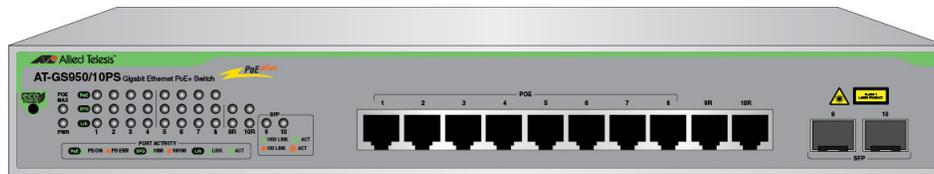


AT-GS950/10PS

Gigabit Ethernet PoE+ Switch



2632

AT-GS950/10PS Switch Web Interface User's Guide

AT-S110 [1.00.013]

Copyright © 2013 Allied Telesis, Inc.

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

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

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

Contents

List of Figures	9
List of Tables	13
Preface	15
Document Conventions.....	16
Allied Telesis Contact Information.....	17
Getting Started	19
Chapter 1: Starting a Web Browser Session	21
Establishing a Remote Connection to the Web Browser Interface	22
Web Browser Tools.....	25
Quitting a Web Browser Management Session	26
Chapter 2: System Configuration	27
System Management Information	28
Configuration of IP Address, Subnet Mask and Gateway Address.....	30
IP Access List Configuration	32
Create an IP Access List	32
Delete an IP Address List Entry.....	33
User Name and Password Configuration.....	34
Add New User Name and Password	34
Modify User Name and Password	35
Delete User Name and Password	36
User Interface Configuration	37
SNMP Interface	37
User Interface Timeout.....	38
System Time	39
Manually Setting System Time	39
Setting SNTP.....	40
Setting Daylight Savings Parameters	41
SSL Settings	42
Configuring SSL	42
DHCP and ATI Web Discovery Tool	44
DHCP Client Configuration	45
DHCP Auto Configuration	47
System Information Display	48
System Log Configuration.....	50
Bridge Configuration	53
Chapter 3: Port Configuration	55
Overview	56
Displaying and Configuring Ports.....	57
Chapter 4: STP and RSTP	61
Overview	62
Bridge Priority and the Root Bridge	63

Forwarding Delay and Topology Changes	65
Mixed STP and RSTP Networks	67
Spanning Tree and VLANs	68
Basic STP and RSTP Configuration	70
Configure RSTP Port Settings	73
Configure the Basic RSTP Port Settings	73
Configure the Advanced RSTP Port Settings	75
Spanning Tree Topology	78
Chapter 5: Multiple Spanning Tree Protocol	79
Multiple Spanning Tree Configuration	80
Port Configuration	83
VLAN Mapping	86
Open MSTP VLAN Mapping Page	86
Create VLAN Mapping to MST Instance	86
Modify MST Instance	87
Delete MST Instance	87
Port Settings	88
Topology Information	90
Chapter 6: Static Port Trunking	93
Overview	94
Create a Port Trunk	97
Modify a Port Trunk	99
Disable a Port Trunk	101
Chapter 7: LACP Port Trunks	103
Overview	104
System Priority	105
Port Priority Value	106
General Guidelines	107
Group Status	109
Configuration Example	110
Port Priority Configuration	112
Chapter 8: Port Mirroring	113
Overview	114
Port Mirroring Configuration	115
Disable Port Mirroring	117
Chapter 9: Loopback Protection	119
Configuration	120
Status	122
Chapter 10: MAC Address Table	123
Overview	124
Static Unicast MAC Address Configuration	126
Modify Static Unicast Address	128
Delete Static Unicast Address	129
Static Multicast Address Configuration	130
Modify Static Multicast Address	133
Delete Static Multicast Address	134
Chapter 11: IGMP Snooping	135
Overview	136
IGMP Snooping Configuration	138
Chapter 12: Storm Control	141
Overview	142

Ingress Rate Limiting	143
Egress Rate Limiting	143
Configuration	144
Ingress Rate Limiting	146
Egress Rate Limiting	148
Chapter 13: Virtual LANs	149
VLAN Overview	150
Port-based VLAN Overview	151
Tagged VLAN Overview	152
General Rules for Creating a Tagged VLAN	154
Assign Ports to a VLAN Mode	155
Tagged VLAN Configuration	157
Create a Tagged VLAN	157
Modify a Tagged VLAN	158
Delete a Tagged VLAN	160
Tagged VLAN Port Settings	162
Port-Based VLAN Configuration	164
Create a Port-Based VLAN	164
Modify a Port-Based VLAN	165
Chapter 14: GVRP	167
Overview and Guidelines	168
General Configuration	169
Port Settings	170
Time Settings	172
Chapter 15: Quality of Service and Cost of Service	175
Overview	176
Packet Priority	176
Egress Queue vs Packet Priority Mapping	177
Prioritizing Untagged Packets	178
Scheduling	178
Mapping CoS Priorities to Egress Queues	180
Associate Ports to CoS Priorities	182
Associate DSCP Classes to Egress Queues	183
Queue Scheduling Algorithm	185
Advanced Features	187
Chapter 16: SNMPv1 and v2c	189
SNMPv1 and SNMPv2c Overview	190
Trap Receiver Attributes	191
Activate SNMP Interface	192
SNMPv1 and SNMPv2c User and Group Names	193
Create User and Group Names	193
Modify User and Group Names	194
Delete User and Group Names	195
SNMP Community Strings	196
Create SNMP Community Strings	196
Modify SNMP Community Strings	197
Delete SNMP Community Strings	197
SNMP Traps	198
Create Trap Host Table Entry	198
Modify a Trap Host Table Entry	199
Delete a Trap Host Table Entry	199
Chapter 17: SNMPv3	201

Overview	202
SNMPv3 Authentication Protocols	202
SNMPv3 Privacy Protocol	203
SNMPv3 MIB Views	203
SNMPv3 Configuration Process	204
SNMPv3 User and Group Names	206
Creating SNMPv3 User and Group Names	206
Modifying SNMPv3 User and Group Names	207
Deleting SNMPv3 User and Group Names	207
SNMPv3 View Names	209
Creating SNMPv3 View Names	209
Modifying SNMPv3 View Names	211
Deleting SNMPv3 View Names	211
SNMPv3 View Table	212
Creating SNMPv3 View Table Entries	212
Modifying SNMPv3 View Table Entries	213
Deleting SNMPv3 View Table Entries	213
SNMPv3 Traps	215
Chapter 18: Access Control Configuration	217
Overview	218
Classifier	219
Creating a Classifier	219
Modifying a Classifier	221
Deleting a Classifier	222
Profile Action	224
Creating a Profile Action	224
Modifying Profile Action	225
Deleting a Profile Action	226
In-Profile Action	227
Creating an In-Profile Action	227
Modifying an In-Profile Action	229
Deleting an In-Profile Action	230
Out-Profile Action	231
Creating a Out-Profile Action	231
Modify Out-Profile Action	233
Delete Out-Profile Action	234
Port List	235
Create Port List	235
Modify Port List	236
Delete Port List	237
Policy	238
Create Policy	238
Modify Policy	240
Delete Policy	241
Policy Sequence Status	243
Chapter 19: RMON	245
Overview	246
Enable and Disable RMON	247
Port Statistics	248
Histories	250
Events	252
Alarms	254
Chapter 20: Voice VLAN	257

Overview	258
CoS with Voice VLAN	258
Organization Unique Identifier (OUI)	258
Dynamic Auto-Detection vs Static Ports	259
General Guidelines	261
Configuration	262
OUI Setting.....	265
Create OUI Setting	265
Modify OUI Setting	266
Delete OUI Setting.....	266
Chapter 21: Security	267
Port Access Control	268
Overview.....	268
Port Access Control Configuration	269
RADIUS Client	273
Overview.....	273
General Guidelines	273
Radius Client Configuration	274
Dial-in User— Local Authentication	276
Overview.....	276
Dial-in User Configuration	276
Destination MAC Filter	279
Overview.....	279
Destination MAC Filter Configuration	279
Delete Destination MAC Filter	280
Chapter 22: Power Over Ethernet (PoE)	283
Overview	284
Power Sourcing Equipment (PSE)	284
Powered Device (PD).....	284
PD Classes	284
Power Budget	284
Port Prioritization	285
PoE Configuration.....	286
Chapter 23: Chapter 23: DHCP Snooping	290
Overview	291
Trusted Ports	291
Untrusted Ports.....	291
Unauthorized DHCP Servers.....	291
DHCP with Option 82	292
General Guidelines	293
General Configuration	294
VLAN Setting.....	296
Creating a VLAN.....	296
Modifying a VLAN.....	297
Deleting a VLAN	297
Trusted and Untrusted Port Configuration	298
Binding Database.....	300
Static IP Addresses	300
Viewing	301
Chapter 24: LLDP	303
Overview	304
Global Configuration	305
Enabling or Disabling LLDP	306

Displaying System Information.....	307
Setting Port States	307
Neighbors Information	309
Chapter 25: Network Statistics	311
Overview.....	312
Traffic Comparison Statistics.....	313
Error Group Statistics	316
Historical Status Charts	318
Tools	321
Chapter 26: Software/Configuration Updates	323
Overview.....	324
Upgrade Firmware Image via HTTP.....	325
Upgrade Firmware Image via TFTP	327
Upload or Download a Configuration File via HTTP.....	329
Configuration File Upload.....	329
Configuration File Download.....	331
Download or Upload a Configuration File via TFTP	332
Configuration File Upload.....	332
Configuration File Download.....	333
Chapter 27: Cable Diagnostics	335
Chapter 28: Rebooting the AT-GS950/10PS	337
Switch Reboot	338
Configure Factory Default Values.....	340
Password Protection of Factory Reset	342
Disabling Factory Default Reset Feature	342
Enabling Factory Default Reset	344
Chapter 29: Pinging a Remote System	347
Appendix A: MSTP Overview	349
Overview.....	350
Multiple Spanning Tree Instance (MSTI).....	352
Resolving VLAN Fragmentation.....	352
Multiple VLANs Assigned to an MSTI	353
General Guidelines.....	355
VLAN and MSTI Associations	356
Ports in Multiple MSTIs.....	357
Multiple Spanning Tree Regions	358
MST Region Guidelines	360
Common and Internal Spanning Tree (CIST)	362
MSTP with STP and RSTP	362
Associating VLANs to MSTIs.....	363
VLANs Across Different Regions.....	365
Summary of Guidelines	367
Appendix B: AT-GS950/10PS Default Parameters	369

List of Figures

Figure 1. Entering a Switch's IP Address in the URL Field.....	22
Figure 2. Management Login Dialog Box	22
Figure 3. AT-GS950/10PS Switch Information Page.....	23
Figure 4. Front Panel Page	24
Figure 5. AT-GS950/10PS Management Page	28
Figure 6. IP Setup Page	30
Figure 7. IP Access List Page	32
Figure 8. Administration Page	34
Figure 9. Modify Administration Page.....	35
Figure 10. User Interface Page	37
Figure 11. System Time Page	39
Figure 12. SSL Settings Page	42
Figure 13. DHCP Auto Configuration Settings Page	47
Figure 14. AT-GS950/10PS Switch Information Page.....	48
Figure 15. System Log Configuration Page.....	50
Figure 16. AT-GS950/10PS Physical Interface Page.....	57
Figure 17. Point-to-Point Ports	67
Figure 18. Edge Port	67
Figure 19. STP and VLAN Fragmentation with Untagged Ports.....	68
Figure 20. STP and VLAN Compatibility with Tagged Ports.....	69
Figure 21. Rapid Spanning Tree Configuration Page.....	70
Figure 22. AT-GS950/10PS RSTP Basic Port Configuration Page.....	73
Figure 23. AT-GS950/10PS RSTP Advanced Port Configuration Page.....	75
Figure 24. AT-GS950/10PS Designated Topology Information Page	78
Figure 25. Multiple Spanning Tree Configuration Page.....	80
Figure 26. AT-GS950/10PS MSTP Port Configuration Page	83
Figure 27. MSTP VLAN Mapping Page	86
Figure 28. MSTP Port Settings Page.....	88
Figure 29. AT-GS950/10PS Topology Information Page.....	90
Figure 30. Static Port Trunk Example.....	94
Figure 31. Trunking Page	97
Figure 32. LACP Group Status Page	109
Figure 33. LACP Group Status Page with No Cables Connected	110
Figure 34. LACP Group Status Page with Three Cables Connected	111
Figure 35. AT-GS950/10PS Port Priority Page.....	112
Figure 36. AT-GS950/10PS Mirroring Page	115
Figure 37. AT-GS950/10PS Loopback Detection Page.....	120
Figure 38. AT-GS950/10PS Static Unicast Address Table Page	126
Figure 39. Static Unicast Address Table with Port-Base VLAN Example.....	127
Figure 40. Modify Static Unicast Address Page	128
Figure 41. AT-GS950/10PS Static Multicast Address Table Page	130
Figure 42. Static Multicast Address Table Example	131
Figure 43. Modify Static Multicast Address Page	133
Figure 44. IGMP Snooping Page.....	138
Figure 45. IGMP Snooping Page with MAC Addresses	139
Figure 46. AT-GS950/10PS Storm Control Page	144
Figure 47. AT-GS950/10PS Ingress Rate Limiting Page.....	146
Figure 48. AT-GS950/10PS Egress Rate Limiting Page	148
Figure 49. AT-GS950/10PS VLAN Mode Page.....	155
Figure 50. AT-GS950/10PS Tagged VLAN Page.....	157

Figure 51. Example of AT-GS950/10PS Tagged VLAN Page	159
Figure 52. AT-GS950/10PS Modify VLAN Page.....	159
Figure 53. AT-GS950/10PS VLAN Port Setting Page	162
Figure 54. Port-Based VLAN Page.....	164
Figure 55. Example of AT-GS950/10PS Port Based VLAN Page	165
Figure 56. GVRP Global Configuration Page	169
Figure 57. GVRP Port Setting Page	170
Figure 58. AT-GS950/10PS GVRP Time Setting Page	172
Figure 59. CoS Page	180
Figure 60. AT-GS950/10PS Port Priority Page.....	182
Figure 61. DSCP Class Mapping Page.....	183
Figure 62. Scheduling Algorithm Page	185
Figure 63. SNMP User/Group Page	193
Figure 64. SNMP User/Group Page Example	194
Figure 65. Community Table Page	196
Figure 66. SNMP Community Table Page Example	197
Figure 67. Trap Management Page	198
Figure 68. Trap Management Page Example	199
Figure 69. MIB Tree	203
Figure 70. SNMPv3 Table Relationships	205
Figure 71. SNMP User Group, SNMPv3 Example.....	207
Figure 72. SNMP Group Access Table.....	209
Figure 73. SNMP Group Access Table Example for SNMPv3	210
Figure 74. SNMP View Table.....	212
Figure 75. SNMP View Table Page Example	213
Figure 76. Create Classifier Page.....	219
Figure 77. Create Classifier Example Page.....	221
Figure 78. Modify Classifier Page	222
Figure 79. Create Profile Action Page	224
Figure 80. Example of Profile Action Entry	225
Figure 81. Modify Profile Action Page.....	226
Figure 82. Create In-Profile Action Page Example	227
Figure 83. Example of In-Profile Action Entry.....	228
Figure 84. Modify In-Profile Action Page	229
Figure 85. Create Out-Profile Action Page	231
Figure 86. Example of Out-Profile Action Entry	232
Figure 87. Modify Out-Profile Action Page.....	233
Figure 88. Create Port List Page	235
Figure 89. Example of Port List Entry	236
Figure 90. Modify Port List Page.....	236
Figure 91. Create Policy Page.....	238
Figure 92. Example of Policy Entry.....	240
Figure 93. Modify Policy Page	241
Figure 94. Policy Sequence Page.....	243
Figure 95. Policy Sequence Page with Display by Index Selected.....	243
Figure 96. RMON Basic Settings Page.....	247
Figure 97. Ethernet Statistics Configuration Page.....	248
Figure 98. Ethernet Statistics Configuration Example	249
Figure 99. History Control Configuration Page	250
Figure 100. History Control Configuration Example Page	251
Figure 101. RMON Event Configuration Page.....	252
Figure 102. RMON Event Configuration Example Page.....	253
Figure 103. RMON Alarm Configuration Page.....	255
Figure 104. RMON Alarm Configuration Example Page (To be provided)	256
Figure 105. AT-GS950/10PS Voice VLAN Setting Page.....	262
Figure 106. Voice VLAN OUI Setting Page.	265
Figure 107. Port Access Control Configuration Page	269
Figure 108. Expanded Port Access Control Configuration Page	270
Figure 109. RADIUS Page.....	274
Figure 110. Dial-In User Page	277

Figure 111. Dial-In User Page Example	277
Figure 112. Destination MAC Filter Page	280
Figure 113. Destination MAC Filter Page Example	280
Figure 114. Power Over Ethernet Configuration Page	286
Figure 115. General Settings Page	294
Figure 116. DHCP Snooping VLAN Settings Page	296
Figure 117. AT-GS950/10PS Trusted Interfaces Page	298
Figure 118. Trusted Interfaces Page Example	299
Figure 119. AT-GS950/10PS Binding Database Page	300
Figure 120. Binding Database Page Example	301
Figure 121. AT-GS950/10PS LLDP Global Settings Page	305
Figure 122. LLDP Neighbors Information Page	309
Figure 123. Traffic Comparison Page	313
Figure 124. Error Group Chart Page	316
Figure 125. Historical Status Chart Page	318
Figure 126. Firmware Upgrade via HTTP Page	326
Figure 127. Firmware Upgrade via TFTP Page	328
Figure 128. Configuration File Upload/Download via HTTP Page	329
Figure 129. Result Page	330
Figure 130. File Download with HTTP	331
Figure 131. Configuration Upload/Download via TFTP Page	332
Figure 132. Cable Diagnostics Page	335
Figure 133. Factory Default Reset/Reboot Page	338
Figure 134. Factory Default Reset/Reboot Page with Password Entry	343
Figure 135. Factory Default Reset Disabled Page	344
Figure 136. Factory Default Reset/Reboot Page with Password Entry	345
Figure 137. Ping Test Configuration Page	347
Figure 138. Ping Test Results Page	348
Figure 139. VLAN Fragmentation with STP or RSTP	352
Figure 140. MSTP Example of Two Spanning Tree Instances	353
Figure 141. Multiple VLANs in a MSTI	354
Figure 142. CIST and VLAN Guideline - Example 1	363
Figure 143. CIST and VLAN Guideline - Example 2	364
Figure 144. Spanning Regions - Example 1	365
Figure 145. Spanning Regions without Blocking	366

List of Tables

Table 1. Bridge Priority Value Increments	63
Table 2. Valid Port Priority Values	65
Table 3. Default Mappings Priority Levels to Priority Queues	177
Table 4. Customized Mappings Priority Levels to Priority Queues	177
Table 5. Example of Weighted Round Robin Priority	179
Table 6. IEEE Powered Device Classes	284
Table 7. PoE Port Priorities	285
Table 8. Traffic Comparison Options	314
Table 9. Historical Status Options	319
Table 10. MSTP Region	359
Table 11. Regional Bridge Priority Value Increments	360
Table 12. AT-S110 Management Software Default Settings	369

Preface

This guide contains instructions on how to use the AT-S110 Management Software to manage and monitor the AT-GS950/10PS Gigabit Ethernet PoE+ Switch.

The AT-S110 Management software has a web browser interface that you can access from any management workstation on your network that has a web browser application.

This preface contains the following sections:

- ❑ “Document Conventions” on page 16
- ❑ “Allied Telesis Contact Information” on page 17

Document Conventions

This document uses the following conventions:

Note

Notes provide additional information.



Caution

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



Warning

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

Allied Telesis Contact Information

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

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

For sales or corporate contact information, go to **www.alliedtelesis.com/purchase** and select your region.

Section I

Getting Started

This section contains the following chapters:

- ❑ Chapter 1, “Starting a Web Browser Session” on page 21
- ❑ Chapter 2, “System Configuration” on page 27

Chapter 1

Starting a Web Browser Session

This chapter contains the procedures for starting, using, and quitting a web browser management session on the AT-GS950/10PS switch. This chapter includes the following sections:

- ❑ “Establishing a Remote Connection to the Web Browser Interface” on page 22
- ❑ “Web Browser Tools” on page 25
- ❑ “Quitting a Web Browser Management Session” on page 26

Establishing a Remote Connection to the Web Browser Interface

The AT-GS950/10PS switch is shipped with a pre-assigned IP address of 192.168.1.1. After your initial login, Allied Telesis suggests that you assign a new IP address to your switch. To manually assign an IP address to the switch, refer to “Configuration of IP Address, Subnet Mask and Gateway Address” on page 30. To configure the switch to obtain its IP configuration from a DHCP server, refer to “DHCP Client Configuration” on page 45.

Whether you use the pre-assigned IP address or assign a new one, you must set your local PC to the same subnet as the switch.

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

1. Start your web browser.
2. In the URL field of the browser, enter 192.168.1.1.

This is the default IP address of the switch. See Figure 1.



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

The AT-S110 Management Software displays the login dialog box. See Figure 2.

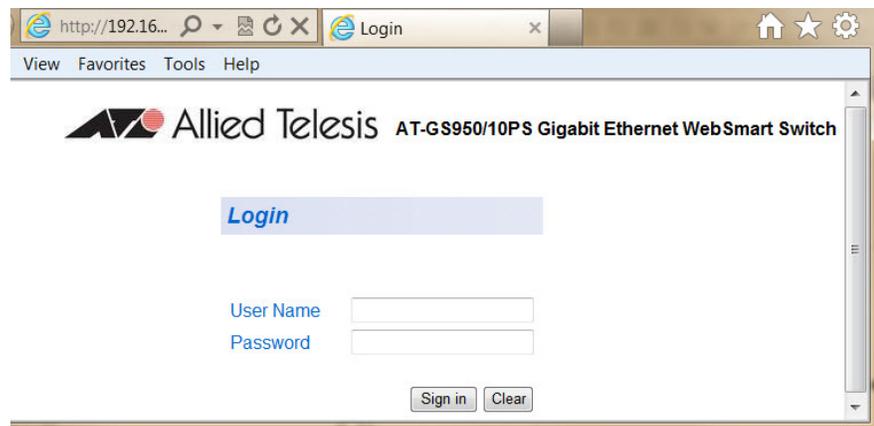


Figure 2. Management Login Dialog Box

3. Enter the AT-S110 management login user name and password.

The default user name is “manager” and the default password is “friend.” The login name and password are case-sensitive.

4. Press **OK**.

The AT-GS950/10PS Switch Information page is displayed. See Figure 3.

Note

To change the user name and password, refer to “User Name and Password Configuration” on page 34.

Switch Information	
System Up For:	0 day(s), 0 hr(s), 0 min(s), 23 sec(s)
Runtime Image:	AT-S110 V1.0.0 [1.00.013]
Boot Loader:	1.01.006
Hardware Information	
• Version:	A1
• DRAM Size:	128 M
• Flash Size:	16 M
Administration Information	
• System Name:	
• System Location:	
• System Contact:	
System MAC Address, IP Address, Subnet Mask and Gateway	
• MAC Address:	EC:CD:6D:10:00:80
• IP Address:	192.168.1.1
• Subnet Mask:	255.255.255.0
• Default Gateway:	0.0.0.0
Automatic Network Features	
• DHCP Client Mode:	Disable
• BOOTP Client Mode:	Disable

Figure 3. AT-GS950/10PS Switch Information Page

The main menu appears on the left side and is common for all of the management pages discussed in this manual. It consists of the following folders and web pages:

- Switch Info
- Front Panel
- System
- Physical Interface
- Bridge
- SNMP
- Access Control
- RMON
- Voice VLAN
- Security

- LLDP
 - Statistics Chart
 - Tools
 - Save Configuration
5. To see the front panel of the switch, select **Front Panel** from the main menu on the left side of the page.

The AT-S110 Management software displays the front of the switch. Ports are green that have a link to an end node. Ports without a link are grey. The AT-GS950/10PS switch front panel page is shown in Figure 4.

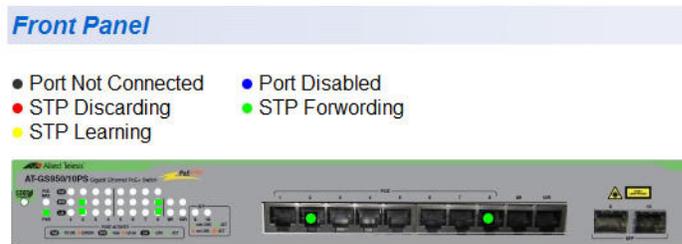


Figure 4. Front Panel Page

A web browser management session remains active even if you link to other sites. You can return to the management web pages anytime as long as you do not quit your browser session or the management session does not time out. The default time-out is 10 minutes.

Web Browser Tools

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

Quitting a Web Browser Management Session

To exit a web browser management session, close the web browser.

Chapter 2

System Configuration

This chapter provides procedures to configuring basic system parameters for the AT-GS950/10PS switch and contains information for the following sections:

- ❑ “System Management Information” on page 28
- ❑ “Configuration of IP Address, Subnet Mask and Gateway Address” on page 30
- ❑ “IP Access List Configuration” on page 32
- ❑ “User Name and Password Configuration” on page 34
- ❑ “User Interface Configuration” on page 37
- ❑ “System Time” on page 39
- ❑ “SSL Settings” on page 42
- ❑ “DHCP and ATI Web Discovery Tool” on page 44
- ❑ “DHCP Client Configuration” on page 45
- ❑ “DHCP Auto Configuration” on page 47
- ❑ “System Log Configuration” on page 50
- ❑ “System Information Display” on page 48

Note

To permanently save your new settings or any changes to the configuration file, select **Save Configuration to Flash** from the main menu on the left side of the page.

System Management Information

This section explains how to assign a name, location, and contact information for the AT-GS950/10PS switch. This information helps in identifying each specific AT-GS950/10PS switch among other switches in the same local area network. Entering this information is optional.

Note

Allied Telesis recommends that you assign a name to the switch. Naming each switch can help you identify the specific switch you want to manage among others. It can also help to avoid performing a configuration procedure on the wrong switch.

To set a switch's administration information, perform the following procedure:

1. From the main menu on the left side of the page, click the **System** folder.
The **System** folder expands.
2. From the **System** folder, select **Management**.
The Management Page is displayed. See Figure 5 for the AT-GS950/10PS Management Page.

Management	
System Description:	AT-GS950/10PS
System Object ID:	1.3.6.1.4.1.207.1.4.199
System Name:	<input type="text"/>
System Location:	<input type="text"/>
System Contact:	<input type="text"/>
	<input type="button" value="Apply"/>

Figure 5. AT-GS950/10PS Management Page

3. Configure the following parameters as necessary:

System Description - Specifies the Allied Telesis switch model. You cannot change this parameter.

System Object ID - Indicates the unique SNMP MIB object identifier that identifies the switch model. You cannot change this parameter.

System Name - Specifies a name for the switch, for example, Sales. The name is optional and may contain up to 15 characters.

System Location - Specifies the location of the switch. The location is optional and may contain up to 30 characters.

System Contact - Specifies the name of the network administrator responsible for managing the switch. This contact name is optional and may contain up to 30 characters.

4. Click **Apply**.
5. From the main menu on the left side of the page, click on **Switch Info**. The Switch Information page is displayed. See "AT-GS950/8 Switch Information Page" on page 21 for more information.
6. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Configuration of IP Address, Subnet Mask and Gateway Address

This procedure explains how to change the IP address, subnet mask, and gateway address of the switch. Before performing the procedure, note the following:

- A gateway address is only required if you want to remotely manage the device from a management station that is separated from the switch by a router.
- To configure the switch to automatically obtain its IP configuration from a DHCP server on your network, go to “DHCP Client Configuration” on page 45.

To change the switch’s IP configuration, perform the following procedure:

1. From the main menu on the left side of the page, click the **System** folder.
The **System** folder expands.
2. From the **System** folder, select **IP Setup**.
The IP Setup Page is displayed. See Figure 6.

The screenshot shows the 'IP Setup' configuration page. It includes the following fields and controls:

- System MAC Address:** 00:01:02:03:04:05
- System IP Address:** 192 . 168 . 1 . 1
- System Subnet Mask:** 255 . 255 . 255 . 0
- System Default Gateway:** 0 . 0 . 0 . 0
- DHCP Mode:** Disable (dropdown menu)
- Apply** button

Figure 6. IP Setup Page

3. Change the IP configuration parameters by observing or entering new information in the following fields:

System MAC Address - This parameter displays the MAC address of the switch. You cannot change this parameter.

System IP Address - Displays the current IP address of the switch. To change the IP address, enter a new IP address. When DHCP is enabled, you cannot change this parameter.

System Subnet Mask - Displays the current subnet mask of the switch. To change the subnet mask, enter a new subnet mask. When DHCP is enabled, you cannot change this parameter.

System Default Gateway - Displays the default gateway of the switch. To change the default gateway, enter a new gateway. When DHCP is enabled, you cannot change this parameter.

DHCP Mode - For information about setting this parameter, refer to "DHCP Client Configuration" on page 45.

4. Click **Apply**.

Note

Changing the IP address ends your management session. To resume managing the device, enter the new IP address of the switch in the web browser's URL field, as shown in Figure 1 on page 20.

5. After you log on to the switch with the new IP address, select **Save Configuration to Flash** from the main menu on the left side of the page to save the new IP address to memory.

**Caution**

If you do not select **Save Configuration to Flash**, the IP address will revert to its original setting when you power cycle or reboot the switch.

IP Access List Configuration

When the IP Access List feature is enabled, remote access to the AT-S110 management software is restricted to the IP addresses entered into the IP Access List.

The procedures in this section describe how to enable or disable the IP Access List feature and how to add or remove IP addresses from the list. See the following sections:

- ❑ “Create an IP Access List” on page 32
- ❑ “Delete an IP Address List Entry” on page 33

Note

To modify IP address that has already been created, it must first be deleted and then re-created using the following procedures.

Create an IP Access List

To create a list of accessible IP addresses, perform the following procedure:

1. From the main menu on the left side of the page, click the **System** folder.
The **System** folder expands.
2. From the **System** folder, select **IP Access List**. The IP Access List Page is displayed. See Figure 7.



Figure 7. IP Access List Page

3. Enter an IP address in the **IP Address** field using a xxx.xxx.xxx.xxx format.
4. Click **Add**.
The IP address is added to the IP Access List table in the **Accessible IP** column.

Note

You can add up to 10 IP address to the IP Access List table.

5. From the **IP Restriction Status** field, select one of the following choices from the pull-down menu:
 - Enable** - This selection restricts the access to the AT-S110 management software to the IP addresses in the table listed under **Accessible IP**.
 - Disable** - This selection allows unrestricted access to the AT-S110 management software.
6. Click **Apply**.
Access to the management software is now restricted to those IP addresses listed in the IP Access List table.
7. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Delete an IP Address List Entry

To delete an IP address from the IP Access List, perform the following procedure:

1. From the main menu on the left side of the page, click the **System** folder.
The **System** folder expands.
2. From the **System** folder, select **IP Access List**.
The IP Access List Page is displayed. See Figure 7 on page 32.
3. Select **Delete** next to the IP address that you want to remove.
The IP address is removed from the IP Access List table. If you remove the last IP address from the table, the **IP Restriction Status** field is set to Disable.
4. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

User Name and Password Configuration

Password protection is always enabled for access to the AT-S110 Management software. This section explains how to create new users names and passwords and how to modify or delete existing users for the web interface. See the following sections:

- ❑ “Add New User Name and Password” on page 34
- ❑ “Modify User Name and Password” on page 35
- ❑ “Delete User Name and Password” on page 36

Add New User Name and Password

The default User Name and Password is “manager” and “friend” - both without the quotes. To configure new User Name and Password information, perform the following procedure:

1. From the main menu on the left side of the page, click the **System** folder.
The **System** folder expands.
2. From the **System** folder, select **Administration**.
The Administration Page is displayed. See Figure 8.

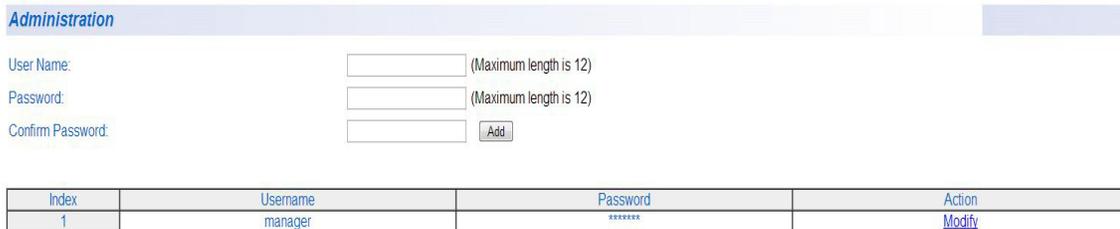


Figure 8. Administration Page

3. To create a user name, enter a user name in the box next to the **User Name** field.

You can enter a value of up to 12 alphanumeric characters. The **User Name** field is case sensitive.

4. To add a password that corresponds to the user name entered in step 3, enter a password of up to 12 alphanumeric characters in the box next to the **Password** field. The **Password** field is case sensitive.
5. To confirm the password entry, retype the password in the box next to the **Confirm Password** field.
6. Click **Add** to activate your changes on the switch.
7. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Modify User Name and Password

To modify the a user name password, perform the following procedure:

1. From the main menu on the left side of the page, click the **System** folder.
The **System** folder expands.
2. From the **System** folder, select **Administration**.
The Administration Page is shown in Figure 8 on page 34.
3. Identify the user name that you want to change and click **Modify** in the **Action** column.
The Modify Administration Page is displayed. See Figure 9.

Note

The default user name cannot be modified or deleted. The default password can be modified.

The screenshot shows a web form titled "Modify Administration". It contains three input fields: "User Name" with the value "manager", "Password", and "Confirm Password". An "Apply" button is located to the right of the "Confirm Password" field.

Figure 9. Modify Administration Page

4. To change a password, enter a password of up to 12 alphanumeric characters in the box next to the **Password** field.
5. To confirm the above password, retype the password in the box next to the **Confirm Password** field.
6. Click **Apply** to activate your changes on the switch.
7. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Delete User Name and Password

To delete a user name that you have previously added, perform the following procedure.

1. From the main menu on the left side of the page, click the **System** folder.
The **System** folder expands.
2. From the **System** folder, select **Administration**.
The Administration Page is shown in Figure 8 on page 34.
3. Identify the user name that you want to delete and click **Delete**.
The user name is removed from the Administration table.

Note

The default user name cannot be modified or deleted. The default password can be modified.

4. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

User Interface Configuration

This procedure explains how to enable and disable the user interfaces on the switch. With this procedure you can enable or disable the AT-GS950/10PS SNMP Agent. For more information about SNMP, go to Chapter 20, “Simple Network Management Protocol SNMPv1 and v2c” on page 263 and Chapter 21, “Simple Network Management Protocol SNMPv3” on page 273.

Note

The **Web Server Status** is displayed as **Enabled** for your information only. The Web Server cannot be disabled.

SNMP Interface

To enable or disable the AT-GS950/10PS SNMP interface, perform the following procedure:

1. From the main menu on the left side of the page, click the **System** folder.
The **System** folder expands.
2. From the **System** folder, select **User Interface**.
The User Interface Page is displayed. See Figure 10.

User Interface

SNMP Agent: Enable ▾

Web Server Status: Enable ▾

Apply

Web Idle Timeout: 10 Min.(3~60)

Figure 10. User Interface Page

3. Choose **Enable** or **Disable** from the pull down list for the **SNMP Agent** parameter.

Enabled - When you enable this parameter, the SNMP agent is active. You can manage the AT-GS950/10PS switch with Network Management Software and the switch’s private MIB.

Disabled - When you enable this parameter, the SNMP agent is inactive.

Note

See Chapter 20, “Simple Network Management Protocol SNMPv1 and v2c” on page 263 and Chapter 21, “Simple Network Management Protocol SNMPv3” on page 273 to configure the remaining SNMP parameters.

4. Click **Apply** located under the **Web Server Status** Enable/Disable field.
5. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

User Interface Timeout

To set the Web Idle Timeout, perform the following procedure:

1. From the main menu on the left side of the page, click the **System** folder.
The **System** folder expands.
2. From the **System** folder, select **User Interface**.
The User Interface Page is displayed. See Figure 10 on page 37.
3. Refer to the bottom portion of the web page. Enter the **Web Idle Timeout** parameter. The range is from 3 to 60 minutes.
4. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

System Time

The procedures in this section describe how to configure the system time by manually entering the time or through SNTP and how to configure the daylight savings time feature. See the following sections:

- ❑ “Manually Setting System Time” on page 39
- ❑ “Setting SNTP” on page 40
- ❑ “Setting Daylight Savings Parameters” on page 41

Manually Setting System Time

To set the system time manually, perform the following procedure:

1. From the main menu on the left side of the page, click the **System** folder.
The **System** folder expands.
2. From the **System** folder, select **System Time**.
The System Time Page is displayed. See Figure 11.

System Time	
Clock Mode :	Local Time
Current Time :	2 Jan 2009 16:22:25
Time Zone :	
Date/Time Settings	
Clock Mode:	Local Time ▼
Local Time Settings	
Date Setting(YYYY:MM:DD):	2009 / 1 / 2
Time Setting(HH:MM:SS):	16 : 22 : 25
Simple Network Time Protocol (SNTP) Settings	
SNTP Primary Server :	0 . 0 . 0 . 0
SNTP Secondary Server :	0 . 0 . 0 . 0
SNTP Poll Interval :	1 Min.(1-60)
Time Zone :	▼
Additional Time Parameters	
Daylight Saving Time Status:	Disabled ▼
From (Month:Day:HH:MM)	January ▼ : 01 ▼ : 00 ▼ : 00 ▼
To (Month:Day:HH:MM)	January ▼ : 01 ▼ : 00 ▼ : 00 ▼
DST Offset	1 hr ▼
Apply	

Figure 11. System Time Page

3. Use the pull down menu to set the **Clock Mode** parameter to **Local** time.

4. In the Local Time Settings section, set the **Date Setting (YYYY:MM:DD)** to the current date in the YYYY:MM:DD format.
5. In the Local Time Settings section, set the **Time Settings (HH:MM:SS)** to the current time in the HH:MM:SS format.
6. Click the **Apply** button at the bottom of the page.
The time will take effect immediately.
7. Save your new settings or any changes to the configuration file by selecting **Save Configuration to Flash** from the main menu on the left side of the page.

Setting SNTP

To configure SNTP, perform the following procedure:

1. From the main menu on the left side of the page, click the **System** folder.
The **System** folder expands.
2. From the **System** folder, select **System Time**.
The System Time Page is displayed. See Figure 11 on page 39.
3. Use the pull down menu to set the **Clock Mode** parameter to **SNTP**.
4. Enter the IP address of the **SNTP Primary Server**. The format is xxx.xxx.xxx.xxx.
5. Enter the IP address of the **SNTP Secondary Server**. The format is xxx.xxx.xxx.xxx.
6. Enter the **SNTP Poll Interval**. The range is 1 - 60 minutes.
7. Enter the local **Time Zone** from the pull down menu.
8. Click the **Apply** button at the bottom of the page.
The switch will immediately start polling the SNTP primary server for time information.
9. Save your new settings or any changes to the configuration file by selecting **Save Configuration to Flash** from the main menu on the left side of the page.

Setting Daylight Savings Parameters

If you want to configure the switch for daylight savings time, perform the following procedure:

1. From the main menu on the left side of the page, click the **System** folder.
The **System** folder expands.
2. From the **System** folder, select System Time.
The System Time Page is displayed. See Figure 11 on page 39.
3. In the **Daylight Savings Time Status** field, select **Enabled**.
4. Specify the Month, Day, Hour and Minute when Daylight Savings will take effect in the **From** time fields.
5. Specify the Month, Day, Hour and Minute when Daylight Savings will end in the **To** time fields.
6. Using the pull down menu, specify the Daylight Savings offset in the **DST Offset** field. You can select either 1 hr or 1/2 hr.
7. Save your new settings or any changes to the configuration file by selecting **Save Configuration to Flash** from the main menu on the left side of the page.

SSL Settings

The AT-GS950/10PS switch has a web browser server for remote management of the unit with a web browser application from management workstations on your network. By default, the server operates in a non-secure HTTP mode and can be configured to communicate in a secure HTTPS mode with SSL protocol.

In many situations, the communication with the switch will be in a controlled environment and it is acceptable to communicate with the management software in the HTTP mode.

However, you may find that your management communications are subject to outside security risks and web sessions conducted in the non-secure HTTP mode are vulnerable to security issues because the packets are sent in clear text. Web browser management sessions that use the secure HTTPS mode with SSL protocol are protected against snooping because the packets exchanged between the switch and your management workstations are encrypted. When operating in this mode, only the AT-GS950/10PS switch and the web browser are able to decipher the packets sent and received between them.

Configuring SSL

To enable or disable the SSL protocol feature, perform the following procedure:

1. From the main menu on the left side of the page, click the **System** folder.
The **System** folder expands.
2. From the **System** folder, select **SSL Settings**.
The SSL Settings Page is displayed. See Figure 12.



Figure 12. SSL Settings Page

3. From the **SSL Settings** field, select one of the following choices from the pull-down menu:
 - Enable** - The secure SSL mode is active. You must log in to the switch's management using the HTTPS mode on your browser.
 - Disable** - The secure SSL mode is inactive. You must log in to the switch's management using the HTTP mode on your browser.

4. Click **Apply**.
The SSL setting that you have selected is now active.
5. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

DHCP and ATI Web Discovery Tool

The AT-GS950/10PS Gigabit Ethernet Smart switch is managed through a web browser interface only. The factory default IP address is 192.168.1.1.

The switch does not have a local console connector, which means that you cannot learn what the switch's management IP address is on a web browser without first knowing what the address is. Once the IP address is known, you can enter it in the browser.

When the DHCP feature is enabled, a DHCP server automatically assigns an IP address which is not advertised over the network. As a consequence, you do not know what IP address has been assigned to the switch.

Note

The new IP address assignment from the DHCP server may take one to two minutes before the process is completed.

Fortunately, there is an ATI Web Discovery Tool available that resolves this issue. It detects the MAC address, IP address and other information of the AT-GS950 series switches that are present on your local area network.

Note

The ATI Web Discovery Tool is available for download on the AT-GS950/10PS product page at alliedtelesis.com.

DHCP Client Configuration

This procedure explains how to activate and deactivate the DHCP client on the AT-GS950/10PS switch. When the client is activated, the switch obtains its IP configuration including an IP address and subnet mask from a DHCP server on your network. Before performing the procedure, note the following:

- By default, the DHCP client is disabled on the switch.
- The DHCP client supports DHCP Auto Configuration Settings or BOOTP. See “DHCP Auto Configuration” on page 47 for more information.
- After you enable DHCP, your current management session ends because a different IP address is assigned to the switch by the DHCP server. The new IP address can be discovered using the ATI Discovery Tool. See “DHCP and ATI Web Discovery Tool” on page 44 for more information.

To activate or deactivate the DHCP client on the switch, perform the following procedure:

1. From the main menu on the left side of the page, click the **System** folder.
The **System** folder expands.
2. From the **System** folder, select **IP Setup**.
The IP Setup Page is shown in Figure 6 on page 30.
3. From the pull-down menu next to the **DHCP Mode** field, select **Enable** or **Disable**.
4. Click **Apply**.
When the DHCP client is **Enabled**, the web server connection to the switch is lost because a different IP address is assigned to the switch by the DHCP server.



Caution

Enabling DHCP may end your current management session.

5. Use the ATI Web Discovery Tool to find the new IP address assigned to the switch by the DHCP server. See “DHCP and ATI Web Discovery Tool” on page 44 for more information.

Note

The ATI Web Discovery Tool is available for download on the AT-GS950/10PS product page at alliedtelesis.com.

6. Follow the procedure to log on with the new IP address provided by the DHCP Server as described in “Establishing a Remote Connection to the Web Browser Interface” on page 20.
7. Save your new settings or any changes to the configuration file by selecting **Save Configuration to Flash** from the main menu on the left side of the page.

If you do not save the new configuration when DHCP is enabled, the software reverts to the previously saved IP address value when the switch is power cycled or rebooted. If no IP address has been previously saved, the IP address value reverts to 192.168.1.1.

If you enable DHCP and then save your configuration, you are saving the DHCP setting (**Enabled**). The next time the switch boots up, it will use the DHCP process to establish the IP address used to manage the AT-GS950/10PS switch.

If you enter a new IP address after disabling DHCP and save your configuration, the DHCP setting (**Disabled**) and the new IP address on the switch is saved. The next time the switch boots up, it will respond to the IP address that you entered when you re-establish contact with the AT-S110 Management software.

DHCP Auto Configuration

If you need to automatically update the switch's configuration files via a remote server, the DHCP Auto Configuration feature is available for this purpose via the DHCP server.

Note

You must enable the DHCP client so that this feature can operate with the DHCP server. See "DHCP Client Configuration" on page 45 for more information.

