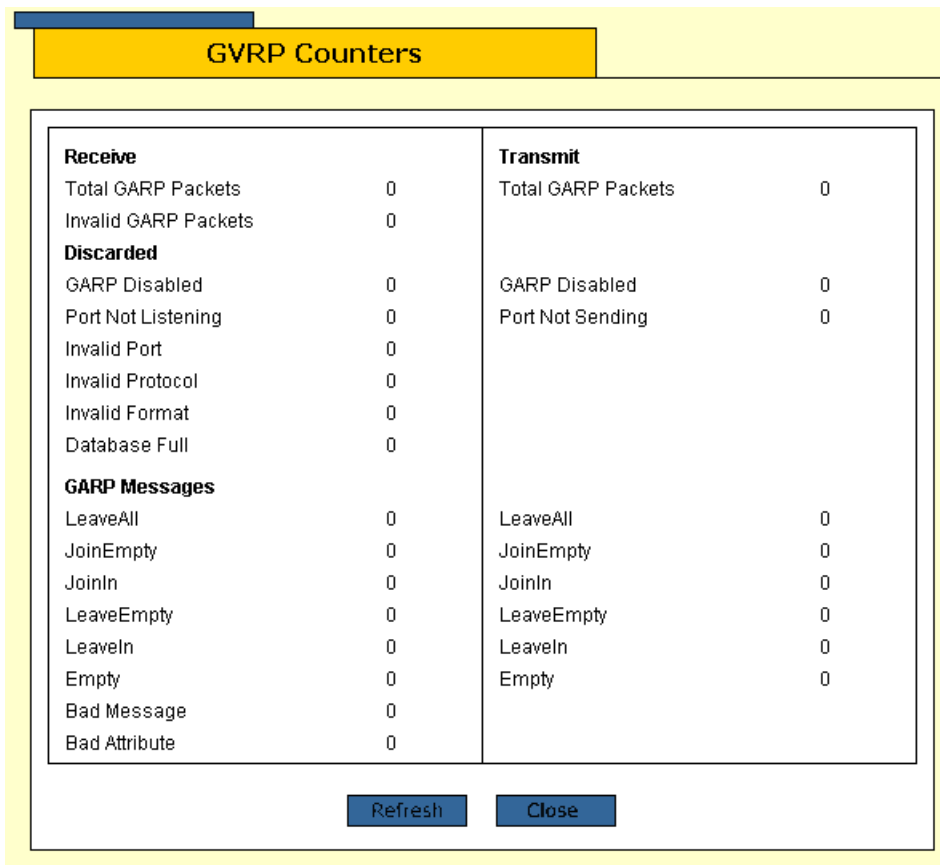


Figure 285 GVRP Counters Page

The information on this page is described below:

Receive: Total GARP Packets

Total number of GARP packets (PDUs) received by this GARP application.

Transmit: Total GARP Packets

Total number of GARP packets (PDUs) transmitted by this GARP application.

Receive: Invalid GARP Packets

Number of invalid GARP packets (PDUs) received by this GARP application.

Receive Discarded: GARP Disabled

Number of received GARP packets (PDUs) discarded because the GARP application was disabled.

Transmit Discarded: GARPDisabled

Number of GARP packets (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 packets (PDUs) discarded because the port that the packets were received on was not listening, that is, MODE=NONE has been set on the port.

Transmit Discarded: Port Not Sending

Number of GARP packets (PDUs) discarded because the port that the packets were to be transmitted on was not sending, that is, MODE=NONE has been set on the port.

Receive Discarded: Invalid Port

Number of GARP packets (PDUs) discarded because the port that the packet was received on does not belong to the GARP application.

Receive Discarded: Invalid Protocol

Number of GARP packets (PDUs) discarded because the GARP PDU contained an invalid protocol.

Receive Discarded: Invalid Format

Number of GARP packets (PDUs) discarded because the format of the GARP PDU was not recognized.

Receive Discarded: Database Full

Number of GARP packets (PDUs) discarded because the database for the GARP application was full, i.e. maximum number of attributes for the GARP application 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.

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: Leaveln

Total number of GARP Leaveln messages received for all attributes in the GARP application.

Transmit GARP Messages: Leaveln

Total number of GARP Leaveln 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 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 194 on page 592.
2. Select the **Layer 2** option.
The Monitoring Layer 2 Page is displayed with the MAC Address Tab selected by default, as shown Figure 212 on page 634.
3. Select the **GVRP** Tab.
The GVRP Tab is shown in Figure 283 on page 772.
4. To display the GVRP Database, click the circle next to **View GVRP Database** in the View GVRP Parameters section of the page. Then click **View**.

The GVRP Database Page is shown in Figure 286.

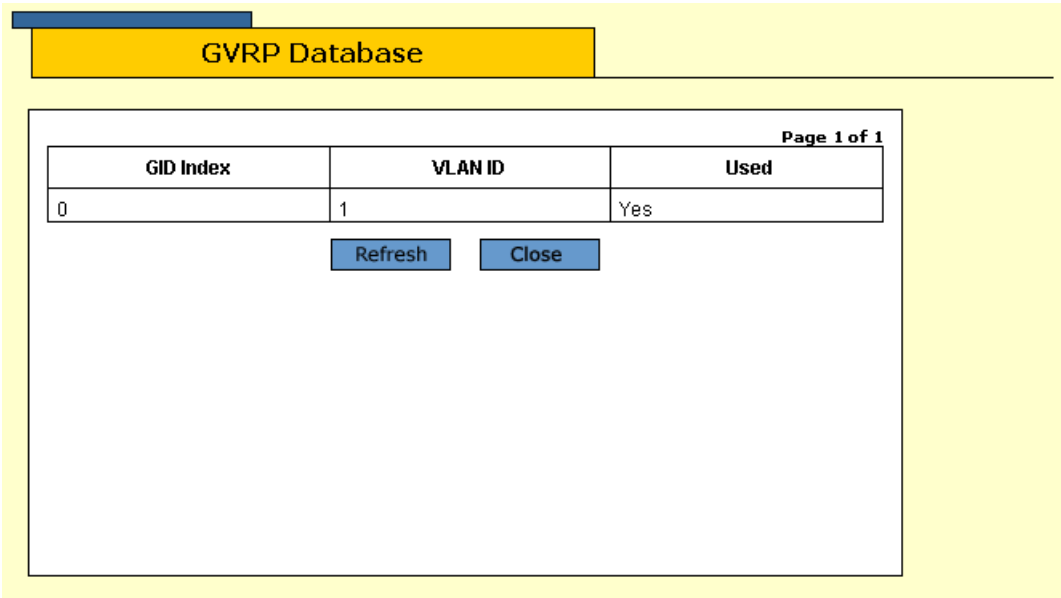


Figure 286 GVRP Database Page

The information on this page is described in Table 18.

Table 18 GARP Database Parameters

Parameter	Meaning
GID index	Value of the GID index corresponding to the attribute. GID indexes begin at 0. If the GARP application has no attributes presently registered, "No attributes have been registered" is displayed.
VLAN ID	Value of the attribute.
Used	Indicates whether the GID index is currently being used by any port in the GARP application. The definition of "used" is whether the Applicant and Registrar state machine for the GID index are in a non-initialized state, that is, not in {Vo, Mt} state. The value of this parameter is either "Yes" or "No".

Displaying GIP Connected Ports Ring

To display the GIP Connected Ports Ring information, 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 194 on page 592.
2. Select the **Layer 2** option.
The Monitoring Layer 2 Page is displayed with the MAC Address Tab selected by default, as shown Figure 212 on page 634.
3. Select the **GVRP** Tab.
The GVRP Tab is shown in Figure 283 on page 772.
4. To display the GIP Connected Ports Ring, click the circle next to **View GIP Connected Ports Ring** in the View GVRP Parameters section of the page. Then click **View**.

The GIP Connected Ports Ring Page is shown in Figure 287 on page 778.

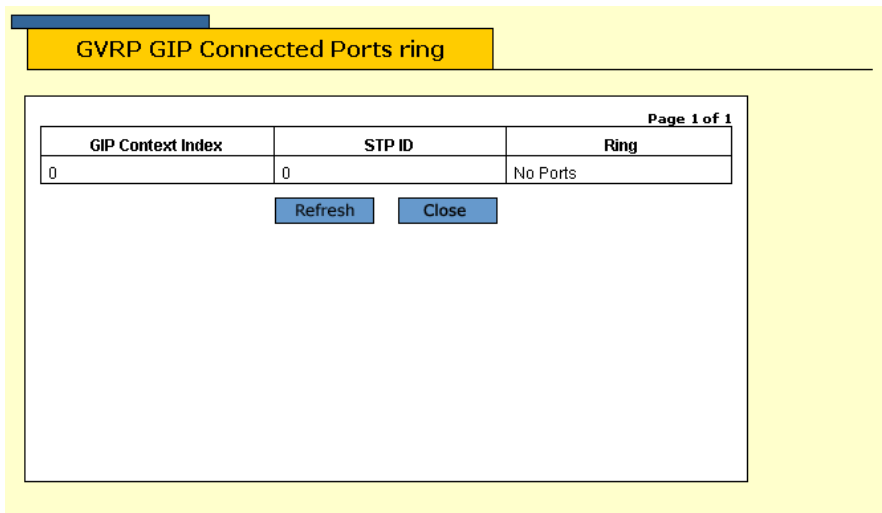


Figure 287 GVRP GIP Connected Ports Ring Page

The information on this page is described in Table 19.

Table 19 GIP Connected Ports Ring Parameters

Parameter	Meaning
GARP Application	Identifies the GARP application, that is, "GVRP."
GIP Context ID	A number assigned to the instance for the GIP context.
STP ID	Present if the GARP application is GVRP; identifies the STP that has these ports connected in the GIP connected ring.
Ring	Ring of connected ports. Only ports presently in the STP Forwarding state are eligible for membership to 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.

Displaying GVRP State Machine

To display the GVRP State Machine for each VLAN ID, perform the following procedures.

1. From the Home Page, select **Monitoring**.
The Monitoring System Page is displayed with the General Tab selected by default, as shown in Figure 194 on page 592.
2. Select the **Layer 2** option.
The Monitoring Layer 2 Page is displayed with the MAC Address Tab selected by default, as shown Figure 212 on page 634.
3. Select the **GVRP** Tab.
The GVRP Tab is shown in Figure 283 on page 772.
4. To display the GVRP State Machine, click the circle next to **View GVRP State Machine for VLAN** in the View GVRP Parameters section of the page.
5. Enter the VLAN ID in the box next to View GVRP State Machine for VLAN. Then click **View**.

The GVRP State Machine Page is shown in Figure 288.

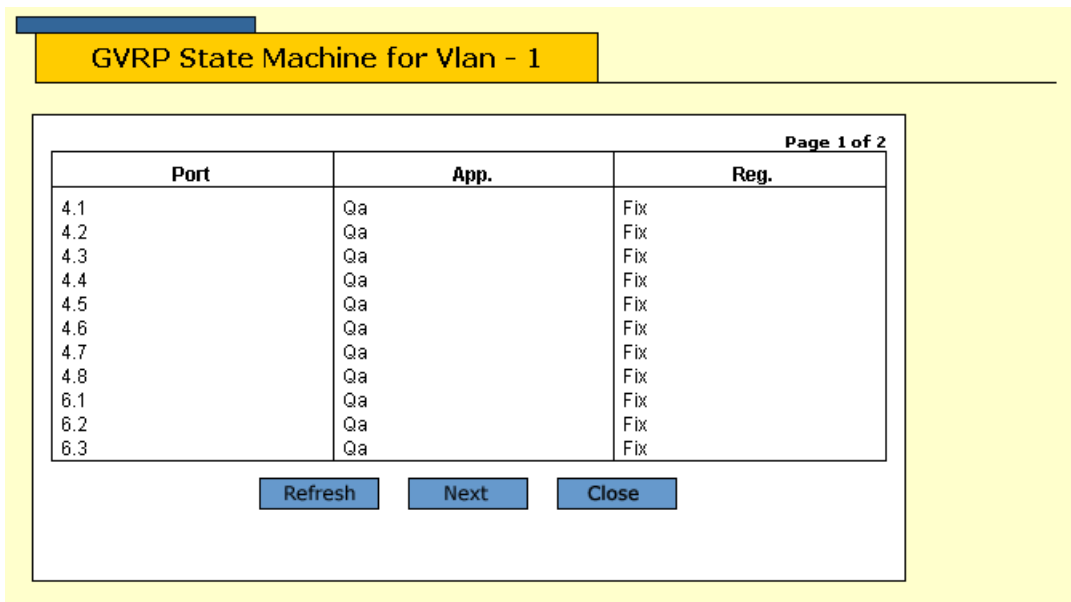


Figure 288 GVRP State Machine Page

The information on this page is described in Table 20.

Table 20 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 20 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

Table 20 GVRP State Machine Parameters (Continued)

Parameter	Meaning
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.
	Reg
"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.	

Chapter 43

Port Security

This chapter explain how to display the port security status using a web browser management session. It contains the following procedure:

- Displaying the Port Security Level on page 784

Note

For background information on port security, refer to Port Security Overview on page 470.

Note

You cannot set up port security from a web browser management session. To set port security, use a local or Telnet management session.

Displaying the Port Security Level

To display the switch's port security levels, 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 194 on page 592.
2. Select the **Layer 2** option.
The Monitoring Layer 2 Page is displayed with the MAC Address Tab selected by default, as shown Figure 212 on page 634.
3. Select the **Port Security** Tab.
A graphical image that reflects the line cards installed in your chassis is displayed on the Port Security Tab, as shown in Figure 289.

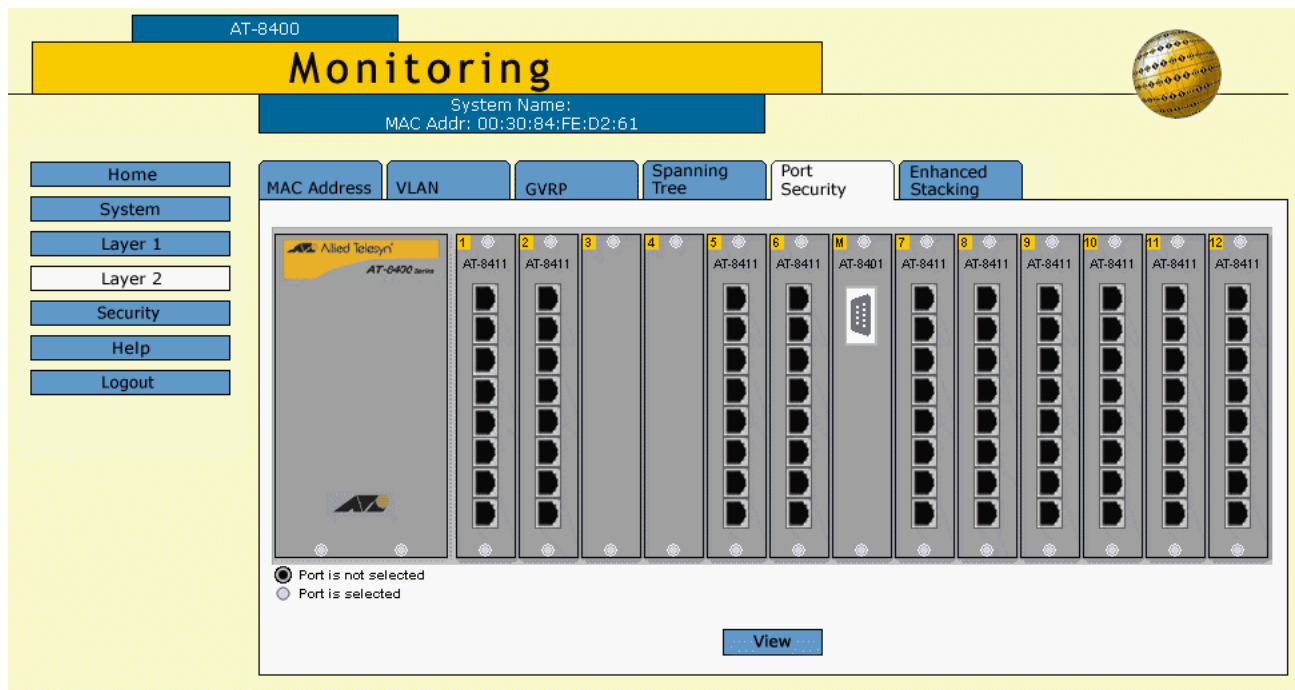


Figure 289 Monitoring Layer 2 Page, Port Security Tab

- Click on the ports to display their security status.

After you click on a port, it turns white. You can select multiple ports to display. (To deselect a port, click it again.)

- Click **View**.

The Security for Ports Page is shown in Figure 290. This page displays the current security levels of the ports you selected.

The screenshot shows a web interface titled "Security for Port(s) - 2.1-8,8.1-8". Below the title is a table with the following data:

Total Ports Selected: 16. Page 1 of 2				
Port	Security Mode	Intruder Action	Participating	MAC Limit
2.1	Automatic	Discard	No	No Limit
2.2	Automatic	Discard	No	No Limit
2.3	Automatic	Discard	No	No Limit
2.4	Automatic	Discard	No	No Limit
2.5	Automatic	Discard	No	No Limit
2.6	Automatic	Discard	No	No Limit
2.7	Automatic	Discard	No	No Limit
2.8	Automatic	Discard	No	No Limit
8.1	Automatic	Discard	No	No Limit
8.2	Automatic	Discard	No	No Limit

Below the table are two buttons: "Next" and "OK".

Figure 290 Security for Ports Page

Following is a description of the headings that appear in the Security for Ports Page:

Port

Identifies the port in the AT-8400 switch in the following format:
slot number of line card. port number

Security Mode

There are four levels of port security:

- Automatic: The Automatic security mode disables port security. It is the default security level for the ports.
- Limited: You can use the Limited security level to manually specify a maximum number of dynamic MAC addresses that each port can learn.
- Secured: The Secured security level instructs a port to forward frames based solely on its static MAC address.

- ❑ **Lock all ports:** The Lock All Ports security level causes the switch to immediately stop learning new dynamic MAC addresses on behalf of the specified port.

For detailed information about the security mode parameter, see Port Security Overview on page 470.

Intruder Action

Indicates the action taken by the port if the security on the port is violated. Violating actions differ depending on the security level, as described below:

- ❑ **Limited** - The port receives a frame with a new source MAC address after the port has learned its maximum number of dynamic MAC addresses.
- ❑ **Secured** - The port receives a frame with a MAC address that has not been entered as a static address on the port.
- ❑ **Locked** - The port receives a frame with a new source MAC address.

You can configure the port to take one of the following intrusion actions if a violating event occurs:

- ❑ **Discard** - Discards the invalid frame.
- ❑ **Trap** - Discards the invalid frame and sends a trap to a management workstation.
- ❑ **Disable** - Discards the invalid frame, sends a trap to a management workstation, and disables the port.

Participating

Indicates the port is participating in port security.

MAC Limit

Indicates the maximum number of dynamic MAC addresses the port can learn when it is operating under the Limited security level.

Chapter 44

Web Server Security

This chapter about web server security contains the following procedures:

- Displaying the Encryption Keys on page 788
- Displaying the PKI Settings on page 790
- Displaying the SSL Settings on page 794

Note

For background information on encryption, refer to Encryption Overview on page 485. For background information on PKI, refer to Public Key Infrastructure Overview on page 502. For information about SSL, refer to Secure Sockets Layer Overview on page 524.

Note

The features described in this chapter only appear in the AT-S60 version 2.1.0 software.

Displaying the Encryption Keys

To display the encryption keys, perform the following procedure:

Note

You cannot set up the encryption keys from a web browser management session. To set the encryption keys, use a local or Telnet management session. For more information, see Configuring Keys for Encryption on page 491.

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

The Monitoring System Page is displayed with the General Tab selected by default, as shown in Figure 194 on page 592.

2. Select the **Layer 2** option.

The Monitoring Layer 2 Page is displayed with the MAC Address Tab selected by default, as shown Figure 212 on page 634.

3. Select the **Security** option.

The Monitoring Security Page opens with the Keys Tab displayed by default, as shown in Figure 291.

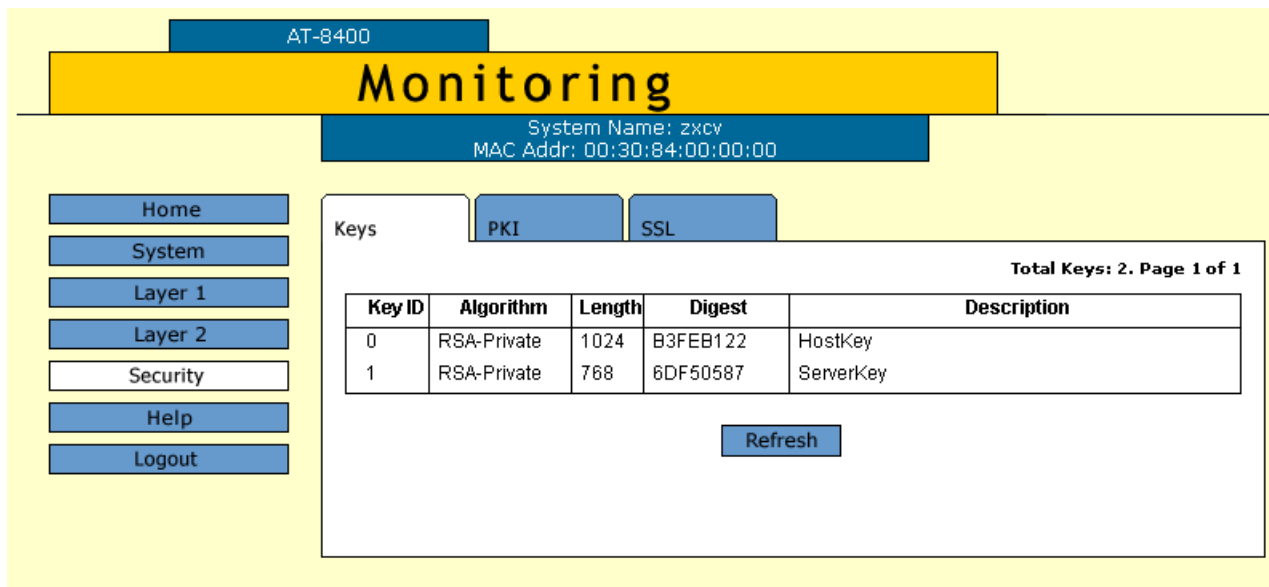


Figure 291 Monitoring Security Page, Keys Tab

The following information is displayed:

Key ID

The identification number for the key.

Algorithm

The encryption algorithm for the key. The only option is RSA.

Length

The length of the key in bytes.

Digest

CRC value of the MD5 digest of the key data.

Description

The name or description of the key.

4. To view the latest list of keys, click **Refresh**.

Displaying the PKI Settings

To display the PKI settings, perform the following procedure:

Note

You cannot set up PKI from a web browser management session. To set up PKI, use a local or Telnet management session. For more information, see **Chapter 24**, Public Key Infrastructure (PKI) on page 501.

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

The Monitoring System Page is displayed with the General Tab selected by default, as shown in Figure 194 on page 592.

2. Select the **Layer 2** option.

The Monitoring Layer 2 Page is displayed with the MAC Address Tab selected by default, as shown Figure 212 on page 634.

3. Select the **Security** option.

The Monitoring Security Page opens with the Keys Tab displayed by default, as shown in Figure 291 on page 788.

4. Select the **PKI** Tab.

The PKI Tab is shown in Figure 292.

AT-8400

Monitoring

System Name:
MAC Addr: 00:30:84:FE:D7:AF

Home
System
Layer 1
Layer 2
Security
Help
Logout

Keys PKI SSL

Maximum Number of Certificates is 256

Total Certificates: 0, Page 1 of 1

	Name	State	MTrust	Type	Source
<input checked="" type="radio"/>	testCertificate	Trusted	True	Self	Command

Refresh View

Figure 292 Monitoring Security Page, PKI Tab

The following information is displayed:

Name

The name of the PKI certificate.

State

Shows whether or not the certificate is automatically trusted.

MTrust

Indicates you verified the certificate is from a trusted authority or from an untrusted authority.