To configure this feature on the switch, perform the following procedure:

1. From the main menu on the left side of the page, click the **System** folder.
The **System** folder expands.
2. From the **System** folder, select **System**.
The DHCP Auto Configuration Settings Page is shown in Figure 13.

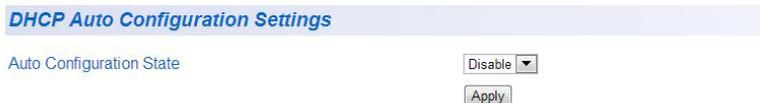


Figure 13. DHCP Auto Configuration Settings Page

3. From the **Auto Configuration State** field, select one of the following choices from the pull-down menu:

Enable - The DHCP Auto Configuration feature is active.

Note

You must enable the DHCP client so that this feature can operate with the DHCP server. See "DHCP Client Configuration" on page 45 for more information.

Disable - The DHCP Auto Configuration feature is inactive.

4. Click **Apply**.
The DHCP Auto Configuration setting that you have selected is now active.
5. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

System Information Display

The Switch Information page is initially displayed when you first log into the AT-GS950/10PS switch. It provides general information about the switch. To view this information, perform the following procedure:

1. From the main menu on the left side of the page, select **Switch Info**. The Switch Information Page is displayed. See Figure 14.

Switch Information	
System Up For:	0 day(s), 4 hr(s), 2 min(s), 9 sec(s)
Runtime Image:	AT-S110 V1.0.0 [1.00.010]
Boot Loader:	1.01.006
Hardware Information	
• Version:	A1
• DRAM Size:	128 M
• Flash Size:	16 M
Administration Information	
• System Name:	
• System Location:	
• System Contact:	
System MAC Address, IP Address, Subnet Mask and Gateway	
• MAC Address:	EC:CD:6D:10:00:80
• IP Address:	192.168.1.1
• Subnet Mask:	255.255.255.0
• Default Gateway:	0.0.0.0
Automatic Network Features	
• DHCP Client Mode:	Disable
• BOOTP Client Mode:	Disable

Figure 14. AT-GS950/10PS Switch Information Page

The Switch Information Page displays the following information:

System Up For - The number of days, hours, and minutes that the switch has been running since it was last rebooted.

Runtime Image - The version number of the runtime firmware.

Boot Loader - The version number of the bootloader firmware.

Hardware Information Section:

Version - The hardware version number.

DRAM Size - The size of the DRAM, in megabytes.

Flash Size - The size of the flash memory, in megabytes.

Administration Information Section:

Switch Name - This parameter displays the name assigned to the switch. To assign the switch a name, refer to “System Management Information” on page 28.

Switch Location - This parameter displays the location of the switch. To assign the location, refer to “System Management Information” on page 28.

Switch Contact - This parameter displays the contact person responsible for managing the switch. To assign the name of a contact, refer to “System Management Information” on page 28.

System MAC Address, IP Address, Subnet Mask, and Gateway Section:

MAC Address - This parameter displays the MAC address of the switch.

IP Address - This parameter displays the system IP address. Refer to “Configuration of IP Address, Subnet Mask and Gateway Address” on page 30 to manually assign an IP address or “DHCP Client Configuration” on page 45 to activate the DHCP client.

Subnet Mask - This parameter displays the subnet mask for the switch. Refer to “Configuration of IP Address, Subnet Mask and Gateway Address” on page 30 to manually assign a subnet mask or “DHCP Client Configuration” on page 45 to activate the DHCP client.

Default Gateway - This parameter displays the default gateway IP address. Refer to “Configuration of IP Address, Subnet Mask and Gateway Address” on page 30 to manually assign a gateway address or “DHCP Client Configuration” on page 45 to activate the DHCP client.

Automatic Network Features Section:

DHCP Mode - This parameter displays the status of the DHCP client on the switch. For information about setting this parameter, refer to “DHCP Client Configuration” on page 45.

System Log Configuration

The System log is designed to monitor the operation the AT-GS950/10PS switch by recording the event messages it generates during normal operation. These events may provide vital information about system activity that can help in the identification and solutions of system problems.

To configure the System log, perform the following procedure:

1. From the main menu on the left side of the page, click the **System** folder.
The **System** folder expands.
2. From the **System** folder, select **System Log Configuration**.
The System Log Configuration Page is displayed. See Figure 15.

The screenshot shows the 'System Log Configuration' page with the following settings:

Syslog Status	Disable
Time Stamp	Enable
Messages Buffered Size (1-200)	50
Syslog Server IP	0.0.0.0
Facility	local0
Logging Level	info

Buttons: Apply, Clear, Refresh

Figure 15. System Log Configuration Page

3. From the **Syslog Status** field, select one of the following choices from the pull-down menu:
 - Enable** - The System log is active.
 - Disable** - The System log is inactive.
4. From the Time Stamp field, select one of the following choices from the pull-down menu:
 - Enable** - Each event message recorded in the log will have a time stamp recorded with it.
 - Disable** - No time stamp will be recorded with the event messages.
5. Enter the **Messages Buffer Size**. The range is between 1 and 200.
6. Enter the **Syslog Server IP Address**. The format is xxx.xxx.xxx.xxx. If the address is left at the default setting of 0.0.0.0, no server is specified.
7. In the **Facility** field, enter the Facility local from the pull-down menu. The choices range from **local0** through **local7**.
8. Select the **Logging Level**. This parameter specifies what level of event messages will be logged into the System log. Your choices are as follows:
 - 0 Emergency** - The system is unusable.
 - 1 Alert** - Action must be taken immediately.
 - 2 Critical** - Critical conditions are displayed.
 - 3 Error** - Error conditions are displayed.
 - 4 Warning** - Warning conditions are displayed.
 - 5 Notice** - Normal but significant conditions are displayed.
 - 6 Informational** - Informational messages are displayed
 - 7 Debug** - Debug-level messages are displayed.
9. Click **Apply**.
The System log is now active.
10. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Section II

Bridge Configuration

This section contains the following chapters:

- ❑ Chapter 3, “Port Configuration” on page 55
- ❑ Chapter 4, “STP and RSTP” on page 61
- ❑ Chapter 5, “Multiple Spanning Tree Protocol” on page 79
- ❑ Chapter 6, “Static Port Trunking” on page 93
- ❑ Chapter 7, “LACP Port Trunks” on page 103
- ❑ Chapter 8, “Port Mirroring” on page 113
- ❑ Chapter 9, “Loopback Protection” on page 119
- ❑ Chapter 10, “MAC Address Table” on page 123
- ❑ Chapter 11, “IGMP Snooping” on page 135
- ❑ Chapter 12, “Storm Control” on page 141
- ❑ Chapter 13, “Virtual LANs” on page 149
- ❑ Chapter 14, “GVRP” on page 167
- ❑ Chapter 15, “Quality of Service and Cost of Service” on page 175

Chapter 3

Port Configuration

This chapter provides a description of the physical characteristics of the ports and a procedure that explains how to view and change the port settings. This chapter includes the following sections:

- “Overview” on page 56
- “Displaying and Configuring Ports” on page 57

Note

To permanently save your new settings or any changes to the configuration file, select **Save Configuration to Flash** from the main menu on the left side of the page.

Overview

This chapter describes how to display and modify the physical characteristics of an AT-GS950/10PS switch. You can display and modify the settings of all the ports on one web page. The port characteristics that are displayed are:

- Trunk Group Number
- Port type
- Link Status
- Admin Status
- Duplex Mode
- Jumbo frame
- Flow control
- EAP Pass
- BPDU frame

These characteristics are described in the next section.

Displaying and Configuring Ports

This procedure explains how to configure the ports on the AT-GS950/10PS switch using the Port Configuration Page. This page allows you to view and configure the parameter settings of individual or all the switch ports at one time.

To configure the ports, perform the following procedure:

1. From the main menu on the left side of the page, select **Physical Interface**.

Physical Interface

Port	Trunk	Type	Link Status	Admin. Status	Mode	Jumbo	Flow Ctrl	EAP	BPDU	Action
All	-	-	-	Ignore ▾	Ignore ▾	Ignore ▾	Ignore ▾	Ignore ▾	Ignore ▾	Apply
1	---	1000TX	Up	Enable ▾	Auto(100F) ▾	Enable ▾	Disable ▾	Disable ▾	Enable ▾	Apply
2	---	1000TX	Down	Enable ▾	Auto ▾	Enable ▾	Disable ▾	Disable ▾	Enable ▾	Apply
3	---	1000TX	Down	Enable ▾	Auto ▾	Enable ▾	Disable ▾	Disable ▾	Enable ▾	Apply
4	---	1000TX	Down	Enable ▾	Auto ▾	Enable ▾	Disable ▾	Disable ▾	Enable ▾	Apply
5	---	1000TX	Down	Enable ▾	Auto ▾	Enable ▾	Disable ▾	Disable ▾	Enable ▾	Apply
6	---	1000TX	Down	Enable ▾	Auto ▾	Enable ▾	Disable ▾	Disable ▾	Enable ▾	Apply
7	---	1000TX	Down	Enable ▾	Auto ▾	Enable ▾	Disable ▾	Disable ▾	Enable ▾	Apply
8	---	1000TX	Down	Enable ▾	Auto ▾	Enable ▾	Disable ▾	Disable ▾	Enable ▾	Apply

Figure 16. AT-GS950/10PS Physical Interface Page

2. Adjust the port settings as needed. Not all parameters are adjustable. The parameters are defined as follows:

Port - Specifies the port number. The All value indicates ports 1 through 10 on the AT-GS950/10PS switch. You cannot change this parameter.

Note

You can use the **All** row value in the **Port** column to set the **Admin. Status**, **Mode**, **Jumbo**, **Flow Ctrl**, **EAP Pass**, and **BPDU** fields to the same values for all ports at the same time. In the **All** row when you select **Ignore**, **Enable** or **Disable** in one of these columns, it applies to all of the AT-GS950/10PS switch ports.

Trunk - This parameter indicates the trunk group number. A number in this column indicates that the port has been added to a trunk. This parameter can not be configured on this page, However, for information about configuring a trunk, refer to Chapter 6, "Static Port Trunking" on page 93.

Type - This parameter indicates the port type. On the AT-GS950/10PS, the port type is 1000TX for 10/100/1000Base-T twisted-pair ports (1 through 8, 9R and 10R) and 100FX or 1000TX

for the SFP ports (9 and 10) for copper or fiber SFP type.

Link Status - This parameter indicates the status of the link between the port and the end node connected to the port. The possible values are:

Up -This parameter i Indicates a valid link exists between the port and the end node.

Down -This parameter i Indicates the port and the end node have not established a valid link.

Admin. Status -This parameter indicates the operating status of the port. You can use this parameter to enable or disable a port. 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. You can enable the port to resume normal operation after the problem has been fixed. You can also disable an unused port to secure it from unauthorized connections. The possible values are:

Ignore -This parameter applies to the **All** row only and i Indicates that the **Admin. Status** field must be set individually for each port.

Enabled - This parameter indicates the port is able to send and receive Ethernet frames.

Disabled - This parameter indicates the port is not able to send and receive Ethernet frames.

Jumbo -This parameter i Indicates whether or not jumbo frames can be accepted by the switch. You may want to activate jumbo frames when your switch will transmit video and audio files. The possible values are:

Ignore -This parameter i Indicates that the **All** setting does not apply to the **Jumbo** field. In other words, each port is set individually.

Enabled -This parameter i Indicates the port is permitted to accept jumbo frames.

Disabled -This parameter i Indicates the port is not permitted to accept jumbo frames.

Note

When **QoS** is enabled on a port, the Jumbo frame parameter can not be enabled. To enable or disable **QoS**, see “Mapping CoS Priorities to Egress Queues,” next and “CoS Page” on page 180

Mode -This parameter i Indicates the speed and duplex mode

settings for the port. You can use this parameter to set the speed and duplex mode of a port. The possible settings are:

Ignore -This parameter indicates that the **All** setting does not apply to the **Mode** field. In other words, each port is set individually.

Auto -This parameter indicates the port is using Auto-Negotiation to set the operating speed and duplex mode. The actual operating speed and duplex mode of the port are displayed in parentheses (for example, "1000F" for 1000 Mbps full duplex mode) after a port establishes a link with an end node.

Auto (1000F) -This parameter indicates the port is configured for 1000Mbps operation in Auto-Negotiation mode.

1000/Full -This parameter indicates the port is configured for 1000Mbps operation in full-duplex mode.

100/Full -This parameter indicates the port is configured for 100Mbps operation in full-duplex mode.

10/Full -This parameter indicates the port is configured for 10Mbps operation in full-duplex mode.

1000/Half -This parameter indicates the port is configured for 1000Mbps operation in half-duplex mode.

100/Half -This parameter indicates the port is configured for 100Mbps operation in half-duplex mode.

10/Half -This parameter indicates the port is configured for 10Mbps operation in half-duplex mode.

When selecting a **Mode** setting, the following points apply:

- When a twisted-pair port is set to Auto-Negotiation, the end node should also be set to Auto-Negotiation to prevent a duplex mode mismatch. A switch port using Auto-Negotiation defaults to half-duplex if it detects that the end node is not using Auto-Negotiation. This can result in a mismatch if the end node is operating at a fixed duplex mode of full-duplex. To avoid this problem when connecting an end node with a fixed duplex mode of full-duplex to a switch port, disable Auto-Negotiation on the port and set the port's speed and duplex mode manually.
- The only valid setting for the SFP ports is Auto-Negotiation.

Flow Control - This parameter reflects the current flow control setting on the port. The switch uses a special pause packet to

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

Ignore - This parameter indicates that the **All** setting does not apply to the **Flow Control** field. In other words, each port is set individually.

Enabled - This parameter indicates that the port is permitted to use flow control.

Disabled - This parameter indicates that the port is not permitted to use flow control.

EAP Pass - This parameter reflects the current Extensible Authentication Protocol (EAP) setting on the port. The possible values are:

Ignore - This parameter indicates that the **All** setting does not apply to the **EAP Pass** field. In other words, each port is set individually.

Enabled - This parameter indicates that the port is able to send and receive EAP packets.

Disabled - This parameter indicates that the port is disabled and is not able to send or receive EAP packets.

BPDU - This parameter reflects the current BPDU setting on the port. The possible values are:

Ignore - This parameter indicates that the **All** setting does not apply to the **BPDU** field. In other words, each port is set individually.

Enabled - This parameter indicates that the switch will pass BPDU frames through the switch and broadcast them through all other ports.

Disabled - This parameter indicates that the switch will not pass BPDU frames through the switch. With RSTP or STP enabled, the switch will receive BPDU frames and process them according to the spanning tree protocol.

3. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Chapter 4

STP and RSTP

This chapter provides background information about the Spanning Tree Protocol (STP) and the Rapid Spanning Tree Protocol (RSTP). In addition, there are procedures to configure STP and RSTP. The sections in the chapter include:

- ❑ “Overview” on page 62
- ❑ “Basic STP and RSTP Configuration” on page 70
- ❑ “Configure RSTP Port Settings” on page 73
- ❑ “Spanning Tree Topology” on page 78

For detailed information about STP, refer to IEEE Std 802.1D. For detailed information about RSTP, refer to IEEE Std 802.1w.

Note

To permanently save your new settings or any changes to the configuration file, select **Save Configuration to Flash** from the main menu on the left side of the page.

Overview

The performance of a Ethernet network can be negatively impacted by the formation of a data loop in the network topology. A data loop exists when two or more nodes on a network can transmit data to each other over more than one data path. The problem that data loops pose is that data packets can become caught in repeating cycles, referred to as broadcast storms, that needlessly consume network bandwidth and can 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. Where multiple paths exist, these protocols place the extra paths in a standby or blocking mode, leaving only one main active path.

In addition, STP and RSTP can 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.

Where the two protocols differ is in the time each takes to complete the process 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 communications between the various network segments. This is the process of convergence.

With STP, convergence can take up to a minute or more to complete in a large network. This can result in the loss of communication between various parts of the network during the convergence process, and the subsequent lost of data packets.

RSTP is much faster. It can complete a convergence in seconds, and so greatly diminish the possible impact the process can have on your network. The STP implementation in the AT-S110 Management software complies with the IEEE 802.1d standard.

Only one spanning tree at a time can be active on the switch. The default protocol is RSTP. 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

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 the *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 lowest bridge priority number, the one with the lowest MAC address is designated as the root bridge.

You can change the bridge priority number in the AT-S110 Management software. You can designate which switch on your network as the root bridge by giving it the lowest bridge priority number. You may 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 bridge priority has a range 0 to 61440 in increments of 4096. To make this easier for you, the AT-S110 Management software divides the range into increments. You specify the increment that represents the desired bridge priority value. The range is divided into sixteen increments, as shown in Table 1.

Table 1 Bridge Priority Value Increments

Increment	Bridge Priority	Increment	Bridge Priority
0x0000	0	0x8000	32768
0x1000	4096	0x9000	36864
0x2000	8192	0xA000	40960
0x3000	12288	0xB000	45056
0x4000	16384	0xC000	49152
0x5000	20480	0xD000	53248
0x6000	24576	0xE000	57344
0x7000	28672	0xF000	61440

Path Costs and Port Costs

After the root bridge has been selected, the bridges determine if the network contains redundant paths and, if one is found, 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 an 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 by evaluating *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 cost of a port on the switch is adjustable through the AT-S110 Management software. For STP and RSTP, the range is from 0 to 200,000,000.

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 which is used as a tie breaker when two paths have the same cost.

The range for port priority is 0 to 240. As with bridge priority, this range is broken into increments, in this case multiples of 16. To select a port priority for a port, you enter the desired value. Table 2 on page 65 lists the values that are valid.

Table 2. Valid Port Priority Values

Step	Port Priority
1	0
2	16
3	32
4	48
5	64
6	80
7	96
8	112
9	128
10	144
11	160
12	176
13	192
14	208
15	224
16	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 also changes. This may trigger a change in the state of some blocked ports. However, a change in a port state is not activated immediately.

It may take time for the root bridge to notify all bridges that a topology change has occurred, especially if it is a large network. A temporary data loop could occur if a topology change is made before all bridges have been notified and that could adversely impact network performance.

To forestall the formation of temporary 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 states 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 in the AT-S110 Management software. The appropriate value for this parameter depends on a number of variables; the size of your network is 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 specify a smaller value so that the time for a topology change is optimized for minimum data loss.

Note

The forwarding delay parameter applies only to ports on the switch that are operating STP-compatible mode.

Hello Time and Bridge Protocol Data Units (BPDU)

The bridges that are part of a spanning tree domain communicate with each other using a bridge broadcast 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 online, it issues a BPDU in order to determine whether a root bridge has already been selected on the network, and if not, whether it has the lowest bridge priority number of all the bridges and should therefore 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 in the AT-S110 Management software. The interval is measured in seconds. Consequently, if the switch is selected as the root bridge of a spanning tree domain, it transmits a BPDU every two seconds.

Point-to-Point and Edge Ports

This section applies only to RSTP. Part of the task of configuring RSTP is defining the port types on the bridge, which is directly related to the device(s) connected to the port. With the port types 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 port
- Edge port

If a bridge port is connected to another bridge or router port, it normally operates in full-duplex mode and is functioning as a point-to-point port. Figure 17 on page 67 illustrates two switches that are connected with one data link. This link is operating between two point-to-point ports.

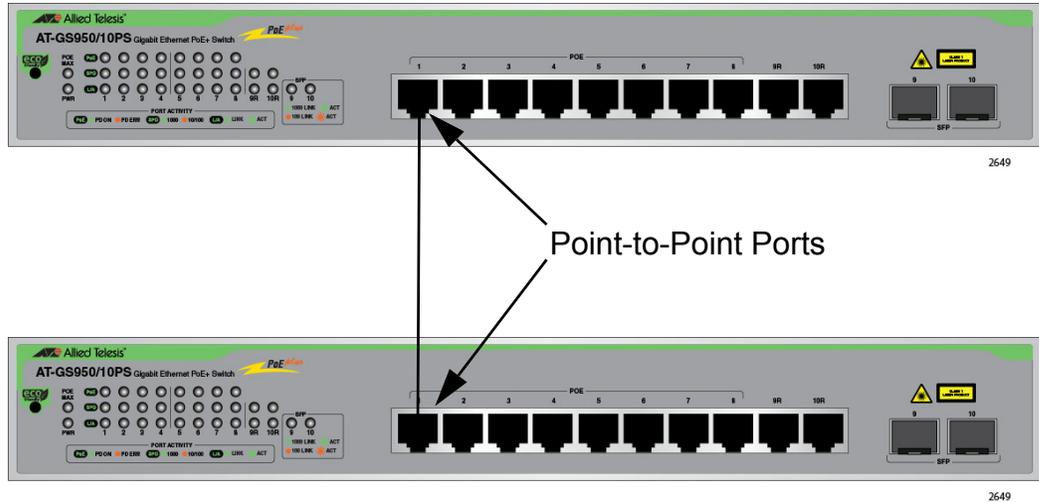


Figure 17. Point-to-Point Ports

A port operates as an edge port when it is connected to a network terminal device such as a workstation or a server. An edge port on a bridge should not have any STP or RSTP devices connected to it either directly or through another device connected to that port. In this configuration since the port has no STP or RSTP devices connected to it, it will always forward network traffic. Figure 18 illustrates a port functioning as an edge port.

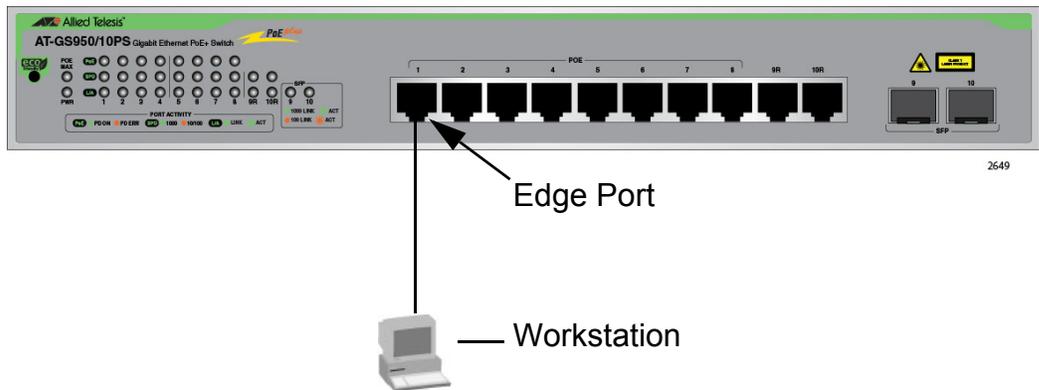


Figure 18. Edge Port

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 can operate together to create a single spanning tree domain.

If you decide to activate spanning tree on the switch, Allied Telesis recommends RSTP instead of STP even when all of other switches in the network are running STP. The AT-GS950/10PS switch can combine RSTP with the STP of the other switches. The switches monitors the traffic on each port for BPDU packets. Ports that receive RSTP BPDU packets operate in RSTP mode while ports receiving STP BPDU packets operate in STP mode.

Spanning Tree and VLANs

The spanning tree implementation in the AT-S110 Management software can be a single-instance spanning tree as described in this chapter. If you choose to define multiple spanning trees on this switch, go to Chapter 5, “Multiple Spanning Tree Protocol” on page 79.

The single spanning tree encompasses all ports on the switch. If the ports are divided into different VLANs, the spanning tree crosses the VLAN boundaries. This can pose a problem in networks containing multiple VLANs that span two bridges and are connected with untagged ports. In this situation, spanning tree blocks a data link because it detects a suspected data loop. This can cause fragmentation of your VLANs.

This issue is illustrated in Figure 42. VLANs 1 – 3 span two switches. One link consisting of untagged ports connect each VLAN. If STP or RSTP is activated on the switches, two of the links are disabled. As a direct result, two VLANs are disconnected between the bridges. In this example, the ports (on the non-root switch) that link the two parts of the VLANs 2 - 3 are changed to the blocking state, which disrupts these VLAN connections.

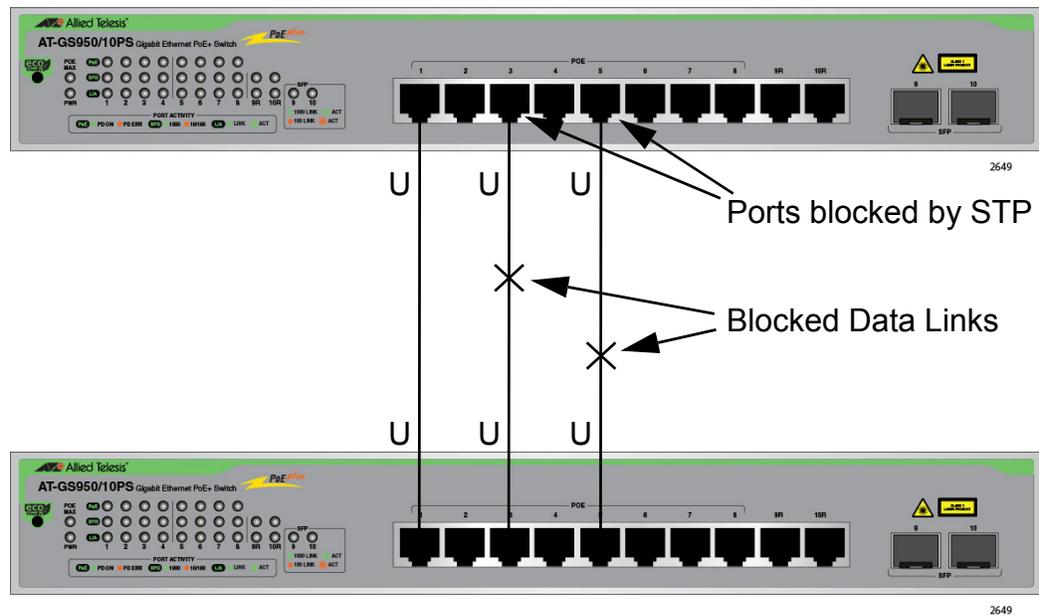


Figure 19. STP and VLAN Fragmentation with Untagged Ports

You can avoid this problem by connecting the switches using tagged instead of untagged ports when you plan to have STP or RSTP enabled on your network. If each port connecting the two bridges is a tagged member of all three VLANs, then traffic for each of the VLANs can still flow through one of the data links if the other two are blocked by Spanning Tree. The second and third data links act as redundant links in case the primary, unblocked data link becomes disabled. See Figure 20 for an example of this solution.

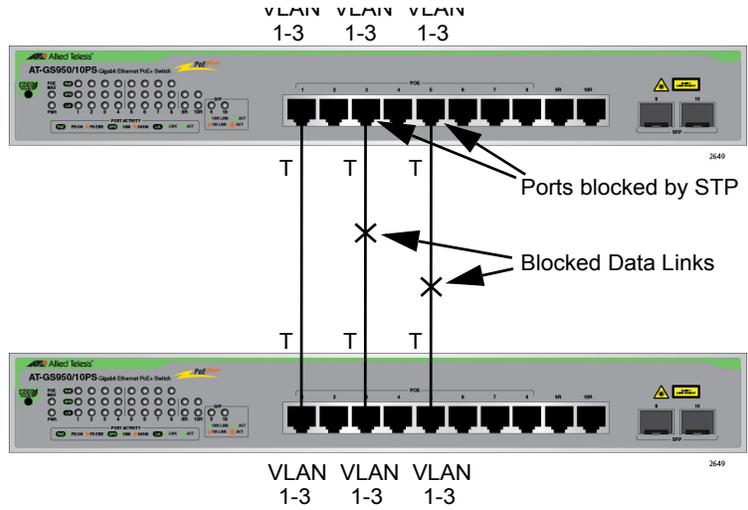


Figure 20. STP and VLAN Compatibility with Tagged Ports

Note

For information about tagged and untagged ports, refer to Chapter 13, "VLAN Overview" on page 150.

Basic STP and RSTP Configuration

To configure the basic STP and RSTP settings, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.
2. From the **Bridge** folder, select the **Spanning Tree** folder. The **Spanning Tree** folder expands.
3. From the **Spanning Tree** folder, select the **RSTP** folder. The **RSTP** folder expands.
4. From the **RSTP** folder, select **RSTP**. The Rapid Spanning Tree Configuration Page is displayed. See Figure 21.

Rapid Spanning Tree Configuration

Global RSTP Status: ▾

Protocol Version: ▾

Note : To enable RSTP Functionality, MSTP should be disabled.
Enable Spanning Tree will cause the system to temporarily stop response!

Root Port:	0
Root Path Cost:	0
Time Since Topology Change:	0 Sec.
Topology Change Count:	0
Designated Root:	00:00:00:00:00:00:00:00
Hello Time:	2 Sec.
Maximum Age:	20 Sec.
Forward Delay:	15 Sec.

Bridge ID:	000 eccd6d100080
Bridge Priority:	0x <input type="button" value="0000"/> ▾ (0x0000 - 0xF000 and in increments of 0x1000)
Bridge Hello Time:	<input type="button" value="2"/> Sec. (1-10 Secs)
Bridge Maximum Age:	<input type="button" value="20"/> Sec. (6-40 Secs)
Bridge Forward Delay:	<input type="button" value="15"/> Sec. (4-30 Secs)

Notes: Disable will reset the setting to default value then turn off the function.

Figure 21. Rapid Spanning Tree Configuration Page

The RSTP Configuration page allows you to configure basic STP (STP-Compatible) or RSTP protocols as well as to view current settings of the feature.

- In the upper portion of the page, you can set the following parameters:

Global RSTP Status - Set this field to activate or de-activate the RSTP feature on the switch. From the **Global RSTP Status** field at the top of the page, select one of the following choices from the pull-down menu:

Enable - The RSTP feature is active. The other parameter fields on the web page become active and are eligible for data to be entered.

Disable - The RSTP feature is inactive. The other parameter fields on the web page become inactive and are greyed out so that data cannot be entered.

Protocol Version - Set this field to activate RSTP or STP on the switch. To activate this field, select RSTP or STP-compatible and then click **Apply** at the top of the page.

- In the middle section of the page, the following fields are listed:

Note

You cannot change these fields.

Root Port - The active port on the switch that is communicating with the root bridge. If the switch is the root bridge for the LAN, then there is no root port and the root port parameter is set to 0.

Root Path Cost - The sum of all the root port costs of all the bridges between the switch's root port and the root bridge including the switch's root port cost.

Time Since Topology Change - The time in seconds since the last topology change took place. When RSTP detects a change to the LAN's topology or when the switch is rebooted, this parameter is reset to 0 seconds and begins incrementing until the next topology change is detected.

Note

To update the **Time Since Topology Change** parameter, you must refresh your browser.

Topology Change Count - An integer that reflects the number of times RSTP has detected a topology change on the LAN since the switch was initially powered on or rebooted.

- The following parameters refer to the designated root bridge. You cannot change these fields.

Designated Root - This parameter includes two fields: the root bridge priority and the MAC address of the root bridge. For example, 1000 00C08F1211BB shows the root bridge priority as 1000, and 00C08F1211BB as the MAC address.

Hello Time - This parameter is the Hello Me. See “Hello Time and Bridge Protocol Data Units (BPDU)” on page 66. This parameter affects only the root bridge.

Maximum Age - The parameter displays the maximum amount of time that BPDU's are stored before being deleted on the root bridge.

Forward Delay - The parameter displays the time interval between generating and sending configuration messages by the root bridge.

- The bottom section of the web page provides information about the bridge. The following parameters appear in the bottom third of the web page:

Bridge ID - The Bridge ID is 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. You cannot change this parameter.

Bridge Priority - The priority number for the bridge, in hexadecimal format. This number is used to determine 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, that is, the lowest value of all the other bridges, then the bridge with the numerically lowest MAC address becomes the root bridge. When a root bridge goes offline, the bridge with the lowest priority number automatically takes over as the root bridge. This parameter can be from 0X0000 to 0XF000, with 0XF000 being the highest priority.

Bridge Hello Time - This is the time interval between generating and sending configuration messages by the bridge. This parameter is active only when the switch is the root bridge.

Bridge Maximum Age - The length of time after which stored bridge protocol data units (BPDU's) are deleted by the bridge.

Bridge Forward Delay - This is the time interval between generating and sending configuration messages by the bridge.

5. Once you have configured the parameters, click **Apply**.
6. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Configure RSTP Port Settings

This section contains the following topics:

- ❑ “Configure the Basic RSTP Port Settings,” next
- ❑ “Configure the Advanced RSTP Port Settings” on page 75

Configure the Basic RSTP Port Settings

To configure the basic RSTP port settings, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.
2. From the **Bridge** folder, select the **Spanning Tree** folder. The **Spanning Tree** folder expands.
3. From the **Spanning Tree** folder, select the **RSTP** folder. The **RSTP** folder expands.
4. From the **RSTP** folder, select the **RSTP Basic Port**. The AT-GS950/10PS RSTP Basic Port Configuration Page is displayed. See Figure 22 for a partial view of this page.

RSTP Basic Port Configuration

Port	Trunk	Link Status	Port State	Role	STP Status	Priority	Path Cost	Action
All	-	-	-	-	Ignore ▾			Apply
1	---	Up	STP forwarding	---	Disable ▾	2	2	Apply
2	---	Down	---	---	Disable ▾	2	2	Apply
3	---	Down	---	---	Disable ▾	2	2	Apply
4	---	Down	---	---	Disable ▾	2	2	Apply
5	---	Down	---	---	Disable ▾	2	2	Apply
6	---	Down	---	---	Disable ▾	2	2	Apply
7	---	Down	---	---	Disable ▾	2	2	Apply
8	---	Down	---	---	Disable ▾	2	2	Apply

Figure 22. AT-GS950/10PS RSTP Basic Port Configuration Page

This page displays the following information about the ports:

Port - Indicates ports 1 through 10 on the AT-GS950/10PS switch. You can select the **All** row to apply the same setting to all ports of your switch for the **STP Status**, **Priority**, and **Path Cost** fields.

Trunk - Indicates the trunk assignment of a port.

Link Status - Indicates if the port link status is active (Up) or inactive (Down).

Port State - Indicates one of the following port states:

Blocking - A blocking state does not allow network traffic to be

sent or received on a the port except for BPDU data. A port with a higher path cost to the root bridge than another on the switch will cause a switching loop and is placed in the blocking state by the Spanning Tree algorithm. The port's state may change to the forwarding state if the other links in use fail and the Spanning Tree algorithm determines the port may transition to the forwarding state.

Listening - This state occurs on a port during the convergence process. The port in the listening state processes BPDUs and awaits new information that would cause the port to return to the blocking state.

Learning - While the port does not yet forward frames (packets) in this state, the port does learn source addresses from frames received and adds them to the filtering (switching) database.

Forwarding - A port that both receives and sends data. This indicates normal operation. STP continues to monitor the port for incoming BPDUs that indicate the port should return to the blocking state to prevent a loop.

Disabled - This state is not strictly part of STP. However, a network administrator can manually disable a port.

Role - Indicates one of the following port roles:

Disabled - The Disabled Port role is assigned if the port is not operational or is excluded from the active topology by management or it is a network access port (IEEE Std 802.1X) and it is Unauthorized, or its Administrative Bridge Port state is Disabled.

Root - If the least cost path to the root is through this port, then it becomes the root port for this bridge.

Designated - If this is the designated bridge for the LAN and if the root path cost information received on this port is greater than the root port's path cost and less than any other port's received information, then this port becomes the designated port.

Backup - Any operational Bridge Port that is not a Root or Designated Port is a Backup Port if the Bridge is the Designated Bridge for the attached LAN.

Alternate - Any operational Bridge Port that is not a Root or a Designated Port is an Alternate Port if that Bridge is *not* the Designated Bridge for the attached LAN.

STP Status - Indicates if spanning tree protocol (either RSTP or STP-Compatible) is active or not on the port. Select one of the following choices from the pull-down menu:

Enable - The spanning tree protocol (both RSTP or STP- Compatible) is enabled on the port.

Disabled - The spanning tree protocol (both RSTP or STP- Compatible) is disabled on the port.

Priority - Indicates the port priority. See “Port Priority” on page 64 for more information.

Path Cost - Indicates the Path Cost assigned to each port. For STP, the range is from 0 to 65,535. For RSTP, the range is from 0 to 200,000,000. The Path cost is described in “Path Costs and Port Costs” on page 64.

5. Click **Apply** for the port you are configuring.
6. To configure all of the ports to the same settings, in the **All** row, configure one, two, or all of the following settings: **STP Status**, **Priority** and **Port Cost**.
7. Click **Apply**.
8. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Configure the Advanced RSTP Port Settings

To configure the advanced RSTP port settings, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.
2. From the **Bridge** folder, select the **Spanning Tree** folder. The **Spanning Tree** folder expands.
3. From the **Spanning Tree** folder, select the **RSTP** folder. The **RSTP** folder expands.
4. From the **RSTP** folder, select **RSTP Advanced Port** folder. The AT-GS950/10PS RSTP Advanced Port Configuration Page is displayed. See Figure 23 on page 75 for a partial view of this page.

RSTP Advanced Port Configuration

Port	Trunk	Link	State	Role	Admin/OperEdge	Admin/OperPtoP	Migration	Action
All	-	-	-	-	Ignore ▾	Ignore ▾	Ignore ▾	Apply
1	---	Up	STP forwarding	---	False ▾ / False	False ▾ / False	False ▾	Apply
2	---	Down	---	---	False ▾ / False	False ▾ / False	False ▾	Apply
3	---	Down	---	---	False ▾ / False	False ▾ / False	False ▾	Apply
4	---	Down	---	---	False ▾ / False	False ▾ / False	False ▾	Apply
5	---	Down	---	---	False ▾ / False	False ▾ / False	False ▾	Apply
6	---	Down	---	---	False ▾ / False	False ▾ / False	False ▾	Apply
7	---	Down	---	---	False ▾ / False	False ▾ / False	False ▾	Apply
8	---	Down	---	---	False ▾ / False	False ▾ / False	False ▾	Apply

Figure 23. AT-GS950/10PS RSTP Advanced Port Configuration Page

This page displays the following information about the ports:

Port - Indicates ports 1 through 10 on the AT-GS950/10PS switch. You can select the **All** row to apply the same setting to all ports of your switch for the **AdminOperEdge**, **Admin/OperPtoP**, and **Migration** fields.

Trunk - Indicates the trunk assignment of a port.

Link - Indicates that the port's link is active (Up) or inactive (Down).

State - Indicates one of the following port states:

Blocking - A blocking state does not allow network traffic to be sent or received on a the port except for BPDU data. A port with a higher path cost to the root bridge than another on the switch causes a switching loop and is placed in the blocking state by the Spanning Tree algorithm. The port's state may change to the forwarding state if the other links in use fail and the Spanning Tree algorithm determines the port may transition to the forwarding **state**.

Listening - This state occurs on a port during the convergence process. The port in the listening state processes BPDUs and awaits new information that would cause the port to return to the blocking state.

Learning - While the port does not yet forward frames (packets), in this state the port does learn source addresses from frames received and adds them to the filtering (switching) database.

Forwarding - A port that both receives and sends data. This indicates normal operation. STP continues to monitor the port for incoming BPDUs that indicate the port should return to the blocking state to prevent a loop.

Disabled - This state is not strictly part of STP. However, a network administrator can manually disable a port.

Role - Indicates one of the following port roles:

Disabled - The Disabled Port role is assigned if the port is not operational or is excluded from the active topology by management or it is a network access port (IEEE Std 802.1X) and it is Unauthorized, or its Administrative Bridge Port state is Disabled.

Root - If the least cost path to the root is through this port, then it becomes the root port for this bridge.

Designated - If this is the designated bridge for the LAN and if

this port receives root path cost information that is greater than the root port's path cost and less than any other port's received information, then this port becomes the designated port.

Backup - Any operational Bridge Port that is not a Root or Designated Port is a Backup Port if the Bridge is the Designated Bridge for the attached LAN.

Alternate - Any operational Bridge Port that is not a Root or a Designated Port is an Alternate Port if that Bridge is *not* the Designated Bridge for the attached LAN.

Admin/OperEdge - Indicates if a port is connected to an edge device in the network topology or not.

True - The port is connected to an edge device and the port will always be in a forwarding state.

False - The port is not connected to an edge device.

Admin/OperPtoP - Indicates if the port is connected to another network device (point-to-point) in the network topology.

True - The port is connected to a network device in the network topology.

False - The port is not connected to a network device in the network topology.

Migration - Indicates if the port is configured to accept RSTP and STP BPDUs

5. Click **Apply** for the port you are configuring.
6. To configure all of the ports to the same settings, in the All row, configure one, two, or all of the following settings: **Admin/OperEdge**, **Admin/OperPtoP**, and **Migration**.
7. Click **Apply**.
8. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Spanning Tree Topology

To view the current spanning tree topology, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**. This folder expands.
2. From the **Bridge** folder, select the **Spanning Tree** folder.
3. From the **Spanning Tree** folder, select **Topology Info**. The AT-GS950/10PS Designated Topology Information Page is displayed. See Figure 24 for a partial view of this page.

Topology Information

Port	Trunk	Link Status	Designated Root	Designated Cost	Designated Bridge	Designated Port
1	---	Up	00:00:00:00:00:00:00	0	00:00:00:00:00:00:00	00:00
2	---	Down	00:00:00:00:00:00:00	0	00:00:00:00:00:00:00	00:00
3	---	Down	00:00:00:00:00:00:00	0	00:00:00:00:00:00:00	00:00
4	---	Down	00:00:00:00:00:00:00	0	00:00:00:00:00:00:00	00:00
5	---	Down	00:00:00:00:00:00:00	0	00:00:00:00:00:00:00	00:00
6	---	Down	00:00:00:00:00:00:00	0	00:00:00:00:00:00:00	00:00
7	---	Down	00:00:00:00:00:00:00	0	00:00:00:00:00:00:00	00:00
8	---	Down	00:00:00:00:00:00:00	0	00:00:00:00:00:00:00	00:00

Figure 24. AT-GS950/10PS Designated Topology Information Page

This page contains status information only and there are no parameters to configure. The following information is displayed about the ports:

Port - Indicates ports 1 through 10 on the AT-GS950/10PS switch.

Trunk - The trunk of which the port is a member.

Link Status - Whether the link on the port is up or down.

Designated Root - The designated root bridge to which the switch's root port is actively connected.

Designated Cost - The sum of all the root port costs on all bridges, including the switch, between the switch and the root bridge.

Designated Bridge - An adjacent bridge to which the root port of the switch is actively connected.

Designated Port - The root bridge to which the root port of the switch is actively connected.

Chapter 5

Multiple Spanning Tree Protocol

This chapter provides the procedures for configuring Multiple Spanning Tree Protocol (MSTP). You can find an overview and configuration guidelines for this feature in “MSTP Overview” on page 349.

When you configure MSTP, the information should be entered in order on the following web pages:

- ❑ “Multiple Spanning Tree Configuration” on page 80
- ❑ “Port Configuration” on page 83
- ❑ “VLAN Mapping” on page 86
- ❑ “Port Settings” on page 88
- ❑ “Topology Information” on page 90

Multiple Spanning Tree Configuration

To configure the MSTP settings, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.
2. From the **Bridge** folder, select the **Spanning Tree** folder. The **Spanning Tree** folder expands.
3. From the **Spanning Tree** folder, select the **MSTP** folder. The **MSTP** folder expands.
4. From the **MSTP** folder, select **MSTP**.

The Multiple Spanning Tree Configuration Page is displayed. See Figure 25 on page 80.

Multiple Spanning Tree Configuration

Global MSTP Status:	<input type="text" value="Disable"/>	
Maximum MST Instances:	<input type="text" value="31"/> * (1-31)	
Bridge Priority:	<input type="text" value="32768"/>	
Region Name:	<input type="text" value="EC:CD:6D:10:00:80"/> *	
Region Revision:	<input type="text" value="0"/> * (0-65535)	
Dynamic Path Cost Calculation:	<input type="text" value="False"/>	<input type="button" value="Apply"/>

Note : To enable MSTP Functionality, RSTP should be disabled.
 Enable Spanning Tree will cause the system to temporarily stop response!

Maximum Age:	0 Sec.	
Forward Delay:	0 Sec.	
Maximum Hop Count:	0	
Transmit Hold Count:	3	

Bridge Maximum Age:	<input type="text"/>	Sec. (6-40)
Bridge Forward Delay:	<input type="text"/>	Sec. (4-30)
Maximum Hop Count:	<input type="text"/>	(6-40)
Transmit Hold Count:	<input type="text"/>	(1-10)

Notes: Disable will reset the setting to default value then turn off the function.

Figure 25. Multiple Spanning Tree Configuration Page

The MSTP Configuration page allows you to configure the MSTP parameters as well as to view current settings of the feature.

- In the upper portion of the page, you can set the

following parameters:

Global MSTP Status - Set this field to **Enable** or **Disable** the MSTP feature on the switch. The Global MSTP Status must be set to **Enable** before the other MSTP configuration parameters can be set.

Note

Both RSTP and BPDU Passthrough must be disabled before you enable MSTP.



Caution

Enabling or disabling MSTP causes the switch to temporarily stop switching Ethernet network traffic.

Maximum MST Instances - This specifies the maximum number of Multiple Spanning Tree Instances (MSTIs) that can be configured. The range is 1 - 31.

Bridge Priority - This parameter specifies the priority used in determining the regional root for a particular MSTI. For more information about **Bridge Priority**, see Table 11 on page 360.

Region Name - This parameter specifies the region's name where the bridge is a member. This name must be identical to the regional names specified on other switches in the same MSTP region. See "Multiple Spanning Tree Regions" on page 358 for more information.

Region Revision - The parameter indicates the region's revision and must be identical to the regional names specified on other switches in the same MSTP region. See "Multiple Spanning Tree Regions" on page 358 for more information.

Dynamic Path Cost Calculation - This parameter is either True or False. When set to True, the path cost of each port on the bridge is dynamically calculated based on the port speed. If the parameter is set to False, the path cost of the bridge is based on the initial value of the port speed.

- In the middle section of the page, the status of the MSTP bridge parameters are shown. The bottom section of the page is where you can adjust the values of these parameters. The following fields are listed:

Maximum Age - The Maximum Age defines the amount of time a port will wait for STP/RSTP information. MSTP uses this parameter when interacting with STP/RSTP domains on the boundary ports. Its range is 6 - 40 seconds.

Forward Delay - The Forward Delay defines the time that the bridge spends in the listening and learning states. Its range is 4 - 30 seconds.

Maximum Hop Count - The Maximum Hop Count is a parameter set in a BPDU packet when it originates. It is decremented by 1 each time it is retransmitted by the next bridge. When the Hop Count value reaches zero, the bridge drops the BPDU packet. Its range is 6 - 40 hops.

Transmit Hold Count - The Transmit Hold Count specifies the maximum number of BPDUs that the bridge can send per second. Its range is 1 - 10.

5. Once you have configured the parameters, click **Apply**.
6. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Port Configuration

To configure the MSTP parameters for each of the ports, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.
2. From the **Bridge** folder, select the **Spanning Tree** folder. The **Spanning Tree** folder expands.
3. From the **Spanning Tree** folder, select the **MSTP** folder. The **MSTP** folder expands.
4. From the **MSTP** folder, select **MSTP Port Configuration**. The AT-GS950/10PS MSTP Port Configuration Page is displayed. See Figure 26 for a partial view of this page.

MSTP Port Configuration

Port	Path Cost	Priority	PointToPoint Status	Edge Port	MSTP Status	Protocol Migration	Hello Time	AutoEdge Status	Restricted Role	Restricted TCN	Action
All	<input type="text"/>	<input type="text"/>	Ignore ▾	Ignore ▾	Ignore ▾	Ignore ▾	<input type="text"/>	Ignore ▾	Ignore ▾	Ignore ▾	Apply
1	<input type="text" value="0"/>	<input type="text" value="0"/>	ForceTrue ▾	True ▾	Disable ▾	True ▾	<input type="text" value="0"/>	True ▾	True ▾	True ▾	Apply
2	<input type="text" value="0"/>	<input type="text" value="0"/>	ForceTrue ▾	True ▾	Disable ▾	True ▾	<input type="text" value="0"/>	True ▾	True ▾	True ▾	Apply
3	<input type="text" value="0"/>	<input type="text" value="0"/>	ForceTrue ▾	True ▾	Disable ▾	True ▾	<input type="text" value="0"/>	True ▾	True ▾	True ▾	Apply
4	<input type="text" value="0"/>	<input type="text" value="0"/>	ForceTrue ▾	True ▾	Disable ▾	True ▾	<input type="text" value="0"/>	True ▾	True ▾	True ▾	Apply
5	<input type="text" value="0"/>	<input type="text" value="0"/>	ForceTrue ▾	True ▾	Disable ▾	True ▾	<input type="text" value="0"/>	True ▾	True ▾	True ▾	Apply
6	<input type="text" value="0"/>	<input type="text" value="0"/>	ForceTrue ▾	True ▾	Disable ▾	True ▾	<input type="text" value="0"/>	True ▾	True ▾	True ▾	Apply
7	<input type="text" value="0"/>	<input type="text" value="0"/>	ForceTrue ▾	True ▾	Disable ▾	True ▾	<input type="text" value="0"/>	True ▾	True ▾	True ▾	Apply
8	<input type="text" value="0"/>	<input type="text" value="0"/>	ForceTrue ▾	True ▾	Disable ▾	True ▾	<input type="text" value="0"/>	True ▾	True ▾	True ▾	Apply

Figure 26. AT-GS950/10PS MSTP Port Configuration Page

You may choose a port and configure its MSTP parameters on this page. The following information is displayed:

Port - Indicates ports 1 through 10 on the AT-GS950/10PS switch. You can select the **All** row to apply the same setting to all ports of your switch for the **Point-to-Point Status**, **Edge Port**, **MSTP Status**, **Protocol Migration**, **AutoEdge Status**, **Restricted Role**, **Restricted TCN** fields.

Path Cost - Specifies the cost of a port to the root.

Priority - Specifies the spanning tree port priority.

PointToPoint Status - Indicates if the port is connected to another network device (point-to-point) in the network topology. See “Point-to-Point and Edge Ports” on page 66 for more information.

ForcedTrue - The port is connected to a network device in the network topology.

ForcedFalse - The port is not connected to a network device in the network topology.

Auto - The switch will automatically determine the port type.

Edge Port - Indicates if a port is connected to an edge device in the network topology or not. See “Point-to-Point and Edge Ports” on page 66 for more information.

True - The port is connected to an edge device and the port will always be in a forwarding state.

False - The port is not connected to an edge device.

MSTP Status - Indicates if MSTP is Enabled or Disabled.

Enabled - MSTP is active on the port.

Disabled - MSTP is inactive on the port.

Protocol Migration - A switch running MSTP supports a built-in protocol migration mechanism that enables it to inter-operate with legacy 802.1D switches.

True - The switch is able to inter-operate with 802.1D BPDU packets.

False - This switch can only operate with RSTP and MSTP packets.

Hello Time - The Hello Time is frequency with which the root bridge sends out a BPDU. See “Hello Time and Bridge Protocol Data Units (BPDU)” on page 66 for more information.

AutoEdge Status - This parameter allows the switch to detect if the port functioning as an edge port.

Restricted Role - This parameter prevents the port from becoming a root port.

True - The port is prevented from being a root port or a port that is used to communicate with the root bridge.

False - This switch can only operate with RSTP and MSTP packets.

The net effect of setting all ports on the switch to True is that it forces the switch into the role of the root bridge regardless of other path costs in the network.

Restricted TCN - The Restricted TCN parameter does not allow Topology Change Notification (TCN) BPDUs to be processed on the port.

True - The port cannot process receive/transmit TCN BPDUs.

False - The port can process receive/transmit TCN BPDU packets.

5. Once you have configured the parameters, click **Apply** in the **Action** column.
6. If you choose to change the MSTP port configuration for other ports, repeat steps 4 and 5.
7. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

VLAN Mapping

You can create, modify and delete MSTP settings with the procedures in the following sections:

- ❑ "Open MSTP VLAN Mapping Page"
- ❑ "Create VLAN Mapping to MST Instance".
- ❑ "Modify MST Instance" on page 87.
- ❑ "Delete MST Instance" on page 87.

Open MSTP VLAN Mapping Page

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.
2. From the **Bridge** folder, select the **Spanning Tree** folder. The **Spanning Tree** folder expands.
3. From the **Spanning Tree** folder, select the **MSTP** folder. The **MSTP** folder expands.
4. From the **MSTP** folder, select **MSTP VLAN Mapping**. The MSTP VLAN Mapping Page is displayed. See Figure 27.

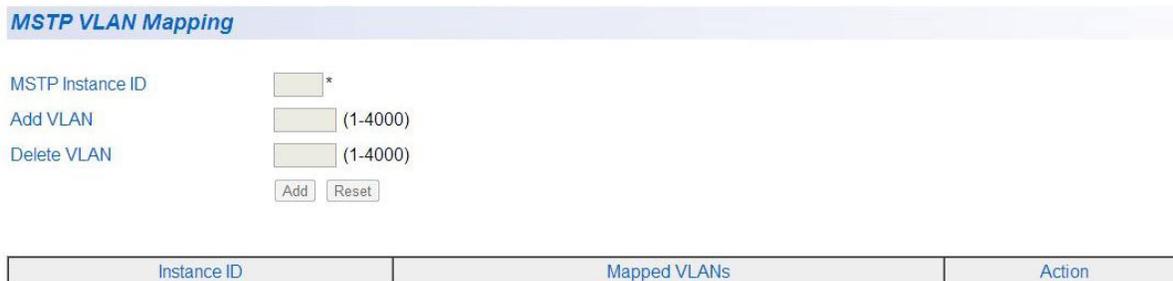


Figure 27. MSTP VLAN Mapping Page

Create VLAN Mapping to MST Instance

1. Enter the **MSTP Instance ID**. You can enter any number of MSTP IDs up to the maximum MSTP ID. See "Multiple Spanning Tree Configuration" on page 80 for more information.
2. Enter an existing VLAN ID in the **ADD VLAN** field that you want to associate with the MSTI ID entered in step 4.
3. Click **Add**.
The Instance ID and the Mapped VLAN will be displayed in the table on the page.
4. You may add as many VLANs to one MST Instance by repeating steps 4 through 6.

5. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Modify MST Instance

If you wish to modify a MST Instance, you must first delete the instance and then redefine it. Refer to “Create VLAN Mapping to MST Instance” on page 86 for more information.

Delete MST Instance

1. In the **Action** column of the table, click on **Delete** for the MST Instance that want to delete.
The instance is deleted along with the mapped associations to the VLANs that are listed.
2. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Port Settings

To configure the MSTP port settings, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.
2. From the **Bridge** folder, select the **Spanning Tree** folder. The **Spanning Tree** folder expands.
3. From the **Spanning Tree** folder, select the **MSTP** folder. The **MSTP** folder expands.
4. From the **MSTP** folder, select **MSTP Port Settings**. The MSTP Port Settings Page is displayed. See Figure 28.

MSTP Port Settings					
Port	MSTP Instance ID	Port State	Priority	Cost	Action
All	-	Ignore ▾	<input type="text"/>	<input type="text"/>	<input type="button" value="Apply"/>

Figure 28. MSTP Port Settings Page

You may choose a port and configure its MSTP parameters on this page. The following information is displayed:

Port - Indicates ports 1 through 10 on the AT-GS950/10PS switch. You can select the **All** row to apply the same settings to all ports on your switch for the **Port State** field.

MSTP Instance ID - Indicates the MSTP Instance that associated with this port.

Port State - This parameter activates or deactivates the port. Select one of the following choices from the pull-down menu:

Enable - Allows the port to forward packets.

Disable - Does not allows the port to forward packets.

Priority - This is the port priority used by MSTP in calculating path costs when two ports on the switch have the same port cost.

Cost - This is the port cost used by MSTP when calculating path cost to the root bridge.

5. Once you have configured the parameters, click **Apply** in the **Action** column.

6. If you choose to change the MSTP port settings for other ports, repeat steps 4 and 5.
7. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Topology Information

To configure the MSTP port settings, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**.
The **Bridge** folder expands.
2. From the **Bridge** folder, select the **Spanning Tree** folder.
The **Spanning Tree** folder expands.
3. From the **Spanning Tree** folder, select the **MSTP** folder.
The **MSTP** folder expands.
4. From the **MSTP** folder, select **MSTP Port Settings**.
The AT-GS950/10PS Topology Information Page is displayed. See Figure 29.
A partial view of the AT-GS950/10PS Topology Information Page is displayed. See Figure 29.

Topology Information											
Port	Designated Root	Root Priority	Designated Bridge	Designated Port	Designated Cost	Regional Root	Regional Root Priority	Regional Path Cost	Type	Role	Port State
1	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	14.d7	0	2c:d7:22:40:2c:d7:22:40	11479	0	0	Disabled	Disabled
2	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	14.d7	0	2c:d7:22:40:2c:d7:22:40	11479	0	0	Disabled	Disabled
3	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	14.d7	0	2c:d7:22:40:2c:d7:22:40	11479	0	0	Disabled	Disabled
4	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	14.d7	0	2c:d7:22:40:2c:d7:22:40	11479	0	0	Disabled	Disabled
5	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	14.d7	0	2c:d7:22:40:2c:d7:22:40	11479	0	0	Disabled	Disabled
6	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	14.d7	0	2c:d7:22:40:2c:d7:22:40	11479	0	0	Disabled	Disabled
7	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	14.d7	0	2c:d7:22:40:2c:d7:22:40	11479	0	0	Disabled	Disabled
8	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	14.d7	0	2c:d7:22:40:2c:d7:22:40	11479	0	0	Disabled	Disabled

Figure 29. AT-GS950/10PS Topology Information Page

The following information displayed on this page shows the current status of MSTP for each port:

Port - Indicates ports 1 through 10 on the AT-GS950/10PS switch.

Designated Root - The designated root bridge to which the switch’s root port is actively connected.

Root Priority - This parameter specifies the priority used in determining the regional root for a particular MSTI. For more information, see Table 11 on page 360.

Designated Bridge - The bridge providing the least cost path to the root bridge from a network segment.

Designated Port - The port providing the least cost path to the root bridge from a network segment.

Designated Cost - The cost from the designated bridge to the root bridge.

Regional Root - The root bridge of the MST instance.

Regional Root Priority - The priority of the regional root port.

Regional Path Cost - The path cost from the regional root port to the regional root bridge.

Type - This specifies the regional port type which can be either a point-to-point or an edge type port. See “Point-to-Point and Edge Ports” on page 66 for more information.

Role - Indicates the port's role which may be Disabled, Root, Designated, Backup, or Alternate. See the parameter definitions described for **Role** under “Configure the Basic RSTP Port Settings” on page 73 for more information.

Port State - Indicates the ports spanning tree state which may be Blocking, Listening, Learning, Forwarding, Disabled. See the parameter definitions described for **Port State** under “Configure the Basic RSTP Port Settings” on page 73 for more information.

Chapter 6

Static Port Trunking

This chapter contains a description of port trunking and the procedures for creating, modifying, and deleting a static port trunk. The following topics are discussed:

- ❑ “Overview” on page 94
- ❑ “Create a Port Trunk” on page 97
- ❑ “Modify a Port Trunk” on page 99
- ❑ “Disable a Port Trunk” on page 101

Note

For information about Link Aggregation Control Protocol (LACP) port trunking, see Chapter 11, “LACP Port Trunks” on page 155.

Note

To permanently save your new settings or any changes to the configuration file, select **Save Configuration to Flash** from the main menu on the left side of the page.

Overview

A port trunk is an economical way for you to increase the bandwidth between the Ethernet switch and another networking device, such as a network server, router, workstation, or another Ethernet switch. A port trunk is a group of ports that have been grouped together to function as one logical path. A port trunk increases the bandwidth between the switch and another network device and is useful in situations where a single physical link between the devices is insufficient to handle the traffic load.

A static port trunk consists of two to eight ports on the switch that function as a single virtual link between the switch and another device. A static port trunk improves performance by distributing the traffic across multiple ports between the devices and enhances reliability by reducing the reliance on a single physical link.

A static trunk is easy to configure. You designate the ports on the switch that are in the trunk and the AT-S110 Management software on the switch automatically groups them together.

The example in Figure 30 illustrates a static port trunk of four links between two AT-GS950/10PS switches.

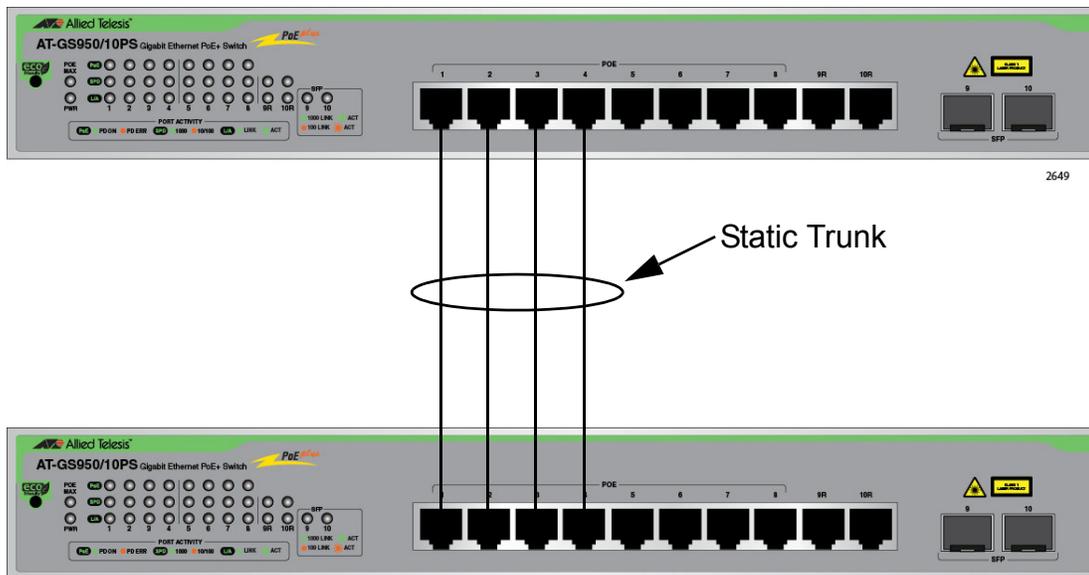


Figure 30. Static Port Trunk Example

Network equipment vendors tend to employ different techniques to implement static trunks. Consequently, a static trunk on one device may be incompatible with the same feature on a device from a different manufacturer. For this reason static trunks are typically employed only between devices from the same vendor. That is not to say that an Allied Telesis Layer 2 managed switch cannot form a static trunk with a device from another manufacturer; however, the implementations of static trunking on the two devices may be incompatible.

Also, note that a static trunk does not provide for redundancy or link backup. If a port in a static trunk loses its link, the trunk's total bandwidth is diminished. Although the traffic carried by the lost link is shifted to one of the remaining ports in the trunk, the bandwidth remains reduced until the lost link is re-established or you reconfigure the trunk by adding another port to it.

General Guidelines

Following are the guidelines for creating a static trunk:

- Allied Telesis recommends setting static port trunks between Allied Telesis networking devices to ensure compatibility.
- A static trunk can contain up to eight ports.
- The ports of a static trunk must be of the same medium type. They can be all twisted-pair ports or all fiber optic ports, but not a combination of the two.
- The ports of a trunk can be either consecutive (for example, Ports 2 through 4) or nonconsecutive (for example, ports 3, 5, and 7).
- Before creating a port trunk, verify that the settings are the same for all ports in the trunk including speed (1000/Full), duplex mode, flow control, back pressure settings and VLAN membership. If these settings are not the same, then the switch does not allow you to create the trunk.

Note

When a trunk group is formed with only combo ports as members, all port members are configured to the forced port mode at 1000/Full. The trunk ports on the connecting network switch should also be configured for 1000/Full to insure speed and duplex compatibility between the switches.

- After you have created a port trunk, a change to the speed, duplex mode, flow control, or back pressure of any port in the trunk automatically implements the same change on all the other member ports.

- A port can belong to only one static trunk at a time.
- The ports of a static trunk can be configured to be members of more than one VLAN.
- The ports of a static trunk can be either untagged or untagged members of the same VLAN.

The switch selects a port in the trunk to handle broadcast packets and packets of unknown destination. The switch makes this choice based on a hash algorithm, depending upon the source and destination MAC addresses.

Create a Port Trunk

This procedure explains how to create a static port trunk.



Caution

Do not connect the cables of a port trunk to the ports on the switch until you have configured the ports on both the switch and the end nodes. Connecting the cables prior to configuring the ports can create loops in your network topology. Loops can result in broadcast storms which can severely limited the effective bandwidth of your network.

To create a port trunk, perform the following procedure:

1. Select the **Bridge** folder.
The **Bridge** folder expands.
2. From the **Bridge** folder, select the **Trunk Config** folder.
The **Trunk Config** folder expands.
3. From the **Trunk Config** folder, select **Trunking**.
A partial view of the Trunking Page is displayed in Figure 31.

Trunking

Trunk ID 1:	<input type="checkbox"/>	Disable ▾	Apply								
Trunk ID 2:	<input type="checkbox"/>	Disable ▾	Apply								
Trunk ID 3:	<input type="checkbox"/>	Disable ▾	Apply								
Trunk ID 4:	<input type="checkbox"/>	Disable ▾	Apply								
Trunk ID 5:	<input type="checkbox"/>	Disable ▾	Apply								
Trunk ID 6:	<input type="checkbox"/>	Disable ▾	Apply								
Trunk ID 7:	<input type="checkbox"/>	Disable ▾	Apply								
Trunk ID 8:	<input type="checkbox"/>	Disable ▾	Apply								

Notes: Disable will reset the setting to default value then turn off the function.

Figure 31. Trunking Page

If the switch does not contain a port trunk, all of the ports on the switch are unchecked. If there is a port trunk, the ports in the trunk are checked.

4. Click the dialog boxes of the ports that will make up the port trunk.

A check in a box indicates the port is a member of the trunk. No check means the port is not a member. A port trunk can contain up to eight ports.

5. Change the **Trunk Status** from **Disable** to another setting. The choice in the status field are the following:

Active - The specific aggregator will broadcast and respond to LACPDU (LACP Data Unit) packets. This setting enables the LACP feature for the trunk.

Passive - The specific aggregator will not broadcast LACPDU packets, but it will respond to them. This setting disables the LACP feature for the trunk.

Manual - Enables static port trunking and disables the LACP feature for the trunk.

Disable - Disables the static port trunk and disables the LACP feature for the trunk.

6. Click **Apply**.
7. If you did not select the trunk mode **Disabled**, the trunk is now operational on the switch.
8. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.
9. Configure the port trunk on the other switch.
10. Connect the Ethernet cables between trunk ports on the AT-GS950/10PS switch and the trunk ports on the other switch.

Modify a Port Trunk

This procedure explains how to change the status of a port trunk and add or remove ports from a port trunk.



Caution

Before you disable or modify a port trunk, disconnect all of the cables from the ports of the trunk. Leaving the cables connected during the reconfiguration of a trunk can create loops in your network topology. Loops can result in broadcast storms which can severely limited the effective bandwidth of your network.

To add or remove ports from a trunk, perform the following procedure:

1. Disconnect all of the Ethernet cables from the ports of the trunk.
2. Select the **Bridge** folder.
The **Bridge** folder expands.
3. From the **Bridge** folder, select the **Trunk Config** folder.
The **Trunk Config** folder expands.
4. From the **Trunk Config** folder, select **Trunking**.
The Trunking Page is shown in Figure 31 on page 97.
5. Click the status of the port trunk you want to modify and change the status to one of the following options:
 - Disable** - Disables the port trunk.
 - Active** - The aggregator will broadcast and respond to LACPDU (LACP Data Unit) packets. This setting enables the LACP feature.
 - Passive** - The aggregator will not broadcast LACPDU packets, but it will respond to them. This setting enables the LACP feature.
 - Manual** - Enables static port trunking and disables the LACP feature.
6. To add or remove a port from a trunk, click the dialog box for the port in the corresponding trunk row.
A check in a box indicates the port is a member of the trunk. No check means the port is not a member. A port trunk can contain up to eight ports.
7. Click **Apply**.
8. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

9. Configure the port trunk on the other switch with the same parameters.
10. Connect the Ethernet cables between trunk ports on the AT-GS950/10PS switch and the trunk ports on the other switch.

Disable a Port Trunk

This procedure explains how to disable a port trunk.



Caution

Before you disable or modify a port trunk, disconnect all of the cables from the ports of the trunk. Leaving the cables connected during the reconfiguration of a trunk can create loops in your network topology. Loops can result in broadcast storms which can severely limited the effective bandwidth of your network.

To disable a port trunk, perform the following procedure:

1. Disconnect all of the Ethernet cables from the ports of the trunk.
2. Select the **Bridge** folder.
The **Bridge** folder expands.
3. From the **Bridge** folder, select the **Trunk Config** folder.
The **Trunk Config** folder expands.
4. From the **Trunk Config** folder, select **Trunking**.
The Trunking Page is shown in Figure 31 on page 97.
5. To disable a port trunk, select **Disable** from the pull-down menu next to the trunk that you want to disable.
6. Click **Apply**.
7. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.
8. Modify the port trunk configuration in the same way on the other switch.

Chapter 7

LACP Port Trunks

This chapter contains overview information about LACP port trunks and the procedures for setting this feature. This chapter contains the following sections:

- ❑ “Overview” on page 104
- ❑ “System Priority” on page 105
- ❑ “Port Priority Value” on page 106
- ❑ “General Guidelines” on page 107
- ❑ “Group Status” on page 109
- ❑ “Port Priority Configuration” on page 112

Note

For information about port trunking, see Chapter 6, “Static Port Trunking” on page 93.

Note

To permanently save your new settings or any changes to the configuration file, select **Save Configuration to Flash** from the main menu on the left side of the page.

Overview

LACP (Link Aggregation Control Protocol) port trunks perform the same function as static trunks. They increase the bandwidth between network devices by distributing the traffic load over multiple physical links. The advantage of an LACP trunk over a static port trunk is its flexibility. While implementations of static trunking tend to be vendor specific, the AT-S110 Management software implementation of LACP is compliant with the IEEE 802.3ad standard, making it interoperable with equipment from other vendors that also comply with the standard. Therefore, you can create an LACP trunk between an Allied Telesis device and network devices from other manufacturers.

Another advantage is that ports in an LACP trunk can function in a standby mode. This adds redundancy and resiliency to the trunk. If a link in a static trunk goes down, the overall bandwidth of the trunk is reduced until the link is re-established or another port is added to the trunk. In contrast, an LACP trunk can automatically activate ports in a standby mode when an active link fails so that the maximum possible bandwidth of the trunk is maintained.

For example, assume you create an LACP trunk of ports 1 to 6 on a switch and the switch is using ports 1 to 4 as the active ports and ports 5 and 6 as reserve. If an active port loses its link, the switch automatically activates one of the reserve ports to maintain maximum bandwidth of the trunk.

The main component of an LACP trunk is an *aggregator* which manages a group of ports on the switch. On the AT-GS950/10PS switch, the ports assigned to a trunk group are automatically assigned to an aggregator. Only one aggregator can be assigned to each trunk group. With LACP activated, each active trunk group is referred to as an *aggregate trunk*.

An aggregate trunk can consist of any number of ports on a switch, but only a maximum of eight ports can be active at a time. If an aggregate trunk contains more ports than can be active at once, the extra ports are placed in a standby mode. Ports in the standby mode do not pass network traffic, but they do transmit and accept LACP Data Unit (LACPDU) packets, which the switch uses to search for LACP-compliant devices.

Only ports that are part of an aggregator transmit LACPDU packets. A port that is part of an aggregator assumes that the other port is not part of an LACP trunk if it does not receive LACPDU packets from its corresponding port on the other device. Instead, it functions as port in standby mode and does not forward network traffic. However, it does continue to send LACPDU packets. If it begins to receive LACPDU packets, it automatically transitions to an active or standby mode as part of an aggregate trunk.

System Priority

It is possible for two devices interconnected by an aggregate trunk to encounter a conflict when they form the trunk. For example, the two devices might not support the same number of active ports in an aggregate trunk or might not agree on which ports are active and which are in standby mode.

If a conflict does occur, the two devices need a mechanism for resolving the problem and deciding whose LACP settings take precedence. This is the function of the system LACP priority value. This value is used whenever the devices encounter a conflict creating a trunk - the lower the number, the higher the priority. As a result, the settings on the device with the higher priority take precedence over the settings on the other device. If both devices have the same system LACP priority value, the settings on the switch with the lowest MAC address take precedence. In the AT-S110 Management software, the MAC address is called the System ID.

The LACP System Priority is pre-assigned and you cannot alter this parameter.

Port Priority Value

The switch uses a port's LACP priority to determine which ports are active and which are in the standby mode in situations where the number of ports in the aggregate trunk exceeds the highest allowed number of active ports. This parameter is a value in a range of 1 to 255, based on the port number. For instance, the priority values for ports 2 and 11 are 002 and 011, respectively. The lower the number, the higher the priority. Ports with the highest priorities are designated as the active ports in an aggregate trunk.

For example, if both 802.3ad-compliant devices support up to six active ports and there are a total of eight ports in the trunk, the six ports with the highest priorities (lowest priority values) are designated as the active ports, and the others are placed in the standby mode. If an active link goes down on a active port, the standby port with the next highest priority is automatically activated to take its place.

The selection of the active links in an aggregate trunk is dynamic and changes as links are added, removed, lost, or reestablished. For example, if an active port loses its link and is replaced by another port in the standby mode, the re-establishment of the link on the originally active port causes the port to return to the active state by virtue of having a higher priority value than the replacement port, which returns to the standby mode.

Two conditions must be met for a port in an aggregate trunk to function in the standby mode. First, the number of ports in the trunk must exceed the highest allowed number of active ports and, second, the port must be receiving LACPDU packets from the other device. A port functioning in the standby mode does not forward network traffic. However, it continues to send LACPDU packets. If a port that is part of an aggregator does not receive LACPDU packets, it functions as a normal Ethernet port and forwards network packets along with LACPDU packets.

Note

You can adjust the value of a port's priority.

General Guidelines

The following guidelines apply when creating aggregators:

- LACP must be activated on both the AT-GS950/10PS switch and its partner device.
- The other device must be 802.3ad-compliant.
- The AT-S110 Management software supports up to eight active ports in an aggregate trunk at a time.
- The AT-GS950/10PS Gigabit Ethernet PoE+ Switch can support up to eight static and LACP aggregate trunk groups at a time (for example, four static trunks and four LACP trunks). An LACP trunk is counted against the maximum number of trunks only when it is active.
- The ports of an aggregate trunk must be the same medium type: all twisted pair ports or all fiber optic ports.
- The ports of a trunk can be consecutive (for example ports 1-5) or nonconsecutive (for example, ports 2, 4, 6, 8).
- A port can belong to only one aggregator at a time.
- A port cannot be a member of an aggregator and a static trunk at the same time.
- The ports of an aggregate trunk must be untagged members of the same VLAN.
- Twisted pair ports must be set to Auto-Negotiation or 1000 Mbps, full-duplex mode. LACP trunking is not supported in half-duplex mode.
- 1000Base-X fiber optic ports must be set to full-duplex mode.
- You can create an aggregate trunk of transceivers with 1000Base-X fiber optic ports.
- Only those ports that are members of an aggregator transmit LACPDU packets.
- A member port of an aggregator functions as part of an aggregate trunk only if it receives LACPDU packets from the remote device. If it does not receive LACPDU packets, it functions as a regular Ethernet port, forwarding network traffic while also continuing to transmit LACPDU packets.
- The port with the highest priority in an aggregate trunk carries broadcast packets and packets with an

unknown destination.

- Prior to creating an aggregate trunk between an Allied Telesis device and another vendor's device, refer to the vendor's documentation to determine the maximum number of active ports the device can support in a trunk. If the number is less than eight, the maximum number for the AT-GS950/10PS switch, you should assign the other vendor's device a higher system LACP priority than your AT-GS950/10PS switch. This can help avoid a conflict between the devices if some ports are placed in the standby mode when the devices create the trunk. For background information, refer to "System Priority" on page 105.
- LACPDU packets are transmitted as untagged packets.

Group Status

To display the LACP Group Status, perform the following procedure:

1. Select the **Bridge** folder.
The **Bridge** folder expands.
2. From the **Bridge** folder, select the **Trunk Config** folder.
The **Trunk Config** folder expands.
3. From the **Trunk Config** folder, select **LACP Group Status**.
The LACP Group Status Page is displayed. See Figure 32.



Figure 32. LACP Group Status Page

Note

Go to "Create a Port Trunk" on page 97 to directly change the parameters on this page:

The **System Priority** is a preassigned value that you cannot alter. This value applies to the switch. See “System Priority” on page 105.

The **System ID** is a MAC address value assigned to the individual switch. You cannot change this value.

Group 1 to 8 indicates the ID number of the trunk (aggregation group).

Configuration Example

Use the procedure given in “Create a Port Trunk” on page 97 to configure **Trunk ID 1** as **Active** with ports 3, 4 and 5.

The LACP Group Status Page is updated. This configuration is shown in Figure 33 before the Ethernet cables are connected.

LACP Group Status	
System Priority	: 32768
System ID	: 00:00:01:03:00:80
Group: 1	
Aggregator	Attached Port List
1	
Group: 2 This group doesn't exist	
Group: 3 This group doesn't exist	
Group: 4 This group doesn't exist	
Group: 5 This group doesn't exist	
Group: 6 This group doesn't exist	
Group: 7 This group doesn't exist	
Group: 8 This group doesn't exist	

Figure 33. LACP Group Status Page with No Cables Connected

4. Physically connect the network cables between the switch and a second LACP device which is pre-configure with an LACP activated trunk of three or more ports.

The LACP Group Status Page is updated. An example of these updates is shown in Figure 34 on page 111 after three trunking cables are installed and the ports have Link-Up status.

LACP Group Status

System Priority : 32768
 System ID : 00:00:01:03:00:80

Group: 1

Aggregator	Attached Port List
1	3,4,5

Group: 2
This group doesn't exist

Group: 3
This group doesn't exist

Group: 4
This group doesn't exist

Group: 5
This group doesn't exist

Group: 6
This group doesn't exist

Group: 7
This group doesn't exist

Group: 8
This group doesn't exist

Figure 34. LACP Group Status Page with Three Cables Connected

You can now see that each port has been grouped under a single aggregator since the ports are now in a Link-Up status.

Port Priority Configuration

To select a priority for an LACP port, perform the following procedure:

1. Select the **Bridge** folder.
The **Bridge** folder expands.
2. From the **Bridge** folder, select the **Trunk Config** folder.
The **Trunk Config** folder expands.
3. From the **Trunk Config** folder, select **Port Priority**.
The AT-GS950/10PS Port Priority Page is displayed. See Figure 35 for a partial view of this page.

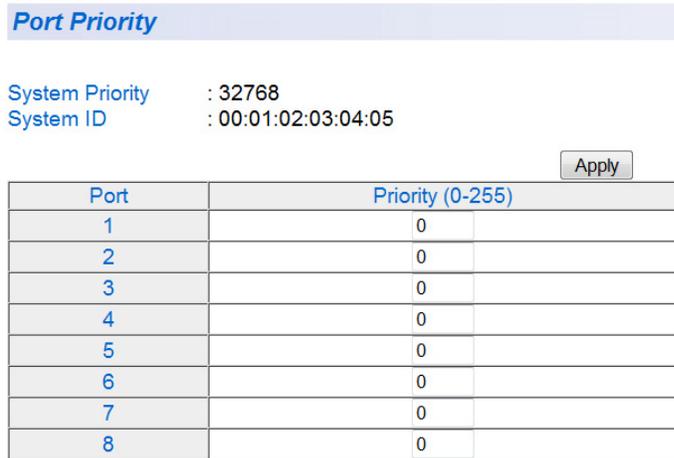


Figure 35. AT-GS950/10PS Port Priority Page

The **System Priority** is a preassigned value that you cannot alter. This value applies to the switch. See “System Priority” on page 105.

The **System ID** is a MAC address value assigned to the switch. You cannot change this value.

4. To set the port priority, select a value from 0 to 255 in the Priority column for the port you want to alter. For more information, see “Port Priority Value” on page 106
5. Select **Apply**.
6. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Chapter 8

Port Mirroring

This chapter describes the Port Mirroring feature and the procedure for setting up port mirroring. Port mirroring allows you to unobtrusively monitor the ingress and egress traffic on a port by having the traffic copied to another port. This chapter contains the following sections:

- “Overview” on page 114
- “Port Mirroring Configuration” on page 115
- “Disable Port Mirroring” on page 117

Note

To permanently save your new settings or any changes to the configuration file, select **Save Configuration to Flash** from the main menu on the left side of the page.

Overview

The port mirroring feature allows you to unobtrusively monitor the traffic received and transmitted on one or more ports by copying the traffic to another switch port. You can connect a data analyzer to the port where the traffic is copied and monitor the traffic on the other ports without impacting network performance or speed.

A port mirror has two component ports. The port or ports whose traffic you want to mirror is called the *source port(s)*. The port where the traffic will be copied to is called the *mirroring port*.

Observe the following guidelines when you create a port mirror:

- You can select more than one source port at a time. However, the more ports you mirror, the less likely the mirroring port is able to handle all the traffic. For example, if you mirror the traffic of six heavily active ports, the destination port is likely to drop packets, meaning that it does not provide an accurate mirror of the traffic of the six source ports.
- The source and mirror ports must be located on the same switch.
- You can mirror the ingress or egress traffic of the source ports or both.
- While the Mirroring feature is enabled, the mirroring port is dedicated to monitoring the traffic from the source ports and cannot be used for regular network operations.

Port Mirroring Configuration

To configure Port Mirroring, perform the following procedure:

1. Select the **Bridge** folder.
The Bridge folder expands.
2. From the **Bridge** folder, select **Mirroring**.
The Mirroring Page is displayed. See Figure 36.

Mirroring

Status:

Mirroring Port:

Ingress Port:

1	2	3	4	5	6	7	8	9	10
<input type="checkbox"/>									

Egress Port:

1	2	3	4	5	6	7	8	9	10
<input type="checkbox"/>									

Figure 36. AT-GS950/10PS Mirroring Page

3. Click the pull-down menu on the **Status** field and select one of the following choices:
 - Enable** - This parameter activates the Port Mirroring feature and the rest of the configuration parameters become active on the page.
 - Disable** - This parameter de-activates the Port Mirroring feature and the rest of the configuration parameters become inactive on the page.
4. Click **Mirroring Port** and from the pull-down menu, select the port.
5. For the source port, select the port(s) whose ingress, egress, or both ingress and egress traffic you want to monitor.
A check in a box indicates the Ingress or Egress traffic for a port has been selected.
6. Click **Apply** on the right-hand side of the page.
The Port Mirroring configuration is implemented immediately on the AT-GS950/10PS switch.
You can connect a data analyzer to the mirroring port to monitor the Ethernet traffic on the source port(s).

7. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Disable Port Mirroring

To disable Port Mirroring, perform the following procedure:

1. Select the **Bridge** folder.
The Bridge folder expands.
2. From the **Bridge** folder, select **Mirroring**.
The Mirroring page is shown in Figure 36 on page 115.
3. From the **Status** field, select **Disable** and click **Apply**.
Port mirroring is immediately disabled on the switch and the parameters on the web page become inactive. You can now use the mirroring port for regular network operations.
4. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Chapter 9

Loopback Protection

This chapter explains how to configure the Loopback Protection feature for specific ports on the AT-GS950/10PS switch. If the Tx and Rx pairs on the same port are connected, then this feature detects this condition and disables the port for a pre-configured amount of time.

This chapter contains the following topics:

- ❑ “Configuration” on page 120
- ❑ “Status” on page 122

Note

To permanently save your new settings or any changes to the configuration file, select **Save Configuration to Flash** from the main menu on the left side of the page.

Configuration

To configure the Loopback Detection feature, perform the following procedure:

- From the main menu on the left side of the page, select **Bridge**.
The **Bridge** folder expands.
- From the **Bridge** folder, select **Loopback Detection**.
A partial view of the AT-GS950/10PS Loopback Detection Page is displayed. See Figure 37.

Loopback Detection

State Enabled Disabled

Loopback Detection Global Settings

Interval (1-32767) sec

Recover Time (0 or 60-1000000) sec

Notes: Disable will reset the setting to default value then turn off the function.

Port	Loopdetect Detection State	Loop Status	Action
All	Ignore ▾	-	<input type="button" value="Apply"/>
1	Disabled ▾	Normal	<input type="button" value="Apply"/>
2	Disabled ▾	Normal	<input type="button" value="Apply"/>
3	Disabled ▾	Normal	<input type="button" value="Apply"/>
4	Disabled ▾	Normal	<input type="button" value="Apply"/>
5	Disabled ▾	Normal	<input type="button" value="Apply"/>
6	Disabled ▾	Normal	<input type="button" value="Apply"/>
7	Disabled ▾	Normal	<input type="button" value="Apply"/>
8	Disabled ▾	Normal	<input type="button" value="Apply"/>

Figure 37. AT-GS950/10PS Loopback Detection Page

- For the **Loopback Detection State** field at the top of the page, select one of the following radio buttons:

Enabled: This selection enables the Loopback Detection feature across the switch. This state must be enabled for the individual port **Loopback Detection State** to be effective.

Disabled: This selection disables the Loopback Detection feature on the switch.

- Under the **Loopback Detection Global Settings**, configure the following parameters:

Interval: This parameter sets the interval of time that the ports are tested. The range is 1 to 32767 seconds.

Recover Time: This parameter sets the amount of time that the port will take to recover once the loopback condition has been removed. The range is 60 to 1000000 seconds.

If the **Recover Time** is set to 0, the port recovery is disabled until it is manually reset. It can be reset by re-configuring the **Recover Time** to its normal operating range or by disabling the Loopback Detection feature on the switch.

- Click the **Apply** button just above the **Action** column in the table at the bottom of the page.

The **Loopback Detection Global Settings** parameters becomes active.

- In the table at the bottom of the page, select one of the **Loopback Detection State** choices from the pull down menu:

Ignore: This parameter indicates that the setting in the **All** row does not apply to the **Loopback Detection State** field. In other words, each port is set individually.

Enabled: This selection enables the Loopback Detection feature for each port. This state must be enabled along with the **State** field at the top of the page before this feature can be active on the selected port.

Disabled: This selection disables the Loopback Detection feature on the selected port.

Note

In the **All** row when you select **Enable** or **Disable** instead of **Ignore**, the selection applies to all of the AT-GS950/10PS switch ports.

- Click the **Apply** button in the Action column of the table.
- Repeat steps 6 and 7 for other individual port settings.
- From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Status

The status of the Loopback Detection is given in the Loop Status column of the table at the bottom of the Loopback Detection page. See Figure 37 on page 120. The status is one of the following states:

Normal: This status indicates that the port does not have the Tx to Rx pairs connected.

Disabled: This status indicates that the port does not have the Tx to Rx pairs connected. The **Disabled** state will be reset to **Normal** after two conditions are both met:

- The loopback condition does not exist anymore.
- The specified **Recovery Time** has elapsed.

Note

If the **Recover Time** is set to 0, the port recovery is disabled until it is manually reset. It can be reset by re-configuring the **Recover Time** to its normal operating range or by disabling the Loopback Detection feature on the switch.

Chapter 10

MAC Address Table

This chapter provides a description of the static multicast MAC address feature and the procedure for configuring it. This chapter includes the following sections:

- ❑ “Overview” on page 124
- ❑ “Static Unicast MAC Address Configuration” on page 126
- ❑ “Static Multicast Address Configuration” on page 130
- ❑ “Modify Static Multicast Address” on page 133
- ❑ “Delete Static Multicast Address” on page 134

Note

To permanently save your new settings or any changes to the configuration file, select **Save Configuration to Flash** from the main menu on the left side of the page.

Overview

The AT-GS950/10PS switch has a MAC address table with a storage capacity of up to 8,000 entries. The table stores the MAC addresses of the network nodes connected to its ports and the port number where each address is learned. There are two types of MAC addresses, dynamic and static.

Dynamic MAC addresses are addresses that the switch learns automatically by examining the source MAC addresses of the frames received by the ports. This type of MAC address is 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 after a specified period of time. The switch assumes that the node 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 MAC address table can also store a *static MAC address* which is a MAC address of an end node that you assign to a switch port manually. A static MAC address remains in the table indefinitely and is never deleted by the switch, even when the end node is inactive. You can only delete a static MAC address by manually configuring the switch with the AT-S110 Management Software.

There are two reasons to enter static MAC addresses. You may want to enter end nodes the switch does not learn in its normal dynamic learning process. Or, you want a MAC address to remain permanently in the table, even when the end node is inactive.

Static multicast addresses are a subset of the static MAC addresses. With the Static Multicast Address feature, you can add static multicast addresses to the MAC address table. You can then assign the static MAC address to a port or ports which are called Group Members in the AT-S110 interface. Each port has a maximum limit of 256 static multicast addresses.

In some network environments that are confined to one LAN (such as an industrial application with a server, a switch and many controllers), there may be various multicast streams that need to be distributed to some network nodes, but not others. If the data sent in these streams is time-sensitive and cannot be delayed because of the configuration time associated with the IGMP Snooping feature, then static multicast addresses may be the solution.

If a multicast address and its associated ports of the switch are predefined within the network design and they will not change over time, then they can be manually entered as static entries into the MAC address table. This allows the multicast stream to be forwarded immediately to those

predefined ports entered in the MAC table without any configuration delays or loss of data.

Static Unicast MAC Address Configuration

This procedure explains how to set the static multicast feature for each port on the AT-GS950/10PS switch. Before beginning this procedure, you must create either an 802.1Q VLAN ID or a Port-Based VLAN Index. For information about defining these parameters, see:

- ❑ “Tagged VLAN Configuration” on page 157 regarding the **802.1Q VLAN ID** parameter.
- ❑ “Port-Based VLAN Configuration” on page 164 regarding the **Port-Based VLAN Index** parameter.