Type

The certificate type: CA, EE, or Self.

Source

Indicates the certificate was created on the switch.

- To view detailed information about the certificate, select the certificate and then click **View**.

The Certificate Page is shown in Figure 293.

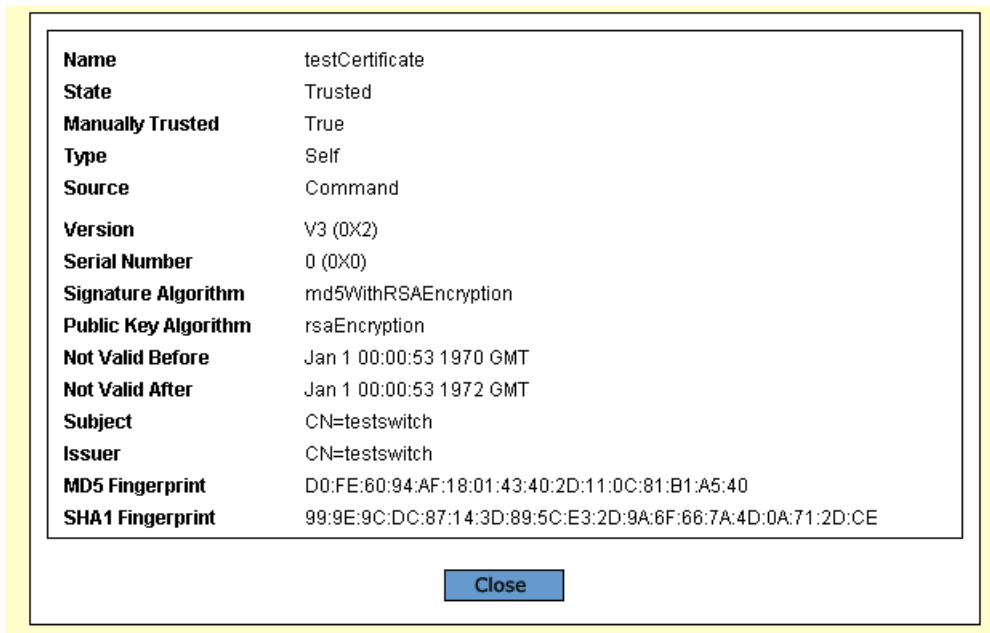


Figure 293 Certificate Page

The following fields are displayed:

- Name** - Lists the name of the certificate.
- State** - Indicates the certificate is Trusted or Untrusted.
- Manually Trusted** - Indicates you verified the certificate is from a trusted authority or from an untrusted authority.
- Type** - Indicates the type of the certificate. Options are EE, SELF, and CA.
- Source** - Indicates the certificate was created on the switch.
- Version** - Indicates the version number of the software.
- Serial Number** - Indicates the serial number of the certificate.
- Signature Algorithm** - Indicates the signature algorithm of the certificate.
- Public Key Algorithm** - Indicates the public key algorithm.
- Not Valid Before** - Indicates the date the certificate became active.
- Not Valid After** - Indicates the date the certificate expires. Self-signed certificates are valid for two years.

Subject - Lists the Subject Distinguished Name.

Issuer - Lists the Distinguished Name of the issuer of the certificate.

MD5 Fingerprint - The MD5 digest of the certificate. This value provides a unique sequence for each certificate consisting of 16 bytes.

SHA1 Fingerprint - The Secure Hash Algorithm digest of the certificate. This value provides a unique sequence for each certificate consisting of 20 bytes.

Displaying the SSL Settings

To view the SSL settings, perform the following procedure:

Note

You cannot set up SSL from a web browser management session. To set up SSL, use a local or Telnet management session. For more information, see Configuring SSL on page 528.

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

The Monitoring System Page is displayed with the General Tab selected by default, as shown in Figure 194 on page 592.

2. Select the **Layer 2** option.

The Monitoring Layer 2 Page is displayed with the MAC Address Tab selected by default, as shown Figure 212 on page 634.

3. Select the **Security** option.

The Monitoring Security Page opens with the Keys Tab displayed by default as shown in Figure 291 on page 788.

4. Select the **SSL** Tab.

The SSL Tab is shown in Figure 294.

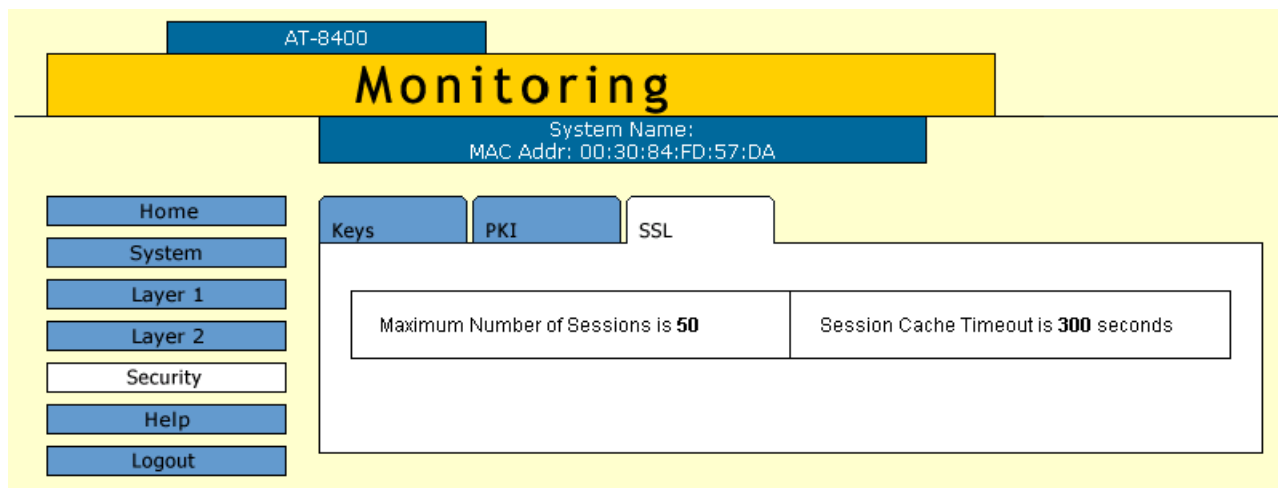


Figure 294 Monitoring Security Page, SSL Tab

The following information is displayed:

Maximum Number of Sessions

The maximum number of SSL sessions allowed in the cache. The cache is used to speed up the SSL connections by removing previous sessions if possible.

Session Cache Timeout

The maximum time that a session is retained in the cache.

Chapter 45

TACACS+ and RADIUS Protocols

This chapter contains instructions on how to configure the authentication protocols. This chapter contains the following procedure:

- Enabling TACACS+ or RADIUS on page 797
- Configuring TACACS+ on page 799
- Configuring RADIUS on page 801
- Displaying the TACACS+ Settings on page 803
- Displaying the RADIUS Settings on page 805

Note

For background information on the authentication protocols, refer to TACACS+ and RADIUS Overview on page 541.

Enabling TACACS+ or RADIUS

To configure the authentication protocols, 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 192 on page 584.

2. Select the **Server-based Authentication** Tab.

The Server-based Authentication Tab is shown in Figure 295.

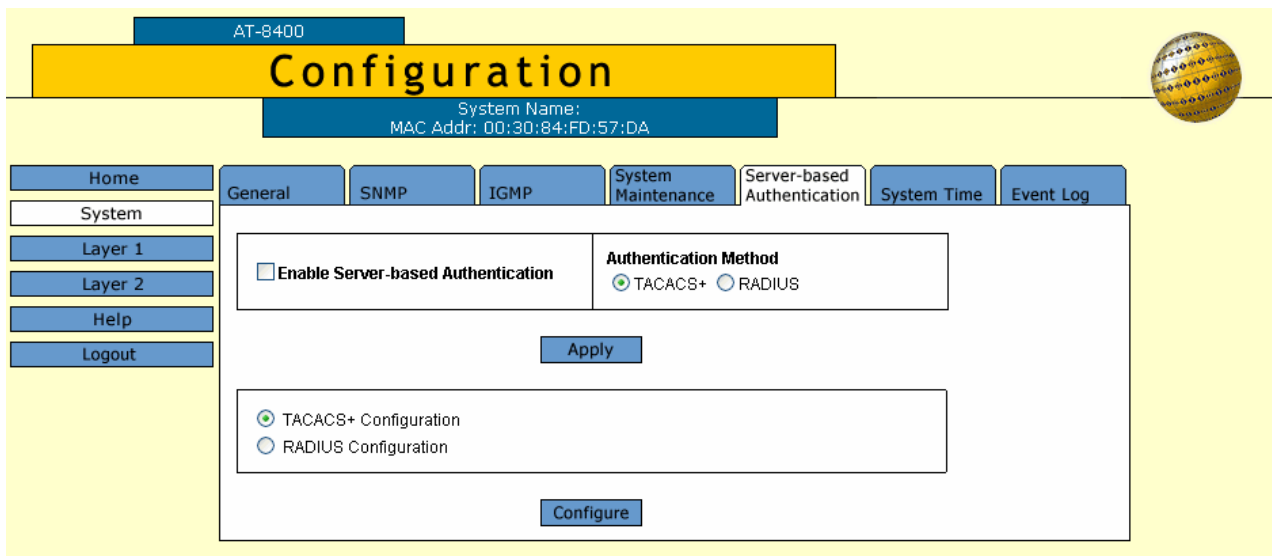


Figure 295 Configuration System Page, Server-based Authentication Tab

3. 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 disabled. The default is disabled. No check in the box indicates the feature is enabled.

4. To select an authentication protocol, click either TACACS+ or RADIUS in the Authentication Method section of the tab. The default is TACACS+.

Note

Only one authentication protocol can be active on the switch at a time.

5. Click **Apply**.
6. To save your changes, return to the General Tab and click **Save Changes**. The changes you made are saved on the switch.

Configuring TACACS+

To configure TACACS+, 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 192 on page 584.

2. Select the **Server-based Authentication** Tab.

The Server-based Authentication Tab is displayed as shown in Figure 295 on page 797.

3. Click the check circle next to TACACS+ Configuration and click **Configure**.

The TACACS+ Client Configuration Page is shown in Figure 296.

Server No.	IP Address	Encryption Key
1	198.45.12.10	mississippiRiver556
2	198.45.12.11	eastRiver332
3	198.45.12.12	ohioRiver899

Figure 296 TACACS+ Client Configuration Page

4. Configure the following parameters as needed:

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 aren't any more servers, then the switch defaults to the standard Manager and Operator accounts. The default is 30 seconds. The range is from 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. After you have finished configuring the parameters, click **Apply**.
6. To save your changes, return to the General Tab and click **Save Changes**. The changes you made are saved on the switch.

Configuring RADIUS

To configure RADIUS, 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 192 on page 584.

2. Select the **Server-based Authentication** Tab.

The Server-based Authentication Tab is displayed as shown in Figure 295 on page 797.

3. Click the check circle next to RADIUS Configuration and click **Configure**.

The RADIUS Client Configuration Page is shown in Figure 297.

Server No.	IP Address	Port # [1-65535]	Encryption Key
1	198.7.35.121	1812	CAFortyNiners49
2	198.7.35.123	1812	CAGoldenGate34
3	198.7.35.125	1812	CASiliconValley84

Figure 297 RADIUS Client Configuration Page

4. Configure the following parameters as needed:

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 are no more servers, then the switch defaults to the standard Manager and Operator accounts. The default is 30 seconds. The range is from 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. After you have finished configuring the parameters, click **Apply**.
6. To save your changes, return to the General Tab and click **Save Changes**. The changes you made are saved on the switch.

Displaying the TACACS+ Settings

To display the TACACS+ RADIUS 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 194 on page 592.

2. Select the **Server-based Authentication** Tab.

The Server-based Authentication Tab is shown in Figure 298.