To add a static MAC address to the switch, perform the following procedure:

1. From the main menu on the left side of the page, select the **Bridge** folder.
The **Bridge** folder expands.
2. From the **Bridge** folder, select **Static Unicast**.
The Static Unicast Address Table Page is displayed. See Figure 38.

Static Unicast Address Table

802.1Q VLAN: (1-4000)
 Port-Based VLAN Index: (1-52)
 MAC Address: : : : : :

Port Member

1	2	3	4	5	6	7	8	9	10
<input type="checkbox"/>									

802.1Q VLAN

VLAN ID	MAC Address	Port Members	Action
<< Static Unicast address table is empty >>			

Port-Based VLAN

VLAN ID	MAC Address	Port Members	Action
<< Static Unicast address table is empty >>			

Figure 38. AT-GS950/10PS Static Unicast Address Table Page

3. Select either the **802.1Q VLAN ID** or **Port-Based VLAN Index** radio button and enter the respective **VLAN ID** (1-4000) or **VLAN Index** (1 - 52).

Note

An error message is generated when you enter a **VLAN ID** or **VLAN Index** which is not been defined or when you enter a **VLAN ID** or **VLAN Index** without also clicking on the respective radio button.

4. In the **Group MAC Address** field, enter a unicast MAC address.
5. Assign the MAC address a **Port Member** (or members) by selecting the check box beside each port number.

Note

You can assign a maximum limit of 256 static unicast addresses on the switch.

6. Click **Add**.
The Static Unicast Address Table is updated and displayed with the new MAC Address.
See Figure 39 for an example of a Port-based VLAN.

Static Unicast Address Table

802.1Q VLAN: (1-4000)
 Port-Based VLAN Index: (1-52)

MAC Address: : : : : :

Port Member

1	2	3	4	5	6	7	8	9	10
<input type="checkbox"/>									

802.1Q VLAN

VLAN ID	MAC Address	Port Members	Action
<< Static Unicast address table is empty >>			

Port-Based VLAN

VLAN ID	MAC Address	Port Members	Action
2	A4.54.86.12.00.00	2	Modify / Delete

Figure 39. Static Unicast Address Table with Port-Base VLAN Example

7. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Modify Static Unicast Address

To modify the port assignment of a unicast MAC address in the MAC address table, perform the following procedure:

1. From the main menu on the left side of the page, select the **Bridge** folder.
2. From the **Bridge** folder, select **Static Unicast**.
The Static Unicast Address Table Page is displayed. See Figure 38 on page 126.
3. Select **Modify** next to the static MAC address that you want to change.
The Modify Static Unicast Address Page is displayed.
See Figure 40.

Modify Static Unicast Address Table

Port-Based VLAN Index:	2								
MAC Address	A4:54:86:12:00:00								
Port Member									
1	2	3	4	5	6	7	8	9	10
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>							
									<input type="button" value="Apply"/> <input type="button" value="Restore"/>

Figure 40. Modify Static Unicast Address Page

4. In the **Group Member** row, select the check boxes for the ports that you want to include or remove in the **Group Member** area. Selected ports are indicated with a check mark.

Note

To restore the original group member ports, click **Restore**.

5. Click **Apply**.
6. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Delete Static Unicast Address

To delete a unicast MAC address from the MAC address table, perform the following procedure:

1. From the main menu on the left side of the page, select the **Bridge** folder.
2. From the **Bridge** folder, select **Static Unicast**.
The Static Unicast Address Table Page is displayed. See Figure 38 on page 126.
3. Select **delete** next to the static unicast address that you want to remove.
The static unicast address is removed from the Static Unicast Address Table Page.
4. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Static Multicast Address Configuration

This procedure explains how to set the static multicast feature for each port on the AT-GS950/10PS switch. Before beginning this procedure, you must create an **802.1Q VLAN ID** or a **Port-Based VLAN Index**. For information about defining these parameters, see:

- ❑ “Tagged VLAN Configuration” on page 157 regarding the **802.1Q VLAN ID** parameter.
- ❑ “Port-Based VLAN Configuration” on page 164 regarding the **Port-Based VLAN Index** parameter.

To add a static MAC address to the switch, perform the following procedure:

1. From the main menu on the left side of the page, select the **Bridge** folder.
The **Bridge** folder expands.
2. From the **Bridge** folder, select **Static Multicast**.
The Static Multicast Address Table Page is displayed.
See Figure 41.

Static Multicast Address Table

802.1Q VLAN: (1-4000)
 Port-Based VLAN Index: (1-52)
 Group MAC Address: : : : : :

Group Member

1	2	3	4	5	6	7	8	9	10
<input type="checkbox"/>									

802.1Q VLAN

VLAN ID	MAC Address	Group Members	Action
<< Static multicast address table is empty >>			

Port-Based VLAN

VLAN ID	MAC Address	Group Members	Action
<< Static multicast address table is empty >>			

Figure 41. AT-GS950/10PS Static Multicast Address Table Page

3. Select either the **802.1Q VLAN ID** or **Port-Based VLAN Index** radio button and enter the respective **VLAN ID** (1-4000) or **VLAN Index** (1 - 52).

Note

An error message is generated when you enter a **VLAN ID** or **VLAN Index** which is not been defined or when you enter a **VLAN ID** or **VLAN Index** without also clicking on the respective radio button.

4. In the **Group MAC Address** field, enter a multicast MAC address. The range is from 01:00:5E:00:01:00 to 01:00:5E:7F:FF:FF.
5. Assign the MAC address a **Group Member** (or members) by selecting the check box beside each port number.

Note

You can assign a maximum limit of 256 static multicast addresses on the switch.

6. Click **Add**.
The Static Multicast Address Table is updated with the new MAC Address.
See Figure 42.

Hello

Static Multicast Address Table

802.1Q VLAN: (1-4000)
 Port-Based VLAN Index: (1-52)

Group MAC Address: : : : : :

Group Member

1	2	3	4	5	6	7	8	9	10
<input type="checkbox"/>									

802.1Q VLAN

VLAN ID	MAC Address	Group Members	Action
<< Static multicast address table is empty >>			

Port-Based VLAN

VLAN ID	MAC Address	Group Members	Action
2	45:2A:B5:00:00:00	2	Modify / Delete

Figure 42. Static Multicast Address Table Example

Note

The **Group MAC Address** values that you enter on the Static Multicast Address Table Page are also displayed on the IGMP Snooping Page. For more information, see “IGMP Snooping Configuration” on page 138.

7. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Modify Static Multicast Address

To modify the port assignment of a multicast MAC address in the MAC address table, perform the following procedure:

1. From the main menu on the left side of the page, select the **Bridge** folder.
2. From the **Bridge** folder, select **Static Multicast**.
The Static Multicast Address Table Page is displayed. See Figure 41 on page 130.
3. Select **Modify** next to the static MAC address that you want to change.
The Modify Static Multicast Address Page is displayed.
See Figure 43.

Hello

[Modify Static Multicast Address Table](#)

Port-Based VLAN Index: 2

Group MAC Address: 45:2A:B5:00:00:00

Group Member

1	2	3	4	5	6	7	8	9	10
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>							

Figure 43. Modify Static Multicast Address Page

4. In the **Group Member** row, select the check boxes for the ports that you want to include or remove in the Group Member area.
5. Selected ports are indicated with a check mark.

Note

To restore the original group member ports, click **Restore**.

6. Click **Apply**.
7. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Delete Static Multicast Address

To delete a multicast MAC address from the MAC address table, perform the following procedure:

1. From the main menu on the left side of the page, select the **Bridge** folder.
1. From the **Bridge** folder, select **Static Multicast**.
The Static Multicast Address Table Page is displayed. See Figure 41 on page 130.
2. Select **delete** next to the static multicast address that you want to remove.
The static multicast address is removed from the Static Multicast Address Table Page.
3. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Chapter 11

IGMP Snooping

This chapter contains a description of the IGMP Snooping procedure as well as procedures for working with IGMP Snooping in the web interface. The following topics are discussed:

- ❑ “Overview” on page 136
- ❑ “IGMP Snooping Configuration” on page 138

Note

To permanently save your new settings or any changes to the configuration file, select **Save Configuration to Flash** from the main menu on the left side of the page.

Overview

IGMP enables IPv4 routers to create lists of nodes that are members of multicast groups. (A group of end nodes that receive multicast packets from a multicast application is defined as a multicast group.) The router creates a multicast membership list by periodically sending out queries to the local area networks connected to its ports.

A node that wants to become a member of a multicast group responds to a query by sending a *report* which indicates an end node's desire to become a member of a multicast group. Nodes that join a multicast group are referred to as *host nodes*. After becoming a member of a multicast group, a host node must continually issue reports on a continuous basis to remain a member.

After 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. Any multicast packets belonging to that multicast group are then forwarded by the router out the port. 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 three versions of IGMP— versions 1, 2, and 3. One of the differences between the versions is how a host node signals that it no longer wants to be a member of a multicast group. In version 1, it 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*, it 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*. After receiving a leave request from a host node, the router removes the node from appropriate membership list. The router also stops sending multicast packets from the port if it determines there are no further host nodes on the port.

Version 3 adds the ability of host nodes to join or leave specific sources in a multicast group.

The IGMP snooping feature on the AT-GS950/10PS switch supports IGMP versions 1 and 2. The switch monitors the flow of queries from a router and reports and leave messages from host nodes to build its own multicast membership lists. It uses the lists to forward multicast packets only to its own 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 ports connected to host nodes.

Without IGMP snooping, a switch floods multicast packets from all of its ports, except the port on which it received the packet. Such flooding of packets can negatively impact network performance.

The AT-GS950/10PS switch maintains a list of 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

By default, IGMP snooping is disabled on the switch.

IGMP Snooping Configuration

This procedure explains how to set IGMP snooping and IGMP Snooping Querier on the switch and set the IGMP Snooping (V1) age-out timer.

To configure IGMP snooping, perform the following procedure:

1. From the main menu on the left side of the page, select the **Bridge** folder.
The **Bridge** folder expands.
2. From the **Bridge** folder, select the **Trunk Config** folder.
3. From the **Trunk Config** folder, select **IGMP Snooping**.
The IGMP Snooping Page is displayed. See Figure 44.

IGMP Snooping

IGMP Snooping Status:

IGMP Snooping Age-Out Timer: Sec. (280-420)

IGMP Snooping Querier Status:

IGMP Snooping Query Interval: Sec. (1-1800)

Show result per 802.1Q VLAN ID Show result per port-based VLAN index

802.1Q VLAN

VLAN ID	Multicast group address
---------	-------------------------

Page

Figure 44. IGMP Snooping Page

4. To enable or disable IGMP Snooping on the switch, select **Enable** or **Disable** from the pull-down menu.
5. To set the age-out timer, type the number of seconds you want the switch to wait before it purges an inactive dynamic MAC address.
The range of this parameter is from 280 to 420 seconds.
6. To enable the IGMP Snooping Querier, select **Enable** or **Disable** from the pull-down menu next to IGMP Snooping Querier Status.
7. To sent the IGMP Snooping Query Interval, set the timer from 1 to 1800 seconds.
8. Click **Apply**.

- The IGMP Snooping Page is updated with active Multicast Group address. See Figure 45.

Note

The **Multicast Group Address** table contains MAC addresses of nodes that are active members of multicast groups. To set a static Multicast Group Address, see “Static Multicast Address Configuration” on page 130.

IGMP Snooping

IGMP Snooping Status: ▾

IGMP Snooping Age-Out Timer: Sec. (280-420)

IGMP Snooping Querier Status: ▾

IGMP Snooping Query Interval: Sec. (1-1800)

802.1Q VLAN

VLAN ID	Multicast group address
---------	-------------------------

Page ▾

Figure 45. IGMP Snooping Page with MAC Addresses

- To display ports that are members of the multicast group address, click on the MAC address.
- From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Chapter 12

Storm Control

This chapter contains a description and configuration procedures for the Storm Control (bandwidth) feature. The following topics are discussed:

- ❑ “Overview” on page 142
- ❑ “Configuration” on page 144
- ❑ “Ingress Rate Limiting” on page 146
- ❑ “Egress Rate Limiting” on page 148

Note

To permanently save your new settings or any changes to the configuration file, select **Save Configuration to Flash** from the main menu on the left side of the page.

Overview

The features available in the AT-S110 Management Software allow you to limit Ethernet traffic within your switch based on specific criteria. You can use Storm Control to limit the bandwidth of various types of Ethernet packets. With Ingress and Egress Rate Limiting, you can limit the traffic volume at the input or output ports respectively.

The Storm Control feature allows you regulate the reception rate of broadcast, multicast, and destination lookup failure (DLF) packets. The AT-S110 Management Software allows you to set separate limits for each port beyond which each of the different packet types are discarded. Each setting can be configured on individual ports or on all of the ports of the AT-GS950/10PS switch. Traffic is measured in packets per second. See the following definitions for more information about these settings.

Destination Lookup Failure - The Destination Lookup Failure (DLF) setting is concerned with comparing the destination MAC address of a packet received by the switch to the forwarding database. When the AT-GS950/10PS switch receives a packet, it scans the forwarding database and looks for a match to the destination MAC address in the received packet. If the MAC address is not present, then the packet is flooded according to the VLAN rules. By default, this setting is disabled on the switch which means that all DLF packets are automatically forwarded according to the VLAN rules.

Broadcast Setting - The broadcast setting applies to allowing or denying broadcast packets on each port.

Multicast Setting - The multicast setting applies to allowing or denying multicast packets on each port.

Threshold Level - In regards to Bandwidth control, the threshold level is the number of DLF, broadcast, and multicast packets that are sent by or received from a port. This value is measured in packets per second. You can set the threshold level to low, medium, or high.

Note

The packet sizes affected by this threshold level can vary in size from 64 Bytes to 1024 Bytes.

**Ingress Rate
Limiting**

The Ingress Rate Limiting feature restricts the traffic to a pre-configured data rate that can flow into a port. This data rate limit can be configured in 64 Kbps increments within a range from 64 Kbps to 1000 Mbps. The formula for calculating the bandwidth limit is as follows:

$$\text{Bandwidth} = 64\text{Kbps} \times \text{rate limit}$$

The rate limit parameter is an integer ranging from 1 to 15625.

**Egress Rate
Limiting**

The Egress Rate Limiting feature restricts the traffic to a pre-configured data rate that can flow out of a port. This data rate limit can be configured in 64 Kbps increments within a range from 64 Kbps to 1000 Mbps. The formula for calculating the bandwidth limit for the 10/100/1000Base-T ports is as follows:

$$\text{Bandwidth} = 64\text{Kbps} \times \text{rate limit}$$

The rate limit parameter is an integer ranging from 1 to 15625.

Configuration

This procedure explains how to set DLF, broadcast, multicast, and threshold levels for each port on the AT-GS950/10PS switch.

To change the settings of the storm control feature, perform the following procedure:

1. From the main menu on the left side of the page, select the **Bridge** folder.
2. From the **Bridge** folder, select **Storm Control**.
The **Storm Control** folder expands.
3. From the **Storm Control** folder, select **Storm Control**.
The AT-GS950/10PS Storm Control page is displayed. See Figure 46 for a partial view of this page.

Storm Control					
Port	DLF	Broadcast	Multicast	Threshold	Action
ALL	Ignore ▾	Ignore ▾	Ignore ▾	Ignore ▾	Apply
1	Disable ▾	Disable ▾	Disable ▾	Low ▾	Apply
2	Disable ▾	Disable ▾	Disable ▾	Low ▾	Apply
3	Disable ▾	Disable ▾	Disable ▾	Low ▾	Apply
4	Disable ▾	Disable ▾	Disable ▾	Low ▾	Apply
5	Disable ▾	Disable ▾	Disable ▾	Low ▾	Apply
6	Disable ▾	Disable ▾	Disable ▾	Low ▾	Apply
7	Disable ▾	Disable ▾	Disable ▾	Low ▾	Apply
8	Disable ▾	Disable ▾	Disable ▾	Low ▾	Apply

Figure 46. AT-GS950/10PS Storm Control Page

4. To enable or disable the **DLF** field, select **Enable** or **Disable** from the **DLF** pull-down menu next to the port that you want to change.
You can select the **ALL** row to set all of the ports to the same setting.

Note

For more information about the Destination Lookup Failure (**DLF**) setting, see “Overview” on page 142.

5. Click **Apply**.
6. To enable or disable ingress and egress **Broadcast** packets, select **Enable** or **Disable** from the **Broadcast** pull-down menu next to the port that you want to change.
You can select the **ALL** row to set all of the ports to the same setting.

Note

For more information, see the **Broadcast** setting definition in “Overview” on page 142.

7. Click **Apply**.
8. To enable or disable ingress and egress **Multicast** packets, select **Enable** or **Disable** from the **Multicast** pull-down menu next to the port that you want to change.
You can select the **ALL** row to set all of the ports to the same setting.

Note

For more information, see the **Multicast** setting definition in “Overview” on page 142.

9. Click **Apply**.
10. To set the **Threshold** field, use the pull-down menu next to the port that you want to change. Select **Low**, **Medium**, or **High** which correspond to the following values:
 - High** - Specifies 2,200 to 2,500 packets per second.
 - Medium** - Specifies 880 to 1,000 packets per second.
 - Low** - Specifies 450 to 550 packets per second.
11. You can select the **ALL** row to set all of the ports to the same setting.

Note

For more information, see the **Threshold** setting definition in “Overview” on page 142.

12. Click **Apply**.
13. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Ingress Rate Limiting

This procedure explains how to set **Bandwidth** levels and **Status** for Ingress Rate Limiting on each port of the AT-GS950/10PS switch.

To change the settings of the ingress rate limiting feature, perform the following procedure:

1. From the main menu on the left side of the page, select the **Bridge** folder.
2. From the **Bridge** folder, select **Storm Control**.
The **Storm Control** folder expands.
3. From the **Storm Control** folder, select **Ingress Rate Limiting**.
The AT-GS950/10PS Ingress Rate Limiting page is displayed. See Figure 47 for a partial view of this page.

Egress Rate Limiting

Bandwidth = 64kbps x rate limit

Port	Bandwidth		Status	Action
All	64kbps x	(1-15625)	Ignore ▾	Apply
1	64kbps x 0	(1-15625)	Disable ▾	Apply
2	64kbps x 0	(1-15625)	Disable ▾	Apply
3	64kbps x 0	(1-15625)	Disable ▾	Apply
4	64kbps x 0	(1-15625)	Disable ▾	Apply
5	64kbps x 0	(1-15625)	Disable ▾	Apply
6	64kbps x 0	(1-15625)	Disable ▾	Apply
7	64kbps x 0	(1-15625)	Disable ▾	Apply
8	64kbps x 0	(1-15625)	Disable ▾	Apply

Notes: Disable will reset the setting to default value then turn off the function.

Figure 47. AT-GS950/10PS Ingress Rate Limiting Page

4. To set the **Bandwidth** field on the AT-GS950/10PS switch, enter a number in the range from 1 to 15625.

Note

See “Ingress Rate Limiting” on page 143 for calculating the bandwidth limit set by the **Bandwidth** field.

You can select the **ALL** row to set all of the ports to the same setting.

5. To enable or disable ingress rate filter, select **Enable** or **Disable** from the **Status** pull-down menu next to the port that you want to change. You can select the **ALL** row to set all of the ports to the same setting.
6. Click **Apply**.

7. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Egress Rate Limiting

This procedure explains how to set **Bandwidth** levels and **Status** for Egress Rate Limiting on each port of the AT-GS950/10PS switch.

To change the settings of the egress rate limiting feature, perform the following procedure:

1. From the main menu on the left side of the page, select the **Bridge** folder.
2. From the **Bridge** folder, select **Storm Control**.
The **Storm Control** folder expands.
3. From the **Storm Control** folder, select **Egress Rate Limiting**.
The AT-GS950/10PS Egress Rate Limiting page is displayed. See Figure 48 for a partial view of this page.

Egress Rate Limiting					
Bandwidth = 64kbps x rate limit					
Port	Bandwidth			Status	Action
All	64kbps x		(1-15625)	Ignore ▾	Apply
1	64kbps x 0		(1-15625)	Disable ▾	Apply
2	64kbps x 0		(1-15625)	Disable ▾	Apply
3	64kbps x 0		(1-15625)	Disable ▾	Apply
4	64kbps x 0		(1-15625)	Disable ▾	Apply
5	64kbps x 0		(1-15625)	Disable ▾	Apply
6	64kbps x 0		(1-15625)	Disable ▾	Apply
7	64kbps x 0		(1-15625)	Disable ▾	Apply
8	64kbps x 0		(1-15625)	Disable ▾	Apply

Notes: Disable will reset the setting to default value then turn off the function.

Figure 48. AT-GS950/10PS Egress Rate Limiting Page

To set the **Bandwidth** field, enter a number in the range of 1 to 15625. You can select the **ALL** row to set all of the ports to the same setting.

Note

See “Egress Rate Limiting” on page 143 for calculating the bandwidth limit set by the **Bandwidth** field.

4. To enable or disable egress rate filter, select **Enable** or **Disable** from the **Status** pull-down menu next to the port that you want to change. You can select the **ALL** row to set all of the ports to the same setting.
5. Click **Apply**.
6. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Chapter 13

Virtual LANs

This chapter contains a description of Virtual Local Area Networks (VLANs) and the procedures for creating, modifying, and deleting both port-based and tagged VLANs. This chapter contains the following sections:

- ❑ “VLAN Overview” on page 150
- ❑ “Assign Ports to a VLAN Mode” on page 155
- ❑ “Tagged VLAN Configuration” on page 157
- ❑ “Port-Based VLAN Configuration” on page 164
- ❑ “Modify a Port-Based VLAN” on page 165
- ❑ “Delete a Port-Based VLAN” on page 165

Note

The Voice VLAN feature is not covered in this section. For more information, see “Voice VLAN” on page 257.

Note

To permanently save your new settings or any changes to the configuration file, select **Save Configuration to Flash** from the main menu on the left side of the page.

VLAN Overview

A virtual LAN or VLAN is a group of ports on an Ethernet switch that form a logical Ethernet segment via the AT-S110 Management software. The ports of a VLAN form an independent traffic domain where the traffic generated by the nodes of a VLAN remains within the VLAN.

With VLANs, you can segment your local area network using the AT-S110's Management software and group nodes with related functions into their own separate, logical, VLAN segments. These VLAN groupings can be based on similar data needs or security requirements. For example, you can create separate VLANs for each department in your company, such as Sales, Accounting and Engineering.

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 each LAN segment vying for bandwidth, the greater the likelihood overall network performance decreases.

VLANs improve network performance because traffic stays within the separate, logical LAN segment of 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 that is not destined for them. It also frees up bandwidth within all the logical workgroups.

In addition, because each VLAN constitutes a separate broadcast domain, broadcast traffic remains within the VLAN and is not shared with other ports of the switch that are not members of that VLAN. Because the broadcast traffic is not shared with ports outside of the VLAN, those non-member ports experience an overall network performance improvement.

- Increased security

Because data traffic generated by a node in a VLAN is restricted only to the other nodes of the same VLAN, you can use VLANs to control the flow of packets in your network and prevent packets from being shared with unauthorized end nodes.

- Simplified network management

VLANs can simplify network management. Before VLANs became a layer 2 feature, physical changes to the network often had to be made at the switches in the wiring closets. For example, if an employee changed departments, changing the employee's LAN segment assignment might require a change to the cabling of the switches.

With VLANs, you can reconfigure the LAN segment assignment of an end node connected to the AT-GS950/10PS switch's management software. Also, you can change the VLAN memberships without moving the workstations physically or change group memberships without moving cables from one port to another.

In addition, a virtual LAN can 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-GS950/10PS Gigabit Ethernet Smart Switch supports the following types of VLANs:

- Port-based VLANs
- Tagged VLANs

Both types of VLANs are described in the following sections.

Port-based VLAN Overview

As explained in the "VLAN Overview" on page 150, a VLAN consists of a group of ports on an Ethernet switch that form an independent traffic domain. This type of VLAN is independent of the header information including VLAN tags in a frame. Traffic generated by the end nodes of a VLAN remains within the VLAN and does not cross over to the end nodes of other VLANs unless there is an interconnection device, such as a router or Layer 3 switch.

A port-based VLAN is a group of ports on the switch that form a logical Ethernet segment. 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 just a few ports.

There are two components of a port-based VLAN in the AT-S110 Management software:

- VLAN Name
- VLAN Index

VLAN Name

To create a port-based VLAN, you must give it a unique name. This name can reflect the function of the network devices that are VLAN members, such as Sales, Production, and Engineering.

VLAN Index

You must assign a unique number to each VLAN in a network. This number is called the Port-Based VLAN Index. This number uniquely identifies a VLAN in the AT-GS950/10PS switch and across the network.

Each port of a port-based VLAN can belong to as many VLANs as needed. Therefore, traffic can be forwarded to the members of the groups to which the port is assigned. For example, port 1 and port 2 are members of group 1 and ports 1 and 3 are members of group 2. In this case, traffic from port 1 is forwarded to ports 2 and 3, traffic from port 2 is forwarded only to port 1, and traffic from port 3 is forwarded only to port 1.

General Rules for Creating a Port-based VLAN

Here is a summary of general rules to observe when creating a port-based VLAN:

- Assign a unique name to each port-based VLAN.
- Assign a unique VLAN Index to each port-based VLAN. If a particular port-based VLAN spans multiple switches, each part of the VLAN on the different switches must be assigned the same VLAN index.
- Create up to 52 port-based VLANs.

Tagged VLAN Overview

The second type of VLAN supported by the AT-S110 Management software is the *tagged VLAN*. In this type of VLAN, membership is determined by tag information within the frames that are received on a port and the VLAN configuration of each port.

The VLAN information within an Ethernet frame is referred to as a *tag* and is contained in a *tagged header* for the frame. A tag, which follows the source and destination addresses in a frame, contains the VLAN ID of the VLAN to which the frame belongs (IEEE 802.3ac standard). 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 whose VLAN ID equals the VLAN tag.

A port that receives or transmits 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 VLAN tagging. The device must be able to process the tagged information on received frames and add tagged information to transmitted frames.

A tagged VLAN consists of the following:

- “VLAN Index” on page 153
- “VLAN Name” on page 153
- “Tagged and Untagged Ports” on page 153
- “Port VLAN Identifier (PVID)” on page 153

VLAN Index

You must assign a unique number to each tagged VLAN in a network. This number is called the tagged VLAN ID. This number uniquely identifies a tagged VLAN in the AT-GS950/10PS switch and across the network.

VLAN Name

To create a tagged VLAN, you must give it a unique name. This name can reflect the function of the network devices that are VLAN members, such as Sales, Production, and Engineering.

Tagged and Untagged Ports

When you specify that a port is a member of a tagged VLAN, you need to specify that it is tagged or untagged. By definition, the port is a static member of a tagged VLAN when it is configured as either a tagged or untagged port. You can have a combination of tagged and untagged ports in the same VLAN.

Note

A port can also be dynamically assigned to a tagged VLAN within a voice VLAN configuration which is a special configuration of a tagged VLAN. For more information concerning static and dynamic membership in a tagged VLAN, see the Overview section for "Voice VLAN" on page 257.

Packet transmission from a tagged port differs from packet transmission from an untagged port. When a packet is transmitted from a tagged port, the tagged information within the packet is maintained when it is transmitted to the next network device. If the packet is transmitted from an untagged port, the VLAN tag information is removed from the packet before it is transmitted to the next network device.

The IEEE 802.1Q standard describes how tagging information within a packet is used to forward or discard traffic throughout the switch. If the incoming packet has a VLAN tag that matches one of the Group IDs of which the port is a member, the packet is accepted and forwarded to the appropriate port(s) within that VLAN. If the incoming packet's VLAN tag does not match one of the Group IDs assigned to the port, the packet is discarded.

Port VLAN Identifier (PVID)

When an untagged packet is received on a port in a tagged VLAN, it is assigned to one of the VLANs of which that port is a member. The deciding factor in this process is the Port VLAN Identifier (PVID). Both tagged and untagged ports in a tagged VLAN must have a PVID assigned to them. The default value of the PVID for each port is 1. The switch

associates a received untagged packet to the VLAN ID that matches the PVID assigned to the port and the packet is only forwarded to those ports that are members.

General Rules for Creating a Tagged VLAN

Here is a summary of the rules to observe when you create a tagged VLAN:

- Assign a unique name to each tagged VLAN.
- Each tagged VLAN must be assigned a unique VLAN ID. If a particular VLAN spans multiple switches, each part of the VLAN on the different switches must be assigned the same VLAN ID.
- A tagged port can be a member of multiple VLANs.
- The AT-GS950/10PS Gigabit Ethernet Smart Switch can support up to 255 tagged VLANs per switch.

Assign Ports to a VLAN Mode

The procedure described in this section allows you to assign ports to tagged or a port-based VLAN. In addition, it permits you to display the current VLAN assignment of ports.

However, you can assign ports to a port-based VLAN only after you have created a port-based VLAN with the procedure described in “Port-Based VLAN Configuration” on page 164.

By default, all of the ports on the switch are assigned as untagged members to the default tagged VLAN with a VLAN ID of 1. The default VLAN is permanent and must have at least one untagged port assigned to it at any time.

To assign ports to a 802.1Q Tagged VLAN or Port-Based VLAN, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.
2. From the **Bridge** folder, select **VLAN**. The **VLAN** folder expands.
3. From the **VLAN** folder, select **VLAN Mode**. The VLAN Mode Page is displayed. See Figure 49.

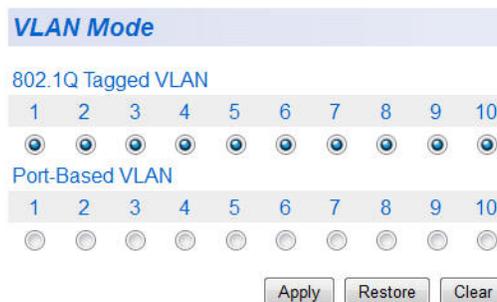


Figure 49. AT-GS950/10PS VLAN Mode Page

4. To add ports to a **802.1Q Tagged VLAN** or **Port-Based VLAN**, select the ports accordingly on the VLAN Mode page.

Note

Before you assign a port as a member of a Port-Base VLAN, you must create the Port-Base VLAN by following the steps defined in “Port-Based VLAN Configuration” on page 164

5. Click **Apply**.

6. If you want to restore the port assignment before saving the configuration, click **Restore**.

Note

Once the VLAN assignment has been saved by clicking first on the **Apply** button and then saving the configuration, the **Restore** button will not be active for those port assignments.

7. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Tagged VLAN Configuration

On a port, the tag information within a frame is examined when it is received to determine if the frame is qualified as a member of a specific tagged VLAN. If it is, it is eligible to be switched to other member ports of the same VLAN. If it is determined that the frame's tag does not conform to the tagged VLAN, the frame is discarded.

You can create and delete tagged VLANs by following the procedures in the following sections:

- ❑ "Create a Tagged VLAN"
- ❑ "Modify a Tagged VLAN" on page 158
- ❑ "Delete a Tagged VLAN" on page 160

Create a Tagged VLAN

To create a tagged VLAN, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.
2. From the **Bridge** folder, select **VLAN**. The **VLAN** folder expands.
3. From the **VLAN** folder, select **Tagged VLAN**. The AT-GS950/10PS Tagged VLAN Page is displayed. See Figure 50.

Tagged VLAN

VLAN ID: (2-4000)

VLAN Name: (32 characters limit)

Management VLAN: Disabled ▾

Static Tagged

1	2	3	4	5	6	7	8	9	10
<input type="radio"/>									

Static Untagged

1	2	3	4	5	6	7	8	9	10
<input type="radio"/>									

Not Member

1	2	3	4	5	6	7	8	9	10
<input type="radio"/>									

VLAN ID	Name	VLAN Type	Management	VLAN Action
1	DefaultVLAN	Permanent	Enable	Modify

Page: 1/1

 Page

Figure 50. AT-GS950/10PS Tagged VLAN Page

4. To assign a VLAN ID, type a VLAN ID in the **VLAN ID** field.
The range for this field is 2 to 4,000. You can create a maximum of 255 tagged VLANs.
5. To assign a name to the VLAN, type a unique name in the **VLAN Name** field.
Enter a value of up to 32 characters. For more information about this field, refer to “VLAN Name” on page 151.
6. Set the **Management VLAN** to one of the following choices from the pull-down menu:

Enable - This parameter enables management access on this VLAN.

Note

- If you enable management on a VLAN other than 1, you can access management only through a tagged port of that VLAN.
- You can access management through the tagged port of all VLANs on which you have enabled management.
- You can still access management through a port that is only an untagged member of VLAN 1 and not a tagged member of another VLAN.

Disable - This parameter disables **Management VLAN** on this VLAN. If you change this parameter from **Enable** to **Disable**, the **Management VLAN** is still enabled on the **DefaultVLAN**.

Note

The Management VLAN is always Enabled on the untagged ports of the DefaultVLAN. It cannot be disabled on the DefaultVLAN.

7. To assign ports to the VLAN, click on the port numbers labeled either **Static Tagged** or **Static Untagged**.
By default, all the ports are assigned to the **Not Member** category when a specific VLAN is created. The **Not Member** ports are part of the DefaultVLAN (VLAN ID=1).
8. Click **Apply**.
9. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Modify a Tagged VLAN

To modify the name or port assignments of a tagged VLAN, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**.
The **Bridge** folder expands.

2. From the **Bridge** folder, select **VLAN**.
The **VLAN** folder expands.
3. From the **VLAN** folder, select **Tagged VLAN**.
An example of a tagged VLAN (Index 2, Sales VLAN) is shown in the table at the bottom of Figure 51 on page 159.

Tagged VLAN

VLAN ID: (2-4000)

VLAN Name: (32 characters limit)

Management VLAN:

Static Tagged

1	2	3	4	5	6	7	8	9	10
<input type="radio"/>									

Static Untagged

1	2	3	4	5	6	7	8	9	10
<input type="radio"/>									

Not Member

1	2	3	4	5	6	7	8	9	10
<input checked="" type="radio"/>									

VLAN ID	Name	VLAN Type	Management	VLAN Action
1	DefaultVLAN	Permanent	Enable	Modify
2	Sales	Static	Enable	Modify/Delete

Page: 1/1 Page

Figure 51. Example of AT-GS950/10PS Tagged VLAN Page

4. In the **VLAN Action** column, click **Modify** in the row of the VLAN that you want to change.
The Modify VLAN Page is displayed. See Figure 52.

Modify VLAN

VLAN ID: 2

VLAN Name: (32 characters limit)

Management Vlan:

Static Tagged

1	2	3	4	5	6	7	8	9	10
<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>					

Static Untagged

1	2	3	4	5	6	7	8	9	10
<input type="radio"/>									

Not Member

1	2	3	4	5	6	7	8	9	10
<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>					

Figure 52. AT-GS950/10PS Modify VLAN Page

5. You cannot modify the VLAN ID on this web page. If you want to delete the VLAN ID, go to “Delete a Tagged VLAN” on page 160 for more information.
6. To change the VLAN Name, type a new VLAN Name in the **VLAN Name** field.
For more information about this field, refer to “VLAN Name” on page 151.
7. To change the **Management VLAN** assignment, select one of the following choices from the pull-down menu:

Enable: This parameter enables **Management VLAN** on this VLAN. The **Management VLAN** will be disabled on all other VLANs and only be operational on this VLAN.



Caution

If you Enable the Management VLAN on this VLAN and you are connected to a **Tagged Member** port, you may lose your connection to the AT-S110 Management software.

Disable - This parameter disables **Management VLAN** on this VLAN. If you change this parameter from **Enable** to **Disable**, the **Management VLAN** will be enabled on the **DefaultVLAN** automatically.

Note

The Management VLAN is always Enabled on the DefaultVLAN and cannot be disabled.

8. To change the port selections, click on the port numbers labeled either **Static Tagged** or **Static Untagged**.
9. Click **Apply**.
10. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Delete a Tagged VLAN

To delete a tagged VLAN, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**.
The **Bridge** folder expands.
2. From the **Bridge** folder, select **VLAN**.
The **VLAN** folder expands.

3. From the **VLAN** folder, select **Tagged VLAN**.
An example of the Tagged VLAN Page is shown in Figure 52 on page 159.
4. In the VLAN Action column, select **Delete** next to the VLAN that you want to delete.
A confirmation prompt is displayed.
5. Click **OK** to delete the VLAN or **Cancel** to cancel the deletion.

Note

You cannot delete the Default VLAN which has a VID of 1.

6. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Tagged VLAN Port Settings

To configure a VLAN port that is a member of a Tagged VLAN, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**.
The **Bridge** folder expands.
2. From the **Bridge** folder, select **VLAN**.
The **VLAN** folder expands.

From the **VLAN** folder, select **Port Setting**.
A partial view of the AT-GS950/10PS VLAN Port Settings is displayed.
See Figure 53.

Port Setting					
Port	PVID	Acceptable Frame Types	Ingress Filtering	Action	
All		Ignore	Ignore	Apply	
1	1	All	Enabled	Apply	
2	1	All	Enabled	Apply	
3	1	All	Enabled	Apply	
4	1	All	Enabled	Apply	
5	1	All	Enabled	Apply	
6	1	All	Enabled	Apply	
7	1	All	Enabled	Apply	
8	1	All	Enabled	Apply	

Figure 53. AT-GS950/10PS VLAN Port Setting Page

3. For a selected port, set the **PVID** field to an existing VLAN ID. For an explanation of the PVID parameter, see the **Port VLAN Identifier** section in “VLAN Overview” on page 150.
4. Set the **Acceptable Frame Type** to one of the following choices from the pull-down menu:

All - This selection allows all incoming ingress frames presented to the port to enter the switch.

Tagged - This selection allows only tagged frames presented to the port to enter the switch. Untagged frames are discarded at ingress.

Untagged and Priority Tagged - This selection allows only untagged frames and frames with a priority tag that are presented to the port to enter the switch. Tagged frames are discarded at ingress.

5. From the Ingress Filtering parameter, select one of the following choices from the pull-down menu:

Enable - This enables Ingress Filtering at the selected port.

Disable - This disables Ingress Filtering at the selected port.

6. Click **Apply**.
The port configuration becomes effective.
7. If you need to configure other ports of the switch for the VLAN Port Settings, repeat steps 4 through 7.
8. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Port-Based VLAN Configuration

A port-based VLAN is a group of ports on the switch that form a logical Ethernet segment. This type of VLAN is independent of the header information including VLAN tags in a frame.

You can create and delete Port-Based VLANs by following the procedures in the following sections:

- “Create a Port-Based VLAN”
- “Modify a Port-Based VLAN” on page 165
- “Delete a Port-Based VLAN” on page 165

Create a Port-Based VLAN

To create a port-based VLAN, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.
2. From the **Bridge** folder, select **VLAN**. The **VLAN** folder expands.
3. From the **VLAN** folder, select **Port-Based VLAN**. The Port-Based VLAN Page is displayed. See Figure 54.

Port-Based VLAN

Index: (1-52)

VLAN Name: (32 characters limit)

Group Member

1	2	3	4	5	6	7	8	9	10
<input type="radio"/>									

Not Member

1	2	3	4	5	6	7	8	9	10
<input checked="" type="radio"/>									

Index	Group Name	Group Member	VLAN Action
<< VLAN database is empty >>			

Page: 1/1 Page

Figure 54. Port-Based VLAN Page

4. To assign a VLAN Index, type a VLAN ID in the **VLAN Index** field. Choose a value between 1 and 64.
5. To assign a name to a VLAN, type a name in the **VLAN Name** field. Enter a value of up to 32 characters. For more information about this field, refer to “VLAN Name” on page 151.

6. To assign ports to the VLAN, click on the port numbers labeled Group Member.
7. Click **Apply**.
8. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Modify a Port-Based VLAN

To modify the name or port assignments of a port-based VLAN, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.
2. From the **Bridge** folder, select **VLAN**. The **VLAN** folder expands.
3. From the **VLAN** folder, select **Port-Based VLAN**.
An example VLAN (Index 2, Sales VLAN) is shown in the table at the bottom of AT-GS950/10PS Port-Based VLAN page. See Figure 55.

Port-Based VLAN

Index: (1-52)
 VLAN Name: (32 characters limit)

Group Member

1	2	3	4	5	6	7	8	9	10
<input type="radio"/>									

Not Member

1	2	3	4	5	6	7	8	9	10
<input checked="" type="radio"/>									

Index	Group Name	Group Member	VLAN Action
2	Sales	2-4	Modify/Delete

Page: 1/1 Page

Figure 55. Example of AT-GS950/10PS Port Based VLAN Page

4. In the VLAN Action column, click **Modify** next to the VLAN that you want to change.
5. Delete a Port-Based VLAN

To delete a port-based VLAN, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.
2. From the **Bridge** folder, select **VLAN**. The **VLAN** folder expands.

3. From the **VLAN** folder, select **Port-Based VLAN**.
The Port-Based VLAN Page is shown in Figure 54 on page 164.
4. In the VLAN Action column, click **Delete** next to the VLAN that you want to delete.
A confirmation prompt is displayed.
5. Click **OK** to delete the VLAN or **Cancel** to cancel the deletion.

Note

You cannot delete the Default VLAN which has a VID of 1.

6. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Chapter 14

GVRP

This chapter contains the following sections:

- ❑ “Overview and Guidelines” on page 168
- ❑ “General Configuration” on page 169
- ❑ “Port Settings” on page 170
- ❑ “Time Settings” on page 172

Overview and Guidelines

The GARP VLAN Registration Protocol (GVRP) allows network devices to share VLAN information and to use the information to modify existing VLANs or create new VLANs, automatically. This makes it easier to manage VLANs that span more than one switch. Without GVRP, you have to manually configure your switches to ensure that the various parts of the VLANs can communicate with each other across the different switches. With GVRP, which is an application of the Generic Attribute Registration Protocol (GARP), this is done for you automatically.

Here are the guidelines for GVRP:

- GVRP is supported with STP or RSTP or without spanning tree.
- Both ports that constitute a network link between the switch and the other device must be running GVRP.
- You cannot modify or delete dynamic GVRP VLANs.
- You cannot remove dynamic GVRP ports from static or dynamic VLANs.
- To be detected by GVRP, a VLAN must have at least one active node or have at least one port with a valid link to an end node. GVRP cannot detect a VLAN that does not have any active nodes or valid port links.
- Resetting the switch erases all dynamic GVRP VLANs and dynamic GVRP port assignments. The dynamic assignments are relearned by the switch as PDUs arrive on the ports from other switches.
- GVRP has three timers: join timer, leave timer, and leave all timer. The values for these timers must be identically configured 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 default port setting on the switch for GVRP is active, meaning that the ports participate in GVRP. Allied Telesis recommends disabling GVRP on those ports that are connected to GVRP-inactive devices, meaning devices that do not feature GVRP.
- PDUs are transmitted from only those switch ports where GVRP is enabled.

General Configuration

Perform the following procedure to enable or disable GVRP:

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.
2. From the **Bridge** folder, select **GVRP**. The **GVRP** folder expands.
3. From the **GVRP** folder, select **GVRP Global Configuration**. The GVRP Global Configuration Page is displayed. See Figure 56.

GVRP Global Configuration

GVRP Status

Figure 56. GVRP Global Configuration Page

4. From the **GVRP Status** field, select one of the following choices from the pull-down menu:
 - Enable** - The GVRP feature is active.
 - Disable** - The GVRP feature is inactive.
5. Click **Apply**. The GVRP setting that you have selected is now active.
6. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Port Settings

Perform the following procedure to configure the GVRP port settings:

1. From the main menu on the left side of the page, select **Bridge**.
The **Bridge** folder expands.
2. From the **Bridge** folder, select **GVRP**.
The **GVRP** folder expands.
3. From the **GVRP** folder, select **Port Setting**.
A partial view of the AT-GS950/10PS Port Settings Page is displayed.
See Figure 57.

GVRP Port Setting					
Port	Dynamic Vlan Status		Restricted VLAN Registration		Action
All	Ignore	▼	Ignore	▼	Apply
1	Enabled	▼	Disabled	▼	Apply
2	Enabled	▼	Disabled	▼	Apply
3	Enabled	▼	Disabled	▼	Apply
4	Enabled	▼	Disabled	▼	Apply
5	Enabled	▼	Disabled	▼	Apply
6	Enabled	▼	Disabled	▼	Apply
7	Enabled	▼	Disabled	▼	Apply
8	Enabled	▼	Disabled	▼	Apply

Figure 57. GVRP Port Setting Page

4. The following fields are listed for each port:

Port - This parameter displays the ports on the switch.

Dynamic Vlan Status - This parameter defines the GVRP status of the port. From the **Dynamic Vlan Status** field, select one of the following choices from the pull-down menu:

Ignore - This parameter indicates that the setting in the **All** row does not apply to the **Dynamic Vlan Status** field. In other words, each port is set individually.

Enable - The **Dynamic Vlan** is activated for the port row selected.

Disable - The **Dynamic Vlan** is de-active for the port row selected.

Restricted VLAN Registration - This parameter controls if the VLAN registration on the port is restricted or not.

Ignore - This parameter indicates that the setting in the **All** row does not apply to the **Restricted VLAN Registration** field. In other words, each port is set individually.

Enable - The **Restricted VLAN Registration** is active for the

port row selected.