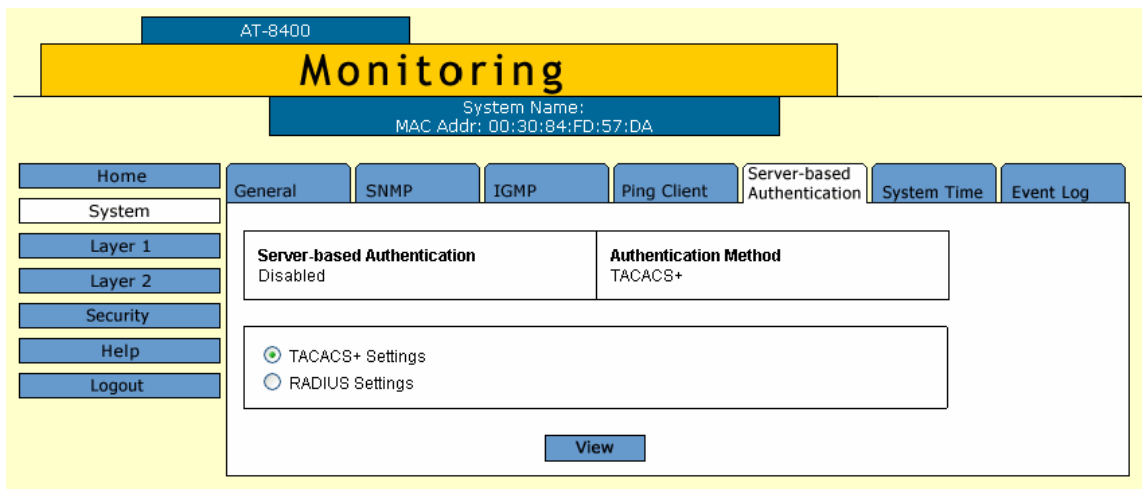


Figure 298 Monitoring System Page, Server-based Authentication Tab

3. Click the **TACACS+ Settings** button.
4. Click **View**.

The TACACS+ Client Configuration Page is shown in Figure 299.

Server No.	IP Address	Encryption Key
1	198.45.12.10	mississippiRiver556
2	198.45.12.11	eastRiver332
3	198.45.12.12	ohioRiver899

Figure 299 TACACS+ Client Configuration Page

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

Displaying the RADIUS Settings

To display the RADIUS 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 194 on page 592.

2. Select the **Server-based Authentication** Tab.

The Server-based Authentication Tab is shown in Figure 298 on page 803.

3. Click on RADIUS Settings.

4. Click **View**.

The RADIUS Client Configuration Page is shown in Figure 300.

Server No.	IP Address	Port # [1-65535]	Encryption Key
1	198.45.12.13	1812	LakeOswego1002
2	198.45.12.14	1812	LakeMichigan1334
3	198.45.12.15	1812	LakeTahoe1546

Figure 300 RADIUS Client Configuration Page

5. To close the page, click **Cancel**.

Chapter 46

802.1x Port-based Network Access Control

This chapter describes how to configure and display port-based access control information using a web browser management session. It contains the following procedures:

- ❑ [Configuring Port Access on page 807](#)
- ❑ [Displaying 802.1x Port-Based Access Control Information on page 816](#)

Note

For background information on this feature, refer to Chapter 28: 802.1x Port-based Access Network Control Overview on page 550.

Configuring Port Access

The 802.1x Port-based Access Control feature uses the RADIUS authentication protocol. Before you configure port-based access on the switch, you must first configure RADIUS with EAP. See Chapter 45: TACACS+ and RADIUS Protocols.

To configure the port-based access feature, there are several tasks you need to accomplish. First, you enable port-based access on the switch. Then you have the option of enabling RADIUS accounting as well. In addition, you must configure ports with the role of authenticator and supplicant. Once you've decided on the port roles, there are parameters specific to authenticator and supplicant ports that you may want to configure. See the following procedures for more information:

- Enabling Port-Based Access Control on page 807
- Configuring RADIUS Accounting on page 809
- Setting the Port Role on page 810
- Configuring an Authenticator Port on page 811
- Configuring a Supplicant Port on page 814

To display the current port access configuration, see Displaying 802.1x Port-Based Access Control Information on page 816.

Enabling Port-Based Access Control

To enable 802.1x Port-based Access Control from a web browser management session, perform the following procedure:

1. On the Home Page, select **Configuration**.
The Configuration System Page is displayed with the General Tab shown by default.
2. Select the **Layer 1** option.
The Layer 1 Page is displayed with the Port Settings Tab shown by default.
3. Select the 802.1x Port Access Tab.
The Configuration 802.1x Port Access Tab is displayed as shown in Figure 301 on page 808.

AT-8400

Configuration

System Name: Jenny's Switch
MAC Addr: 00:30:84:FD:57:DA

Home System Layer 1 Layer 2 Help Logout

Port Settings Port Mirroring Port Trunking 802.1x Port Access

Configure Port Access Parameters

Enable Port Access Authentication Method
RADIUS EAP

Configure RADIUS Accounting

Enable Accounting Trigger Type
Start Stop

Port Number: 1813 Type
Network

Enable Update Update Interval
60

Allied Telesyn AT-8400 Series	1	2	3	4	5	6	M	7	8	9	10	11	12
AT-8411				AT-8411		AT-8411	AT-8401						

R Port in Authenticator role
S Port in Supplicant role
● Regular port

Figure 301 802.1x Port Access Tab

4. Click the Enable Port Access check box.

A check in the box means the feature is activated on the switch. No check means the feature is disabled. Port Access is disabled by default.

Note

Authentication Method - RADIUS EAP is the only selection.

5. After setting the parameters, click **Apply**.
Your changes are activated on the switch.
6. To save your changes, return to the General Tab and click **Save Changes**.

Configuring RADIUS Accounting

This section describes how to configure the RADIUS accounting feature from a web browser management session. For background information, refer to Configuring RADIUS Accounting on page 568.

To enable or disable RADIUS accounting and its associated settings access, perform the following procedure:

1. On the Home Page, select **Configuration**.
The Configuration System Page is displayed with the General Tab shown by default.
2. Select the **Layer 1** option.
The Layer 1 Page is displayed with the Port Settings Tab shown by default.
3. Select the 802.1x Port Access Tab.
The Configuration 802.1x Port Access Tab is displayed as shown in Figure 301 on page 808.
4. Configure the parameters in the RADIUS Accounting section of the tab. The parameters are described below:

Enable Accounting

Activates and deactivate RADIUS accounting on the switch. A check in the box indicates the feature is activated. The default is Disabled.

Trigger Type

Specifies the action that causes the switch to send accounting information to the RADIUS server. The choices 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

Specifies the type of RADIUS accounting. The default is Network. This value cannot be changed.

Enable Update

Controls whether the switch is to send interim accounting updates to the RADIUS server. The default is disabled. If you enable this feature, use the next option to specify the intervals at which the switch is to send the accounting updates.

Update Interval

Specifies the intervals at which the switch is to send interim accounting updates to the RADIUS server. The range is 30 to 300 seconds. The default is 60 seconds.

5. After setting the parameters, click **Apply**.
Your changes are activated on the switch.
6. To save your changes, return to the General Tab and click **Save Changes**.

Setting the Port Role

Before you can configure authenticator or supplicant settings, you need to set the role of the port on the switch. By default, the port role is set to None.

For more information about the authenticator and supplicant port roles, refer to 802.1x Port-based Access Network Control Overview on page 550.

To set a port with the role of authenticator or supplicant, perform the following procedure:

1. On the Home Page, select **Configuration**.
The Configuration System Page is displayed with the General Tab shown by default.
2. Select the **Layer 1** option.
The Layer 1 Page is displayed with the Port Settings Tab shown by default.
3. Select the 802.1x Port Access Tab.
The Configuration 802.1x Port Access Tab is displayed as shown in Figure 301 on page 808.
4. To set the role for a port or ports, click on the port or ports you want to configure with the same role. Then click **Port Role**.

The Port Role Configuration Page is displayed, as shown in Figure 302.

The screenshot shows a web browser window with a yellow header bar containing the text "Port Role Configuration - 3.2". Below the header is a white rectangular form. Inside the form, the text "Port Role" is followed by three radio button options: "None" (which is selected), "Authenticator", and "Supplicant". At the bottom of the form, there are two blue buttons labeled "Apply" and "Cancel".

Figure 302 Port Role Configuration Page

- To assign a role to a port, click the circle next to **None**, **Authenticator**, or **Supplicant**.

N - The port does not participate in access control. This is the default.

A - The port performs the role of authenticating the supplicants that are connected to the port.

S - The port becomes a Supplicant to the Authenticator port.

- Click **Apply**.

The page closes and the 802.1x Port Access Tab is updated.

- To save your changes, return to the General Tab and click **Save Changes**.

Configuring an Authenticator Port

This section provides a procedure to configure the authenticator port settings using a web browser management session. Before you can configure authenticator settings, you need to set the role of the port on the switch to authenticator. See Setting the Port Role on page 810.

To configure an authenticator port, perform the following procedure:

- On the Home Page, select **Configuration**.

The Configuration System Page is displayed with the General Tab shown by default.

- Select the **Layer 1** option.

The Layer 1 Page is shown with the Port Settings Tab shown by default.

- Select the 802.1x Port Access Tab.

The Configuration 802.1x Port Access Tab is displayed as shown in Figure 301 on page 808.

Note

You must set the port role as authenticator before you can configure an authenticator port. See Setting the Port Role on page 810.

4. Click on an authenticator port or ports and click **Settings**.

The Authenticator Parameters Page is displayed, as shown in Figure 303.

Figure 303 Authenticator Parameters Page

5. Configure the following parameters:

Port Control

Choose from the following values:

- 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. The switch requests the identity of the client and begins relaying authentication messages between the client and the authentication server. Each client that attempts to access the network is uniquely identified by the switch by using the client's MAC address. This is the default value.

- ❑ **Force-authorized:** Disables 802.1X port-based authentication and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client.
- ❑ **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.

Tx Period

Sets the number of seconds the switch waits for the EAP-request/identity frame response from the supplicant before retransmitting the request. The default value is 30 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 is 30 seconds. The range is from 1 to 600 seconds.

Max Requests

This parameter 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 is 2 retransmissions. The range is 1 to 10 retransmissions.

Quiet Period

Sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. The default value is 60 seconds. The range is 0 to 65,535 seconds.

Reauth Period

Enables periodic re-authentication of the client, which is disabled by default. The default value is 3,600 seconds. The range is from 1 to 65,535 seconds.

Server Timeout

This is the timer used by the switch to determine authentication server timeout conditions. The default value is 30 seconds. The range is from 1 to 65,535 seconds.

6. Click **Apply** to save the settings and close the page. If you click **Close**, the page is closed but the settings are not saved.
7. To save your changes, return to the General Tab and click **Save Changes**.

Configuring a Supplicant Port

This section provides a procedure to configure the supplicant port settings using a web browser management session. Before you can configure supplicant settings, you need to set the role of the port on the switch to supplicant. See *Setting the Port Role* on page 810.

To configure a supplicant port, perform the following procedure:

1. On the Home Page, select **Configuration**.

The Configuration System Page is displayed with the General Tab shown by default.

2. Select the **Layer 1** option.

The Layer 1 Page is shown with the Port Settings Tab shown by default.

3. Select the 802.1x Port Access Tab.

The Configuration 802.1x Port Access Tab is displayed as shown in Figure 301 on page 808.

Note

You must set the port role as supplicant before you can configure a supplicant port. See *Setting the Port Role* on page 810.

4. Click on a supplicant port or ports and click **Settings**.

The Supplicant Parameters Page is displayed, as shown in Figure 304.

Supplicant Parameters - 2.4	
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" value="chitra"/>	User Password <input type="text" value="westcoast4891"/>
<input type="button" value="Apply"/> <input type="button" value="Close"/>	

Figure 304 Supplicant Parameters Page

5. Configure the following parameters:

Auth Period - This is the initialization time used by the authentication timer. The value is in seconds. The default is 30 seconds. The range is 1 to 300 seconds.

Max Start - This parameter determines the maximum number of successive EAPOL Start messages that are sent before the Supplicant assumes there is no Authenticator. The value is in whole numbers. The default is 3 messages. The range is from 1 to 10 messages.

User Name - Enter a user name to access the supplicant port. The values of Manager and Operator are not permitted. There is no default value. This is an alphanumeric value of up to 40 characters.

Held Period - This is the initialization value for the supplicant held timer. The value is in seconds. The default is 60 seconds. The range is 0 to 65,535 seconds.