Disable - The **Restricted VLAN Registration** is de-active for the port row selected.

5. Once you have configured the parameters, click **Apply** for the affected port.
6. If you want to configure GVRP for other ports, repeat steps 4 and 5.
7. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Time Settings

Perform the following procedure to configure the GVRP port settings:

1. From the main menu on the left side of the page, select **Bridge**.
The **Bridge** folder expands.
2. From the **Bridge** folder, select **GVRP**.
The **GVRP** folder expands.
3. From the **GVRP** folder, select **Time Setting**.
A partial view of the AT-GS950/10PS GVRP Time Setting Page is displayed. See Figure 58.

GVRP Time Setting

Port No	GarpJoinTime (10 ~ 2 ³⁰ -14)(msecs)	GarpLeaveTime (30 ~ 2 ³¹ -18)(msecs)	GarpLeaveAllTime (40 ~ 2 ³¹ -8)(msecs)	Action
All				Apply
1	200	600	10000	Apply
2	200	600	10000	Apply
3	200	600	10000	Apply
4	200	600	10000	Apply
5	200	600	10000	Apply
6	200	600	10000	Apply
7	200	600	10000	Apply
8	200	600	10000	Apply

Note: Leave Timer must be greater than (Join Timer x2 + 10) and
Leave all Timer must be greater than (Leave Timer + 10).
The scale of input value is 10.

Figure 58. AT-GS950/10PS GVRP Time Setting Page

Note

The GARPLeaveTimer must be greater than (GARPJoinTimer x2 + 10) and the GARPLeaveAllTimer must be greater than (GARPLeaveTimer + 10). The acceptable input values are multiples of 10. If you try to enter a value that is not a multiple of 10, the value is rounded down.

4. The following fields are listed for each port:

Port - This parameter displays the ports on the switch.

GarpJoinTime - This parameter is the GARP Join Timer. Its range is 10 - 1073741810 milli-seconds.

GarpLeaveTime - This parameter is the GARP Leave Timer. Its range is 30 - 2147483630 milli-seconds. This timer must be set in relation to the GVRP Join Timer according to the following equation:

$$\text{GARPLeaveTimer} \geq (\text{GARPJoinTimer} \times 2) + 10$$

GarpLeaveAllTime - This parameter is the GARP Leave Timer. Its range is 30 - 2147483630 milli-seconds. This timer must be set in relation to the GVRP Leave Timer according to the following equation:

$$\text{GARPLeaveAllTimer} > (\text{GARPLeaveTimer} + 10)$$

Note

To ensure compatibility between network devices, you need to configure the same values for the GARP Join Timer, GARP Leave Timer, and GARP Leave All Timer on all participating GVRP devices in your network.

5. Once you have configured the parameters, click **Apply** for the affected port.
6. If you want to configure the GVRP timers for other ports, repeat steps 4 and 5.
7. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Chapter 15

Quality of Service and Cost of Service

This chapter provides descriptions of both the Quality of Service (QoS) and Cost of Service (CoS) features. The following topics are covered:

- ❑ “Overview” on page 176
- ❑ “Associate Ports to CoS Priorities” on page 182
- ❑ “Associate DSCP Classes to Egress Queues” on page 183
- ❑ “Queue Scheduling Algorithm” on page 185

Note

Before mapping the QoS Priorities and the egress Queues, you must disable the Jumbo frame parameter on each port. See the Jumbo parameter definition in “Displaying and Configuring Ports” on page 57.

Note

To permanently save your new settings or any changes to the configuration file, select **Save Configuration to Flash** from the main menu on the left side of the page.

Overview

When a port on an Ethernet switch becomes oversubscribed, its egress queues contain more packets than the port can handle in a timely manner. In this situation, the port may be forced to delay the transmission of some packets, resulting in the delay of packets reaching their destinations. A port may be forced to delay transmission of packets while it handles other traffic, and, in some situations, some packets 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 applications, referred to as delay or time sensitive applications, that can be impacted by packet delays. Voice transmission and video conferences are two examples. If packets carrying data in either of these cases are delayed from reaching their destination, the audio or video quality may suffer.

This is where Cost of Service (CoS) is of value. It allows you to manage the flow of traffic through a switch by having the switch ports give higher priority to some packets, such as delay sensitive traffic, over other packets. This is referred to as prioritizing traffic.

The various aspects of CoS are:

- ❑ “Packet Priority,” next
- ❑ “Egress Queue vs Packet Priority Mapping” on page 177
- ❑ “Prioritizing Untagged Packets” on page 178
- ❑ “Scheduling” on page 178

Packet Priority

CoS applies primarily to tagged packets. A tagged packet contains information within it that specifies the VLAN to which the packet belongs.

A tagged packet can also contain a priority level. This priority level is used by network switches and other networking devices to know how important (delay sensitive) that packet is compared to other packets. Packets of a high priority are handled before packets 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 packet is received on a port on the switch, it is examined by the AT-S110 Management software for its priority. The switch software uses the priority to determine which ingress priority queue the packet should be directed to on the ingress port.

Egress Queue vs Packet Priority Mapping

Each port has four egress queues, labeled Q0, Q1, Q2, and Q3. Q0 is the lowest priority queue and Q3 is the highest. A packet in a high priority egress queue is typically transmitted sooner than a packet in a low priority queue. Table 3 lists the default mappings between the eight CoS priority levels and the four egress queues of a switch port.

Table 3. Default Mappings Priority Levels to Priority Queues

IEEE 802.1p Priority Level	Port Priority Queue
0	Q0
1	Q0
2	Q0
3	Q0
4	Q0
5	Q0
6	Q0
7	Q0

You can change these mappings. For example, you might decide that packets with a priority of 6 and 7 need to be handled by egress queue Q3 and packets with a priority of 2 and 3 should be handled in Q1. The result is shown in Table 4.

Table 4. Customized Mappings Priority Levels to Priority Queues

IEEE 802.1p Priority Level	Port Priority Queue
0	Q0
1	Q0
2	Q1
3	Q1
4	Q2
5	Q2
6	Q3
7	Q3

The procedure for changing the default mappings is found in “Associate Ports to CoS Priorities” on page 182. Note that because all ports must use the same priority-to-egress queue mappings, these mappings are applied at the switch level. They cannot be set on a per-port basis.

One last thing to note is that the AT-S110 Management Software does not change the priority level in a tagged packet. The packet leaves the switch with the same priority it had when it entered. This is true even if you change the default priority-to-egress queue mappings.

Prioritizing Untagged Packets

CoS relates primarily to tagged packets rather than untagged packets because untagged packets do not contain a priority level. However, the AT-GS950/10PS switch has a priority associated with each individual ingress port. By default, each port’s priority is 0. You can redefine this parameter as described in “Associate Ports to CoS Priorities” on page 182.

Scheduling

A switch port needs a mechanism for knowing the order in which it should handle the packets in its four egress queues. For example, if all the queues contain packets, should the packets in queue Q3, the highest priority queue, be processed through the switch before moving on to the other queues, or should it instead just do a few packets from each queue in a sequential fashion and, if so, how many?

This control mechanism is referred to as the *scheduling algorithm*. Scheduling determines the order in which a port handles the packets in its egress queues. The AT-S110 software has two types of scheduling:

- Strict priority
- Weighted round robin priority

To specify the scheduling, refer to “Associate Ports to CoS Priorities” on page 182.

Note

Scheduling is set at the switch level. You cannot set this parameter on a per-port basis.

Strict Priority Scheduling

With this type of scheduling, a port transmits all packets out of higher priority queues before transmitting any from the lower priority queues. For instance, as long as there are packets in Q3 it does not handle any packets in Q2. The value of this type of scheduling is that high priority packets are always handled before low priority packets which is required for voice or video data.

The problem with this method is that some low priority packets might never be transmitted from the switch because the algorithm might never have time to process the packets waiting in the lower priority queues.

Weighted Round Robin Priority Scheduling

The weighted round robin (WRR) scheduling method functions as its name implies. The port transmits a set number of packets from each queue, in a round robin fashion, so that each has a chance to transmit traffic. Normally, the higher the queue's priority the more packets are transmitted in as the algorithm cycles through the queues in turn. This method guarantees that every queue receives some attention from the port for transmitting packets.

Table 5 shows the WRR settings for the number of packets transmitted from each queue. These values are permanent and you cannot be change these values.

Table 5. Example of Weighted Round Robin Priority

Port Egress Queue	Maximum Number of Packets
Q3	8
Q2	4
Q1	2
Q0	1

Mapping CoS Priorities to Egress Queues

Before mapping the CoS priorities and the egress queues, you must disable the **Jumbo** frame parameter on each port. See the **Jumbo** parameter definition in “Displaying and Configuring Ports” on page 57.

Note

When **Jumbo** frames are enabled, COS can not be enabled.

To configure CoS mapping, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**.
The **Bridge** folder expands.
2. From the **Bridge** folder, select **QoS**.
The **QoS** folder expands.
3. From the **QoS** folder, select **CoS**.
The CoS Page is displayed. See Figure 59.



Notes: Disable will reset the setting to default value then turn off the function.

Figure 59. CoS Page

4. For each **Traffic Class** whose queue you want to change, click on the **Queue** (0, 1, 2, or 3) radio button that applies to your configuration.
5. After you have completed this mapping process, select **Enable** in the **QoS Status** field,
6. Click **Apply**.
7. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Associate Ports to CoS Priorities

The Port Priority values is assigned to an untagged frame at ingress for internal processing in the switch. This procedure explains how to change the default mappings of port priorities to the User Priority. This is set at the switch level. You cannot set this at the per-port level.

To change the port priority mappings, perform the following procedure.

1. From the main menu on the left side of the page, select **Bridge**.
The **Bridge** folder expands.
2. From the **Bridge** folder, select **QoS**.
The **QoS** folder expands.
3. From the **QoS** folder, select **Port Priority**.
The AT-GS950/10PS Port Priority Page page is displayed. See Figure 60 for a partial view of this page.

Port Priority		
Port	User Priority	Action
All	Ignore ▾	Apply
1	0 ▾	Apply
2	0 ▾	Apply
3	0 ▾	Apply
4	0 ▾	Apply
5	0 ▾	Apply
6	0 ▾	Apply
7	0 ▾	Apply
8	0 ▾	Apply

Note : User priority will left as blank when the port in trunk member.

Figure 60. AT-GS950/10PS Port Priority Page

4. For each port whose priority you want to change, select a priority (0-7) in the **User Priority** column.
5. Click **Apply** for each port.
6. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Associate DSCP Classes to Egress Queues

If you choose to use the DSCP tags in your Access Control policy configuration, each DSCP value (0-63) that is relevant to your configuration needs to be mapped to one of the four egress queues (0-3). The default queue for all DSCP values is 0. To assign the queue mappings to the DSCP values, perform the following procedure.

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.
2. From the **Bridge** folder, select **QoS**. The **QoS** folder expands.
3. From the **QoS** folder, select **DSCP**. The DSCP Class Mapping Page page is shown in Figure 61.

DSCP Class Mapping

DSCP Mapping Disabled ▼

DSCP In	Queue						
0	0 ▼	16	0 ▼	32	0 ▼	48	0 ▼
1	0 ▼	17	0 ▼	33	0 ▼	49	0 ▼
2	0 ▼	18	0 ▼	34	0 ▼	50	0 ▼
3	0 ▼	19	0 ▼	35	0 ▼	51	0 ▼
4	0 ▼	20	0 ▼	36	0 ▼	52	0 ▼
5	0 ▼	21	0 ▼	37	0 ▼	53	0 ▼
6	0 ▼	22	0 ▼	38	0 ▼	54	0 ▼
7	0 ▼	23	0 ▼	39	0 ▼	55	0 ▼
8	0 ▼	24	0 ▼	40	0 ▼	56	0 ▼
9	0 ▼	25	0 ▼	41	0 ▼	57	0 ▼
10	0 ▼	26	0 ▼	42	0 ▼	58	0 ▼
11	0 ▼	27	0 ▼	43	0 ▼	59	0 ▼
12	0 ▼	28	0 ▼	44	0 ▼	60	0 ▼
13	0 ▼	29	0 ▼	45	0 ▼	61	0 ▼
14	0 ▼	30	0 ▼	46	0 ▼	62	0 ▼
15	0 ▼	31	0 ▼	47	0 ▼	63	0 ▼

Figure 61. DSCP Class Mapping Page

4. For each DSCP In value that is relevant to your configuration, select a queue (0-3) in the **Queue** column.

5. After you have completed this mapping process, click **Apply**.
6. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Queue Scheduling Algorithm

To change the scheduling algorithm for the egress queues, perform the following procedure.

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.
2. From the **Bridge** folder, select **QoS**. The **QoS** folder expands.
3. From the **QoS** folder, select **Scheduling Algorithm**. The Scheduling Algorithm Page page is shown in Figure 62.



Figure 62. Scheduling Algorithm Page

4. In the **Scheduling Algorithm** list, select the algorithm, one of the following:
 - Strict Priority** - The port transmits all packets out of higher priority queues before transmitting any from the lower priority queues.
 - WRR (Weighted RoundRobin)** - The port transmits a set number of packets from each queue, in a round robin fashion, so that each has a chance to transmit traffic. See Table 5 on page 179 for number of packets versus the port egress queue.
5. Click **Apply**.
6. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Section III

Advanced Features

This section contains the following chapters:

- ❑ Chapter 16, “SNMPv1 and v2c” on page 189
- ❑ Chapter 17, “SNMPv3” on page 201
- ❑ Chapter 18, “Access Control Configuration” on page 217
- ❑ Chapter 19, “RMON” on page 245
- ❑ Chapter 20, “Voice VLAN” on page 257
- ❑ Chapter 21, “Security” on page 267
- ❑ Chapter 22, “Power Over Ethernet (PoE)” on page 283
- ❑ Chapter 23, “DHCP Snooping” on page 290
- ❑ Chapter 24, “LLDP” on page 303
- ❑ Chapter 25, “Network Statistics” on page 311

Chapter 16

SNMPv1 and v2c

This chapter contains a description of SNMPv1 and SNMPv2c and the procedures for configuring with these protocols. This chapter contains the following sections:

- ❑ “SNMPv1 and SNMPv2c Overview” on page 190
- ❑ “Trap Receiver Attributes” on page 191
- ❑ “SNMPv1 and SNMPv2c User and Group Names” on page 193
- ❑ “SNMP Community Strings” on page 196
- ❑ “SNMP Traps” on page 198

Note

To permanently save your new settings or any changes to the configuration file, select **Save Configuration to Flash** from the main menu on the left side of the page.

SNMPv1 and SNMPv2c Overview

You can manage a switch by viewing and configuring the management information base (MIB) objects on the device with the Simple Network Management Program (SNMP). This chapter describes how to configure SNMPv1 and SNMPv2c. A Group Name, IP address of the switch and at least one community string is the minimum required to manage the switch using SNMPv1 and SNMPv2c. To configure SNMPv3, see “SNMPv3” on page 201 for more information.

In the SNMPv1 and SNMPv2c protocols, the terms agent and manager may be used. An agent is software which runs on managed equipment such as the AT-GS950/10PS switch. A manager is a workstation or server that runs the SNMP Network Management System (NMS) software.

The NMS software is capable of querying status, modifying existing configurations, and loading new configurations via the agent in the managed equipment. The NMS and agent communicate with each other using variables organized into pre-defined hierarchies called Management Information Bases or MIBs.

To manage a switch using an SNMP application program, you must do the following:

- Activate SNMP management on your switch. See “User Interface Configuration” on page 37. By default, the SNMP manager is enabled.
- Compile the Allied Telesis private MIB associated with your switch with the Network Management Software (NMS) on your management workstation.
- Configure the SNMP interface parameters in the AT-S110 Management Software.

Note

The MIB file is available from the Allied Telesis web site at www.alliedtelesis.com/support/software. Enter your hardware product model in the **Search by Product Name** field; for example, enter “AT-GS950/10PS.” Links for the latest product software and documentation are displayed. To obtain the latest MIB file, click the link of the most recent version of the AT-S110 Management Software.

Trap Receiver Attributes

A trap is a message sent by the agent to one or more managers to indicate the occurrence of a particular event on the device. There are numerous events that can trigger a trap. For instance, when the switch reboots or when the Spanning Tree Root Bridge changes. You use traps to monitor activities on the switch.

Trap receivers are the typically SNMP management stations, that you want to receive the traps sent by the switch. You specify a trap receiver by its IP address which is assigned to a specific community string.

The community string name is included when the switch sends a trap. The management station may use the community string as a verification of the trap source.

If you are not interested in having SNMP stations receive traps, then you do not need to enter any IP addresses of trap receivers.

Activate SNMP Interface

The SNMP interface is activated by default. If you want to de-activate it or re-activate it, go to “User Interface Configuration” on page 37.

SNMPv1 and SNMPv2c User and Group Names

SNMPv1 and SNMPv2c User Name and Group Name definitions is the basis for creating SNMP communities. Use the following sections to create and delete User and Group Names:

- “Create User and Group Names” on page 193
- “Modify User and Group Names” on page 194
- “Delete User and Group Names” on page 195

A community string has attributes for controlling who can use the string and what the string allows a network management station to do on the switch.

The AT-S110 Management Software does not provide any default community strings. You must first define an SNMP User and Group Name on the SNMP User/Group page and then define a Community Name on the SNMP Community Table page.

Create User and Group Names

To create an SNMP User and Group Name, perform the following procedure:

1. From the main menu on the left side of the page, select the **SNMP** folder.
The **SNMP** folder expands.
2. From the **SNMP** folder, select **SNMP User/Group**.
The SNMP User/Group Page is displayed in Figure 63.

SNMP User/Group

User Name *

Group Name *

SNMP Version v1 ▾ encrypted

Auth-Protocol MD5 ▾ Password

Priv-Protocol DES ▾ Password

User Name	Group Name	SNMP Version	Auth-Protocol	Priv-Protocol	Action
<input type="text" value="ReadOnly"/>	<input type="text" value="ReadOnly"/>	<input type="text" value="v1"/>	<input type="text" value="None"/>	<input type="text" value="None"/>	<input type="button" value="Delete"/>
<input type="text" value="ReadOnly"/>	<input type="text" value="ReadOnly"/>	<input type="text" value="v2c"/>	<input type="text" value="None"/>	<input type="text" value="None"/>	<input type="button" value="Delete"/>
<input type="text" value="ReadWrite"/>	<input type="text" value="ReadWrite"/>	<input type="text" value="v1"/>	<input type="text" value="None"/>	<input type="text" value="None"/>	<input type="button" value="Delete"/>
<input type="text" value="ReadWrite"/>	<input type="text" value="ReadWrite"/>	<input type="text" value="v2c"/>	<input type="text" value="None"/>	<input type="text" value="None"/>	<input type="button" value="Delete"/>

Figure 63. SNMP User/Group Page

Note

If you choose to use the default User and Group Names (ReadOnly and ReadWrite) that are already displayed in the table, proceed to step 7 below.

3. Type a new **User Name**.
Enter a name up to 31 characters in length.
4. Type a previously defined **Group Name**.
Enter a name up to 31 characters in length.
5. Select either **v1** or **v2c** as the SNMP Version.

Note

The encryption check-box and **Auth-Protocol**, **Priv-Protocol**, and **password** fields are intended for SNMPv3 configurations only and are not used for SNMPv1 or v2c configurations.

6. Click **Add**.
See Figure 64 for an example of the SNMP User/Group page.

SNMP User/Group

User Name *

Group Name *

SNMP Version encrypted

Auth-Protocol Password

Priv-Protocol Password

User Name	Group Name	SNMP Version	Auth-Protocol	Priv-Protocol	Action
Jill	ATI-SJ	v2c	None	None	<input type="button" value="Delete"/>
Holly	Contractors	v1	None	None	<input type="button" value="Delete"/>
ReadOnly	ReadOnly	v1	None	None	<input type="button" value="Delete"/>
ReadOnly	ReadOnly	v2c	None	None	<input type="button" value="Delete"/>
ReadWrite	ReadWrite	v1	None	None	<input type="button" value="Delete"/>
ReadWrite	ReadWrite	v2c	None	None	<input type="button" value="Delete"/>

Figure 64. SNMP User/Group Page Example

7. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Modify User and Group Names

If you need to modify an entry in the SNMP User/Group page, you must first delete the entry and then re-enter it. For information about how to delete an entry in this table, see “Delete User and Group Names,” next.

To create a new entry in this table, see “Create User and Group Names” on page 193.

Delete User and Group Names

This procedure explains how to delete an entry on the SNMP User/Group page.

1. From the main menu on the left side of the page, select the **SNMP** folder.

The **SNMP** folder expands.

2. From the **SNMP** folder, select **SNMP User/Group**.

The SNMP User/Group Page is displayed. See Figure 63 on page 193.

3. In the **Action** column of the table, click **Delete** for the **User Name** and **Group Name** that you want to remove.
4. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

SNMP Community Strings

A community string has attributes for controlling who can use the string and what the string will allow a network management station to do on the switch. The AT-S110 Management Software does not provide any default community strings. You must first define an SNMP User and Group Name on the SNMP User/Group page and then define a Community Name on the SNMP Community Table page.

Create SNMP Community Strings

To create an SNMPv1 or SNMPv2c community string, do the following:

1. From the main menu on the left side of the page, select the **SNMP** folder.

The **SNMP** folder expands.

2. From the **SNMP** folder, select **Community Table**.
The Community Table Page is displayed. See Figure 65.

The screenshot shows the 'SNMP Community Table' page. It features two input fields: 'Community Name' and 'User Name(View Policy)', both with asterisks indicating they are required. Below these fields are 'Add' and 'Reset' buttons. At the bottom, there is a table with three columns: 'Community Name', 'User Name(View Policy)', and 'Action'.

Figure 65. Community Table Page

3. Enter a new **Community Name**.

A name can be up to 31 characters in length.

4. Enter a **User Name(View Policy)** that has been previously defined.

Note

This name must match one of the User Names displayed on the **SNMP User/Group** page. See “Create User and Group Names” on page 193. If you enter a user name that has not been pre-defined on the SNMP User/Group page, the Community entry is displayed, but the agent/manager communication fails.

- Click **Add**.

The values of the new **Community Name** and **User Name** are displayed. See Figure 66 for an example.

SNMP Community Table

Community Name *

User Name(View Policy) *

Community Name	User Name(View Policy)	Action
Group1	Holly	<input type="button" value="Delete"/>
Group2	Jill	<input type="button" value="Delete"/>

Figure 66. SNMP Community Table Page Example

- From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Modify SNMP Community Strings

If you need to modify a Community Table entry, you must first delete the entry by using the procedure below and then re-enter it with the modification by creating a new Community table entry. See “SNMPv1 and SNMPv2c User and Group Names” on page 193.

Delete SNMP Community Strings

Use the following procedure to delete a community name of an SNMP community from the Community Table.

- From the main menu on the left side of the page, select the **SNMP** folder.
The **SNMP** folder expands.
- From the **SNMP** folder, select **Community Table**.
The Community Table Page is shown in Figure 65 on page 196.
- To delete a **Community Name**, click **Delete** next to the entry in the table that you want to remove.
The deleted **Community Name** is no longer displayed in the Community table. No confirmation message is displayed.
- From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

SNMP Traps

A Host IP address is used to specify a management device that needs to receive SNMP traps sent by the switch. This IP address is associated with the SNMP Version and a valid Community Name in the Host table of the switch.

Create Trap Host Table Entry

Use the following procedure to create a trap Host table entry:

1. From the main menu on the left side of the page, select the **SNMP** folder.
The **SNMP** folder expands.
2. From the **SNMP** folder, select **Trap Management**.
The Trap Management Page is displayed. See Figure 67.

The screenshot shows the 'Trap Management' page. At the top, there is a section for 'Trap' management with radio buttons for 'Enabled' (selected) and 'Disabled', and an 'Apply' button. Below this is the 'Add Host Table' section, which includes three input fields: 'Host IP Address' (text input with an asterisk), 'SNMP Version' (dropdown menu with 'v1' selected), and 'Community Name/User Name' (text input with an asterisk). There are 'Add' and 'Reset' buttons below the input fields. At the bottom, there is a table header with four columns: 'Host Ip Address', 'SNMP Version', 'Community Name/User Name', and 'Action'.

Figure 67. Trap Management Page

3. Enable trap management by selecting the radio button next to **Enabled** at the top of the page.
By default, trap management is enabled.
4. Enter the **Host IP Address** for the management device that is to receive the SNMP traps.
The IP address must be in the xxx.xxx.xxx.xxx format.
5. Enter the **SNMP Version**, either **v1** or **v2c**, that is configured for the host management device.
6. Enter a **Community Name** that you have defined previously in the SNMP Community table.

Note

The **Community Name** must correlate with one of the communities displayed on the SNMP Community Table page. See “SNMP Community Strings” on page 196. If you enter a **Community Name** that has not been pre-defined, the Trap Host entry is displayed, but agent/manager communication fails.

- Click **Add**.
The new host is added to the table.

Trap Management

Trap Enabled Disabled

Add Host Table

Host IP Address *

SNMP Version ▼

Community Name/User Name *

Host Ip Address	SNMP Version	Community Name/User Name	Action
192.168.1.15	v1	Holly	<input type="button" value="Delete"/>

Figure 68. Trap Management Page Example

- From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Modify a Trap Host Table Entry

If you need to modify an SNMP Trap entry, you must first delete the entry by using the procedure below and then re-enter it with the modification by creating a new SNMP trap- see “SNMP Traps” on page 198.

Delete a Trap Host Table Entry

Use the following procedure to delete a Host table entry:

- From the main menu on the left side of the page, select the **SNMP** folder.
The **SNMP** folder expands.
- From the **SNMP** folder, select **Trap Management**.
- The Trap Management Page is displayed. See Figure 67 on page 198.

4. To delete an entry in the host table, click **Delete** next to the entry in the table that you want to remove.
The Host table entry is removed from the table. No confirmation message is displayed.
5. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Chapter 17

SNMPv3

This chapter contains a description of SNMPv3 and the procedures for configuring this protocol. This chapter contains the following sections:

- ❑ “Overview” on page 202
- ❑ “SNMPv3 User and Group Names” on page 206
- ❑ “SNMPv3 View Names” on page 209
- ❑ “SNMPv3 View Table” on page 212
- ❑ “SNMPv3 Traps” on page 215

Note

To permanently save your new settings or any changes to the configuration file, select **Save Configuration to Flash** from the main menu on the left side of the page.

Overview

The SNMPv3 protocol builds on the existing SNMPv1 and SNMPv2c protocol implementation which is described in Chapter 16 on page 189. In SNMPv3, User-based Security Model (USM) authentication is implemented along with encryption, allowing you to configure a secure SNMP environment.

The SNMPv3 protocol uses different terminology than the SNMPv1 and SNMPv2c protocols. In the SNMPv1 and SNMPv2c protocols, the terms agent and manager are used. An agent is the software within an SNMP user while a manager is an SNMP host. In the SNMPv3 protocol, agents and managers are called entities. In any SNMPv3 communication, there is an authoritative entity and a non-authoritative entity. The authoritative entity checks the authenticity of the non-authoritative entity. And, the non-authoritative entity checks the authenticity of the authoritative entity.

With the SNMPv3 protocol, you create users, determine the protocol used for message authentication and determine if data transmitted between two SNMP entities is encrypted. In addition, you can restrict user privileges by defining which portions of the Management Information Bases (MIB) that can be viewed by specific users. In this way, you restrict which MIBs a user can display and modify. In addition, you can restrict the types of messages, or traps, the user can send. (A trap is a type of SNMP message.) 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 configurations because you configure IP addresses of trap receivers, or hosts.

This section describes the features of the SNMPv3 protocol. The following subsections are included:

- ❑ “SNMPv3 Authentication Protocols”
- ❑ “SNMPv3 Privacy Protocol” on page 203
- ❑ “SNMPv3 MIB Views” on page 203
- ❑ “SNMPv3 Configuration Process” on page 204

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 and the user password. You can 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. You may want to make

this configuration for someone with super-user capabilities.

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-S110 Management 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 a privacy value, then SNMPv3 messages are sent in plain text format.

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 69.

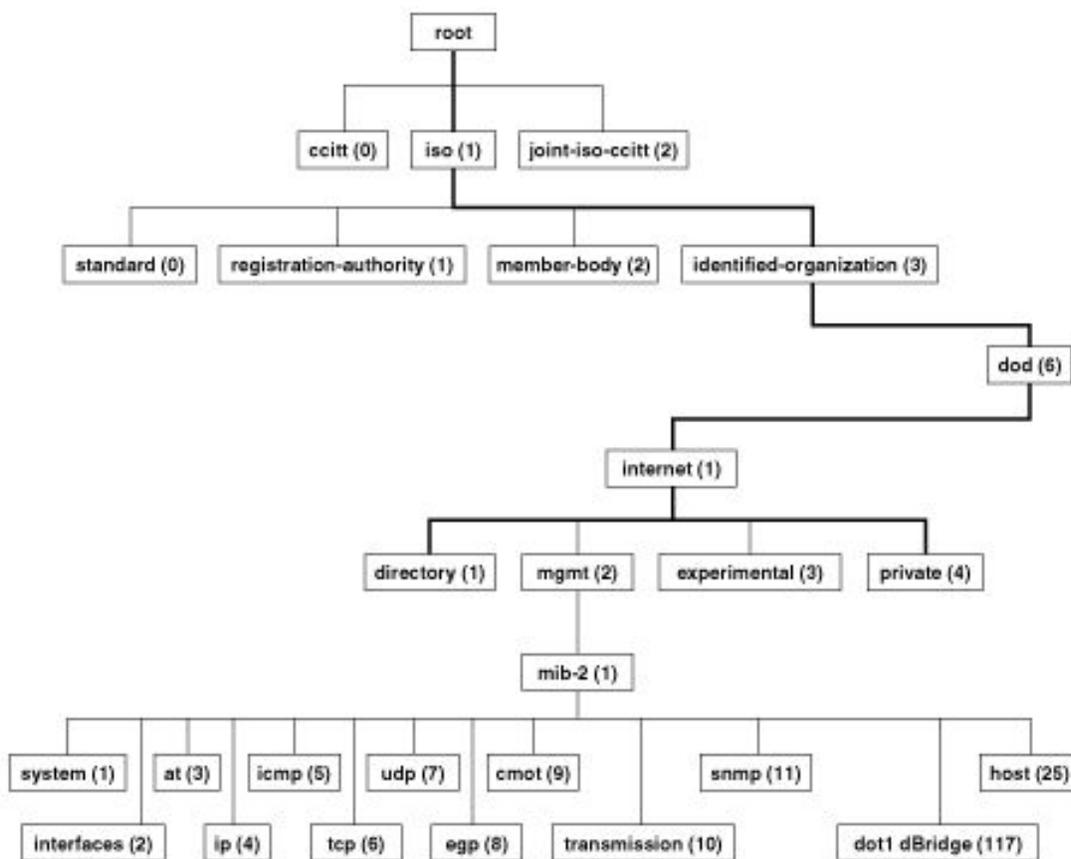


Figure 69. MIB Tree

The AT-S110 Management 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. You need a thorough understanding of the OID MIB table to define a subtree mask.

SNMPv3 Configuration Process

The SNMPv3 parameters are contained in the following tables for user configuration:

- SNMPv3 User/Group table
- SNMPv3 Access table
- SNMPv3 View table
- SNMPv3 Community table
- Trap Management

The SNMPv3 configuration information must be entered in a specific sequence:

Note

The SNMP Interface must be activated first. See “User Interface Configuration” on page 37.

1. You create a User Name and associated Group Name in the SNMPv3 User/Group table.
2. The View Names are defined in the Access table for each Group Name.
3. The MIB view is then defined in the SNMPv3 View table for each View Name.
4. You must enter information in the Community table based on a pre-defined User Name.

Note

The Community Strings do not have a default value defined and are initially blank.

- Finally, the traps can be defined on the Trap Management page based on the Community or User Name.

See Figure 70 for an illustration of how the user configuration tables are linked.

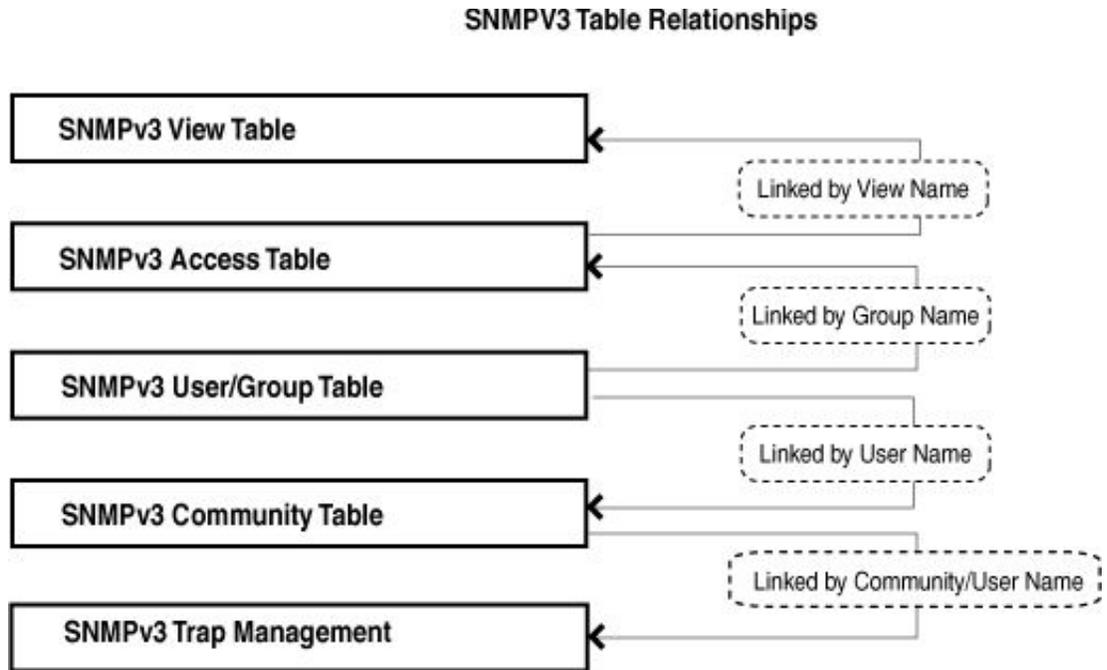


Figure 70. SNMPv3 Table Relationships

SNMPv3 User and Group Names

An SNMPv3 User Name and Group Name definition is the basis for all the other SNMPv3 tables. You can create and delete View Names by following the procedures in the following sections:

- ❑ “Creating SNMPv3 User and Group Names” on page 206
- ❑ “Modifying SNMPv3 User and Group Names” on page 207
- ❑ “Deleting SNMPv3 User and Group Names” on page 207

Creating SNMPv3 User and Group Names

Use this procedure to create SNMPv3 User Names and Group Names:

1. From the main menu on the left side of the page, select the **SNMP**

The **SNMP** folder expands.

2. From the **SNMP** folder, select **SNMP User/Group**.

The SNMP User/Group page is displayed. See Figure 63 on page 193.

Note

There are no default User Names or Group Names defined for SNMPv3.

3. Type a new **User Name**.

Enter a name up to 31 characters in length.

4. Type a new **Group Name**.

Enter a name up to 31 characters in length.

5. From the **SNMP Version** pull down menu, select **v3**.

The **encryption** check-box becomes active.

6. Check the **encryption** check-box.

The **Auth-Protocol**, **Priv-Protocol**, and associated password fields become active.

7. Select one of the following choices for the **Auth-Protocol** field:

MD5: The MD5 authentication protocol. SNMPv3 Users are authenticated with the MD5 authentication protocol after a message is received.

SHA - The SHA authentication protocol. Users are authenticated with the SHA authentication protocol after a message is received.

8. Enter the password for the **Auth-Protocol**.
9. Select one of the following choices for the **Priv-Protocol** field:

DES: Specifies DES encryption scrambles the SNMP data so that outside observers are prevented from seeing the data content.

none: Specifies no encryption is applied to SNMP data.

Note

If you specify a privacy password, the privacy protocol is set to DES and you must also specify an authentication protocol and password.

10. Click **Add**.

The new User Name and Group Name are displayed on the SNMP User/Group page. See Figure 71.

The screenshot shows the 'SNMP User/Group' configuration page. It includes a sidebar with navigation links: User Name, Group Name, SNMP Version, Auth-Protocol, and Priv-Protocol. The main form contains:

- User Name: text input field with an asterisk.
- Group Name: text input field with an asterisk.
- SNMP Version: dropdown menu with 'v1' selected.
- Auth-Protocol: dropdown menu with 'MD5' selected.
- Priv-Protocol: dropdown menu with 'DES' selected.
- encrypted: checkbox (unchecked).
- Password: two text input fields.
- Buttons: 'Add' and 'Reset'.

User Name	Group Name	SNMP Version	Auth-Protocol	Priv-Protocol	Action
Jared	Managers	v3	MD5	DES-CBC	Delete
Jordan	Managers	v3	MD5	DES-CBC	Delete
Kieran	Managers	v3	MD5	DES-CBC	Delete
Kendall	Managers	v3	MD5	DES-CBC	Delete
ReadOnly	ReadOnly	v1	None	None	Delete
ReadOnly	ReadOnly	v2c	None	None	Delete
ReadWrite	ReadWrite	v1	None	None	Delete
ReadWrite	ReadWrite	v2c	None	None	Delete

Figure 71. SNMP User Group, SNMPv3 Example

11. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

**Modifying
SNMPv3 User
and Group
Names**

If you need to modify an entry in the **SNMP User/Group** page, you must first delete the entry and then re-enter it. For information about how to delete an entry in this table, see “Deleting SNMPv3 User and Group Names” on page 207. For information about how to create a new entry in this table, see “Creating SNMPv3 User and Group Names” on page 206

**Deleting SNMPv3
User and Group
Names**

This procedure explains how to delete and entry on the SNMP User/Group page.

1. From the main menu on the left side of the page, select the **SNMP**

folder.

The **SNMP** folder expands.

2. From the **SNMP** folder, select **SNMP User/Group**.

The SNMP User/Group Page is displayed. See Figure 63 on page 193.

3. In the **Action** column of the table, click **Delete** for the **User Name** and **Group Name** that you want to remove.
4. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

SNMPv3 View Names

The SNMPv3 View names are defined in the SNMP Group Access table and are based on the User and Group Names. You can create and delete View Names with the following procedures:

- ❑ “Creating SNMPv3 View Names” on page 209
- ❑ “Modifying SNMPv3 View Names” on page 211
- ❑ “Deleting SNMPv3 View Names” on page 211

Creating SNMPv3 View Names

Before you can create an SNMPv3 View name, you must defined a Group Name using the SNMP User/Group page. See “Creating SNMPv3 User and Group Names” on page 206.

Use this procedure to create SNMPv3 View Names.

1. From the main menu on the left side of the page, select the **SNMP** folder.

The **SNMP** folder expands.

2. From the **SNMP** folder, select **Group Access Table**.

The SNMP Group Access Table page is displayed. See Figure 72.

SNMP Group Access Table

Group Name *

Read View Name

Write View Name

Notify View Name

Security Model v1 ▾

Security Level NoAuthNoPriv ▾

Group Name	Read View	Write View	Notify View	Security Model	Security Level	Action
ReadOnly	ReadWrite	---	ReadWrite	v1	NoAuthNoPriv	<input type="button" value="Delete"/>
ReadOnly	ReadWrite	---	ReadWrite	v2c	NoAuthNoPriv	<input type="button" value="Delete"/>
ReadWrite	ReadWrite	ReadWrite	ReadWrite	v1	NoAuthNoPriv	<input type="button" value="Delete"/>
ReadWrite	ReadWrite	ReadWrite	ReadWrite	v2c	NoAuthNoPriv	<input type="button" value="Delete"/>

Figure 72. SNMP Group Access Table

3. Enter the **Group Name**.

Note

This entry must be pre-defined on the SNMP User/Group page. See “Creating SNMPv3 View Names” on page 209.

4. Enter the **Read View Name**.

This name is an optional field. It can be up to 31 characters in length.

5. Enter the **Write View Name**.

This name is an optional field. It can be up to 31 characters in length.

6. Enter the **Notify View Name**.

This name is an optional field. It can be up to 31 characters in length.

7. From the **Security Model** pull-down menu, select **v3**.

8. Enter the **Security Level** from the pull-down menu. The selection options are:

NoAuthNoPriv: This selection is the appropriate selection when no **Auth-Protocol** or **Priv-Protocol** (no encryption) are selected on the SNMP User/Group page.

AuthNoPriv: Choose this selection when encryption has been enabled but only the **Auth-Protocol** has a password assigned and the **Priv-Protocol** has been selected as **none** on the SNMP User/Group page.

AuthPriv: When both the **Auth-Protocol** or **Priv-Protocol** have been enabled, choose this selection.

9. Click the **Add** button.
See Figure 73 for an example.

SNMP Group Access Table

Group Name *

Read View Name

Write View Name

Notify View Name

Security Model v1 ▾

Security Level NoAuthNoPriv ▾

Group Name	Read View	Write View	Notify View	Security Model	Security Level	Action
Managers	---	---	---	v3	AuthPriv	<input type="button" value="Delete"/>
ReadOnly	ReadWrite	---	ReadWrite	v1	NoAuthNoPriv	<input type="button" value="Delete"/>
ReadOnly	ReadWrite	---	ReadWrite	v2c	NoAuthNoPriv	<input type="button" value="Delete"/>
ReadWrite	ReadWrite	ReadWrite	ReadWrite	v1	NoAuthNoPriv	<input type="button" value="Delete"/>
ReadWrite	ReadWrite	ReadWrite	ReadWrite	v2c	NoAuthNoPriv	<input type="button" value="Delete"/>

Figure 73. SNMP Group Access Table Example for SNMPv3

10. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Modifying SNMPv3 View Names

If you need to modify an entry in the SNMP Group Access page, you must first delete the entry and then re-enter it. For information about how to delete an entry in this table, see “Deleting SNMPv3 View Names” on page 211. For information about how to create a new entry in this table, see “Creating SNMPv3 View Names” on page 209.

Deleting SNMPv3 View Names

This procedure explains how to delete an entry on the SNMP Group Access Table page.

1. From the main menu on the left side of the page, select the **SNMP** folder.

The **SNMP** folder expands.

2. From the **SNMP** folder, select **SNMP Access Table**.

The SNMP Group Access Table page is displayed. See Figure 72 on page 209.

3. In the **Action** column of the table, click **Delete** for the **View Name** that you want to remove.

Note

The views corresponding to the **ReadOnly** and **ReadWrite Group Names** are default values and cannot be removed.

4. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

SNMPv3 View Table

The SNMPv3 View table specifies the MIB object access criteria for each View Name. If the View Name is not specified on this page, then it has access to all MIB objects. You can specify specific areas of the MIB that can be accessed or denied based on the entries in this table. You can create and delete entries in the View table by following the procedures in the following sections:

- “Creating SNMPv3 View Table Entries” on page 212
- “Modifying SNMPv3 View Table Entries” on page 213
- “Deleting SNMPv3 View Table Entries” on page 213

Creating SNMPv3 View Table Entries

This procedure explains how to create entries in the SNMPv3 View Table.

1. From the main menu on the left side of the page, select the **SNMP** folder.

The **SNMP** folder expands.

2. From the **SNMP** folder, select **View Table**.

The SNMP View Table page is displayed. See Figure 74.

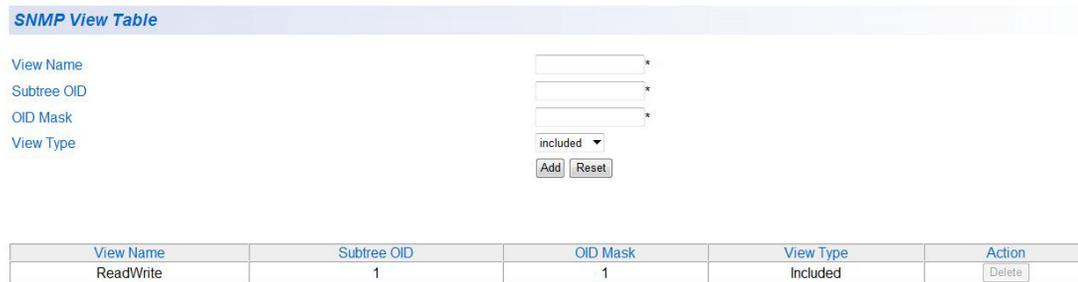


Figure 74. SNMP View Table

3. Enter the **View Name**.

Note

This entry must be pre-defined on the SNMP User/Group page. See “Creating SNMPv3 View Names” on page 209.

4. Enter the **Subtree OID**.
5. Enter “1” for the **OID Mask**.
6. Enter the **View Type**. Choose from the following:

Included: This selection allows the specified MIB object to be included in the view.

Excluded: This selection blocks the view of the specified MIB object.

- Click the **Add** button.

The updated view is displayed in the View Table. See Figure 75.

SNMP View Table

View Name *

Subtree OID *

OID Mask *

View Type included ▾

View Name	Subtree OID	OID Mask	View Type	Action
Read	1	1	Included	<input type="button" value="Delete"/>
ReadWrite	1	1	Included	<input type="button" value="Delete"/>

Figure 75. SNMP View Table Page Example

- From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Modifying SNMPv3 View Table Entries

If you need to modify an entry in the View Table page, you must first delete the entry and then re-enter it. For information about how to delete an entry in this table, see “Deleting SNMPv3 View Table Entries”. For information about how to create a new entry in this table, see “Creating SNMPv3 View Table Entries” on page 212.

Deleting SNMPv3 View Table Entries

- From the main menu on the left side of the page, select the **SNMP** folder.

The **SNMP** folder expands.

- From the **SNMP** folder, select **View Table**.

The SNMP View Table page is displayed. See Figure 74 on page 212.

In the **Action** column of the table, click **Delete** for the View table entry that you want to remove.

Note

The views corresponding to the **ReadOnly** and **ReadWrite Group Names** are default values and cannot be removed.

3. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

SNMPv3 Traps

The creation, modification and deletion of traps for SNMPv3 is identical to the procedure for SNMPv1/v2. See “SNMP Traps” on page 198.

Chapter 18

Access Control Configuration

This chapter contains a description of the AT-GS950/10PS switch's Access Control Configuration feature and the procedures to create, modify, and delete a Access Control configuration. This chapter contains the following sections:

- "Overview" on page 218
- "Classifier" on page 219
- "Profile Action" on page 224
- "In-Profile Action" on page 227
- "Out-Profile Action" on page 231
- "Port List" on page 235
- "Policy" on page 238
- "Policy Sequence Status" on page 243

Overview

Access Control configuration allows you to control different aspects of the Ethernet traffic as it enters the switch ports and is processed through the switch. You can specify what traffic is permitted or denied to flow through the switch by setting up specific filter criteria at an ingress port. You can also manage the switching priority of ethernet packets. All of this is done by specifying policies that define the filtering and priority behavior.

Note

Before you specify the Access Control policies, be sure to configure the QoS parameters. The QoS entries may have a direct effect on each policy's behavior. For more information, see Chapter 15, "Quality of Service and Cost of Service" on page 175.

Before a policy can be defined, you need to specify Access Control configuration information. This information must be entered sequentially on the following web pages:

- ❑ "Classifier" on page 219
- ❑ "Profile Action" on page 224
- ❑ "In-Profile Action" on page 227
- ❑ "Out-Profile Action" on page 231
- ❑ "Port List" on page 235

With the unique index number from each of these web pages, you can configure a "Policy" on page 238

If you define multiple policies for different ports, you can go to "Policy Sequence Status" on page 243 to display the order that policies are applied to each port.

Classifier

The Create Classifier page allows you to specify packet settings for filtering Ethernet traffic.

You can create, modify or delete a Classifier by following the procedures in the following sections:

- ❑ “Creating a Classifier,” next
- ❑ “Modifying a Classifier” on page 221
- ❑ “Deleting a Classifier” on page 222

Creating a Classifier

To create a classifier, perform the following procedure:

1. From the main menu on the left side of the page, select the **Access Control Config** folder.
The **Access Control Config** folder expands.
2. From the **Access Control Config** folder, select **Classifier**.
The Create Classifier page is displayed in Figure 76.

Create Classifier

Classifier Index: (1-65535)

Source MAC Address: : : : : : (XX:XX:XX:XX:XX)

Source MAC Mask Length: (1-48)

Destination MAC Address: : : : : : (XX:XX:XX:XX:XX)

Destination MAC Mask Length: (1-48)

VLAN ID: (1-4000)

802.1p Priority: (0-7)

Ether Type: 0x (0000-FFFF, ex: 0806; 0800)

DSCP: (0-63)

Protocol: (1-255) Note: TCP(6), UDP(17), ICMP(1), IGMP(2), RSVP(46)

Source IP Address: . . .

Source IP Mask Length: (1-32)

Destination IP Address: . . .

Destination IP Mask Length: (1-32)

Source Layer 4 Port: (1-65535)

Destination Layer 4 Port: (1-65535)

Total Entries: 0

Classifier Index	Source MAC Addr. / Mask	Dest. MAC Addr. / Mask	VLAN ID	802.1p	Ether Type	DSCP	Proto.	Source IP Addr. / Mask	Dest. IP Addr. / Mask	Source L4 Port	Dest. L4 Port	Action
<< Classifier table is empty >>												

Page: 0/0 Page

Figure 76. Create Classifier Page

3. Enter a number in the **Classifier Index** field.
The Classifier Index must be a unique number within the range of 1 - 65535.

Note

The **Classifier Index** is a required parameter when you create a Policy. See “Create Policy” on page 238 for more information.

4. Enter data one or more of the remaining parameters. They are listed here:

Source MAC Address - Specifies the source MAC address. The format is xx.xx.xx.xx.xx.xx.

Source MAC Mask Length - Indicates the length of the Source MAC Mask ranging from 1- 48.

Destination MAC Address - Specifies the destination MAC address. The format is xx.xx.xx.xx.xx.xx.

Destination MAC Mask Length - Indicates the length of the Destination MAC Mask ranging from 1 - 48.

VLAN ID - A unique number identifying a VLAN ranging from 1 to 4000.

802.1p Priority - 802.1p priority level of the frame ranging from 0 to 7.

Ether Type - Indicates the protocol of the ethernet frame protocol ranging from 0000 to FFFF.

DSCP - The DSCP (Differentiated Services Code Point) value in the IP header ranging from 0 - 63.

Protocol - Indicates the packet protocol ranging from 0 to 255.

Source IP Address - Specifies the source IP address.

Source IP Mask Length - Specifies the mask length of the source IP address ranging from 0 - 32.

Destination IP Address - Specifies the destination IP address.

Destination IP MAC Mask Length - Specifies the mask length of the destination IP address ranging from 0 - 32.

Source Layer 4 Port - Indicates the source layer 4 port ranging from 1 - 65535.

Destination Layer 4 Port - Indicates the destination layer 4 port ranging from 1 - 65535.

5. Click **ADD**.

The classifier entry is displayed in the table at the bottom of the page. If you do not see your new entry, you may need to navigate to another page of the table with the **First Page**, **Previous Page**, **Next Page**, and **Last Page** buttons located below the table. An example of a classifier table entry is shown in Figure 77.

Create Classifier

Classifier Index: (1-65535)

Source MAC Address: : : : : : (XX:XX:XX:XX:XX:XX)

Source MAC Mask Length: (1-48)

Destination MAC Address: : : : : : (XX:XX:XX:XX:XX:XX)

Destination MAC Mask Length: (1-48)

VLAN ID: (1-4000)

802.1p Priority: (0-7)

Ether Type: 0x (0000-FFFF, ex: 0806; 0800)

DSCP: (0-63)

Protocol: (1-255) Note: TCP(6), UDP(17), ICMP(1), IGMP(2), RSVP(46)

Source IP Address: . . .

Source IP Mask Length: (1-32)

Destination IP Address: . . .

Destination IP Mask Length: (1-32)

Source Layer 4 Port: (1-65535)

Destination Layer 4 Port: (1-65535)

Total Entries: 1

Classifier Index	Source MAC Addr. / Mask	Dest. MAC Addr. / Mask	VLAN ID	802.1p	Ether Type	DSCP	Proto.	Source IP Addr. / Mask	Dest. IP Addr. / Mask	Source L4 Port	Dest. L4 Port	Action
1	A4:54:86:12:00:00/24	45:2A:B5:00:00:00/24	10	7	0x0806	5	6	192.168.1.7/24	192.168.1.7/24	5	10	Modify / Delete

Page: 1/1 Page

Figure 77. Create Classifier Example Page

6. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Modifying a Classifier

To modify the entries for a Classifier, perform the following procedure:

Note

You must enter a classifier before you can modify it. See “Creating a Classifier” on page 219 for more information.

1. From the main menu on the left side of the page, select the **Access Control Config** folder. The **Access Control Config** folder expands.

- From the **Access Control Config** folder, select **Classifier**.
An example of a classifier table entry on the Create Classifier page is displayed in Figure 77.
- From the Create Classifier page, identify which classifier that want to modify and click the **Modify** link in the Action column.
The Modify Classifier page is displayed in Figure 78.

Create Classifier

Classifier Index: (1-65535)

Source MAC Address: (XX:XX:XX:XX:XX:XX)

Source MAC Mask Length: (1-48)

Destination MAC Address: (XX:XX:XX:XX:XX:XX)

Destination MAC Mask Length: (1-48)

VLAN ID: (1-4000)

802.1p Priority: (0-7)

Ether Type: 0x (0000-FFFF, ex: 0806, 0800)

DSCP: (0-63)

Protocol: (1-255) Note: TCP(6), UDP(17), ICMP(1), IGMP(2), RSVP(46)

Source IP Address: . . .

Source IP Mask Length: (1-32)

Destination IP Address: . . .

Destination IP Mask Length: (1-32)

Source Layer 4 Port: (1-65535)

Destination Layer 4 Port: (1-65535)

Total Entries: 1

Classifier Index	Source MAC Addr. / Mask	Dest. MAC Addr. / Mask	VLAN ID	802.1p	Ether Type	DSCP	Proto.	Source IP Addr. / Mask	Dest. IP Addr. / Mask	Source L4 Port	Dest. L4 Port	Action
3015	Ignore	Ignore	Ignore	Ignore	Ignore	Ignore	Ignore	149.55.65.0/24	Ignore	Ignore	Ignore	modify / <input type="button" value="Delete"/>

Page: 1/1 Page

Figure 78. Modify Classifier Page

- Change the parameters as required.

Note

See “Creating a Classifier” on page 219 for the definitions of each parameters.

- Click **Apply**.
The modified classifier entry is displayed in the table at the bottom of the page of the Create Classifier page.
- From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Deleting a Classifier

To delete a classifier entry, perform the following procedure:

- From the main menu on the left side of the page, select the **Access Control Config** folder.
The **Access Control Config** folder expands.

2. From the **Access Control Config** folder, select **Classifier**.
The Example of Create Classifier page is displayed in Figure 77 on page 221.
3. From the Create Classifier page, identify which classifier table entry that want to delete and click the **Delete** link in the Action column.
You are prompted with a verification message.
4. Click on the **OK** button.
The classifier entry is deleted from the classifier table.
5. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Profile Action

The Create Profile Action page defines the priority parameters for policing on DSCP (layer 3) and/or class of service (layer 2).

Note

You must enter a Profile Index on this page even if you do not define the **Policed-DHCP** and **Policed-CoS** parameters because the Profile Index is a required parameter for creating both the In-Profile and Out-Profile Actions. Refer to “Creating an In-Profile Action” on page 227 and “Creating a Out-Profile Action” on page 231 for more information.

You can create, modify or delete a Profile Action by following the procedures in the following sections:

- “Creating a Profile Action,” next
- “Modifying Profile Action” on page 225
- “Deleting a Profile Action” on page 226

Creating a Profile Action

To create a profile action, perform the following procedure:

1. From the main menu on the left side of the page, select the **Access Control Config** folder.
The **Access Control Config** folder expands.
2. From the **Access Control Config** folder, select **Profile Action**.
The Create Profile Action page is displayed in Figure 79.

Create Profile Action

Index: (1-72)

Policed-DSCP: (0-63)

Policed-CoS: (0-7)

Free Profile Actions: 48
Total Entries: 0

Index	Policed-DSCP	Policed-CoS	Action
<< Profile action table is empty >>			

Page: 0/0 Page

Figure 79. Create Profile Action Page

3. Enter a number in the Profile Action **Index** field.
The Index must be a unique number ranging from 1 to 72.
4. Enter a number in the **Policed DSCP** field within the range of 0 to 63.
This field indicates the DSCP level of interest. This field is not mandatory and you may elect to leave it blank.
5. Enter a number in the **Policed-CoS** field ranging from 0 to 7. This field indicates the CoS level of interest. This field is not mandatory and you may elect to leave it blank.
6. Click **Add**.
The Profile Action is added to the status table. If you do not see your new entry, you may need to navigate to another page of the table with the **First Page**, **Previous Page**, **Next Page**, and **Last Page** buttons located below the table. An example of a Profile Action table entry is displayed in Figure 80.

Create Profile Action

Index: (1-72)

Policed-DSCP: (0-63)

Policed-CoS: (0-7)

Free Profile Actions: 47

Total Entries: 1

Index	Policed-DSCP	Policed-CoS	Action
5	0	7	Modify / Delete

Page: 1/1 Page

Figure 80. Example of Profile Action Entry

7. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Modifying Profile Action

To modify a profile action entry, perform the following procedure:

Note

You must first enter a profile action before you can modify it. See "Creating a Profile Action" on page 224 for more information.

1. From the main menu on the left side of the page, select the **Access Control Config** folder.
The **Access Control Config** folder expands.

- From the **Access Control Config** folder, select **Profile Action**. An example of the Create Profile Action page with a Profile Action table entry is shown in Figure 79 on page 224.
- Select the table entry that you want to modify and click the **Modify** link in the Action column. The Modify Profile Action page will be displayed. See Figure 81.

Modify Profile Action

Index: 5

Policed-DSCP: (0-63)

Policed-CoS: (0-7)

Figure 81. Modify Profile Action Page

- Change the parameters as required.

Note

See “Creating a Profile Action” on page 224 for the definitions of each parameters.

- Click **Apply**. The modified profile action entry is displayed in the table at the bottom of the page of the Create Profile Action page.
- From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Deleting a Profile Action

To delete a profile action entry, perform the following procedure:

- From the main menu on the left side of the page, select the **Access Control Config** folder. The **Access Control Config** folder expands.
- From the **Access Control Config** folder, select **Profile Action**. An example of the Create Profile Action page with a Profile Action table entry is shown in Figure 81.
- From the Create Profile Action page, identify which profile action table entry that want to delete and click the **Delete** link in the Action column. You are prompted with a verification message.
- Click on the **OK** button. The profile action entry is deleted from the profile action table.
- From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

In-Profile Action

The Create In-Profile Action page allows you to specify a Profile Action's **Permit** or **Deny** privilege for packets in the ingress queue.

Note

A **Profile Action Index** is required to create an In-Profile Action. See "Creating a Profile Action" on page 224 for more information.

You can create, modify or delete an In-Profile Action by following the procedures in the following sections:

- "Creating an In-Profile Action," next
- "Modifying an In-Profile Action" on page 229
- "Deleting an In-Profile Action" on page 230

Creating an In-Profile Action

To create an in-profile action, perform the following procedure:

1. From the main menu on the left side of the page, select the **Access Control Config** folder. The **Access Control Config** folder expands.
2. From the **Access Control Config** folder, select **In-Profile Action**. The Create In-Profile Action page is displayed in Figure 82.

Create In-Profile Action

Index: (1-65535)

Deny/Permit:

Profile Action ID: (1-72)

Total Entries: 0

Index	Deny / Permit	Action ID	Policed-DSCP	Policed-CoS	Action
<< In-Profile action table is empty >>					

Page: 0/0 Page

Figure 82. Create In-Profile Action Page Example

3. Enter a number in the In-Profile Action **Index** field. The Index must be a unique number within the range of 1 - 65535. This field is mandatory.

Note

The In-Profile Action **Index** is a required parameter when you create a Policy. See “Create Policy” on page 238 for more information.

4. Enter a number in the **Profile Action ID** field ranging from 0 to 72. This field is mandatory.

Note

This field must be pre-defined on the Create Profile page - see “Creating a Profile Action” on page 224 for more information.

5. In the **Deny/Permit** field, use the pull down menu to select one of the following parameters:

Deny - This selection drops ingress packets that conform to the specified **Profile Action ID**.

Permit - This selection allows ingress packets that conform to the specified **Profile Action ID** to be processed by the switch.

Note

You must enter a selection for **Deny/Permit** field even if the Profile Action ID that you have entered ignores both the Policed-DSCP and **Policed-CoS** fields.

6. Click **Add**.
The In-Profile Action entry is added to the status table. If you do not see your new entry, you may need to navigate to another page of the table with the **First Page**, **Previous Page**, **Next Page**, and **Last Page** buttons located below the table. An example of an In-Profile Action table entry is displayed in Figure 83.

Create In-Profile Action

Index: (1-65535)

Deny/Permit: ▾

Profile Action ID: (1-72)

Total Entries: 1

Index	Deny / Permit	Action ID	Policed-DSCP	Policed-CoS	Action
5	Permit	5	0	7	Modify / Delete

Page: 1/1 Page

Figure 83. Example of In-Profile Action Entry

- From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Modifying an In-Profile Action

To modify a In-Profile action entry, perform the following procedure:

Note

You must first enter a In-Profile action before you can modify it. See “Creating an In-Profile Action” on page 227 for more information.

- From the main menu on the left side of the page, select the **Access Control Config** folder.
The **Access Control Config** folder expands.
- From the **Access Control Config** folder, select **In-Profile Action**.
An example of the Create In-Profile Action page with a In-Profile Action table entry is shown in Figure 83 on page 228.
- Select the table entry that you want to modify and click the **Modify** link in the **Action** column.
The Modify In-Profile Action page is displayed. See Figure 84 on page 229.

Modify In-Profile Action

Index: 5

Deny/Permit: Permit ▼

Profile Action ID: 7 (1-72)

Apply

Figure 84. Modify In-Profile Action Page

- Change the parameters as required.

Note

See “Creating an In-Profile Action” on page 227 for the definitions of each parameters.

- Click **Apply**.
The modified In-Profile action entry is displayed in the table at the bottom of the page of the Create In-Profile Action page.
- From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Deleting an In-Profile Action

To delete a In-Profile action entry, perform the following procedure:

1. From the main menu on the left side of the page, select the **Access Control Config** folder.
The **Access Control Config** folder expands.
2. From the **Access Control Config** folder, select **In-Profile Action**.
An example of the Create In-Profile Action page with a In-Profile Action table entry is shown in Figure 83.
3. From the Create In-Profile Action page, identify which In-Profile action table entry that want to delete and click the **Delete** link in the Action column.
You are prompted with a verification message.
4. Click on the **OK** button.
The In-Profile action entry is deleted from the In-Profile action table.
5. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Out-Profile Action

The Create Out-Profile Action page allows you to specify a Profile Action's **Permit** or **Deny** privilege and bandwidth restrictions for packets in the egress queue.

You can create, modify or delete an Out-Profile Action by following the procedures in the following sections:

- ❑ "Creating a Out-Profile Action," next
- ❑ "Modify Out-Profile Action" on page 233
- ❑ "Delete Out-Profile Action" on page 234

Creating a Out-Profile Action

To create a Out-Profile Action, perform the following procedure:

1. From the main menu on the left side of the page, select the **Access Control Config** folder.
The **Access Control Config** folder expands.
2. From the **Access Control Config** folder, select **Out-Profile Action**.
The Create Out-Profile Action page is displayed in Figure 85.

Create Out-Profile Action

Index: (1-65535)

Deny/Permit:

Committed Rate: (64-1000000 (1Kbps/unit))

Burst Size (Byte):

Profile Action ID: (1-72)

Free Out-Profile Actions: 128
Total Entries: 0

Index	Committed Rate	Burst Size(KB)	Deny/Permit	Action ID	DSCP	CoS	Action
<< Out-Profile action table is empty >>							

Page: 0/0 Page

Figure 85. Create Out-Profile Action Page

3. Enter a number in the Out-Profile Action **Index** field.
The Index must be a unique number within the range of 1 - 65535. This field is mandatory.

Note

The Out-Profile Action **Index** must match a Policy Index that has been pre-defined when you created a Policy. See "Create Policy" on page 238 for more information.

4. Enter a number in the **Profile Action ID** field ranging from 0 to 72. This field is mandatory.

Note

This field must be pre-defined on the Create Profile page - see "Creating a Profile Action" on page 224 for more information.

5. In the **Deny/Permit** field, use the pull down menu to select one of the following parameters:

Deny - This selection drops ingress packets that conform to the specified **Profile Action ID**.

Permit - This selection allows ingress packets that conform to the specified **Profile Action ID** to be processed by the switch.

Note

You must enter a selection for **Deny/Permit** field even if the Profile Action ID that you have entered ignores both the Policed-DSCP and **Policed-CoS** fields.

6. Click **Add**.
The Out-Profile Action entry is added to the status table. If the **Page** field located below the table displays a page number and you do not see your new entry, then there are multiple pages of the table that you can navigate. This is done by clicking on the **First Page**, **Previous Page**, **Next Page**, and **Last Page** buttons located below the table. An example of a Out-Profile Action table entry is displayed in Figure 86 on page 232.

Create Out-Profile Action

Index: (1-65535)
 Deny/Permit:
 Committed Rate: (64-1000000 (1Kbps/unit))
 Burst Size (Byte):
 Profile Action ID: (1-72)

Free Out-Profile Actions: 127
 Total Entries: 1

Index	Committed Rate	Burst Size(KB)	Deny/Permit	Action ID	DSCP	CoS	Action
3	1000	32K	Permit	5	0	7	Modify / Delete

Page: 1/1 Page

Figure 86. Example of Out-Profile Action Entry

- From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Modify Out-Profile Action

To modify a Out-Profile action entry, perform the following procedure:

Note

Before you can modify an entry, you must first enter a Out-Profile action - see "Creating an In-Profile Action" on page 227.

- From the main menu on the left side of the page, select the **Access Control Config** folder.
The **Access Control Config** folder expands.
- From the **Access Control Config** folder, select **Out-Profile Action**.
An example of the Create Out-Profile Action page with a Out-Profile Action table entry is shown in Figure 86 on page 232.
- Select the table entry that you want to modify and click the **Modify** link in the Action column.
The Modify Out-Profile Action page is displayed. See Figure 87.

The screenshot shows the 'Modify Out-Profile Action' page with the following fields and values:

Index:	3
Deny/Permit:	Permit
Committed Rate:	1000 (64-1000000 (1Kbps/unit))
Burst Size (Byte):	32K
Profile Action ID:	5 (1-72)
Apply	

Figure 87. Modify Out-Profile Action Page

- Change the parameters as required.

Note

See "Creating an In-Profile Action" on page 227 for the definitions of each parameters.

- Click **Apply**.
The modified Out-Profile action entry is displayed in the table at the bottom of the page of the Create Out-Profile Action page.
- From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Delete Out-Profile Action

To delete a Out-Profile action entry, perform the following procedure:

1. From the main menu on the left side of the page, select the **Access Control Config** folder.
The **Access Control Config** folder expands.
2. From the **Access Control Config** folder, select **Out-Profile Action**.
An example of the Create Out-Profile Action page with a Out-Profile Action table entry is shown in Figure 86 on page 232.
3. From the Create Out-Profile Action page, identify which Out-Profile action table entry that want to delete and click the **Delete** link in the Action column.
You are prompted with a verification message.
4. Click on the **OK** button.
The Out-Profile action entry is deleted from the Out-Profile action table.
5. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Port List

The Create Port List page allows you to specify a list of ports that will be used as part of the policy specification.

You can create, modify or delete a Port List by following the procedures in the following sections:

- ❑ “Create Port List,” next
- ❑ “Modify Port List” on page 236
- ❑ “Delete Port List” on page 237

Create Port List

To create an Port List, perform the following procedure:

1. From the main menu on the left side of the page, select the **Access Control Config** folder.
The **Access Control Config** folder expands.
2. From the **Access Control Config** folder, select **Port List**.
The Create Port List page is displayed in Figure 88.

Create Port List

Index: (1-65535)

Port List: (e.g. 1,3,5-8)

Total Entries: 0

Index	Port List	Action
<< Port list is empty >>		

Page: 0/0 Page

Figure 88. Create Port List Page

3. Enter a number in the Port List **Index** field.
The Index must be a unique number within the range of 1 - 65536
4. 35. This field is mandatory.

Note

The Port List **Index** is a required parameter when you create a Policy. See “Create Policy” on page 238 for more information.

5. Enter a port or group of ports. The Port List can be specified as a consecutive list, a non- consecutive list or a combination of the two. At least one or more ports must be specified.

- Click **Add**.
The Out-Profile Action entry is added to the status table. If the **Page** field located below the table displays a page number and you do not see your new entry, then there are multiple pages of the table that you can navigate. This is done by clicking on the **First Page**, **Previous Page**, **Next Page**, and **Last Page** buttons located below the table. An example of a Port List table entry is displayed in Figure 89.

Create Port List

Index: (1-65535)

Port List: (e.g. 1,3,5-8)

Total Entries: 1

Index	Port List	Action
7	1-3	Modify / Delete

Page: 1/1 Page

Figure 89. Example of Port List Entry

- From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Modify Port List

To modify a Port List entry, perform the following procedure:

Note

Before you can modify an entry, you must first enter a Port List - see "Create Port List" on page 235.

- From the main menu on the left side of the page, select the **Access Control Config** folder.
The **Access Control Config** folder expands.
- From the **Access Control Config** folder, select **Port List**.
An example of the Create Port List page with a Port List table entry is shown in Figure 89.
- Select the table entry that you want to modify and click the **Modify** link in the Action column.
The Modify Port List page is displayed. See Figure 90.

Modify Port List

Index: 9

Port List: (e.g. 1,3,5-8)

Figure 90. Modify Port List Page

4. Change the parameters as required.

Note

See "Create Port List" on page 235 for the definitions of each parameters.

5. Click **Apply**.
The modified Port List entry is displayed in the table at the bottom of the page of the Create Port List page.
6. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Delete Port List

To delete a Port List entry, perform the following procedure:

1. From the main menu on the left side of the page, select the **Access Control Config** folder.
The **Access Control Config** folder expands.
2. From the **Access Control Config** folder, select **Port List**.
An example of the Create Port List page with a Port List table entry is shown in Figure 89 on page 236.
3. From the Create Port List page, identify which Port List table entry that want to delete and click the **Delete** link in the Action column.
You are prompted with a verification message.
4. Click on the **OK** button.
The Port List entry is deleted from the Port List table.
5. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Policy

The Create Policy page allows you to specify the filtering criteria for one policy. Before creating a policy, you must pre-define the following indexes:

Classifier Index: See “Creating a Classifier” on page 219 for more information.

In-Profile Action Index: See “Creating an In-Profile Action” on page 227 for more information.

Out-Profile Action Index: See “Creating a Out-Profile Action” on page 231 for more information.

Port List Index: See “Create Port List” on page 235 for more information.

You can create, modify or delete a Policy by following the procedures in the following sections:

- “Create Policy,” next
- “Modify Policy” on page 240
- “Delete Policy” on page 241

Create Policy

To create an Policy, perform the following procedure:

1. From the main menu on the left side of the page, select the **Access Control Config** folder.
The **Access Control Config** folder expands.
2. From the **Access Control Config** folder, select **Policy**.
The Create Policy page is displayed in Figure 91.

Create Policy

Policy Index:	<input type="text"/>	(1-65535)
Classifier Index:	<input type="text"/>	(1-65535)
Policy Sequence:	<input type="text"/>	(1-64)
In-Profile Action Index:	<input type="text"/>	(1-65535)
Out-Profile Action Index:	<input type="text"/>	(1-65535)
Port List Index:	<input type="text"/>	(1-65535)
<input type="button" value="Add"/>		

Free Policies: 240
Total Entries: 0

Index	Classifier	Sequence	In-Profile	Out-Profile	Port List	Status	Action
<< Policy table is empty >>							

Page: 0/0 Page

Figure 91. Create Policy Page

3. Enter a number in the Policy **Index** field.
The Policy Index is a unique number within the range of 1 - 65535 which identifies the policy. This field is mandatory.
4. Enter data in the remaining parameters. All parameters listed below must be entered to form the policy:

Classifier Index - Classifier table The Classifier Index is a unique number within the range of 1 - 65535. This field is mandatory. It must match one of the Classifier Indexes that you have previously defined. All defined Classifier Indexes appear in the Classifier table at the bottom of the Create Classifier page. See Figure 77 on page 221 for an example of the Classifier table .

Policy Sequence - The Policy Sequence field is a unique number within the range of 1 - 64. This field is mandatory. It identifies the ranking of the specific policy and defines when it will be executed relative to the other policies . A policy with a Policy Sequence number 1 will be executed first, number 2 will be executed second, etc. until the highest Policy Sequence number is reached which will be executed last. For the status of the order of the policies applied to specific ports, see "Policy Sequence Status" on page 243.

In-Profile Action Index - The In-Profile Action Index is a unique number within the range of 1 - 65535. This field is mandatory and must match an In-Profile Action Index that has been previously defined on the Create In-Profile Action page. See the In-Profile Action table described in "Creating an In-Profile Action" on page 227 for more information.

Out-Profile Action Index - The Out-Profile Action Index is a unique number within the range of 1 - 65535. This field is mandatory and must match an Out-Profile Action Index that has been previously defined on the Out-Profile Action page. See the Out-Profile Action table in "Creating a Out-Profile Action" on page 231 for more information.

Port List Index - The Port List Index is a unique number within the range of 1 - 65535. This field is mandatory and must match a Port List Index that has been previously entered on the Create Port List page. See the Port List table "Create Port List" on page 235 for more information.

5. Click **Add**.
The Policy entry is added to the status table. If you do not see your new entry, you may need to navigate to another page of the table with the **First Page**, **Previous Page**, **Next Page**, and **Last Page** buttons located below the table. An example of a Policy table entry is displayed in Figure 92 on page 240.

Create Policy

Policy Index: (1-65535)
 Classifier Index: (1-65535)
 Policy Sequence: (1-64)
 In-Profile Action Index: (1-65535)
 Out-Profile Action Index: (1-65535)
 Port List Index: (1-65535)

Free Policies: 237
 Total Entries: 1

Index	Classifier	Sequence	In-Profile	Out-Profile	Port List	Status	Action
10	1	1	2	3	7	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	Modify / Delete

Page: 1/1 Page

Figure 92. Example of Policy Entry

- From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Modify Policy

To modify a Policy entry, perform the following procedure:

Note

Before you can modify an entry, you must first enter a Policy - see "Create Policy" on page 238.

- From the main menu on the left side of the page, select the **Access Control Config** folder.
The **Access Control Config** folder expands.
- From the **Access Control Config** folder, select **Policy**.
An example of the Create Policy page with a Policy table entry is shown in Figure 92.
- Select the table entry that you want to modify and click the **Modify** link in the Action column.
The Modify Policy page is displayed. See Figure 93 on page 241.

Modify Policy	
Policy Index:	10
Classifier Index:	<input type="text" value="1"/> (1-65535)
Sequence:	<input type="text" value="1"/> (1-64)
In-Profile Action Index:	<input type="text" value="2"/> (1-65535)
Out-Profile Action Index:	<input type="text" value="3"/> (1-65535)
Port List Index:	<input type="text" value="7"/> (1-65535)
	<input type="button" value="Apply"/>

Classifier Index: 1	
Source MAC Address:	A4:54:86:12:00:00/24
Destination MAC Address:	45:2A:B5:00:00:00/24
802.1P Priority:	7
Ether Type:	0x0806
VLAN ID:	10
Source IP Address:	192.168.1.7/24
Destination IP Address:	192.168.1.7/24
DSCP:	5
Protocol:	6
Source Layer 4 Port:	5
Destination Layer 4 Port:	10
Policy Sequence: 1	
In-Profile Index: 2	
In-Profile Action:	Permit, DSCP=0, CoS=7
Out-Profile Index: 3	
Committed Rate:	1000 Kbps
Committed Burst Size:	32 KB
Out-Profile Action:	Permit, DSCP=0, CoS=7
Ports List Index: 7	
Ports List:	1-3

Figure 93. Modify Policy Page

- Change the parameters as required.

Note

See “Create Policy” on page 238 for the definitions of each parameters.

- Click **Apply**.
The modified Policy entry is displayed in the table at the bottom of the page of the Create Policy page.
- From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Delete Policy

To delete a Policy entry, perform the following procedure:

- From the main menu on the left side of the page, select the **Access**

Control Config folder.

The **Access Control Config** folder expands.

2. From the **Access Control Config** folder, select **Policy**.
An example of the Create Policy page with a Policy table entry is shown in Figure 92 on page 240.
3. From the Create Policy page, identify which Policy table entry that want to delete and click the **Delete** button in the Action column.
You are prompted with a verification message.
4. Click on the **OK** button.
The Policy entry is deleted from the Policy table.
5. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Policy Sequence Status

The Policy Sequence page displays the status of the order that policies are applied to each port. You can order the display by Policy Index or by Policy Sequence number.

To display the policy sequence, perform the following procedure:

1. From the main menu on the left side of the page, select the **Access Control Config** folder.
The **Access Control Config** folder expands.
2. From the **Access Control Config** folder, select **Policy Sequence**.
The Policy Sequence page is displayed in Figure 94.



Figure 94. Policy Sequence Page

3. Select the switch port from the **Select Port** pull down menu that you want to view.
4. Click either the **Display by Index order** or **Display by Sequence order** button to view the Policy Sequence.
The Policy Sequence page with the Display by Index pull down menu selected is displayed in Figure 95.

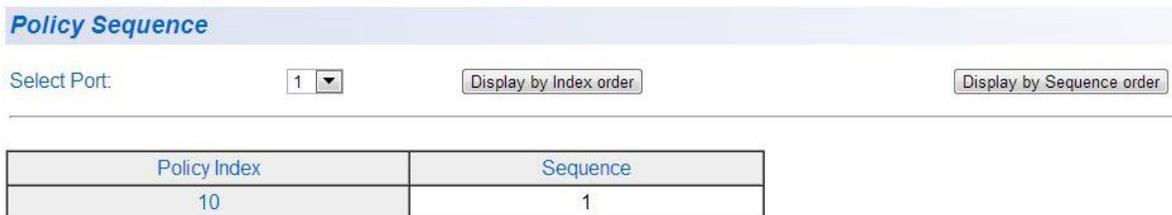


Figure 95. Policy Sequence Page with Display by Index Selected

Chapter 19

RMON

This chapter contains the following sections:

- ❑ “Overview” on page 246
- ❑ “Enable and Disable RMON” on page 247
- ❑ “Port Statistics” on page 248
- ❑ “Histories” on page 250
- ❑ “Events” on page 252
- ❑ “Alarms” on page 254

Overview

The RMON (Remote MONitoring) MIB is used with SNMP applications to monitor the operations of network devices. The switch supports the four RMON MIB groups listed here:

- **Statistic group**— This group is used to view port statistics remotely with SNMP programs. For information about configuring a Statistics group, refer to “Port Statistics” on page 248.
- **History group**— This group is used to collect histories of port statistics to identify traffic trends or patterns. For information about configuring a History group, refer to “Histories” on page 250.
- **Event group**— This group is used with alarms to define the actions of the switch when packet statistic thresholds are crossed. For information about configuring an Event group, refer to “Events” on page 252
- **Alarm group**—This group is used to create alarms that trigger event log messages or SNMP traps when statistics thresholds are exceeded. For information about configuring an Alarm group, refer to “Alarms” on page 254.

Enable and Disable RMON

You can use your SNMP Network Management System (NMS) software and the RMON section of the MIB tree to view the RMON statistics, history and alarms associated with specific ports. Since RMON uses the SNMP agent for communicating with your NMS software, the SNMP Agent must be enabled and the SNMP feature must be configured on your switch.

Since RMON works in conjunction with the SNMP agent, the SNMP agent must be enabled for the RMON feature to be active. See “User Interface Configuration” on page 37 for activating SNMP. For instructions on how to configure SNMP on your switch, refer to Chapter 16, “SNMPv1 and v2c” on page 189 or Chapter 17, “SNMPv3” on page 201.

Perform the following procedure to activate RMON:

1. From the main menu on the left side of the page, click the **RMON** folder.
The **RMON** folder expands.
2. From the **RMON** folder, select **Basic Settings**.
The RMON Basic Settings Page is displayed. See Figure 96.

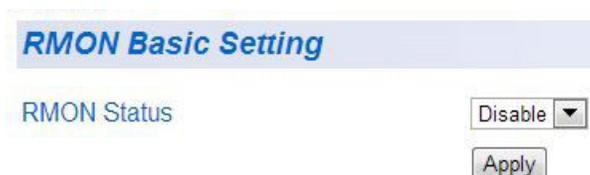


Figure 96. RMON Basic Settings Page

3. Select the **RMON Status** field and select one of the following choices from the pull-down menu:

Enable: The RMON feature is active.

Disable: The RMON feature is inactive.

Note

Insure the that the SNMP agent is Enabled.

4. Click **Apply**.
The RMON setting that you have selected is now active.
5. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Port Statistics

You can remotely view individual port statistics with RMON by using your SNMP NMS software and the RMON portion of the MIB tree.

Perform the following procedure to configure RMON port statistics for a specific port:

1. From the main menu on the left side of the page, click the **RMON** folder.

The **RMON** folder expands.

2. From the **RMON** folder, select **Statistics**.

The Ethernet Statistics Configuration Page is displayed. See Figure 97.

Ethernet Statistics Configuration

Index (1~65535) *

Port *

Owner

Index	Port	Drop Events	Octets	Packets	Broadcast Packets	Multicast Packets	Owner	Action
<< Table is empty >>								

Page: 0/0 Page

Figure 97. Ethernet Statistics Configuration Page

3. The following fields are listed:

Index: This parameter specifies the ID number of the new group. The range is 1 to 65535.

Port: This parameter specifies the port where you want to monitor the statistical information of the Ethernet traffic.

Owner: This parameter is used to identify the person who created an entry. It is primarily intended for switches that are managed by more than one person, and is an optional field.

4. Once you have configured the parameters, click **Add**.

Your entry appears in the table at the bottom of the page. See Figure 98 on page 249.

Ethernet Statistics Configuration

Index (1~65535) *

Port *

Owner

Index	Port	Drop Events	Octets	Packets	Broadcast Packets	Multicast Packets	Owner	Action
1	8	0	0	0	0	0	Jenny	<input type="button" value="Delete"/>

Page: 1/1 Page

Figure 98. Ethernet Statistics Configuration Example

5. If you want to configure RMON statistics for other ports, repeat steps 3 and 4.
6. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Histories

RMON histories are snapshots of port statistics. They are taken by the switch at predefined intervals and can be used to identify trends or patterns in the numbers or types of ingress packets on the ports on the switch. The snapshots can be viewed with your SNMP NMS software with the history group of the RMON portion of the MIB tree.

A history group is divided into buckets. Each bucket stores one snapshot of statistics of a port. A group can have from 1 to 50 buckets. The more buckets in a group, the more snapshots it can store.

Perform the following procedure to configure RMON history:

1. From the main menu on the left side of the page, click the **RMON** folder.

The **RMON** folder expands.

2. From the **RMON** folder, select **History**.

The History Control Configuration Page is displayed. See Figure 99.

History Control Configuration

Index (1~65535) *

Port *

Buckets Requested (1~50)

Interval (1~3600 secs)

Owner

Index	Port	Buckets Requested	Buckets Granted	Interval	Owner	Action
<< Table is empty >>						

Page: 0/0 Page

Figure 99. History Control Configuration Page

3. The following fields are listed:

Index: This parameter specifies the ID number of the new group. The range is 1 to 65535.

Port: This parameter specifies the port where you want to monitor the statistical information of the Ethernet traffic.

Buckets Requested: This parameter defines the number of snapshots of the statistics for the port. Each bucket can store one

snapshot of RMON statistics. Different ports can have different numbers of buckets. The range is 1 to 50 buckets.

Interval: This parameter specifies how frequently the switch takes snapshots of the port's statistics. The range is 1 to 3600 seconds (1 hour). For example, if you want the switch to take one snapshot every minute on a port, you specify an interval of sixty seconds.

Owner: This parameter is used to identify the person who created an entry. It is primarily intended for switches that are managed by more than one person, and is an optional field.

- Once you have configured the parameters, click **Add**.

Your entry appears in the table at the bottom of the page. See Figure 100.

History Control Configuration

Index (1~65535) *

Port *

Buckets Requested (1~50)

Interval (1~3600 secs)

Owner

Index	Port	Buckets Requested	Buckets Granted	Interval	Owner	Action
1	8	20	20	60	Jenny	<input type="button" value="Delete"/>

Page: 1/1 Page

Figure 100. History Control Configuration Example Page

- If you want to configure additional RMON histories for other ports, repeat steps 3 and 4.
- From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Events

An event specifies the action of the switch when the ingress packet activity on a port crosses a statistical threshold defined in an alarm. The choices are to log a message in the event log of the switch, send an SNMP trap to an SNMP workstation, or both. Since there are only three possible actions and since events can be used with more than one alarm, you probably will not create more than three events - one for each of the three actions.

Perform the following procedure to configure RMON history.

1. From the main menu on the left side of the page, click the **RMON** folder.

The **RMON** folder expands.

2. From the **RMON** folder, select **Event**.

The RMON Event Configuration Page is displayed. See Figure 101.

RMON Event Configuration

Index (1~65535) *

Description *

Type ▼

Community

Owner

Index	Description	Type	Community	Owner	Last Time Sent	Action
<< Table is empty >>						

Page: 0/0 Page

Figure 101. RMON Event Configuration Page

3. The following fields are listed:

Index: This parameter specifies the ID number of the new group. The range is 1 to 65535.

Description: This parameter specifies a text description of the event that you are configuring.

Type: This parameter specifies where to log the event when it occurs. The choices are to log a message in the event log of the switch, send an SNMP trap to the SNMP NMS software, or both.

Community: This parameter specifies the community where you want to send the SNMP trap.

Owner: This parameter is used to identify the person who created an entry. It is primarily intended for switches that are managed by more than one person, and is an optional field.

- Once you have configured the parameters, click **Add**.

Your entry appears in the table at the bottom of the page. See Figure 102.

RMON Event Configuration

Index (1~65535) *

Description *

Type ▼

Community

Owner

Index	Description	Type	Community	Owner	Last Time Sent	Action
2	Temperature	SNMP Trap	Managers	Kendall	0	<input type="button" value="Delete"/>

Page: 1/1 Page

Figure 102. RMON Event Configuration Example Page

- If you want to configure additional RMON events, repeat steps 3 and 4.
- From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Alarms

RMON alarms are used to generate alert messages when packet activity on designated ports rises above or falls below specified threshold values. The alert messages can take the form of messages that are entered in the event log on the switch or traps that are sent to your SNMP NMS software or both.

RMON alarms consist of two thresholds. There is a rising threshold and a falling threshold. The alarm is triggered if the value of the monitored RMON statistic of the designated port exceeds the rising threshold. The response of the switch is to enter a message in the event log, send an SNMP trap, or both. The alarm is reset if the value of the monitored statistic drops below the falling threshold.

The frequency with which the switch samples the thresholds of an alarm against the actual RMON statistic is controlled by a time interval parameter. You can adjust this interval for each alarm.

Here are the three components that comprise RMON alarms:

- ❑ RMON statistics group: A port must have an RMON statistics group configured if it is to have an alarm. When you create an alarm, you specify the port to which it is to be assigned not by the port number, but rather by the ID number of the port's statistics group. (As explained in "Port Statistics" on page 248, statistics groups are also used to remotely view port statistics in the RMON portion of the MIB tree.)
- ❑ RMON event: An event specifies the action of the switch when the ingress packet activity on a port crosses a statistical threshold defined in an alarm. The choices are to log a message in the event log of the switch, send an SNMP trap to an SNMP workstation, or both. Since there are only three possible actions and since events can be used with more than one alarm, you probably will not create more than three events.
- ❑ Alarm: The last component is the alarm itself. It defines the port statistic to be monitored and the rising and falling thresholds that trigger the switch to perform an event. The thresholds of an alarm can have the same event or different events. The switch supports up to eight alarms.

Perform the following procedure to configure RMON alarms.

1. From the main menu on the left side of the page, click the **RMON** folder.

The **RMON** folder expands.

- From the **RMON** folder, select **Alarm**.

The RMON Alarm Configuration Page is displayed. See Figure 103.

RMON Alarm Configuration

Index (1~65535) *

Interval (1~2³¹-1 secs)

Variable *

Sample type ▼

Rising Threshold (0~2³¹-1)

Falling Threshold (0~2³¹-1)

Rising Event Index (1~65535)

Falling Event Index (1~65535)

Owner

Index	Interval	Variable	Sample Type	Rising Threshold	Falling Threshold	Rising Event Index	Falling Event Index	Owner	Action
<< Table is empty >>									

Page: 0/0 Page

Figure 103. RMON Alarm Configuration Page

- The following fields are listed:

Index: This parameter specifies the ID number of the new group. The range is 1 to 65535.

Interval: This parameter specifies the time (in seconds) over which the data is sampled. Its range is 1 to 2147483647 seconds.

Variable: This parameter specifies the RMON MIB object that the event is monitoring.

Sample type: This parameter defines the type of change that has to occur to trigger the alarm on the monitored statistic. There are two choices from the pull-down menu - DELTA value and ABSOLUTE value. The DELTA setting compares a threshold against the difference between the current and previous values of the statistic, while the ABSOLUTE setting compares a threshold against the current value of the statistic.

Rising Threshold: This parameter specifies a specific value or threshold level of the monitored statistic. When the value of the monitored statistic becomes greater than this threshold level, an alarm event is triggered. The parameter's range is 1 to 2147483647

Falling Threshold: This parameter specifies a specific value or threshold level of the monitored statistic. When the value of the monitored statistic becomes less than this threshold level, an alarm event is triggered. The parameter’s range is 1 to 2147483647.