Start Period - This parameter provides the initialization value for the timer that determines when EAPOL Start messages are sent. The value is in seconds. The default is 30 seconds. The range is from 1 to 60 seconds.

User Password - Enter a password to access the supplicant port. There is no default value. This is an alphanumeric value of up to 40 characters.

6. Click **Apply** to save the settings and close the page. If you click **Close**, the page is closed but the settings are not saved.
7. To save your changes, return to the General Tab and click **Save Changes**.

Displaying 802.1x Port-Based Access Control Information

To view host nodes and multicast routers, perform the following procedure:

1. From the Home Page, select **Monitoring**.
The Monitoring System Page is displayed with the General Tab shown by default.
2. Select the **Layer 1** option.
The Layer 1 Page is displayed with the Port Settings Tab shown by default.
3. Select the 802.1x Port Access Tab.
The 802.1x Port Access Tab is displayed as shown in Figure 305.

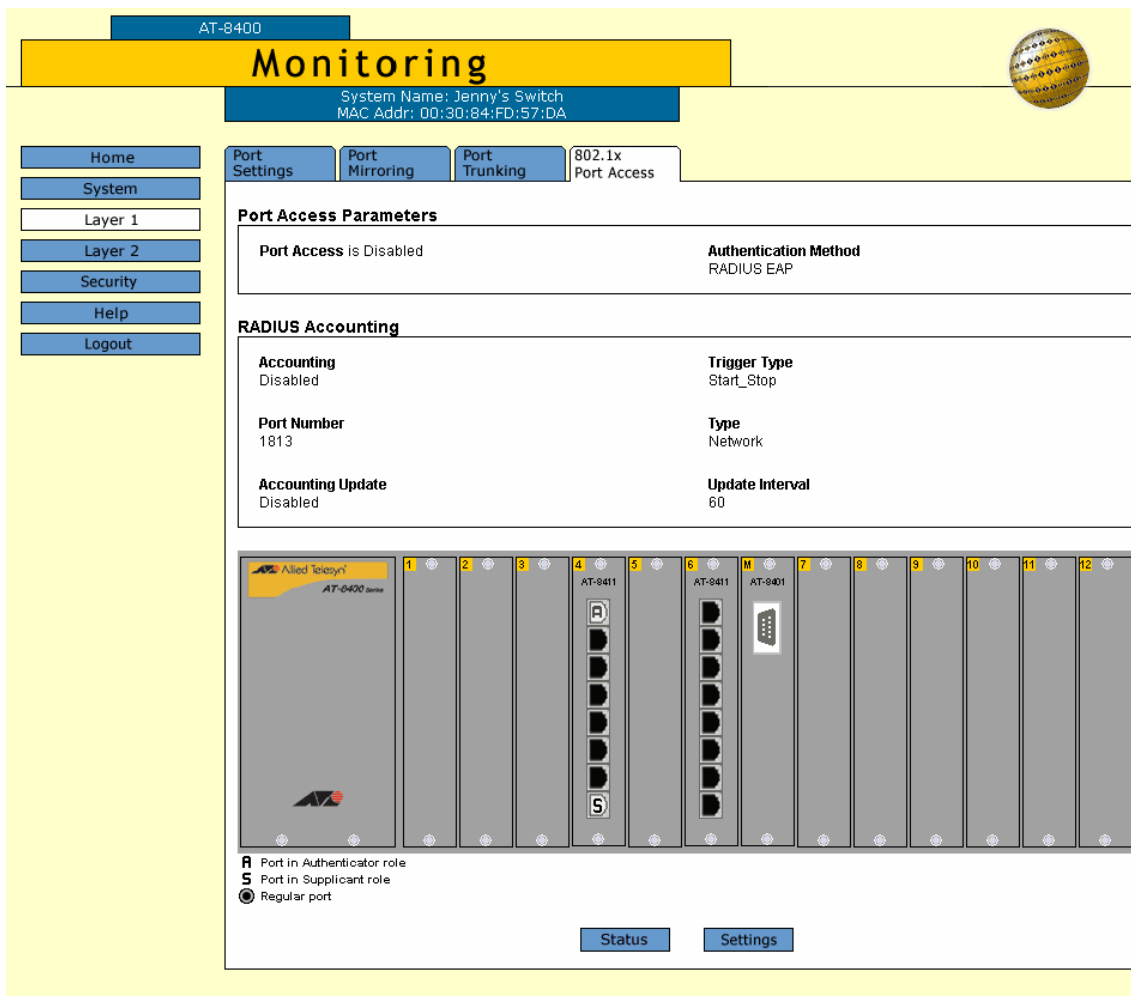


Figure 305 Monitoring, 802.1x Port Access Tab

4. To display the status of the port, click the port or ports to select it and click **Status**. Or, to display the port access settings, go to step 5.

Note

All the ports must have the same port role (authenticator or supplicant) to view the status of multiple ports.

A Port Status Page is displayed, as shown in Figure 306.

The screenshot shows a web interface titled "Port Access Port Status - 4.1,4.8". Below the title is a table with the following data:

Total Ports = 2. Page 1 of 1			
Port	Port Role	Status	Additional Info.
4.1	Authenticator	Disabled	-----
4.8	Supplicant	Disabled	-----

Below the table is a blue "OK" button.

Figure 306 Port Access Port Status Page

5. To display the port access settings, select a port or ports and click **Settings**.

For authenticator port(s), the Authenticator Port Parameters Page is displayed, as shown in Figure 307.

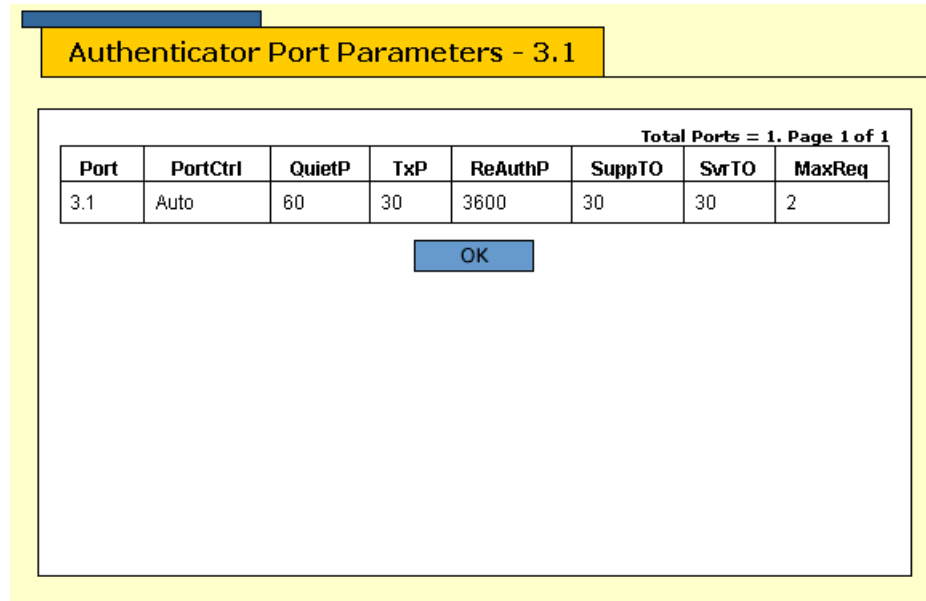


Figure 307 Authenticator Port Parameters Page

For a description of the parameters displayed on the above page, refer to Configuring an Authenticator Port on page 811.

For supplicant port(s), the Supplicant Port Parameters Page is displayed, as shown in Figure 308.

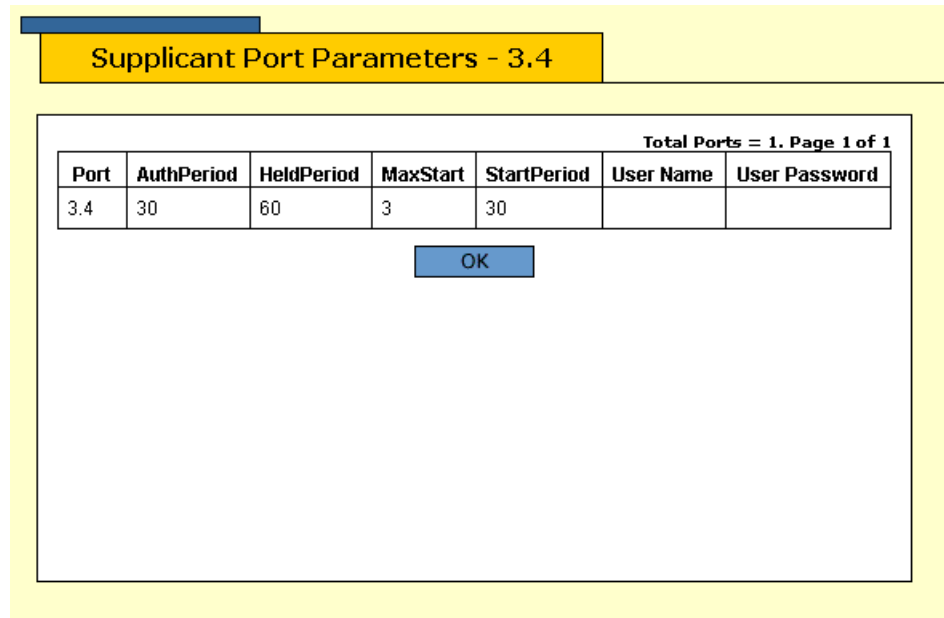


Figure 308 Supplicant Port Parameters Page

For a description of the parameters displayed on the Supplicant Port Parameters page, refer to [Configuring a Supplicant Port](#) on page 814.

Appendix A

AT-S60 Default Settings

This appendix lists the AT-S60 factory default settings. It contains the following sections in alphabetical order:

- Basic Switch Default Settings** on page 821
- Enhanced Stacking Default Setting** on page 824
- Event Log Settings** on page 825
- IGMP Snooping Default Settings** on page 826
- PKI Default Settings** on page 827
- Port Configuration Default Settings** on page 828
- Port Security Default Settings** on page 829
- Server-Based Authentication Default Settings** on page 830
- SNMP Default Settings** on page 831
- SSH Default Settings** on page 832
- SSL Default Settings** on page 833
- STP, RSTP, and MSTP Default Settings** on page 834
- VLAN Default Settings** on page 837
- Web Server Default Settings** on page 838
- 802.1x Port-Based Network Access Control Default Settings**
on page 839

Basic Switch Default Settings

This section lists the default settings for basic switch parameters. The following topics are covered:

- File Menu Default Setting** on page 821
- Management Access Default Settings** on page 821
- Management Interface Default Settings** on page 821
- RS-232 Port Default Settings** on page 822
- SNTP Default Settings** on page 822
- Switch Administration Default Settings** on page 823
- System Software Default Settings** on page 823

File Menu 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.

Management Access Setting	Default
Telnet	Enabled
SNMP	Disabled
TFTP	Enabled
Web Server	Enabled
SSH	Disabled

Management Interface Default Settings

The following table lists the management Interface default settings.

Management Interface Setting	Default
Manager Login Name	manager
Manager Password	friend (case-sensitive)
Operator Login Name	operator

Management Interface Setting	Default
Operator Password	operator (case-sensitive)
Console Disconnect Timer Interval	10 minutes
Negotiation	Auto (see Note)
STP State	Forwarding
Security Mode	Automatic

Note

For the AT-8412/SC FX and AT-8412/MT FX line cards, the default setting for Negotiation is Manual. For all the other line cards, the default setting for Negotiation is Auto.

RS-232 Port Default Settings

The following table lists the RS-232 port default settings.

RS-232 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
Console Baud Rate	9600 bps
MAC Address Aging Time	300 seconds

System Software Default Settings

The following table lists the system software default settings.

System Software Setting	Default
Switch Mode	Tagged
Console Startup Mode	Menu

Enhanced Stacking Default Setting

The following table lists the Enhanced Stacking default setting.

Enhanced Stacking Setting	Default
Switch State	Slave

Event Log Settings

This section lists the default settings for the Event Log feature.

Event Log	Default
Event Logging	Disabled
Log Full Action	Wrap
Display Output	Temporary (Memory)
Display Order	Chronological
Display Mode	Normal
Display Severity	E, W, I
Display Module	All

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

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

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
Negotiation	Auto

Port Security Default Settings

The following table lists the port security default settings.