Rising Event Index: This parameter specifies the event index for the rising threshold. Its range is 1 to 65535. This field is mandatory and must match an Event Index that you previously entered in “Events” on page 252.

Falling Event Index: This parameter specifies the event index for the falling threshold. Its range is 1 to 65535. This field is mandatory and must match an Event Index that you previously entered in “Events” on page 252.

Owner: This parameter is used to identify the person who created an entry. It is primarily intended for switches that are managed by more than one person, and is an optional field.

- Once you have configured the parameters, click **Apply**.

Your entry appears in the table at the bottom of the page. See Figure 104.

RMON Alarm Configuration

Index (1~65535) *

Interval (1~2^31-1 secs)

Variable *

Sample type Absolute value ▼

Rising Threshold (0~2^31-1)

Falling Threshold (0~2^31-1)

Rising Event Index (1~65535)

Falling Event Index (1~65535)

Owner

Index	Interval	Variable	Sample Type	Rising Threshold	Falling Threshold	Rising Event Index	Falling Event Index	Owner	Action
1	10000	1.3.6.1.2.1.31.1.1.1.3.1	Absolute value	600	600	3	4	Jared	<input type="button" value="Delete"/>

Page: 1/1 Page

Figure 104. RMON Alarm Configuration Example Page (To be provided)

- If you want to configure additional RMON alarms, repeat steps 3 and 4.
- From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Chapter 20

Voice VLAN

This chapter contains a description of the AT-GS950/10PS switch's Voice VLAN feature and the procedures to create, modify, and delete a voice VLAN configuration. This chapter contains the following sections:

- ❑ “Overview” on page 258
- ❑ “General Guidelines” on page 261
- ❑ “Configuration” on page 262
- ❑ “OUI Setting” on page 265

Note

To permanently save your new settings or any changes to the configuration file, select **Save Configuration to Flash** from the main menu on the left side of the page.

Overview

The AT-GS950/10PS Voice VLAN feature is specifically designed to maintain high quality, uninterrupted voice traffic through the switch. When talking on a voice over IP phone, a user expects to have no interruptions in the conversation and excellent voice quality. The Voice VLAN feature can be configured to meet these requirements.

CoS with Voice VLAN

The Voice VLAN CoS parameter maintains the voice quality between the ingress and egress ports of the AT-GS950/10PS switch. CoS must be enabled for the Voice VLAN CoS priority to take effect. The CoS priority level that you configure is applied to voice traffic on all ports of the voice VLAN.

Normally, most (non-Voice) Ethernet traffic transverses the AT-GS950/10PS switch through lower order egress queues. To avoid delays and interruptions in the voice data flow, the CoS priority level assigned to the voice VLAN should be mapped to a higher order queue and the scheduling algorithm should be set to Strict Priority. These settings ensure that the voice data packets are processed before other types of data so that the voice quality is maintained as the voice data passes through the AT-GS950/10PS switch.

Note

For more information about how to configure these CoS parameters, see “Mapping CoS Priorities to Egress Queues” on page 180 and “Queue Scheduling Algorithm” on page 185.

Organization Unique Identifier (OUI)

Each IP phone manufacturer can be identified by one or more Organization Unique Identifiers (OUIs). An OUI is three bytes long and is usually expressed in hexadecimal format. It is imbedded into the first part of each MAC address of an Ethernet network device. You can find the OUI of an IP phone in the first three complete bytes of its MAC address. Typically, you will find that all of the IP phones you are installing have the same OUI in common.

The AT-GS950/10PS switch identifies a voice data packet by comparing the OUI information in the packet’s source MAC address with an OUI table that you configure when you initially set up the voice VLAN. This is important when the Auto-Detection feature for a port and is a dynamic voice VLAN port.

Note

See “Dynamic Auto-Detection vs Static Ports” on page 259 for more information about the Auto-Detection feature.

When you are configuring the voice VLAN parameters, you must enter the complete MAC address of at least one of your IP phones. An “OUI Mask” is automatically generated and applied by the AT-S110 management software to yield the manufacturer’s OUI. If the OUI of the remaining phones from that manufacturer is the same, then no other IP phone MAC addresses need to be entered into the configuration.

However, it is possible that you can find more than one OUI from the same manufacturer among the IP phones you are installing. It is also possible that your IP phones are from two or more different manufacturers in which case you will find different OUIs for each manufacturer. If you identify more than one OUI among the IP phones being installed, then one MAC address representing each individual OUI must be configured in the voice VLAN. You can enter a total of 10 OUIs.

Dynamic Auto-Detection vs Static Ports

Prior to configuring the voice VLAN, you must configure a tagged VLAN which is the basis for the voice VLAN configuration. The VLAN must be configured with one or more tagged or untagged ports that will serve as the voice VLAN uplink/downlink. By default, a tagged or untagged port is a static member of a tagged VLAN.

Note

See “Create a Tagged VLAN” on page 157 for more information about configuring a tagged VLAN with “Not Member” and Static ports.

The ports that you choose to configure as dynamic Auto-Detection ports must be connected directly to an IP phone. When you initially define the ports of a tagged VLAN for your voice VLAN configuration, they must be configured as a “Not Member” ports. The “Not Member” ports are eligible to dynamically join the voice VLAN when voice data is detected with a pre-defined OUI in the source MAC address. The port will leave the voice VLAN after a specified timeout period. This port behavior is configured with the voice VLAN Auto-Detection feature.

Note

See “Organization Unique Identifier (OUI)” on page 258 for more information concerning OUIs.

For the Auto-Detection feature to function, your IP phone(s) must be capable of generating 802.1Q packets with imbedded VLAN ID tags. You must manually configure your IP phone(s) for the same VLAN ID as the AT-GS950/10PS switch’s voice VLAN ID. When voice data is detected on one of the “Not Member” ports, the packets from the IP phone will contain the voice VLAN ID so they are switched within the AT-GS950/10PS switch’s voice VLAN.

One or more ports in your voice VLAN must be configured as Static tagged or untagged members. Static VLAN members are permanent member ports of the voice VLAN and there is no dependency on the configuration of the devices connected to the ports. These ports might be connected to other voice VLAN network nodes such as other Ethernet switches, a telephone switch, or a DHCP server. The voice VLAN Auto-Detection feature cannot be enabled on Static tagged or tagged ports.

Note

Any Static tagged members of the voice VLAN are required to have the port VLAN ID (PVID) configured to be the same as the voice VLAN ID. This insures that all untagged packets entering the port are switched within the voice VLAN as the voice data passes through the AT-GS950/10PS switch.

If the IP phone(s) that you are installing cannot be configured with a VLAN ID, then the switch ports should be configured as Static tagged ports within the voice VLAN.

Note

Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) is *not* supported on the AT-GS950/10PS switch. Each IP phone that is VLAN aware should be manually configured for the VLAN ID that matches your AT-GS950/10PS voice VLAN ID. Each of the AT-GS950/10PS voice VLAN ports connected to an IP phone should be configured as “Not Member” ports of the tagged VLAN.

General Guidelines

Here is a summary of the rules to observe when you create a voice VLAN:

- One voice VLAN can be configured on the switch at any time.
- A voice VLAN is based on a pre-defined tagged VLAN.
- The voice VLAN Auto-Detection feature can only be enabled on ports that are initially defined as non-members of the tagged VLAN.
- On ports that are configured for the voice VLAN Auto-Detection feature, each IP phone must be manually configured per the manufacturer's instructions for the VLAN ID that matches your AT-GS950/10PS voice VLAN ID.
- Member ports of a tagged VLAN are static and cannot have the voice VLAN Auto-Detection feature enabled.
- IP phones that are not VLAN aware should be connected to Static tagged ports of the voice VLAN.
- The voice VLAN uplink/downlink port(s) must be configured as Static tagged or tagged ports.
- Any Static tagged members of the voice VLAN are required to have the port VLAN ID (PVID) configured to be the same as the voice VLAN ID.
- The Organization Unique Identifier (OUI) is configured by entering an IP phone's MAC address into the configuration.
- Only one MAC address representing each unique OUI can be configured at one time.
- Up to 10 IP phone MAC addresses/OUIs can be configured at one time.
- Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) is not supported on the AT-GS950/10PS switch.

Configuration

Prior to configuring your voice VLAN, you must first configure a tagged VLAN. This VLAN will be used as a basis for your voice VLAN.

Note

See “Create a Tagged VLAN” on page 157 for more information about configuring a tagged VLAN with Not Member and Static tagged ports.

The procedure described in this section allows you to configure a voice VLAN on the AT-GS950/10PS switch.

To configure a voice VLAN, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.
2. From the **Bridge** folder, select **Voice VLAN**. The **Voice VLAN** folder expands.
3. From the **Voice VLAN** folder, select **Voice VLAN Settings**. The AT-GS950/10PS Voice VLAN Setting Page is displayed. See Figure 105 for a partial view of this page.

Voice VLAN Setting

Voice VLAN Enabled Disabled
Notes: Disable will reset the setting to default value then turn off the function.

Voice VLAN Global Settings

VLAN ID Aging Time (1~120 hours)
 COS

Port	Auto Detection	Status	Action
All	Ignore ▾	-	<input type="button" value="Apply"/>
1	Disable ▾	None	<input type="button" value="Apply"/>
2	Disable ▾	None	<input type="button" value="Apply"/>
3	Disable ▾	None	<input type="button" value="Apply"/>
4	Disable ▾	None	<input type="button" value="Apply"/>
5	Disable ▾	None	<input type="button" value="Apply"/>
6	Disable ▾	None	<input type="button" value="Apply"/>
7	Disable ▾	None	<input type="button" value="Apply"/>
8	Disable ▾	None	<input type="button" value="Apply"/>

Figure 105. AT-GS950/10PS Voice VLAN Setting Page

Before entering any configuration parameters, you must enable the voice VLAN to activate the other parameter fields in the Voice Vlan Global Settings section which are greyed out.

4. From the **Voice VLAN** field at the top of the page, select one of the following choices from the pull-down menu:

Enable - The voice VLAN feature is active. The other parameter fields in the voice VLAN Global Settings section become active and are eligible for data to be entered.

Disable - The voice VLAN feature is inactive. The other parameter fields in the voice VLAN Global Settings section become inactive and are greyed out so that data cannot be entered.

5. In the voice VLAN Global Settings section, enter the configuration information for the following parameters:

VLAN ID - This parameter is the tagged VLAN ID that has been configured in “Tagged VLAN Configuration” on page 157 that you intend for the voice VLAN. It is a pull-down menu showing the tagged VLAN IDs that have been defined.

Aging Time - This parameter indicates the amount of time, in hours, after the last IP phone's OUI was received on a port, after which this port will be removed from the voice VLAN. The range is 1 to 120 hours.

COS - This parameter is CoS priority level assigned to the voice data packets received on each voice VLAN port.

Note

For the **COS** priority to be effective, QoS must be **Enabled**. See “Mapping CoS Priorities to Egress Queues” on page 180 for information about enabling the QoS feature.

6. Click **Apply**. The values in the Voice VLAN Global Settings section take effect.
7. In the table at the bottom of the page, The voice VLAN **Auto-Detection** status is defined. From the **Auto-Detection** column, select one of the port rows and then one of the following choices from the pull-down menu:

Ignore - This parameter indicates that the setting in the **All** row does not apply to the **Dynamic Vlan Status** field. In other words, each port is set individually.

Enable - The voice VLAN **Auto-Detection** feature is activated for the port row selected.

Disable - The voice VLAN **Auto-Detection** feature is active for the port row selected.

Note

The voice VLAN Auto-Detection feature can only be enabled on “Not Member” ports of the voice VLAN. Member ports cannot have the voice VLAN Auto-Detection feature enabled. The **Status** column displays **Static** for the member ports. See “Dynamic Auto-Detection vs Static Ports” on page 259 for more information.

8. Click **Apply** in the **Action** column of the table.
9. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

OUI Setting

You can create and delete Voice VLAN OUI Settings by following the procedures in these sections:

- ❑ “Create OUI Setting”
- ❑ “Modify OUI Setting” on page 266

Create OUI Setting

To create a Voice OUI configuration, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.
2. From the **Bridge** folder, select **Voice VLAN**. The **Voice VLAN** folder expands.
3. From the **Voice VLAN** folder, select **Voice VLAN OUI Setting**. The Voice VLAN OUI Setting Page is displayed. See Figure 106.

Voice VLAN OUI Setting

User defined OUI Description Telephony OUI (XX:XX:XX:XX:XX:XX)

(Maximum user defined OUI : 10)

ID	Description	Telephony OUI	OUI Mask	Action
----	-------------	---------------	----------	--------

Figure 106. Voice VLAN OUI Setting Page.

4. Enter a text description that helps you identify the manufacturer's OUI in the **User Defined OUI - Description** field. This parameter can be up to 20 characters in length.
5. Enter the MAC address in the **User Defined OUI - Telephony OUI** field of one of the IP phones with the manufacturer's OUI described in step 4.
6. Click **Add**. The new OUI entry is displayed in the table at the bottom of the page.
7. If you find more than one OUI among the IP phones you are installing, enter one MAC address that represents each individual OUI by following steps 4 through 6. You can enter a total of 10 OUIs.

8. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Modify OUI Setting

To modify or delete an OUI, it must be first be deleted and then re-entered by following the procedure in “Create OUI Setting” on page 265.

Delete OUI Setting

To delete an OUI, perform the following procedure:

1. From the main menu on the left side of the page, select **Bridge**. The **Bridge** folder expands.
2. From the **Bridge** folder, select **Voice VLAN**. The **Voice VLAN** folder expands.
3. From the **Voice VLAN** folder, select **Voice VLAN OUI Setting**. The Voice VLAN OUI Setting Page is displayed. See Figure 106 on page 265.
4. To delete a specific OUI that had already been entered in the table at the bottom of the page, click on **Delete** in the **Action** column of the table. The specific OUI will be deleted from the table.
5. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Chapter 21

Security

This chapter contains information about the Port-based security features and the procedures for setting this feature.

This chapter includes the following sections:

- ❑ “Port Access Control” on page 268
- ❑ “RADIUS Client” on page 273
- ❑ “Dial-in User— Local Authentication” on page 276
- ❑ “Destination MAC Filter” on page 279

Note

To permanently save your new settings or any changes to the configuration file, select **Save Configuration to Flash** from the main menu on the left side of the page.

Port Access Control

This section contains information and configuration procedures for the Port-based Access Control. The following information is provided:

- “Overview” on page 268
- “Port Access Control Configuration” on page 269

Note

After configuring the Port-based Network Access Control, you can choose to use either the local authentication server in the AT-S110 for 802.1x authentication or a remote RADIUS server for 802.1x authentication. See “Dial-in User— Local Authentication” on page 276 or “RADIUS Client” on page 273.

Overview

Port-based Network Access Control (IEEE 802.1x) is used to control who can send traffic through and receive traffic from a switch 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 logs on by entering a user name and password.

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 a user name and password are able to use the switch to access the network.

This feature can be used with one of two authentication methods:

- The RADIUS authentication protocol requires that a remote RADIUS server is present on your network. The RADIUS server performs the authentication of the user name and password combinations. See “Port Access Control Configuration” on page 269 and “RADIUS Client” on page 273 for more information.
- The Dial-in User (local) authentication method allows you to set up the authentication parameters internally in the switch without an external server. In this case, the user name and password combinations are entered in the associated with an optional VLAN when they are defined. Based on these entries, the authentication process is done locally by the AT-S110 using a standard EAPOL transaction.

Note

RADIUS with Extensible Authentication Protocol (EAP) extensions is the only supported authentication server for this feature.

Port Access Control Configuration

To configure port-based access control, perform the following procedure:

1. Select the **Security** folder from the main menu on the left side of the page.
The **Security** folder expands.
2. From the **Security** folder, select **Port Access Control**. The Port Access Control Configuration Page is displayed. See Figure 107.

Port Access Control Configuration

NAS ID: (Max. length: 16 characters)

Port Access Control:

Authentication Method:

Figure 107. Port Access Control Configuration Page

3. Configure the following parameters as required:

NAS ID - This parameter assigns an 802.1x identifier to the switch that applies to all ports. The NAS ID can be up to sixteen characters. Valid characters are 0 to 9, a to z, and A to Z. Spaces are allowed. Specifying an NAS ID is optional.

Port Access Control - This parameter enables or disables Port Access Control. Select one of the following choices from the pull-down menu:

Enable: The Port Access Control feature is activated.

Disable: The Port Access Control feature is de-activated.

Authentication Method - This parameter indicates the authentication method used by the switch. Select one of the following choices:

RADIUS: This parameter configures port security for remote authentication. After completing steps 4 - 6, you must configure the "RADIUS Client" on page 273.

Local: This parameter configures port security for local authentication. After completing steps 4 - 6, you must configure the parameters for "Dial-in User— Local Authentication" on page 276.

4. Click **Apply** when you are finished configuring the parameters.

- To set the advanced configuration parameters, click **Settings**. The Port Access Control Configure page is expanded. See Figure 108.

Port Access Control Configuration

NAS ID: (Max. length: 16 characters)

Port Access Control:

Authentication Method:

Port:

Authentication Mode:

Port Control:

Re-authentication Status:

Control Direction:

Supplicant Mode:

Piggyback Mode:

VLAN Assignment:

Secure VLAN:

Guest VLAN ID: (0-4000, 0 for disable)

Transmission Period:	<input type="text" value="30"/> Sec. (1-65535)	Maximum Request:	<input type="text" value="2"/> (1-10)
Quiet Period:	<input type="text" value="60"/> Sec. (1-65535)	Re-authentication Period:	<input type="text" value="3600"/> Sec. (1-65535)
Supplicant Timeout:	<input type="text" value="30"/> Sec. (1-65535)	Server Timeout:	<input type="text" value="30"/> Sec. (1-65535)

Figure 108. Expanded Port Access Control Configuration Page

- Set the following parameters as needed:

Port: This parameter specifies the port being configured for authentication.

Authentication Mode: This parameter specifies the port-based authentication mode. The pull-down menu choices are as follows:

802.1x: 802.1x is specified as the authentication mode. This setting applies to configuration for either RADIUS or Dial-In User authentication. For configuration information, see either “RADIUS Client” on page 273 or “Dial-in User— Local Authentication” on page 276.

MAC Based: MAC Based authentication mode is specified. For more information about configuring this mode, see “Destination MAC Filter” on page 279.

Port Control: This parameter specifies the port-based authentication role. The pull-down menu choices are as follows:

Forced Unauthorized: This parameter sets the port to the

802.1x authenticator role, in the unauthorized state. Although the ports are in the authenticator role, the switch blocks all authentication on the ports, which means that no clients can log on and forward packets through them.

Auto: Sets the port to the 802.1X port-based authenticator role. Ports begin in the unauthorized state, forwarding only EAPOL frames, until a client has successfully logged on.

Forced Authorized: Sets a port to Forced-Authorized port control. Ports that are set to the force-authorized state transition to the authorized state without any authentication exchanges required. The ports transmit and receive traffic normally without 802.1X based authentication of the clients.

Re-authentication Status: This parameter activates or deactivates the reauthentication on the authenticator ports.

Enabled: Configures the port to activate reauthentication on the authenticator ports. The clients must periodically reauthenticate according to the time interval set with the Re-authentication Period.

Disabled: Configures the port to remove reauthentication from authenticator ports so that clients do not have to periodically reauthenticate after the initial authentication. Reauthentication is still required if there is a change to the status of the link between a client and the switch or the switch is reset or power cycled.

Control Direction: The port authentication is set to “Both” meaning both transmit and receive packets are affected. You cannot change this parameter.

Supplicant Mode: This parameter specifies if one or more supplicants can be authenticated on a port.

Single: The port is set to permit only one supplicant to log on and forwards only the traffic of that supplicant. After one supplicant has logged on, the port discards packets from any other supplicant.

Multiple: The port is set to permit multiple clients on an authenticator port. An authenticator mode forwards packets from all clients once one client has successfully logged on.

Piggyback Mode: This mode is used in conjunction with the Multiple Supplicant Mode. This mode is typically used in situations where you want to add 802.1x port-based network access control to a switch port that is supporting multiple clients, but do not want to create individual accounts for all the clients on the RADIUS server. After one client has successfully logged, the port permits the other clients to piggy-back onto the initial client's log on, so that they can forward packets through the port without being

authentication.

Enabled: The Piggyback Mode is Enabled.

Disabled: The Piggyback Mode is Disabled.

VLAN Assignment - This parameter enables the VLAN assignment that you select with the **Guest VLAN ID** parameter. Choose from the following:

Enabled: The VLAN Assignment is Enabled.

Disabled: The VLAN Assignment is Disabled.

Secure VLAN: This field is inactive

Guest VLAN ID: This parameter specifies the VLAN ID that is designated as a Guest VLAN. The range is 0 to 4000 where 0 is disabled.

When a supplicant account is created on the RADIUS server, a VLAN identifier must be entered along with a username and password combination or MAC address information. If the switch receives a valid VLAN ID or VLAN name from the RADIUS server, it moves the authenticator port to the designated Guest VLAN and changes the port to the authorized state.

Transmission Period: Sets the switch-to-client retransmission time for EAP request frames. The range is 1 to 65535 seconds.

Quiet Period: Sets the number of seconds that authenticator ports wait after a failed authentication before accepting authentication requests again. The range is 1 to 65535 seconds.

Supplicant Timeout: Sets the switch-to-client retransmission time for EAP request frames. The range is 1 to 65535 seconds.

Maximum Request: Specifies the maximum number of times authenticator ports transmit EAP Request packets to clients before timing out authentication sessions. The range is 1 to 10.

Re-authentication Period: Specifies the time interval for reauthentication of clients on an authenticator port. The range is 1 to 65535 seconds

Server Timeout: Sets the length of time the switch waits for a response from the authentication server. The range is 1 to 65535 seconds.

7. To permanently save your changes, select **Save Configuration to Flash** from the main menu on the left side of the page.

RADIUS Client

You can use the RADIUS client with 802.1x port-based access control to authenticate which packets are forwarded through the switch. This section explains how to configure the RADIUS client on the switch and contains the following sections:

- ❑ “Overview” on page 273
- ❑ “Radius Client Configuration” on page 274

Note

To activate the RADIUS feature, you must also configure the port-based network access control feature. See “Port Access Control” on page 268.

Note

To permanently save your new settings or any changes to the configuration file, select **Save Configuration to Flash** from the main menu on the left side of the page.

Overview

RADIUS (Remote Authentication Dial In User Services) is an authentication protocol for enhancing the security of your network. The protocol transfers the task of authenticating network access from a network device to an authentication protocol server.

The AT-S110 Management software comes with RADIUS client software. You can use the client software together with 802.1x port-based access control. To control which end users and end nodes can send packets through the switch, you can configure the RADIUS client at “Radius Client Configuration” on page 274.

General Guidelines

The following guidelines apply when using the RADIUS protocol.

- ❑ You must install RADIUS server software on a network server or management station. Authentication protocol server software is not available from Allied Telesis.
- ❑ The RADIUS server must communicate with the switch through a port that is an untagged member of the Default VLAN and is configured for Forced-Authorized (802.1x) port control.
- ❑ If the RADIUS server is on a different subnet from switch, be sure to specify a System Default Gateway in the IP Setup Page, so that the switch and server can communicate with each other via the gateway. See “Configuration of IP Address, Subnet Mask and Gateway Address” on page 30.

- ❑ You need to specify the user name and password combinations when configuring the RADIUS server software on the authentication server.

Note

This manual does not explain how to configure RADIUS server software. Refer to the documentation that comes with the RADIUS server software for instructions.

- ❑ You must activate the RADIUS client software on the switch using the AT-S110 Management Software and configure the settings. This is explained in “Port Access Control Configuration” on page 269 and “Radius Client Configuration”.
- ❑ For more information about the RADIUS authentication protocol, refer to the RFC 2865 standard.

Radius Client Configuration

To configure the RADIUS client, perform the following procedure:

1. From the main menu on the left side of the page, select the **Security** folder.
The **Security** folder expands.
2. From the **Security** folder, select **RADIUS**.
The RADIUS Page is displayed. See Figure 109.

The screenshot shows the RADIUS configuration page with the following fields and values:

RADIUS	
Server IP Address:	0 . 0 . 0 . 0
Server Port:	1812 (1-65535)
Accounting Port:	1813 (1-65535)
Shared Secret:	(Maximum length is 20)
Apply	

Figure 109. RADIUS Page

3. To enter the RADIUS server’s IP address, enter the address in the **Server IP Address** field in the format xxx.xxx.xxx.xxx.
4. Type the port number in the **Server Port** field that you want to assign to UDP.
You may only assign one port number to this parameter.
5. Type the port number in the **Accounting Port** field that you want to assign to UDP.
You may only assign one port number to this parameter.
6. To specify the server’s encryption key, enter the encryption key in the **Shared Secret** field.
7. Click **Apply** to save your changes.

8. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Dial-in User— Local Authentication

Dial-in User feature provides the local authentication server for port security when a remote (RADIUS) server is not available. This section includes the following:

- ❑ “Overview” on page 276
- ❑ “Dial-in User Configuration” on page 276

Note

To permanently save your new settings or any changes to the configuration file, select **Save Configuration to Flash** from the main menu on the left side of the page.

Overview

The Dial-in User (local) authentication method allows you to set up 802.1x authentication parameters internally in the switch. In this case, the user name and password combinations are entered with an optional VLAN when they are defined. Based on these entries, the authentication process of a supplicant is done locally by the AT-S110 Management software using a standard EAPOL (EAP over LAN) transaction.

Dial-in User Configuration

The procedures in this section describe how to create, delete, and modify dial-in users. See the following procedures:

- ❑ “Add a Dial-in User” on page 276
- ❑ “Modify a Dial-in User” on page 277
- ❑ “Delete a Dial-in User” on page 278

Add a Dial-in User

To set up a user’s dial-in access, do the following:

1. From the main menu on the left side of the page, select the **Security** folder.
The **Security** folder expands.
2. From the **Security** folder, select **Dial-in User**.
The Dial-in User page is displayed. See Figure 110 on page 277.

Dial-In User

User Name: (Maximum length is 23)

Password: (Maximum length is 23)

Dynamic VLAN: (1-4000. 0 for ignore)

Username	Password	Dynamic VLAN	Modify	Delete
<< Dial-in user list is empty >>				

Figure 110. Dial-In User Page

3. In the **User Name** field, type a name for the user.
4. In the **Password** field, type a password for the user.
5. In the **Dynamic VLAN** field, enter the VID of the VLAN which you will allow the user to access. If you enter 0, this field will be ignored.
6. Click the **Add** button.
The Dial-in User page is refreshed. See Figure 111.

Dial-In User

User Name: (Maximum length is 23)

Password: (Maximum length is 23)

Dynamic VLAN: (1-4000. 0 for ignore)

Username	Password	Dynamic VLAN	Modify	Delete
Jenny	2	<input type="button" value="Apply"/>	<input type="button" value="Delete"/>

Page: 1/1 Page

Figure 111. Dial-In User Page Example

7. To permanently save these settings in the configuration file, select **Save Configuration to Flash** from the main menu to permanently save your changes.

Modify a Dial-in User

To modify the settings for a dial-in user, do the following:

1. From the main menu on the left side of the page, select the **Security** folder.

The **Security** folder expands.

2. From the **Security** folder, **Dial-in User**.

The Dial-in User page is displayed. See Figure 110 on page 277.

3. In the list of dial-in users, highlight the user you want to modify.
The user's information is displayed in fields above.
4. In the **Password** field, enter the new password.
5. In the **Dynamic VLAN** field, enter the new VID of the VLAN which you want the user to access.
6. Click **Apply**.
7. To permanently save these settings in the configuration file, select **Save Configuration to Flash** from the main menu to permanently save your changes.

Delete a Dial-in User

To delete a dial-in user, perform the following procedure:

1. From the main menu on the left side of the page, select the **Security** folder.
The Security folder expands.
2. From the **Security** folder, **Dial-in User**.
The Dial-in User page is displayed. See Figure 110 on page 277.
3. In the list of dial-in users, highlight the user you want to delete.
4. Click **Delete**.
The user name, password, and dynamic vlan are removed from the Dial-in User page.
5. To permanently save these settings in the configuration file, select **Save Configuration to Flash** from the main menu to permanently save your changes.

Destination MAC Filter

This section contains an explanation of the Destination MAC Filter feature as well a procedure for configuring it. This section includes the following information:

- “Overview” on page 279
- “Destination MAC Filter Configuration” on page 279
- “Delete Destination MAC Filter” on page 280

Overview

The Destination MAC Filter feature prevents the AT-GS950/10PS switch from forwarding packets to a specified device. On the Destination MAC Filter Page of the AT-S110 Management software, enter the MAC address of the device that you want to filter.

After the switch receives a packet, it examines the destination MAC address of the packet. If the destination MAC address matches a MAC address set in the filter, the software prevents the switch from forwarding it and drops the packet.

You may want to block access to a device within your organization. For instance, you may not want users on the Sales group switch to have access to a server on the Accounting group switch. You can enter the MAC address of the Accounting server as a destination MAC address filter on the Sales group switch. When a packet destined for the Accounting server is received by the Sales group switch, the switch drops the packet.

The Destination MAC Filter is a subset of the static MAC address. For more information about MAC addresses, see Chapter 10, “Overview” on page 124.

Destination MAC Filter Configuration

To set MAC address in the Destination MAC Filter, perform the following procedure:

1. From the main menu on the left side of the page, select the **Security** folder.

The **Security** folder expands.

2. From the **Security** folder, select **Destination MAC Filter**.

The Destination MAC Filter Page is displayed. See Figure 112 on page 280.

Destination MAC Filter

MAC Address: : : : : : (e.g. 00:11:ab:cd:ef:22)

MAC Address	Action
<< Destination MAC Filter is empty >>	

Figure 112. Destination MAC Filter Page

- To enter the MAC address that you want filtered, enter the MAC address into the **MAC Address** field.
- Click the **Add** button to save your entry. See Figure 113.

Dial-In User

User Name: (Maximum length is 23)
 Password: (Maximum length is 23)
 Dynamic VLAN: (1-4000. 0 for ignore)

Username	Password	Dynamic VLAN	Modify	Delete
Jenny	2	<input type="button" value="Apply"/>	<input type="button" value="Delete"/>

Page: 1/1 Page

Figure 113. Destination MAC Filter Page Example

- After you have configured a destination MAC address, the Destination MAC Filter Page is updated with the MAC address.
- From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Delete Destination MAC Filter

To delete a MAC address from the Destination MAC Filter, perform the following procedure:

- From the main menu on the left side of the page, select the **Security** folder.

The **Security** folder expands.

- From the **Security** folder, select **Destination MAC Filter**.

The Destination MAC Filter Page is shown in Figure 113.

3. Select the **Delete** button next to the MAC address that you want to delete.
The MAC address is removed from the MAC address table.
4. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Chapter 22

Power Over Ethernet (PoE)

This chapter provides background information about PoE and includes procedures to configure the PoE feature on each port. The sections in this chapter include:

- ❑ “Overview” on page 284
- ❑ “PoE Configuration” on page 286

Note

To permanently save your new settings or any changes to the configuration file, select **Save Configuration to Flash** from the main menu on the left side of the page.

Overview

The AT-GS950/10PS switch features Power over Ethernet (PoE) on the 10/100Base-Tx ports on ports 1 - 8. PoE is used to supply power to network devices over the same twisted pair cables that carry the network traffic.

The main advantage of PoE is that it can make installing a network easier. The selection of a location for a network device is often limited by whether there is a power source nearby. This constraint limits equipment placement or requires the added time and cost of having additional electrical sources installed. However, with PoE, you can install PoE-compatible devices wherever they are needed without having to worry about whether there is power source nearby.

Power Sourcing Equipment (PSE)

A device that provides PoE to other network devices is referred to as power sourcing equipment (PSE). The AT-GS950/10PS switch is a PSE device which provides DC power to the network cable and functions as a central power source for other network devices.

Powered Device (PD)

A device that receives power from a PSE device is called a *powered device* (PD). Examples include wireless access points, IP phones, webcams, and even other Ethernet switches.

PD Classes

PDs are grouped into five classes. The classes are based on the amount of power that PDs require. The AT-GS950/10PS PoE switch supports all five classes listed in Table 6.

Table 6. IEEE Powered Device Classes

Class	Maximum Power Output from a Switch Port	Power Ranges of the PDs
0	15.4W	0.44W to 12.95W
1	4.0W	0.44W to 3.84W
2	7.0W	3.84W to 6.49W
3	15.4W	6.49W to 12.95W
4	34.2W	25.5W to 38.9W

Power Budget

Power budget is the maximum amount of power that the PoE switch can provide at one time to the connected PDs. The AT-GS950/10PS can supply up to 75 Watts maximum.

Port Prioritization

As long as the total power requirements of the PDs is less than the total available power of the switch, it can supply power to all of the PDs. However, when the PD power requirements exceed the total available power, the switch denies power to some ports based on a process called port prioritization.

The ports on the PoE switch are assigned to one of three priority levels. These levels and descriptions are listed in Table 7.

Table 7. PoE Port Priorities

Priority Level	Description
Critical	This is the highest priority level. Ports set to the Critical level are guaranteed to receive power before any of the ports assigned to the other priority levels.
High	Ports set to the High level receive power only when all the ports assigned to the Critical level are already receiving power.
Low	This is the lowest priority level. Ports set to the Low level receive power only when all the ports assigned to the Critical and High levels are already receiving power. This level is the default setting.

Without enough power to support all the ports set to the same priority level at one time, the switch provides power to the ports based on the port number, in ascending order. For example, when all of the ports in the switch are set to the low priority level and the power requirements are exceeded on the switch, port 1 has the highest priority level, port 2 has the next highest priority level and so forth.

PoE Configuration

To configure the basic STP and RSTP settings, perform the following procedure:

1. From the main menu on the left side of the page, select **Power Over Ethernet Configuration**.
The **Power Over Ethernet Configuration** page is displayed. See Figure 114.

Power Over Ethernet Configuration								
Power Budget	75 W							
Power Consumption	0 W							
Port	Admin	Status	Class	Priority	Power(mW)	Voltage(V)	Current(mA)	Action
All	Ignore ▼	-	-	Ignore ▼	-	-	-	Apply
1	Disable ▼	POWER OFF	N/A	Low ▼	0	0	0	Apply
2	Disable ▼	POWER OFF	N/A	Low ▼	0	0	0	Apply
3	Disable ▼	POWER OFF	N/A	Low ▼	0	0	0	Apply
4	Disable ▼	POWER OFF	N/A	Low ▼	0	0	0	Apply
5	Disable ▼	POWER OFF	N/A	Low ▼	0	0	0	Apply
6	Disable ▼	POWER OFF	N/A	Low ▼	0	0	0	Apply
7	Disable ▼	POWER OFF	N/A	Low ▼	0	0	0	Apply
8	Disable ▼	POWER OFF	N/A	Low ▼	0	0	0	Apply

Figure 114. Power Over Ethernet Configuration Page

The Power Over Ethernet Configuration page displays the PoE status and allows you to configure PoE feature with the following parameters:

Port - Indicates the port with a specific PoE status and that you are configuring.

Admin - To activate or deactivate PoE on a specific port, select **Enable** or **Disable**. By default the PoE feature is disabled on all switch ports.

You can select the **ALL** row to set all of the ports to the same setting.

Status - The PoE port status is given as follows:

Power ON - The port is supplying PoE power.

Power OFF - The port is not supplying PoE power.

Class - The PoE class is indicated the class of the PD. N/A is displayed when the port is not supplying power.

Note

See Table 6 on page 284 for a definition of the PD PoE classes.

Priority - Indicates the port priority: Low, High, or Critical. For more details, see "Port Prioritization" on page 285.

Power(mW) - Indicates the Power in milliwatts that the port is supplying power to the PD.

Voltage(V) - Indicates the Voltage in volts as measured at the port when the port is supplying power to the PD.

Current(mA) - Indicates the Current in milliamps that the port is supplying to the PD.

2. Once you have configured the parameters, click **Apply** for the applicable port(s).
3. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Chapter 23

Chapter 23

DHCP Snooping

This chapter contains a description of the DHCP Snooping feature and the procedures for creating, modifying, and deleting the DHCP Snooping configuration. This chapter contains the following sections:

- ❑ “Overview” on page 291
- ❑ “General Configuration” on page 294
- ❑ “VLAN Setting” on page 296
- ❑ “Trusted and Untrusted Port Configuration” on page 298
- ❑ “Binding Database” on page 300

Note

To permanently save your new settings or any changes to the configuration file, select **Save Configuration to Flash** from the main menu on the left side of the page.

Overview

The DHCP Snooping feature provides security by inspecting ingress packets for the correct IP and MAC address information. The DHCP Snooping feature defines the AT-GS950/10PS ports as either trusted or untrusted. With DHCP Snooping enabled, two network security issues are addressed:

- All ingress DHCP packets are examined on the untrusted ports and only authorized packets are passed through the switch. Unwanted ingress DHCP packets are discarded. See "Unauthorized DHCP Servers" below.
- DHCP ingress packets on an untrusted port are inspected to insure that the source IP Address and MAC Address combination in each packet is valid when compared to the DHCP Snooping Binding Table. If match is not found, the packet is discarded.

Trusted Ports

By definition, trusted ports inherently trust all ingress Ethernet traffic. There is no checking or testing on ingress packets for this type of port. A trusted port connects to a DHCP server in one of the following ways:

- Directly to the legitimate trusted DHCP Server
- A network device relaying DHCP messages to and from a trusted server
- Another trusted source such as a switch with DHCP Snooping enabled.

Untrusted Ports

The Ethernet traffic on an untrusted port is inherently not trusted. The ingress packets are consequently tested against specific criteria to determine if they can be forwarded through the switch or should be immediately discarded. Untrusted ports are connected to DHCP clients and to traffic that originates outside of the LAN.

Unauthorized DHCP Servers

Normally in a network, a single DHCP server exists in a local area network (LAN). The DHCP server supplies network configuration information to individual devices on the network including the assigned IP address for each host. A trusted DHCP server is connected to a trusted port on the switch.

It is possible that another unauthorized and unwanted DHCP server could be connected to the network. This situation can occur if a client on the network happens to enable a DHCP server application on his workstation or if someone outside the network attempts to send DHCP packets to your network. These situations pose a security risk.

A network device initially sends out a DHCPDISCOVER packet so that a DHCP server will respond. It waits for and then accepts the first DHCPOFFER packet from the server that it receives. This packet contains the DHCP server's IP address and mask. If the unauthorized DHCP server responds first, then the network device will use the information from the unintended DHCP server for the default gateway or DNS server.

Untrusted ports are connected to the DHCP clients and to traffic that originated outside the LAN. By definition, untrusted ports do not accept DHCP packets originating from a DHCP server and immediately drop them when they are detected. The DHCP packets types that are not accepted are DHCPOFFER and DHCPACK.

However, untrusted ports do accept both DHCP DISCOVER and DHCPREQUEST packets sent from DHCP clients. This behavior allows DHCP clients to respond to a trusted DHCP server and not respond to a DHCP server that is untrusted.

DHCP with Option 82

You can configure the AT-GS950/10PS to pass DHCP packets containing Option 82 information through the switch without altering the information within the packet. You can also configure the AT-GS950/10PS switch to insert DHCP Option 82 information directly into the DHCP packets as they pass through the switch.

General Guidelines

Here is a summary of the rules to observe when you configure DHCP Snooping:

- A trusted port is connected to one of the following:
 - Directly to the legitimate trusted DHCP Server.
 - A network device relaying DHCP messages to and from a trusted server.
 - Another trusted source such as a switch with DHCP Snooping enabled.
- Untrusted ports are connected to DHCP clients and to traffic that originates outside of the local area network.
- The VLANs to which the DHCP Snooping feature applies must be specified in the DHCP Snooping VLAN Setting configuration.
- Any static IP addresses on the network must be manually added to the Binding Database.

General Configuration

The following procedure describes how to configure the DHCP Snooping feature on the AT-GS950/10PS switch:

1. From the main menu on the left side of the page, select **DHCP Snooping**.

The **DHCP Snooping** folder expands.

2. From the **DHCP Snooping** folder, select **General Settings**. The General Settings page is displayed. See Figure 115.

General Setting

DHCP Snooping: Enabled Disabled

Pass Through Option 82: Disabled ▼

Verify MAC Address: Enabled ▼

Backup Database: Disabled ▼

Database Update Interval: 1200 (600-86400)(Sec)

DHCP Option 82 Insertion: Disabled ▼

Figure 115. General Settings Page

3. In the **DHCP Snooping** field, select one of the following radio button choices:

Enabled - This parameter activates the DHCP Snooping feature on the AT-GS950/10PS switch.

Disabled - This parameter de-activates the DHCP Snooping feature on the AT-GS950/10PS switch.

4. From the **Pass Through Option 82** field, select one of the following choices from the pull-down menu:

Enable - Allows an Option 82 packet to be passed through the AT-GS950/10PS switch without being altered.

Disable - Blocks an Option 82 packet from passing through the AT-GS950/10PS switch.

5. From the **Verify MAC Address** field, select one of the following choices from the pull-down menu:

Enable - The MAC address of each ingress ARP packet is validated when compared against the Binding Table entries. Invalid ARP packets are discarded.

Disable - The MAC address of each ingress ARP packet is not validated against the Binding Table. All ARP packets are forwarded through the switch without regard to the IP and MAC Address information in the packet header.

6. From the **Backup Database** field, select one of the following choices from the pull-down menu:

Enable - The AT-S110 Management Software saves a backup copy of the Binding Table to flash at a specified interval (Database Update Interval) of time.

Disable - The AT-S110 Management Software does not save a backup copy of the Binding Table to flash.

7. Select an interval of time for the **Database Update Interval** field. The range of this interval is 600 to 86400 seconds.

8. From the **DHCP Option 82 Insertion** field, select one of the following choices from the pull-down menu:

Enable: The AT-S110 Management software inserts the DHCP Option 82 information into the DHCP packets.

Disable: The AT-S110 Management software does not insert the DHCP Option 82 information into the DHCP packets.

9. Click **Apply**. The values for the DHCP Snooping General Settings take effect.
10. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

VLAN Setting

You can create and delete DHCP Snooping VLAN settings by following the procedures in these sections:

- "Creating a VLAN"
- "Modifying a VLAN" on page 297
- "Deleting a VLAN" on page 297

Creating a VLAN

To define a VLAN that will be a part of the DHCP Snooping feature, do the following:

1. From the main menu on the left side of the page, select **DHCP Snooping**.

The **DHCP Snooping** folder expands.

2. From the **DHCP Snooping** folder, select **VLAN Settings**.

The VLAN Settings page is displayed. See Figure 116.

The screenshot shows the 'VLAN Settings' page. At the top, there is a blue header with the text 'VLAN Settings'. Below the header, there is a label 'VLAN ID:' followed by an empty text input field. Underneath the input field are two buttons: 'Add' and 'Reset'. Below these elements is a table with two columns: 'VLAN ID' and 'Action'. The table contains one row with the text '<< VLAN Setting is empty >>'.

Figure 116. DHCP Snooping VLAN Settings Page.

3. In the **VLAN ID** field, enter a VLAN ID that has been pre-defined.

See "Tagged VLAN Configuration" on page 157 for information about configuring VLANs.

4. Click **Add**.

The new VLAN ID entry is displayed in the table on the page.

5. If you find more than one VLAN ID to configure for DHCP Snooping, enter them one at a time by following steps 3 and 4.
6. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Modifying a VLAN

To modify or delete a VLAN ID, you must first delete it (using the procedure below) and then re-enter it by following the procedure outline in "Creating a VLAN" on page 296.

Deleting a VLAN

To delete a VLAN ID, do the following:

1. From the main menu on the left side of the page, select **DHCP Snooping**.

The **DHCP Snooping** folder expands.

2. From the **DHCP Snooping** folder, select **VLAN Settings**.

The VLAN Settings page is displayed. See Figure 116 on page 296.

3. To delete a VLAN ID, click the **Delete** button in the Action column of the table.

The VLAN ID is removed from the table.

4. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Trusted and Untrusted Port Configuration

The following procedure describes how to configure the DHCP Snooping trusted interfaces on the AT-GS950/10PS switch:

1. From the main menu on the left side of the page, select **DHCP Snooping**.

The **DHCP Snooping** folder expands.

2. From the **DHCP Snooping** folder, select **Trusted Interfaces**. A partial view of the AT-GS950/10PS Trusted Interfaces page is displayed. See Figure 117.

Trusted Interfaces		
Port	Trust	Action
All	Ignore ▾	Apply
1	Disabled ▾	Apply
2	Disabled ▾	Apply
3	Disabled ▾	Apply
4	Disabled ▾	Apply
5	Disabled ▾	Apply
6	Disabled ▾	Apply
7	Disabled ▾	Apply
8	Disabled ▾	Apply

Figure 117. AT-GS950/10PS Trusted Interfaces Page

3. From the **Trust** column, select one of the following choices from the pull-down menu:

Disable: This parameter defines the port as untrusted for the DHCP Snooping feature.

Enable: This parameter defines the port as trusted for the DHCP Snooping feature.