Port Security Setting	Default
Security Mode	Automatic
Intrusion Action	Discard
Participating	No
MAC Limit	No Limit

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
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

SNMP Default Settings

This section lists the default settings for the SNMPv1 and SNMPv2c protocols. There are no default settings for the SNMPv3 protocol.

The following table describes the SNMPv1 and SNMPv2c default settings.

SNMPv1 and SNMPv2c 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
OpenAcc	Yes

SSH Default Settings

The following table lists the SSH and the SSH server default settings.

SSH Setting	Default
SSH Server Status	Disabled
Host Key ID	Not Defined
Server Key ID	Not Defined
Server Key Expiry Time	0 hours
Login Timeout	180 seconds

SSL Default Settings

The following table lists the SSL default settings.

SSL Setting	Default
Maximum Number of Sessions	50
Session Cache Timeout	300 seconds

STP, RSTP, and MSTP Default Settings

This section provides the STP switch, 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 describes the MSTP default settings.

MSTP Setting	Default
Force Version	MSTP
Hello Time	2
Forwarding Delay	15
Max Age	20
Max Hops	20
Configuration Name	None
Revision Level	0
CIST Priority	32768
Associated VLANs	1
MSTI/CIST	0
Edge Port	Yes
Point-to-Point	Auto Detect
External Cost	200 000

MSTP Setting	Default
Internal Cost	Auto Update
Port Priority	128

VLAN Default Settings

This section provides VLAN, GARP, and GVRP default settings.

VLAN Default Settings

The following table lists the 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

GARP and GVRP Default Settings

The following table lists the GARP and GVRP default settings.

GARP and GVRP Setting	Default
GVRP Status	Disabled
GVRP GIP Status	Enabled
GVRP Join Timer	20
GVRP Leave Timer	60
GVRP Leave All Timer	1000
Port Mode	Normal
Mode Normal	(all ports on your switch)
Mode None	None

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

802.1x Port-Based Network Access Control Default Settings

The following table describes the 802.1x Port Access Control default settings.

802.1x Port Access Control Setting	Default
Port Access Control	Disabled
Authentication Method	RADIUS EAP
Port Role	None

Appendix B

SNMPv3 Configuration Examples

This appendix provides two examples of SNMPv3 configuration using the SNMPv3 Table menus. In addition, a worksheet is provided which you can use as an aid when configuring the SNMPv3 protocol. This appendix includes the following sections:

- SNMPv3 Manager Configuration on page 841
- SNMPv3 Operator Configuration on page 842
- SNMPv3 Worksheet on page 843

SNMPv3 Configuration Examples

This appendix provides SNMPv3 configuration examples for the following types of users:

- a Manager
- an Operator

In addition an SNMPv3 Configuration Table is provided to record your SNMPv3 configuration.

For more information about the SNMPv3 protocol, see Chapter 17: SNMPv3 Configuration on page 293.

SNMPv3 Manager Configuration

This section provides a sample configuration for a Manager with a User Name of systemadmin24. Each table is listed with its parameters.

Configure SNMPv3 User Table Menu

```
User Name: systemadmin24
Authentication Protocol: MD5
Privacy Protocol: DES
Storage Type: NonVolatile
```

Configure SNMPv3 View Table Menu

```
View Name: internet
View Subtree OID: internet (or 1.3.6.1)
Subtree Mask:
View Type: Included
Storage Type: NonVolatile
```

Configure SNMPv3 Access Table

```
Group Name: Managers
Security Model: SNMPv3
Security Level: P-Authentication and Privacy
Read View Name: internet
Write View Name: internet
Notify View Name: internet
Storage Type: NonVolatile
```

Configure SNMPv3 SecurityToGroup Table

User Name:systemadmin24
Security Model:v3
Group Name: Managers
Storage Type: NonVolatile

Configure SNMPv3 Notify Table

Notify Name: sysadminTrap
Notify Tag: sysadminTag
Notify Type: Trap
Storage Type: NonVolatile

Configure SNMPv3 Target Address Table

Target Address Name: host451
Target IP Address: 198.35.11.1
UDP Port#: 162
Timeout: 1500
Retries: 3
Tag List: sysadminTag
Target Parm Name: SNMPmanagerPC
Storage Type: NonVolatile

Configure SNMPv3 Target Parameters Table

Target Parameters Name:SNMPmanagerPC
User Name:systemadmin24
Security Model: v3
Security Level: P-Authentication and Privacy
Storage Type: NonVolatile

SNMPv3 Operator Configuration

This section provides a sample configuration for an Operator with a User Name of nikoeng73. Since this user will only send messages to a group and not an SNMP host, you do not need to configure message notification for this user.

Configure SNMPv3 User Table Menu

User Name: nikoeng73
Authentication Protocol: MD5
Privacy Protocol: None
Storage Type: NonVolatile

Configure SNMPv3 View Table Menu

View Name: internet
 View Subtree OID: 1.3.6.1 (or internet)
 Subtree Mask:
 View Type: Included
 Storage Type: NonVolatile

Configure SNMPv3 Access Table

Group Name: Operators
 Security Model: SNMPv3
 Security Level: Authentication
 Read View Name: internet
 Write View Name:
 Notify View Name:

SNMPv3 Worksheet

This section provides a table that you can use as a worksheet when configuring SNMPv3. Each SNMPv3 Table is listed with its associated parameters.

SNMPv3 Parameters	
SNMPv3 User Table	
User Name	
Authentication Protocol	
Authentication Password	
Privacy Protocol	
Privacy Password	
Storage Type	
SNMPv3 View Table Menu	
View Name	
View Subtree OID	
Subtree Mask	
View Type	
Storage Type	

SNMPv3 Parameters (Continued)	
SNMPv3 Access Table Menu	
Group Name	
Security Model	
Security Level	
Read View Name	
Write View Name	
Notify View Name	
Storage Type	
SNMPv3 SecurityToGroup Table	
User Name	
Security Model	
Group Name	
Storage Type	
SNMPv3 Notify Table	
Notify Name	
Notify Tag	
Notify Type	
Storage Type	
SNMPv3 Target Address Table	
Target Address Name	
Target IP Address	
UDP Port	
Timeout	
Retries	
Tag List	
Target Params Name	

SNMPv3 Parameters (Continued)	
Storage Type	
SNMPv3 Target Parameters Table	
Target Parameters Name	
User (Security) Name	
Security Model	
Security Level	
Storage Type	

Index

- 802.1x port-based network access control
 - access role, configuring 559, 807
 - authentication process 551
 - authentication process diagram 555
 - authentication server diagram 555
 - authenticator port
 - configuring 561, 811
 - described 550
 - displaying 573, 816
 - configuring 559, 807
 - defined 550
 - disabling 557, 807
 - displaying 571, 816
 - enabling 557, 807
 - overview 549, 550
 - port access status, displaying 571, 816
 - port role, configuring 559, 807
 - port roles 552
 - RADIUS accounting
 - configuring 568, 809
 - described 556
 - setting the port role 560, 810
 - supplicant port
 - configuring 565, 814
 - described 550
 - displaying 574, 816

A

- administrator parameter 49, 585, 823
- aging time
 - changing 126, 593, 640
 - defined 117

- app (applicant state machine) parameter 466, 781
- app parameter 466, 781
- associated VLANs parameter 281, 835
- associations
 - defined 263
 - VLANs to MSTI IDs 283, 687
- asymmetrical encryption algorithms 487
- AT-S60 default settings 820
- AT-S60 software
 - displaying information 69, 594
 - resetting to factory defaults 72, 606
 - security 64
 - version number 68
- AT-S60 software updates
 - downloading from a local session 172
 - downloading from a web browser session 609
- auth port parameter 830
- authentication failure trap status parameter 87, 831
- authentication method parameter 544, 797, 808, 830, 839
- authentication protocols 541, 797
- authentication server 551
- authentication server diagram 555
- authenticator port role 552
- authenticator port, described 550
- Automatic security level 470, 785
- Auto-Negotiation parameter 109, 622

- B**
- back pressure parameter 108, 625, 828
 - Basic VLAN mode
 - defined 417
 - setting 432, 765
 - baud rate parameter 40
 - Boot Protocol (BootP)
 - activating 57, 591
 - defined 57
 - bootloader version number 68
 - BOOTP/DHCP parameter 49, 586, 823
 - BPDU. *See* bridge protocol data unit
 - bridge forwarding delay parameter
 - Multiple Spanning Tree Protocol (MSTP) 278, 683
 - Rapid Spanning Tree Protocol (RSTP) 250, 678
 - Spanning Tree Protocol (STP) 244, 674
 - bridge forwarding parameter 834, 835
 - bridge hello time parameter
 - default 834, 835
 - Multiple Spanning Tree Protocol (MSTP) 278, 683
 - Rapid Spanning Tree Protocol (RSTP) 250, 678
 - Spanning Tree Protocol (STP) 243, 674
 - bridge hello time, described 234
 - bridge identifier parameter
 - Multiple Spanning Tree Protocol (MSTP) 279
 - Rapid Spanning Tree Protocol (RSTP) 250, 678
 - Spanning Tree Protocol (STP) 244, 674
 - bridge identifier, defined 230
 - bridge max age parameter 834, 835
 - Multiple Spanning Tree Protocol (MSTP) 278, 683
 - Rapid Spanning Tree Protocol (RSTP) 250, 678
 - Spanning Tree Protocol (STP) 244, 674
 - bridge priority parameter 834, 835
 - Rapid Spanning Tree Protocol (RSTP) 249, 677
 - Spanning Tree Protocol (STP) 243, 673
 - bridge priority, described 230
 - bridge protocol data unit (BPDU) 244
 - broadcast filter parameter 107, 624, 828
 - browser tools 581
- C**
- CA certificates
 - configuring 482
 - described 481
 - CBC. *See* Cipher Block Chaining (CBC)
 - Certificate Authority (CA), root 506
 - certificate database 507
 - certificate format 522
 - Certificate Revocation List (CRL), described 506
 - certificate type parameter 522
 - certificates, PKI
 - adding to database 513
 - chains 505
 - creating 508
 - database 507
 - database storage 507
 - deleting 515
 - described 503
 - displaying 518, 790
 - modifying 515
 - validating 505
 - certificates, SSL
 - authentication 526
 - described 526
 - certificates, X.509 503
 - certification authority 505
 - CFB. *See* Cipher Feedback (CFB)
 - Cipher Block Chaining (CBC), described 486
 - Cipher Feedback (CFB), described 487
 - ciphers available parameter 539
 - CIST priority parameter 280, 684, 835
 - CIST. *See* Common and Internal Spanning Tree
 - Class of Service (CoS)
 - configuring 217
 - overview 215
 - comments parameter 49, 585, 823
 - Common and Internal Spanning Tree (CIST)
 - configuring 279, 684
 - defined 267
 - priority 267
 - community name parameter 89, 598, 831
 - community name parameter, SNMPv3 protocol 383, 742, 744
 - configuration file. *See* system configuration file

configuration name 264
 configuration name parameter 278, 683, 835
 console baud rate parameter 50, 823
 console disconnect timer interval parameter
 66, 822
 console startup mode parameter 74, 823
 console startup mode, configuring 74
 CoS. *See* Class of Service (CoS)
 CRL. *See* Certificate Revocation List (CRL)

D

data authentication, described 489
 data bits parameter 40
 data compression parameter 539
 Data Encryption Standard (DES), described 486
 data encryption, described 486
 daylight savings time (DST) parameter 62, 589,
 822
 default configuration file parameter 163, 821
 default gateway parameter 49, 585
 default values, AT-S60 820
 default VLAN name parameter 404, 837
 DER certificate format 522
 DES privacy protocol 296
 DES. *See* Data Encryption Standard (DES)
 DHCP. *See* Dynamic Host Control Protocol
 (DHCP)
 digital certificates. *See* certificates
 digital signatures 503
 display mode parameter 825
 display module parameter 825
 display order parameter 825
 display output parameter 825
 display severity parameter 825
 distinguished name
 creating 491, 585
 defined 491
 distinguished name parameter 492, 585, 827
 document conventions 24
 documentation 25
 dynamic GVRP port 445
 dynamic GVRP VLAN 445
 Dynamic Host Control Protocol (DHCP)
 activating 57, 591
 defined 57
 dynamic MAC address, defined 117

E

ECB. *See* Electronic Code Book (ECB)
 edge port
 diagram 236
 Multiple Spanning Tree Protocol (MSTP)
 290, 690
 Rapid Spanning Tree Protocol (RSTP) 253
 edge port parameter 253, 290, 835
 Electronic Code Book (ECB), described 486
 encryption (ENCO) 485
 encryption (SSL) 525
 encryption key
 creating 491
 deleting 495
 displaying 788
 exporting 497
 importing 498
 modifying 495
 Secure Shell (SSH) 531
 encryption key parameter 800, 802, 830
 encryption secret parameter, 800
 End Entity 504
 Engine ID, defined 295
 enhanced stacking
 changing switches 81, 617
 configuring 80, 616
 defined 42, 46, 76
 diagram 78
 guidelines 76
 setting switch status 79, 615
 Ethernet port statistics, displaying 112
 Event Log
 clearing 213, 661
 configuring 205, 656
 disabling 205, 656
 displaying 207, 658
 enabling 205, 656
 overview 204
 saving to a file 212, 660
 severity codes 209
 software modules list 210
 event logging parameter 825

F

factory defaults
 list 820
 resetting 72, 606

file system, overview 153
 files
 downloading 172, 180
 naming 154
 uploading 187, 194
 flow control parameter 40, 104, 108, 625, 629, 828
 force version parameter
 default 835
 Multiple Spanning Tree Protocol (MSTP) 277, 683
 Rapid Spanning Tree Protocol (RSTP) 249, 677
 format parameter 522, 827
 forwarding delay parameter 835
 forwarding delay, described 233

G

GARP Information Declaration (GID), diagram 451
 GARP Information Propagation (GIP), defined 449
 GARP VLAN Registration Protocol (GVRP)
 configuring 453
 database 463
 diagram 446
 disabling on a port 455
 displaying
 GVRP state machine 465
 parameters 458, 771, 773
 statistics 458
 enabling on a port 455
 GIP connected ports ring 464
 guidelines 447
 GVRP counters 459
 GVRP state machine, displaying 465
 intermediate switches 448
 overview 445
 parameters, displaying 458, 771, 773
 port configuration, displaying 772
 port configuration, modifying 770
 resetting to defaults 769
 security issues 448
 statistics, displaying 458
 GARP. *See* Generic Attribute Registration Protocol (GARP)
 gateway address

 configuring 49, 585
 displaying 593
 gateway address parameter 49, 585, 823
 Generic Attribute Registration Protocol (GARP)
 Applicant state machine 451
 defined 449
 diagram 450
 overview 449
 Registrar state machine 452
 GID index parameter 463, 777
 GID. *See* GARP Information Declaration (GID)
 GIP connected ports ring 464
 GIP. *See* GARP Information Propagation (GIP)
 global encryption key parameter 547, 801, 830
 global secret parameter 799
 global server timeout parameter 547, 800, 801
 global server timeout period parameter 830
 GVRP counters 459
 GVRP database 463
 GVRP GIP status parameter 453, 768, 837
 GVRP join timer parameter 454, 768, 837
 GVRP leave all timer parameter 454, 768, 837
 GVRP leave timer parameter 454, 768, 837
 GVRP status parameter 453, 768, 837
 GVRP. *See* GARP VLAN Registration Protocol (GVRP)

H

hardware information 68, 594
 hash algorithm 489
 hello time parameter
 default 834, 835
 Multiple Spanning Tree Protocol (MSTP) 278
 Rapid Spanning Tree Protocol (RSTP) 250
 Spanning Tree Protocol (STP) 243
 hello time, described 234
 HMAC authentication algorithm 489
 HMAC-MD5-96 (MD5) authentication protocol 295
 HMAC-SHA-96 (SHA) authentication protocol 295
 HOL blocking parameter 108, 623, 828
 host key ID parameter 536, 832
 host nodes, displaying 666, 816
 host/router timeout interval parameter 222, 664, 826

HTTP 478
 HTTPS 478

I

IEEE 802.1d standard 242, 248, 672, 676
 IGMP snooping status parameter 222, 663, 826
 IGMP snooping. *See* Internet Group Management Protocol (IGMP) snooping
 image file
 downloading 173
 uploading 188
 inner CBC encryption mode 487
 Internet Group Management Protocol (IGMP)
 snooping
 configuring 221, 663
 disabling 221, 663
 displaying
 host nodes 224
 multicast routers 226
 enabling 221, 663
 host nodes, displaying 224
 multicast routers, displaying 226
 overview 219
 Internet Protocol (IP) address
 configuring 49, 585
 defined 46
 displaying 593
 intruder action parameter 786
 intrusion action parameter 475, 829
 IP address parameter 49, 585, 823

K

key exchange algorithms 490
 key pair ID parameter 522, 827

L

Limited security level 470, 785
 line cards, displaying
 information 51
 statistics 53
 link parameter 104, 628
 local management session
 defined 29
 quitting 42
 starting 39
 Lock All Ports security level 786
 Locked security level 471

log full action parameter 825
 login timeout parameter 537, 832

M

MAC (message authentication code)
 definition 525
 MAC address aging time parameter 126, 586, 640, 823
 MAC address table
 defined 116
 displaying 118, 634
 MAC addresses
 adding 122, 637
 defined 116
 deleting 124, 639
 displaying 118, 634
 MAC limit parameter 476, 786, 829
 MAC. *See* Message Authentication Code (MAC)
 MACs available parameter 539
 Main Menu 41
 management access levels 33, 65
 Management Information Base. *See* MIBs
 management VLAN 433
 management VLAN ID parameter 434, 837
 Manager access 33, 65
 Manager password 65, 586
 manager password parameter 821
 master switch
 assigning 79, 615
 defined 79
 defined, 615
 returning to 83, 619
 max age parameter
 default 834, 835
 Multiple Spanning Tree Protocol (MSTP) 278
 Rapid Spanning Tree Protocol (RSTP) 250
 Spanning Tree Protocol (STP) 244
 max hops parameter
 default 835
 Multiple Spanning Tree Protocol (MSTP) 278, 684
 maximum multicast groups parameter 222, 826
 maximum number of certificates parameter 509, 827
 maximum number of sessions parameter 528, 833

- MCHECK parameter 254, 290, 679
- MD5 authentication algorithm 489
- MD5 authentication protocol 295
- Message Authentication Code (MAC),
described 489
- message encryption 503
- MIB Subtree view 297
- MIB tree
 - diagram 297
 - RFC 296
- MIB view 296
- MIBs
 - viewing 295
- MIBs, supported 32
- mode (web server) parameter 480
- mode parameter 838
- MSTI association to a VLAN
 - creating 286
 - removing 286
- MSTI ID association to a VLAN
 - adding 687
 - modifying 688
- MSTI priority, defined 266
- MSTI. *See* Multiple Spanning Tree Instance (MSTI)
- multicast groups, maximum 222, 665
- multicast host topology parameter 222, 663, 826
- multicast MAC address
 - adding 122, 637
 - deleting 124, 639
 - displaying 118, 634
- multicast router ports mode parameter 223, 664, 826
- multicast routers, displaying 226, 666
- Multiple Spanning Tree Instance (MSTI)
 - associating to VLANs 687
 - defined 259
 - diagram 262
 - guidelines 263
 - MSTI ID
 - associating to VLANs 287
 - creating 685
 - deleting 282, 686
 - list 281
 - modifying 283, 686
 - removing a VLAN association 287
 - port priority 281
 - removing a VLAN association 687
- Multiple Spanning Tree Protocol (MSTP)
 - associating VLANs to MSTI ID 283
 - associating VLANs to MSTI IDs 687
 - associations 263
 - bridge forwarding delay 278, 683
 - bridge hello time 278, 683
 - bridge identifier 279
 - bridge max age 278, 683
 - bridge settings, configuring 277, 681
 - configuration name 264, 278, 683
 - configuring 274, 681
 - connecting to VLANs 271, 687
 - diagram 261
 - disabling 240, 274, 670
 - edge port 290, 690
 - enabling 240, 274, 670
 - force version 277, 683
 - max hops 278, 684
 - MSTI ID
 - creating 280, 685
 - deleting 280, 686
 - modifying 283, 686
 - MSTI priority, defined 266
 - overview 258
 - parameters, displaying 691
 - point-to-point port 289, 690
 - port external path cost 289, 690
 - port internal path cost 289, 689
 - port parameters, configuring 288, 689
 - port priority 289, 689
 - port settings, displaying 290, 691
 - port status, displaying 291
 - regional root 266
 - regions 263
 - revision level 278
 - revision number 264
 - with STP and RSTP 268
- multiple VLAN
 - 802.1Q compliant 437
 - 802.1Q-compliant 437
 - defined 436
 - mode
 - activating 440
 - deactivating 440
 - non-802.1Q compliant 438

- non-802.1Q compliant multiple VLANs 438
 - overview 436
 - uplink port, changing 442
- N**
- negotiation parameter 104, 109, 622, 822, 828
 - none port role 552
 - NonVolatile storage, described 297
- O**
- OFB. *See* Output Feedback (OFB)
 - open acc(ess) parameter 90
 - openacc parameter 831
 - Operator access 33, 65
 - Operator password 65, 586, 822
 - outer CBC encryption mode 487
 - Output Feedback (OFB), described 487
 - override priority parameter 107, 623, 828
- P**
- parity parameter 40
 - participating parameter 786, 829
 - password
 - changing 49, 586
 - default 44
 - path cost parameter 281
 - path cost, defined 231
 - PEM certificate format 522
 - pinging 71, 605
 - PKI certificates
 - adding to database 513
 - certificate database 507
 - chains 505
 - creating 508
 - database storage 507
 - deleting 515
 - described 503
 - displaying 518
 - modifying 515
 - validating 505
 - PKI. *See* Public Key Infrastructure (PKI)
 - point-to-point (port) parameter 253, 289, 835
 - point-to-point port
 - Multiple Spanning Tree Protocol (MSTP) 289, 690
 - Rapid Spanning Tree Protocol (RSTP) 253
 - point-to-point ports, Rapid Spanning Tree Protocol (RSTP) 680
 - poll interval parameter 62, 590, 822
 - port
 - configuring parameters, basic 106, 621
 - disabling 107, 624
 - specifying 34
 - statistics, displaying 630
 - status, displaying 626
 - port access control parameter 557, 839
 - port cost parameter 835
 - default 834
 - Multiple Spanning Tree Protocol (MSTP) 689
 - Rapid Spanning Tree Protocol (RSTP) 253, 679
 - Spanning Tree Protocol (STP) 246, 675
 - port cost, defined 231
 - port external path cost parameter 289, 835
 - port internal path cost parameter 289, 836
 - port mirror
 - creating 144, 649
 - deleting 146, 148, 651
 - destination port mirror
 - deleting 148, 651
 - disabling 150
 - enabling 149
 - displaying 654
 - modifying 652
 - source mirror, deleting 146, 651
 - port mirroring, defined 143
 - port mode parameter 456, 837
 - port number (web server) parameter 480
 - port number parameter 838
 - port parameters, configuring
 - basic 106
 - Multiple Spanning Tree Protocol (MSTP) 288, 681
 - Rapid Spanning Tree Protocol (RSTP) 252, 254, 676
 - Spanning Tree Protocol (STP) 245, 672
 - port priority parameter 835
 - default 834, 836
 - displaying 105
 - Multiple Spanning Tree Instance (MSTI) 281
 - Multiple Spanning Tree Protocol (MSTP) 289, 689

- Rapid Spanning Tree Protocol (RSTP) 253, 679
 - Spanning Tree Protocol (STP) 246, 675
 - port priority, defined 232
 - port role parameter 560, 810, 839
 - port security
 - Automatic level 470, 785
 - configuring 473
 - defined 470
 - displaying 784
 - Limited level 470
 - Lock All Ports level 786
 - Locked level 471
 - overview 470
 - Secured level 471, 785
 - security violations 472
 - port security intrusion actions 472, 786
 - port security violations 472, 786
 - port speed parameter 104, 109, 622
 - port statistics, displaying 112
 - port status parameter 624, 828
 - port status, displaying, Rapid Spanning Tree Protocol (RSTP) 254
 - port trunk
 - creating 132, 642
 - deleting 134, 644
 - displaying 647
 - modifying 135, 645
 - name, changing 137
 - ports
 - adding 137
 - deleting 139
 - replacing 140
 - port trunking
 - defined 128
 - diagram 128
 - guidelines 129
 - port VLAN identifier (PVID), defined 405
 - port-based access control. *See* 802.1x port-based network access control
 - port-based VLAN
 - creating 421, 756
 - creating, example 425
 - defined 404
 - deleting 431, 762
 - diagram 408
 - displaying 443, 763
 - drawbacks 406
 - modifying 427, 760
 - overview 404
 - rules 406
 - privacy 296
 - private keys 502
 - public key encryption 502
 - Public Key Infrastructure (PKI)
 - Certificate Authority (CA), root 506
 - certificate database 507
 - certificates
 - adding 507
 - adding to database 513
 - chains 505
 - creating 508
 - deleting 515
 - displaying 518, 790
 - fingerprint 507
 - modifying 515
 - retrieving 507
 - validating 505
 - certification authority 505
 - End Entity 504
 - overview 502
 - standards 507
 - structure 504
 - X.509 certificates 503
- R**
- RADIUS
 - configuring 547, 801
 - disabling 544, 797
 - enabling 544, 797
 - overview 541
 - settings, displaying 803
 - setup overview 542
 - RADIUS accounting
 - described 556
 - RADIUS server configuration parameter 548, 830
 - Rapid Spanning Tree Protocol (RSTP)
 - bridge forwarding delay 250, 678
 - bridge hello time 250, 678
 - bridge identifier 678
 - bridge max age 250, 678
 - bridge priority 249, 677
 - bridge settings, configuring 248, 676

- configuring 248, 676
 - disabling 240, 274, 670
 - edge port, configuring 253, 680
 - enabling 240, 274, 670
 - force version 249, 677
 - MCHECK 254, 290, 679
 - overview 229
 - parameters, displaying 691
 - point-to-point ports
 - configuring 253, 680
 - described 235
 - diagram 235
 - port cost 253, 679
 - port parameters, configuring 252, 254, 677
 - port priority 253, 679
 - port settings, displaying 691
 - port state, displaying 254
 - port status, displaying 254
 - Rapid Spanning Tree Protocol (STP)
 - bridge parameters, configuring 248
 - reg (registrar state machine) parameter 467, 782
 - regional root ID parameter 281
 - regional root path cost parameter 281
 - regional root, described 266
 - Remote Authentication Dial In User Services.
 - See RADIUS
 - request name parameter 522, 827
 - revision level parameter 278, 684, 835
 - revision number 264
 - root bridge, described 230
 - RS-232 port default settings 822
 - RS-232 port, default settings 40
 - RSTP. See Rapid Spanning Tree Protocol (RSTP)
- S**
- Secure Shell (SSH)
 - AT-8400 switch implementation 530
 - ciphers 530
 - clients, described 532
 - configuration overview 534
 - encryption algorithms 530
 - encryption keys 531
 - overview 530
 - server
 - configuring 535
 - described 531
 - displaying information 538
 - users
 - adding 531
 - deleting 531
 - modifying 531
 - Secure Sockets Layer (SSL)
 - certificates
 - authenticating 526
 - described 526
 - certificates, configuring 481
 - configuring 528
 - data transfer 525
 - displaying 794
 - encryption 525
 - message types 525
 - overview 524, 527
 - session 525
 - user verification 525
 - Secured security level 471, 785
 - security mode parameter 474, 785, 829
 - security. See 802.1x port-based network access control
 - self-signed certificates
 - configuring 481
 - described 481
 - server authentication UDP port parameter 548
 - server encryption key parameter 548, 802
 - server key expiry time parameter 536, 832
 - server key ID parameter 536, 832
 - server port (SSH) parameter 539
 - server timeout parameter 800
 - server-based authentication parameter 544, 797, 830
 - session cache timeout parameter 528, 833
 - set password parameter 49
 - SHA authentication algorithm 489
 - SHA authentication protocol 295
 - Simple Network Management Protocol. See SNMP
 - Simple Network Time Protocol (SNTP)
 - configuring 59, 590
 - servers 59

- slave switch
 - assigning 79, 615
 - defined 79, 615
- SNMP community
 - configuring 88, 595
 - deleting 91, 601
 - displaying 100, 601
 - enabling 86, 595
 - modifying 92, 599
- SNMP community access
 - configuring 696
 - enabling 696
- SNMP management session 32, 64
- SNMP status parameter 87, 831
- SNMP. *See* Simple Network Management Protocol (SNMP)
- SNMPv3 Access Table entry
 - creating 324, 710
 - deleting 329, 714
 - displaying 394, 749
 - modifying 714
 - notify view 336
 - read view 331
 - storage type 338
 - write view name 334
- SNMPv3 Access Table, described 301
- SNMPv3 community 381
- SNMPv3 Community Table entry
 - creating 382, 740
 - deleting 385, 743
 - displaying 399, 754
 - modifying 743
 - community name 386
 - security name 388
 - storage type 389
 - transport tag 388
- SNMPv3 Community Table, described 303
- SNMPv3 Engine ID, defined 295
- SNMPv3 Notify Table entry
 - creating 348, 722
 - deleting 350, 724
 - displaying 396, 751
 - modifying 724
 - notify tag 351
 - storage type 354
- SNMPv3 Notify Table, described 302
- SNMPv3 protocol
 - authentication protocols 295
 - community name parameter 383, 742, 744
 - Engine ID 295
 - message notification 297
 - MIB views 296
 - overview 294
 - privacy protocols 296
 - SNMPv3 Access Table 301, 710
 - SNMPv3 Community Table 303, 740
 - SNMPv3 Notify Table 302, 722
 - SNMPv3 SecurityToGroup Table 302, 717
 - SNMPv3 Target Address Table 302, 727
 - SNMPv3 Target Parameters Table 302, 733
 - SNMPv3 User Table 301, 698
 - SNMPv3 View Table 301, 705
 - storage types 297
 - tables 298
- SNMPv3 SecurityToGroup Table entry
 - creating 340, 717
 - deleting 343, 719
 - displaying 395, 750
 - modifying 720
 - group name 344
 - storage type 346
- SNMPv3 SecurityToGroup Table, described 302
- SNMPv3 Target Address Table entry
 - creating 356, 727
 - deleting 358, 730
 - displaying 397, 752
 - modifying 730
 - storage type 366
 - target address retries 363
 - target address tag list 364
 - target address timeout 362
 - target address UDP port 361
 - target IP address 360
 - target parameters 365
- SNMPv3 Target Address Table, described 302
- SNMPv3 Target Parameters Table entry
 - creating 369, 733
 - deleting 372, 736
 - displaying 398, 753
 - modifying 737
 - message process model 378
 - security level 377
 - security model 376

- storage type 380
- user name 374
- SNMPv3 Target Parameters Table, described 302
- SNMPv3 trap 297
- SNMPv3 User Table entry
 - creating 305, 698
 - deleting 309, 701
 - displaying 391, 747
 - modifying 702
 - authentication protocol 310
 - authentication protocol password 310
 - privacy protocol 312
 - privacy protocol password 312
- SNMPv3 User Table, described 301
- SNMPv3 View Table entry 319, 321
 - creating 315, 705
 - deleting 318, 707
 - displaying 393, 748
 - modifying 708
 - storage type, modifying 322
- SNMPv3 View Table, described 301
- snoop topology 222, 663
- SNTP server (IP address) parameter 61, 590
- SNTP server parameter 61, 822
- SNTP status parameter 61, 590, 822
- SNTP. *See* Simple Network Time Protocol (SNTP)
- software updates
 - downloading from a local session 172
 - downloading switch to switch 201
 - uploading 188
- Source Address (SA) Trunking load distribution method 131
- Spanning Tree Protocol (STP)
 - and VLANs 237
 - bridge forwarding delay 244, 674
 - bridge hello time 243, 674
 - bridge identifier 244, 674
 - bridge max age 244, 674
 - bridge parameters, configuring 242, 672
 - bridge priority 243, 673
 - defined 229
 - disabling 240, 274, 670
 - enabling 240, 274, 670
 - forwarding delay 244
 - overview 229
 - parameters, displaying 691
 - port cost 246, 675
 - port cost, defined 232
 - port parameters, configuring 245
 - port priority 246, 675
 - port settings, displaying 247, 691
 - SSH server status parameter 536, 832
 - SSH. *See* Secure Shell (SSH)
 - SSL key ID parameter 480, 838
 - SSL messages 525
 - SSL. *See* Secure Sockets Layer (SSL)
 - starting session
 - local 39
 - Telnet 43
 - web browser 579
 - static unicast MAC address
 - adding 122, 637
 - defined 117
 - deleting 124, 639
 - displaying 118, 634
 - status (of a port) parameter 103, 828
 - status (web server) parameter 480, 838
 - stop bits parameter 40
 - STP ID parameter 464, 779
 - STP state parameter 105, 822
 - STP. *See* Spanning Tree Protocol (STP)
 - subject distinguished name parameter 512
 - subnet mask
 - configuring 49, 585
 - displaying 593
 - subnet mask parameter 49, 585, 823
 - subtree mask 297
 - subtree mask, modifying 319
 - supplicant port
 - described 550
 - supplicant role 553
 - switch
 - hardware information 68, 592
 - rebooting 63
 - resetting 63, 604
 - software information 69, 592
 - switch mode parameter 586, 594, 823
 - switch name, configuring 48, 583
 - switch state parameter 80, 824
 - symmetrical encryption 486

system configuration file

- copying 162
- creating 158
- renaming 162
- setting 156
- viewing 159
- See also* system files

system files

- copying 162
- deleting 163
- displaying 165
- downloading 180
- renaming 162
- uploading 188
- See also* system configuration file
- system name parameter 49, 585, 823
- system name, configuring 49, 585
- system software default settings 823
- system time parameter 61, 588, 822
- system time, setting 59, 588

T

- TAC global secret parameter 546, 830
- TAC server order parameter 546, 830
- TAC server parameter 545, 830
- TAC timeout parameter 546, 830

TACACS+

- configuring 545, 799
- disabling 544, 797
- enabling 544, 797
- overview 541
- settings, displaying 803
- setup overview 542

tagged VLAN

- creating 421, 426, 756
- creating, example 426
- defined 412
- deleting 431, 762
- diagram 415
- displaying 443, 763
- modifying 427, 760
- overview 412
- rules 414

target IP address 348

Telnet management interface, quitting 44

Telnet management session

- defined 30
- disabling 64
- starting 43

Terminal Access Controller Access Control System. *See* TACACS+

TFTP, downloading and uploading files 172

Triple DES (3DES) encryption algorithms, described 487

type (of certificate) parameter 514, 791

type parameter 827

U

unavailable status, defined 79, 615

uplink port parameter 440, 837

uplink port, changing 442

used parameter 463, 777

user name

configuring 567, 815

user name, default 41, 44

user password

configuring 567, 815

User-based Security Model (USM)

authentication 294

UTC offset parameter 62, 589, 822

V

versions supported (SSH) parameter 538

view type, modifying 321

virtual LAN (VLAN)

creating 421, 426, 756

defined 402

deleting 431, 762

displaying 418, 443, 763

mode, changing 432, 765

modifying 427, 760

multiple

802.1Q-compliant 437

defined 436

non-802.1Q compliant 438

overview 436

overview 402

port-based, defined 404

tagged, defined 412

See also port-based VLAN*See also* tagged VLAN

Virtual LANs (VLANs)

- associating to MSTI IDs 687
- VLAN and MSTI associations 263
- VLAN ID parameter 463, 777
- VLAN identifier (VID) 404, 423, 758
- VLAN mode parameter 440, 837
- VLAN, port-based. *See* port-based VLAN
- VLAN, tagged. *See* tagged VLAN
- VLAN. *See* virtual LAN (VLAN)
- Volatile storage 297

W

- web browser management session
 - defined 31
 - disabling 64
 - limitations 31
 - quitting 581
 - starting 579
- web server
 - configuring 479
 - overview 478
- web server mode parameter 480
- web server status parameter 480, 838

X

- X.509
 - certificate 504
 - specification 503