4. Click **Apply** for the port. The port is now configured for your selection. See Figure 118 on page 299 for a partial view of this page.

Trusted Interfaces		
Port	Trust	Action
All	Ignore ▼	Apply
1	Enabled ▼	Apply
2	Enabled ▼	Apply
3	Enabled ▼	Apply
4	Enabled ▼	Apply
5	Disabled ▼	Apply
6	Disabled ▼	Apply
7	Disabled ▼	Apply
8	Disabled ▼	Apply
9	Disabled ▼	Apply
10	Disabled ▼	Apply

Figure 118. Trusted Interfaces Page Example

5. If you choose to configure other switch ports as trusted or untrusted, repeat steps 3 and 4.
6. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Binding Database

The Binding Database displays learned and statically assigned MAC Address and IP Address information for each host on the local area network. Dynamically assigned IP addresses from the DHCP server will automatically populate the table on the Binding Database page as they are assigned by the server. Statically assigned IP addresses are entered manually by entering the host's address information and clicking on the **Add** button.

The following procedure describes how to configure the DHCP Snooping Binding Database on the AT-GS950/10PS switch for static IP addresses and how to view the MAC Address and IP Address information for all of the hosts on your local area network:

1. From the main menu on the left side of the page, select **DHCP Snooping**.

The **DHCP Snooping** folder expands.

2. From the **DHCP Snooping** folder, select **Binding Database**. The AT-GS950/10PS Binding Database page is displayed. See Figure 119.

Figure 119. AT-GS950/10PS Binding Database Page

Static IP Addresses

To enter a statically assigned IP address for a host, perform the following procedure:

1. Enter the host information into the following fields:

MAC Address - Enter the host's MAC Address.

IP Address - Enter the static IP Address assigned to the host.

VLAN - Enter the host's VLAN ID.

Port - Enter the port number where the host is connected.

Type - Because the IP Address being entered is static, you must select **Static**.

Lease Time - Enter the time that IP address assignment is valid. The range is 10 to 4294967295 seconds.

2. Click **Add**.

The static address information is entered into the Binding Database. See Figure 120 for an example.

Binding Database

MAC Address : : : : :

IP Address

VLAN

Port ▼

Type ▼

Lease Time (10 - 4294967295)(Sec)

MAC Address	VLAN ID	IP Address	Port	Type	Lease Time	Action
<input type="text"/>	<input type="text"/>	<input type="text"/>	All ▼	All ▼	All	<input type="button" value="Query"/>
A4:54:86:12:00:00	2	192.168.1.12	1	Static	Infinite	<input type="button" value="Delete"/>

Page: 1/1 Page

Figure 120. Binding Database Page Example

Viewing A dynamically assigned IP address from the DHCP server automatically populates the table on the Binding Database page. You must enter statically assigned IP Addresses and their corresponding fields at the top of the web page. See “Static IP Addresses” on page 300 for more information.

The Binding Database table at the bottom of the web page displays the following information:

MAC Address: This parameter shows the host's MAC Address.

VLAN ID: This parameter shows the host's VLAN ID of which the DHCP client is a member.

IP Address: This parameter is the IP Address assigned by the DHCP server to the DHCP client.

Port: This parameter is the port number where the DHCP client is connected.

Type: This parameter indicates the following:

Learned: The host IP Address is dynamically assigned by the DHCP server.

Static: The host IP Address is statically assigned. See “Static IP Addresses” on page 300 for more information.

Lease Time: This parameter is the time that IP address assignment by the DHCP server is valid.

If the **Page** field located below the table displays a page number, then there are multiple pages of the table that you can navigate. Click on the **First Page**, **Previous Page**, **Next Page**, and **Last Page** buttons located below the table.

Chapter 24

LLDP

Link Layer Discovery Protocol (LLDP) allows Ethernet network devices, such as switches and routers, to receive and transmit device-related information to directly connected devices on the network and to store data that is learned about other devices. This chapter provides the following information:

- “Overview” on page 304
- “Global Configuration” on page 305
- “Neighbors Information” on page 309

Note

To permanently save your new settings or any changes to the configuration file, select **Save Configuration to Flash** from the main menu on the left side of the page.

Overview

The data sent and received by LLDP are useful for many reasons. The switch can discover other devices directly connected to it. Neighboring devices can use LLDP to advertise some parts of their Layer 2 configuration to each other, which may highlight inconsistencies in the neighboring device's configuration which can then be corrected.

LLDP is a "one hop" protocol. LLDP information can only be sent to and received by devices that are directly connected to each other, or connected via a hub or repeater. Devices that are directly connected to each other are called neighbors. Advertised information is not forwarded on to other devices on the network. Also, LLDP is a one-way protocol. That is, the information transmitted in LLDP advertisements flows in one direction only, from one device to its neighbors, and the communication ends there. Transmitted advertisements do not solicit responses, and received advertisements do not solicit acknowledgements. LLDP cannot solicit any information from other devices. LLDP operates over physical ports only. For example, it can be configured on switch ports that belong to static port trunks or LACP trunks, but not on the trunks themselves, and on switch ports that belong to VLANs, but not on the VLANs themselves.

Each port can be configured to transmit local information, receive neighbor information, or both. LLDP transmits information as packets called LLDP Data Units (LLDPDUs). An LLDPDU consists of a set of Type-Length-Value elements (TLV), each of which contains a particular type of information about the device or port transmitting it.

Global Configuration

The LLDP Global Setting page has three sections:

- ❑ On the top of the page contains the enabling or disabling LLDP selections.
- ❑ The middle of the page contains LLDP System Information.
- ❑ The LLDP port settings are on the bottom of the page.

3. See Figure 121 for an example of this page.

A partial view of the AT-GS950/10PS LLDP Global Settings Page is displayed. See Figure 121.

LLDP Global Setting

LLDP Enabled Disabled

Message TX Hold Multiplier (2 - 10)

Message TX Interval (5 - 32768)

LLDP Reinit Delay (1 - 10)

LLDP TX Delay (1 - 8192)

LLDP System Information	
Chassis ID Subtype	macAddress
Chassis ID	EC:CD:6D:10:00:80
System Name	
System Description	AT-GS950/10PS Gigabit Ethernet WebSmart Switch

Port	State	Action
All	Disabled <input type="button" value="v"/>	<input type="button" value="Apply"/>
1	Enabled <input type="button" value="v"/>	<input type="button" value="Apply"/>
2	Enabled <input type="button" value="v"/>	<input type="button" value="Apply"/>
3	Enabled <input type="button" value="v"/>	<input type="button" value="Apply"/>
4	Enabled <input type="button" value="v"/>	<input type="button" value="Apply"/>
5	Enabled <input type="button" value="v"/>	<input type="button" value="Apply"/>
6	Enabled <input type="button" value="v"/>	<input type="button" value="Apply"/>
7	Enabled <input type="button" value="v"/>	<input type="button" value="Apply"/>
8	Enabled <input type="button" value="v"/>	<input type="button" value="Apply"/>
9	Enabled <input type="button" value="v"/>	<input type="button" value="Apply"/>
10	Enabled <input type="button" value="v"/>	<input type="button" value="Apply"/>

Figure 121. AT-GS950/10PS LLDP Global Settings Page

Perform the following procedures to configure the global parameters for LLDP:

- ❑ “Enabling or Disabling LLDP” on page 306
- ❑ “Displaying System Information” on page 307

- “Setting Port States” on page 307

You must enable LLDP before changing the LLDP System Information settings or the port settings.

Enabling or Disabling LLDP

To enable or disable the LLDP feature, perform the following procedure:

1. From the main menu on the left side of the page, click the **LLDP** folder. The **LLDP** folder expands.
2. From the **LLDP** folder, select **LLDP Global Setting**.

The AT-GS950/10PS LLDP Global Settings Page is displayed. See Figure 121 on page 305.

A partial view of the AT-GS950/10PS LLDP Global Settings Page is displayed. See Figure 121 on page 305.

3. From the **LLDP** parameter, select one of the following radio button choices:

Enable: The LLDP feature is active.

Disable: The LLDP feature is inactive.

Note

The LLDP feature is not dependent on the DHCP feature. As a result, the DHCP feature can be set to either enabled or disabled without affecting LLDP.

4. Click the **Apply** button to the right of the either the **Enable** or **Disable** radio buttons.

The LLDP setting that you have selected is now active.

5. Below the **Enable** or **Disable** radio buttons, you may adjust the following parameters as needed:

Message TX Hold Multiplier: Sets the hold multiplier value. The hold time multiplier is multiplied by the transmit interval to give the Time To Live (TTL) that the switch advertises to the neighbors. The range is from 2 to 10.

Message TX Interval: Sets the transmit interval, which is the interval between regular transmissions of LLDP advertisements. The range is from 1 to 10 seconds.

LLDP Reinit Delay: Sets the reinitialization delay, which is the number of seconds that must elapse after LLDP is disabled on a port before it can be reinitialized. The range is from 1 to 10 seconds.

LLDP TX Delay: Sets the value of the transmission delay timer, which is the minimum time interval between transmissions of LLDP advertisements due to a change in LLDP local information. The range is from 1 to 8192 seconds.

- From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Displaying System Information

To display system information about the switch, do the following:

- From the main menu on the left side of the page, click the **LLDP** folder. The **LLDP** folder expands.
- From the **LLDP** folder, select **LLDP Global Setting**.

The AT-GS950/10PS LLDP Global Settings Page is displayed. See Figure 121 on page 305.

- The following parameters display the system information:

Chassis ID Subtype: This parameter describes the Chassis ID subtype which is "macAddress". You cannot change this parameter.

Chassis ID: This parameter lists the MAC Address of the switch. You cannot change this parameter.

System Name: This parameter lists the System Name of the switch. You can assign the system name. For more information, see "System Management Information" on page 28.

System Description: This parameter lists the product name of the switch. You cannot change this parameter.

Setting Port States

Each port on the switch can be assigned a LLDP states as follows:

- Refer to the lower section of Figure 121 on page 305 for the LLDP port states.
- In the State column, select one of the following states from a port's pull-down menu:

Disabled: Indicates LLDP is disabled on the port. The port can not receive or transmit LLDP data packets.

Enabled: Indicates LLDP is enabled on the port. The port can receive and transmit LLDP data packets.

RxOnly: Indicates LLDP is enabled on the port. The port can receive LLDP data packets.

TxOnly: Indicates LLDP is enabled on the port. The port can

transmit LLDP data packets.

To change the settings of all the ports to the same state, select a state setting next to All In the Port column.

3. In the Action column, click the **Apply** button that corresponds to the port to make the state change active.

Neighbors Information

To view the information received from the neighboring network devices, perform the following procedure:

1. From the main menu on the left side of the page, click the **LLDP** folder. The **LLDP** folder expands.
2. From the **LLDP** folder, select **LLDP Neighbors Information**.

The LLDP Neighbors Information Page is displayed. See Figure 122.

LLDP Neighbors Information							
Entity	Port	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	Port Description	Show Normal

Figure 122. LLDP Neighbors Information Page

The following parameters are displayed when the switch receives LLDP information from neighboring devices in the LAN:

Entity: This parameter is a number assigned to the reporting neighbors in the order that the LLDP information is received from them.

Port: This parameter specifies the AT-GS950/10PS local port number where the LLDP information was received.

Chassis ID Subtype: This parameter describes the Chassis ID subtype of the neighboring network device which is reporting the LLDP information.

Chassis ID: This parameter is the neighboring device's chassis ID.

Port ID Subtype: This parameter describes the Port ID subtype of the neighboring network device's port that is connected directly to the AT-GS950/10PS switch port.

Port ID: This parameter specifies the neighboring network device's port number from which the LLDP information was transmitted.

Port Description: This parameter describes the neighboring network device's port.

Show Normal: If you click on this button, a detailed report of the neighboring network device will be displayed.

Chapter 25

Network Statistics

The sections in this chapter explain how to display traffic, error, and history statistics about the network traffic on the AT-GS950/10PS switch and its ports. This chapter includes the following sections:

- ❑ “Overview” on page 312
- ❑ “Traffic Comparison Statistics” on page 313
- ❑ “Error Group Statistics” on page 316
- ❑ “Historical Status Charts” on page 318

Note

To permanently save your new settings or any changes to the configuration file, select **Save Configuration to Flash** from the main menu on the left side of the page.

Overview

Statistics provide important information for troubleshooting switch problems at the port level. The AT-S110 Management Software provides a versatile set of statistics charts that you can customize for your needs, including (depending upon the chart) the ports whose statistics you want to view and the color used to draw the chart.

There are three types of statistics charts:

- ❑ **Traffic Comparison:** The Traffic Comparison statistics chart allows you to display a specified traffic statistic over all of the ports. You can select 12 statistic types and 12 colors for each port. This chart is described in “Traffic Comparison Statistics” on page 313.
- ❑ **Error Group:** The Error Group chart displays the discard and error counts for a specified port and is described in “Error Group Statistics” on page 316.
- ❑ **Historical Status:** This chart allows you to select from 12 statistics to view for a selection of ports for however long this chart is running on the management workstation. The Historical Status chart is described in “Historical Status Charts” on page 318.

Traffic Comparison Statistics

The Traffic Comparison statistics chart allows you to display a specified traffic statistic over all of the ports. You can select 12 statistic types and 12 colors for each port.

To display traffic comparison statistics, perform the following procedure:

1. Select the **Statistics Chart** folder.

The **Statistics Chart** folder expands.

2. From the **Statistics Chart** folder, select **Traffic Comparison**.

The Traffic Comparison Page opens as shown in Figure 123.

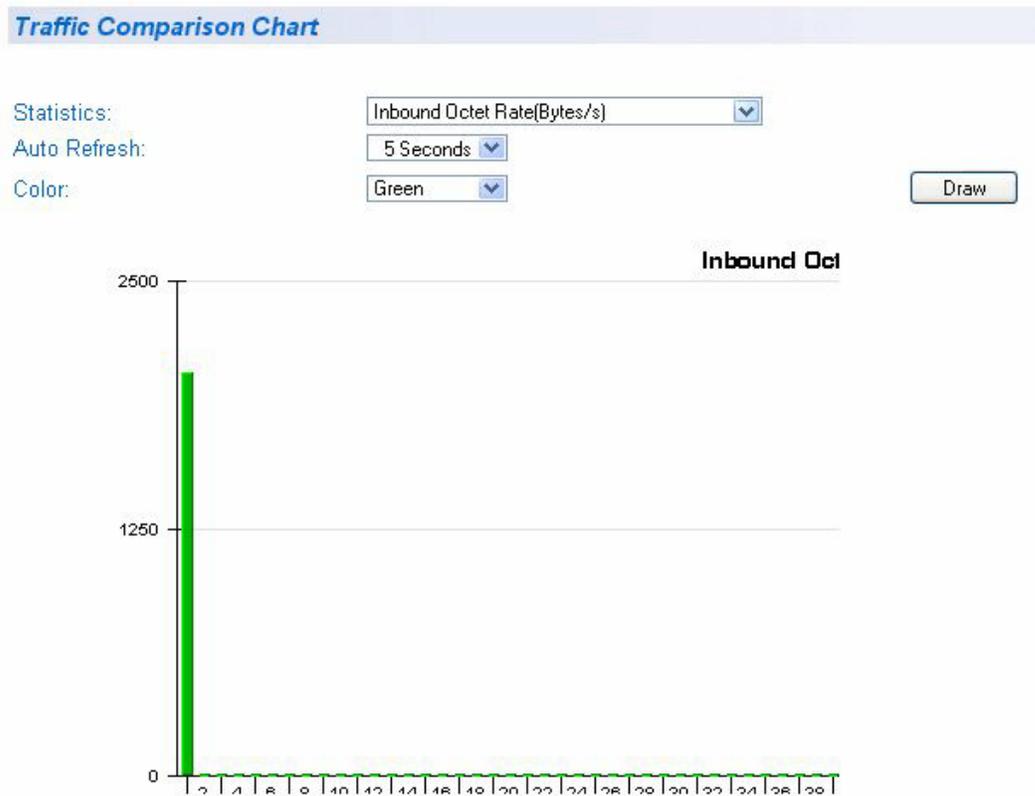


Figure 123. Traffic Comparison Page

3. To view traffic statistics, click on the arrow next to “Statistics” and select one of the options in Table 8.

Table 8 Traffic Comparison Options

Option	Definition
Inbound Octets (Bytes/s)	Measures the number of inbound octet bits in bytes per second.
Inbound Unicast Packets (Pkts)	Measures the number of inbound unicast packets in packets per second.
Inbound Non-unicast Packets (Pkts)	Measures the number of inbound non-unicast packets (such as broadcast and multicast packets) in packets per second.
Inbound Discards (Pkts)	Measures the number of inbound discarded packets in packets per second.
Inbound Errors (Pkts/s)	Measures the number of inbound errors in packets per second.
Outbound Octets (Bytes/s)	Measures the rate of outbound octet bits in bytes per second.
Outbound Unicast Packets (Pkts)	Measures the number of outbound unicast packets in packets per second.
Outbound Non-unicast Packets (Pkts)	Measures the number of outbound non-unicast (such as broadcast and multicast packets) packets.
Outbound Discards (Pkts)	Measures the number of outbound discarded packets.
Outbound Errors (Pkts)	Measures the number of outbound error packets.
Ethernet Undersize Packets (Pkts)	Measures the number of undersized Ethernet packets.
Ethernet Oversize Packets (Pkts)	Measures the number of oversized Ethernet packets.

4. To select the amount of time before the screen is refreshed, click **Auto Refresh**. Choose from the following options:

- **5 seconds**
- **10 seconds**
- **15 seconds**
- **30 seconds**

5. To select the color of the traffic comparison graph, select **Color**.
Choose one of the following colors:
 - **Green**
 - **Blue**
 - **Red**
 - **Purple**
 - **Yellow**
 - **Orange**
 - **Gray**
 - **Light Red**
 - **Light Blue**
 - **Light Green**
 - **Light Yellow**
 - **Light Gray**
6. To create the traffic comparison graph, select **Draw**.
7. From the menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Error Group Statistics

The Error Group chart displays the discard and error counts for a specified port.

To display error group statistics for a port, perform the following procedure:

1. Select the **Statistics Chart** folder.

The **Statistics Chart** folder expands.

2. From the **Statistics Chart** folder, select **Error Group**.

The Error Group Chart Page is displayed in Figure 124.

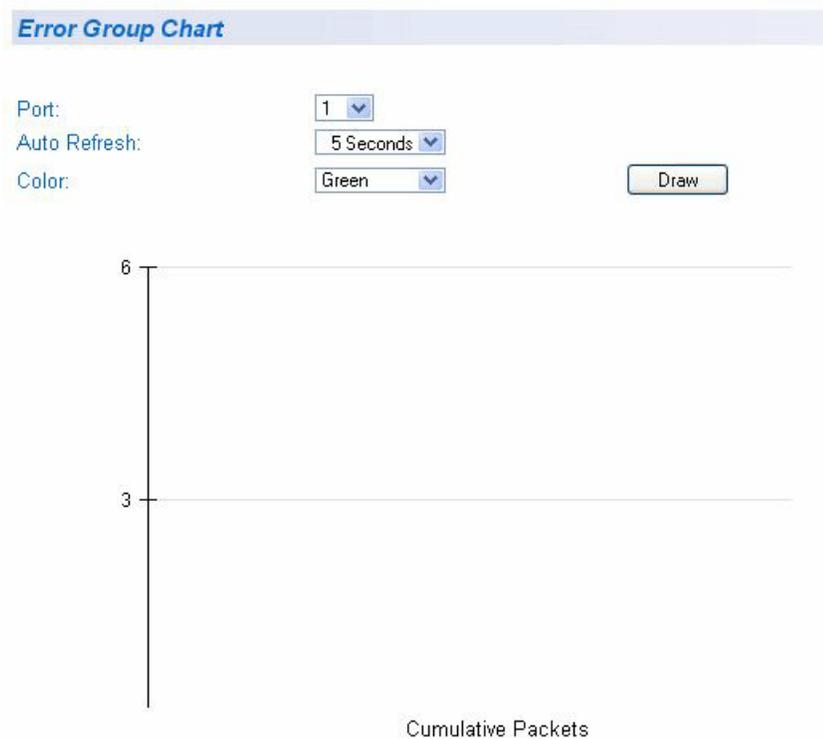


Figure 124. Error Group Chart Page

3. Select a port number from the pull down menu next to **Port**.

4. To select the amount of time before the screen is refreshed, click **Auto Refresh**. Choose from the following options:
 - **5 seconds**
 - **10 seconds**
 - **15 seconds**
 - **30 seconds**

5. To select the color of the traffic comparison graph, select **Color**. Choose one of the following colors:
 - **Green**
 - **Blue**
 - **Red**
 - **Purple**
 - **Yellow**
 - **Orange**
 - **Gray**
 - **Light Red**
 - **Light Blue**
 - **Light Green**
 - **Light Yellow**
 - **Light Gray**

6. To create the Error Group Chart, select **Draw**.

7. From the menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Historical Status Charts

The Historical Status chart allows you to select from 12 statistics to view for a selection of ports for however long this chart is running on the management workstation. To display historical status charts statistics for a port, perform the following procedure:

1. Select the **Statistics Chart** folder.

The **Statistics Chart** folder expands.

2. From the **Statistics Chart** folder, select **Historical Status**.

The Historical Status Chart Page is displayed in Figure 125.

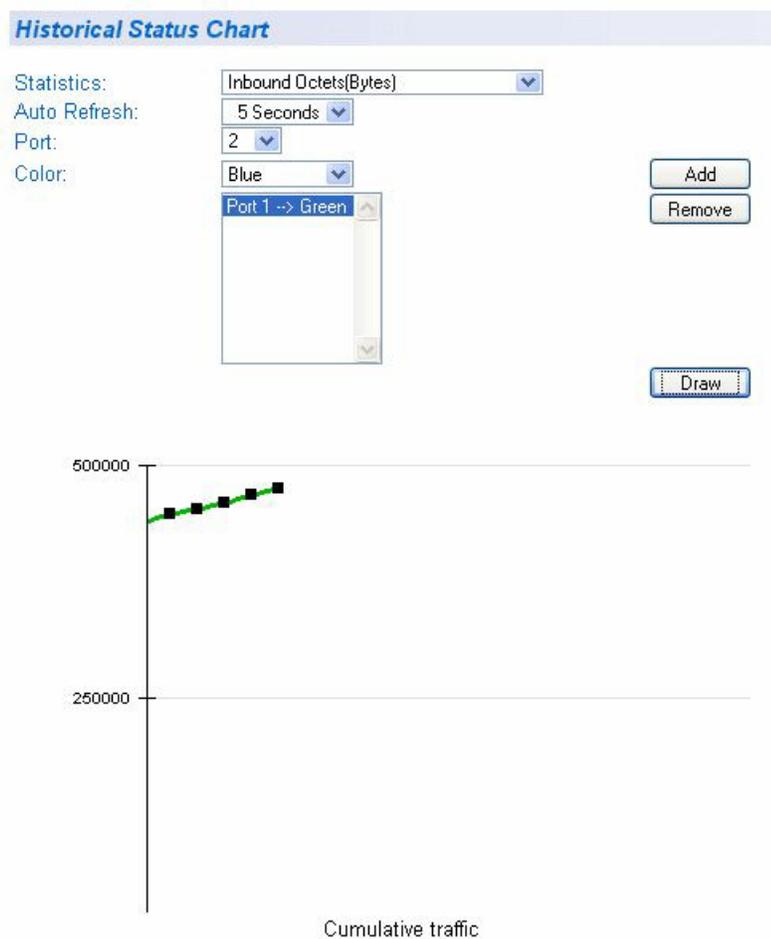


Figure 125. Historical Status Chart Page

3. To view historical statistics, click on the arrow next to "Statistics" and select one of the options in Table 9 on page 319.

Table 9 Historical Status Options

Option	Definition
Inbound Octet Rate (Bytes)	Measures the rate of inbound octet bits in bytes per second.
Inbound Unicast Packet Rate (Pkts)	Measures the rate of inbound unicast packets in packets per second.
Inbound Non-unicast Packet Rate (Pkts)	Measures the rate of inbound non-unicast packets (such as broadcast and multicast packets) in packets per second.
Inbound Discards (Pkts)	Measures the number of inbound discarded packets in packets per second.
Inbound Errors (Pkts)	Measures the number of inbound errors in packets per second.
Outbound Octets (Bytes)	Measures the number of outbound octet bits in bytes per second.
Outbound Unicast Packets (Pkts)	Measures the number of outbound unicast packets in packets per second.
Outbound Non-unicast Packets (Pkts)	Measures the number of outbound non-unicast (such as broadcast and multicast packets) packets.
Outbound Discards (Pkts)	Measures the number of outbound discarded packets.
Outbound Errors (Pkts)	Measures the number of outbound error packets.
Ethernet Undersize Packets (Pkts)	Measures the number of undersized Ethernet packets.
Ethernet Oversize Packet Rate (Pkts)	Measures the number of oversized Ethernet packets.

4. To select the amount of time before the screen is refreshed, click **Auto Refresh**. Choose from the following options:
 - **5 seconds**
 - **10 seconds**
 - **15 seconds**
 - **30 seconds**
5. To select the color of the traffic comparison graph, select **Color**. Choose one of the following colors:
 - **Green**
 - **Blue**
 - **Red**
 - **Purple**
 - **Yellow**
 - **Orange**
 - **Gray**
 - **Light Red**
 - **Light Blue**
 - **Light Green**
 - **Light Yellow**
 - **Light Gray**
6. To create the history group chart, select **Add**.
7. Click **Draw**.
8. To draw the historical group chart, select **Draw**.
9. From the menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Section IV

Tools

This section contains the following chapters:

- ❑ Chapter 26, “Software/Configuration Updates” on page 323
- ❑ Chapter 27, “Cable Diagnostics” on page 335
- ❑ Chapter 28, “Rebooting the AT-GS950/10PS” on page 337
- ❑ Chapter 29, “Pinging a Remote System” on page 347

Chapter 26

Software/Configuration Updates

This chapter explains the methods for upgrading the AT-S110 Management Software on the switch and saving configuration files. This chapter contains the following sections:

- ❑ “Overview” on page 324
- ❑ “Upgrade Firmware Image via HTTP” on page 325
- ❑ “Upgrade Firmware Image via TFTP” on page 327
- ❑ “Upload or Download a Configuration File via HTTP” on page 329
- ❑ “Download or Upload a Configuration File via TFTP” on page 332

Note

For information about how to obtain new releases of the AT-S110 Management Software, see “Allied Telesis Contact Information” on page 17.

Note

To permanently save your new settings or any changes to the configuration file, select **Save Configuration to Flash** from the main menu on the left side of the page.

Overview

You can use the Management Software Updates features to upgrade the AT-S110 Management Software to a new version, save a configuration file or load a configuration file. In addition, you can:

- Upload a configuration file from the switch onto a PC
- Download a configuration file from a PC onto the switch

There are two methods to upgrade the AT-S110 Management software or upload or download your configuration file:

- Using a web browser via HTTP
- Using a TFTP server

To perform one of these operations using HTTP, you only need to have access to an Internet browser. However, to perform one of these operations using TFTP, you must have access to a TFTP server.

In addition, you can save a configuration file from your AT-GS950/10PS switch, which can be downloaded to other AT-GS950/10PS switches on your network. This ensures identical configurations on all of your switches. In addition, loading an existing configuration saves time.

Upgrade Firmware Image via HTTP

This section describes how to upgrade an firmware image of the AT-S110 Management Software using HTTP on an Internet server. Before downloading a new version of the AT-S110 Management Software onto the switch with HTTP, note the following:

- ❑ The current configuration of the switch is retained when a new AT-S110 software image is installed. To return a switch to its default configuration values, see “Configure Factory Default Values” on page 340.
- ❑ When downloading the new image file, your switch must have an IP address and subnet mask assigned, either manually or via DHCP. For instructions on how to set the IP address and subnet mask on a switch, see “Configuration of IP Address, Subnet Mask and Gateway Address” on page 30. To enable a DHCP client, see “DHCP Client Configuration” on page 45.



Caution

Downloading a new version of management software onto the switch causes the device to reset. Some network traffic may be lost during the reset process.

This procedure assumes that you have already obtained the software and have stored it on the computer from which you will be performing this procedure.

To download the AT-S110 image software onto the switch using HTTP, perform the following procedure:

1. From the menu on the left side of the home page, select the **Tools** folder.
This folder expands to show the **Firmware Upgrade** folder.

2. From the **Firmware Upgrade** folder, select **via HTTP**.

The Firmware Upgrade via HTTP Page is displayed. See Figure 126.

Firmware Upgrade via HTTP

Image Version: AT-S110 V1.0.0 [1.00.013]

Firmware File:

Note: System will reset automatically after burning image to flash.

Figure 126. Firmware Upgrade via HTTP Page

3. Change the following parameter as necessary:

Firmware File: Enter the path and the firmware file name or click the **Browse** button and select the file name.

4. To begin the upgrade process on the switch, click **Apply**.

The software begins to download onto the switch immediately. This process takes a few minutes. After the software download is complete, the switch initializes the software and reboots. You will lose your web browser connection to the switch during the reboot process.

Upgrade Firmware Image via TFTP

This section describes how to upgrade an firmware image of the AT-S110 Management software using TFTP on an TFTP server. Before downloading a new version of the AT-S110 Management Software onto the switch, note the following:

- ❑ The current configuration of a switch is retained when a new AT-S110 Management Software image is installed. To return a switch to its default configuration values, see “Configure Factory Default Values” on page 340.
- ❑ Your network must have a TFTP server.
- ❑ You must specify the path to the new AT-S110 image file on the TFTP server.
- ❑ Start the TFTP server software *before* you begin the download procedure.



Caution

Downloading a new version of management software onto the switch causes the device to reset. Some network traffic may be lost during the reset process.

This procedure assumes that you have already obtained the software and have stored it on the computer from which you will be performing this procedure.

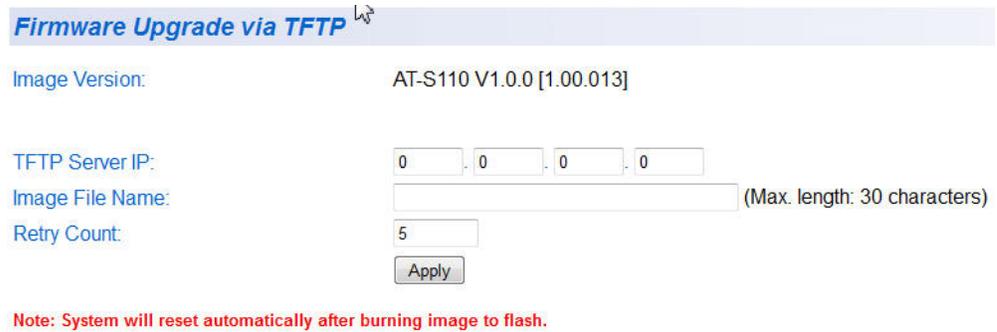
To download the AT-S110 image software onto the switch using a TFTP server, perform the following procedure:

1. From the menu on the left side of the home page, select the **Tools** folder.

This folder expands to show contents of the **Firmware Upgrade** folder.

2. From the **Firmware Upgrade** folder, select **via TFTP**.

The Firmware Upgrade via TFTP page is shown in Figure 127 on page 328.



Firmware Upgrade via TFTP

Image Version: AT-S110 V1.0.0 [1.00.013]

TFTP Server IP: 0 . 0 . 0 . 0

Image File Name: (Max. length: 30 characters)

Retry Count: 5

Apply

Note: System will reset automatically after burning image to flash.

Figure 127. Firmware Upgrade via TFTP Page

The **Image/Version Date** shows the current version and date of software installed on the switch.

3. Change the following parameters as necessary:

TFTP Server IP: The IP address of the TFTP server from which you are downloading the new software.

Image File Name: The full name of the AT-S110 file (including the file extension) you are downloading.

Retry Count: The number of times the firmware upgrade is retried. The range is 1 - 20.

4. To activate your changes on the switch, click **Apply**.

The software immediately begins to download onto the switch. This process takes a few minutes. After the software download is complete, the switch initializes the software and reboots. You will lose your web browser connection to the switch during the reboot process.

Upload or Download a Configuration File via HTTP

This section describes how to upload or download a configuration file using HTTP on an Internet server. Before you upload or download a configuration file via HTTP, note the following:

- ❑ You must be able to access the new AT-S110 configuration file from your PC when downloading a file from a PC to the switch.
- ❑ The switch that you are working with must have an IP address and subnet mask assigned, either manually or via DHCP. For instructions on how to manually set the IP address and subnet mask on a switch, see “Configuration of IP Address, Subnet Mask and Gateway Address” on page 30. To enable a DHCP client, see “DHCP Client Configuration” on page 45.

To upload or download an AT-S110 configuration file onto the switch using a web browser, perform the following procedure:

1. From the menu on the left side of the home page, select the **Tools** folder.

The **Tools** folder expands.

2. From the **Tools** folder, select **Config File Upload/Down** folder.

The **Config File Upload/Down** folder expands.

3. From the **Config File Upload/Down** folder, select **via HTTP**.

The Configuration File Upload/Download via HTTP page is displayed. See Figure 128.

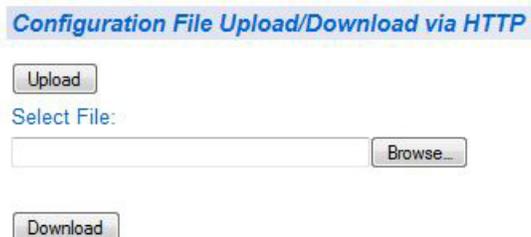


Figure 128. Configuration File Upload/Download via HTTP Page

Configuration File Upload

To upload an AT-S110 configuration file from your PC to the switch, perform the following procedure:

1. Click the **Browse** button under the **Select File** field and select the path and file name.
See Figure 128. The path and file name are displayed in the Select File field.

2. Select the **Upload** button.
The download process begins immediately.



Caution

If you are uploading a configuration file, the file will be implemented immediately after download. A short interruption in network service will be experienced while the new configuration file is loaded.

Note

If the IP address contained in the new configuration file is different than the one you currently have in your browser URL, you will lose connectivity with the AT-S110 Management software on the AT-GS950/10PS switch after the new configuration file is loaded. If this is the case, you can identify the new IP address by using the ATI Web Discovery Tool. See “DHCP and ATI Web Discovery Tool” on page 44 for more information.

3. The Results page will be displayed indicating that the file has been successfully downloaded. See Figure 129.

Result

Upload/Download-> 1310 bytes data transferred!
[Return to previous page](#)

Figure 129. Result Page

4. Click on the “Return to previous page” link.

Configuration File Download

To download or save the AT-S110 configuration file from the switch to your PC, perform the following procedure:

1. Select the **Download** button. Select this button to download a configuration file from the switch to your PC.
The following window shown in Figure 130 is displayed.

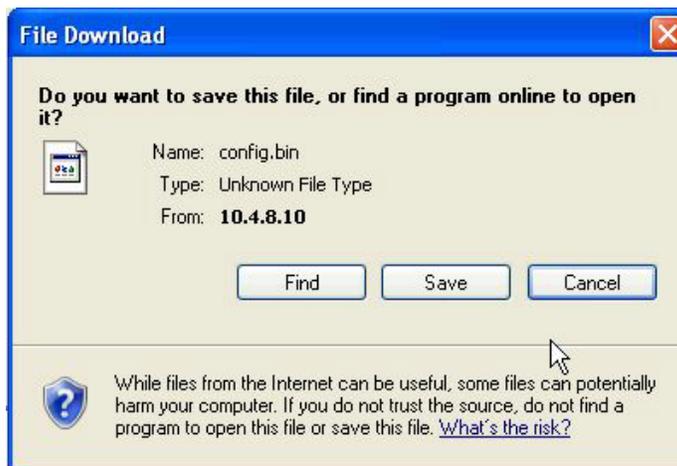


Figure 130. File Download with HTTP

2. Click **Save** to save the configuration file onto the switch.
3. The **Save As** window is displayed.
4. Save the file in the appropriate directory.

The software immediately begins to upload and be saved on your PC.

Download or Upload a Configuration File via TFTP

This section describes how to upload or download a configuration file using TFTP on an TFTP server. Before you upload or download a configuration file onto the switch using TFTP, note the following:

- ❑ Your network must have a TFTP server.
- ❑ You must specify the path to the configuration file on the TFTP server.
- ❑ Start the TFTP server software *before* you begin the download procedure.

To upload or download an AT-S110 configuration file onto the switch using a TFTP server, perform the following procedure:

1. From the menu on the left side of the home page, select the **Tools** folder.
The **Tools** folder expands.
2. From the **Tools** folder, select the **Config File Upload/Download** folder.
The **Config File Upload/Download** folder expands.
3. From the **Config File Upload/Down** folder, select **via TFTP**.
The Configuration Upload/Download via TFTP Page is displayed. See Figure 131.

Figure 131. Configuration Upload/Download via TFTP Page

Configuration File Upload

To upload an AT-S110 configuration file onto the switch, perform the following procedure:

1. Enter the IP address of the TFTP server in the field next to the **TFTP Server IP** parameter.
2. Select the **Upload** button.
3. The software immediately begins to upload the configuration file from the switch to the TFTP server.



Caution

If you are uploading a configuration file, the file will be implemented immediately after download. A short interruption in network service will be experienced while the new configuration file is loaded.

Note

If the IP address contained in the new configuration file is different than the one you currently have in your browser URL, you will lose connectivity with the AT-S110 Management software on the AT-GS950/10PS switch after the new configuration file is loaded. If this is the case, you can identify the new IP address by using the AT Web Discovery Tool. See “DHCP and AT Web Discovery Tool” on page 44 for more information.

**Configuration
File Download**

To download an AT-S110 configuration file to your PC, perform the following procedure:

1. Enter the IP address of the TFTP server in the field next to the **TFTP Server IP** parameter.
2. Enter the name of the configuration file in the field next to the **Config File Name** parameter.
3. Select the **Download** button.
The Results page is displayed indicating that the file has been successfully downloaded. See Figure 129 on page 330.
4. Click on the “Return to previous page” link.

Chapter 27

Cable Diagnostics

This chapter provides procedures to run cable diagnostics on the cables connected to the switch ports. If a port is selected, a cable must be connected to it for meaningful test results to be displayed.

Note

To permanently save your new settings or any changes to the configuration file, select **Save Configuration to Flash** from the main menu on the left side of the page.

To do these cable diagnostics, perform the following procedure:

1. From the main menu on the left side of the page, click the **Tools** folder.

The **Tools** folder expands.

2. From the **Tools** folder, select **Cable Diagnostics**.

The Cable Diagnostics page is displayed. See Figure 132.

Cable Diagnostics

Port

Port	Test Result	Cable Fault Distance (meters)	Cable Length (meters) [in range]
------	-------------	-------------------------------	----------------------------------

The cable diagnostics feature is designed primarily for administrators or customer service representatives to verify and test copper cables; it can rapidly determine the quality of the cables and the types of error.

Note:

1. If cable length is displayed as "N/A" it means the cable length is "Not Available".
This is due to the port being unable to obtain cable length/either because its link speed is 10M or 100M, or the cables used are broken and/or bad in quality.
2. The deviation of "Cable Fault Distance" is +/-2 meters,
therefore No cable may be displayed under Test Result, when the cable used is less than 2 m in length.
3. It also measures cable fault and identifies the fault in length according to the distance from this switch.

Figure 132. Cable Diagnostics Page

3. Select the **Port** number from the drop-down menu.
4. Click **Test Now**.
5. The following information is displayed:

Port: This parameter displays the port (cable) selected.

Test Results: Displays the diagnostic results for each pair in the cable. One of the following cable status parameters is displayed:

OK: There is not problem detected with the cable.

Open in Cable: There is an open wire within the cable.

Short in Cable: Two wires are shorted together within the cable.

Cross talk in Cable: There is crosstalk detected between one pair of wires and another pair within the cable.

Cable Fault Distance: This parameter specifies the distance from the switch port to the cable fault.

Cable Length: This parameter specifies the length of the cable connected to the switch port.

Note

If length is displayed as “N/A” it means the cable length is “Not Available”. This is due to the port being unable to obtain cable length/either because its link speed is 10M or 100M, or the cables used are broken and/or of bad in quality.

Note

The deviation of “Cable Fault Distance” is +/-2 meters, therefore No cable may be displayed under Test Result, when the cable used is less than 2 m in length.

Rebooting the AT-GS950/10PS

This chapter provides the procedures for rebooting the AT-GS950/10PS switch by using the **Normal** reboot function provided in the AT-S110 management software.

Note

Alternately, you can reboot the AT-GS950/10PS switch by pressing the front panel eco-friendly switch between 5 to 9 seconds.

In addition to rebooting the switch in the AT-S110 management software, you have the option to reset the configuration parameters on the switch to the original factory default settings. There are two ways to accomplish this:

- Press the front panel ecofriendly button for more than 10 seconds and release it.
- Reboot the switch in the AT-S110 management software and follow the procedures to reset to factory defaults.

Note

Refer to the AT-GS950 Installation guide for more information about how to use the eco-friendly button to reboot or reset the switch.

Note

The AT-S110 Management software default values are listed in “AT-GS950/8 Default Parameters” on page 347.

The following procedures are included in this chapter:

- “Switch Reboot” on page 338
- “Configure Factory Default Values” on page 340
- “Password Protection of Factory Reset” on page 342

Switch Reboot

The following procedure outlines how to reboot your AT-GS950/10PS switch.



Caution

This procedure reboots the switch and reloads the AT-S110 Management software configuration from flash memory. Insure that your current configuration is saved before rebooting the switch by selecting **Save Configuration to Flash** from the main menu on the left side of the page to permanently save your changes.

All configuration parameters that have not been previously saved are lost. After the switch is reboots, they are reset to the values stored in the flash memory.



Caution

This procedure causes the switch to reboot. The switch does not forward network traffic during the reboot process. Some network traffic may be lost.

1. From the main menu on the left side of the page, select the **Tools** folder.
The **Tools** folder expands.
2. From the **Tools** folder, select **Reboot**.
The Factory Default Reset/Reboot Page is displayed. See Figure 133.

Factory Default Reset

Factory Default Reset:

Reboot

Reboot Type:

Note: System will reset in a few seconds after pressing Apply button.

Figure 133. Factory Default Reset/Reboot Page

3. Go to the lower part of the page to the Reboot section.

4. In the **Reboot Type** field, select **Normal** from the pull-down menu. When the switch is rebooted with this selection, all configuration parameters that are saved in flash memory are loaded into the switch's active memory.

Note

Two additional options are available in the **Reboot Type** field. The procedures for these options are described in "Configure Factory Default Values".

5. Click **Apply**.
The switch immediately begins to reload the AT-S110 Management software and configuration parameters. This process takes approximately two minutes to complete. You can not manage the device during the reboot. After the reboot is finished, you can log in again if you want to continue to manage the switch.

Configure Factory Default Values

The following procedure returns all AT-S110 Management software parameters to their factory default values and deletes all tagged and port-based VLANs on the switch.

Note

The AT-S110 Management software factory default values are listed in “AT-GS950/8 Default Parameters” on page 347.



Caution

This procedure causes the switch to reboot. The switch does not forward network traffic during the reboot process. Some network traffic may be lost.

1. From the main menu on the left side of the page, select the **Tools** folder.
The **Tools** folder expands.
2. From the **Tools** folder, select **Reboot**.
The Reboot Page is displayed. See Figure 133 on page 338.
3. Go to the lower part of the page to the Reboot section.
4. In the **Reboot Type** field, use the pull-down menu to select one of the following options:

Normal - This setting reloads all configuration parameters that are saved in flash memory. See “Switch Reboot” on page 338 for more information when using this selection.

Factory Default - Resets all switch parameters to the factory default settings, including the IP address, subnet mask, and gateway address.



Caution

This setting will cause the IP address to be reset to 192.168.1.1. You will lose connectivity with the switch management software after the reboot is completed and you can login again with this IP address.

Factory Default Except IP Address - Resets all switch parameters to the factory default settings, but retains the current IP address, subnet mask, and gateway settings saved in flash memory. If the DHCP client is enabled, it remains enabled after this reset and assignment of the IP

address, subnet mask, and gateway settings are managed by the DHCP server.

5. Click **Apply**.
The switch begins the reboot process. You must wait approximately two minutes for the switch to complete the reboot process before you can re-establish your management session and network traffic begins flowing normally again.

Password Protection of Factory Reset

If your switch is located in a controlled environment such as a locked switching closet or limited access equipment room, it may be desirable to have the ability to easily reset the switch to factory defaults at any time by using either the front panel ecofriendly switch or the AT-S110 management software.

However, if your switch is installed in an uncontrolled environment, you may want to protect the switch's configuration from unwanted or accidental resets. The AT-S110 management software allows you to disable the factory default reset feature and lock it with your own password. When this is done, two areas are affected:

- The reset and factory default reset features on the front panel ecofriendly switch are disabled.
- The factory default reset feature in the AT-S110 management software is disabled. However, you can still reset the switch via the management software without affecting the switch's configuration.

The factory default reset can be enabled again by using the password that you initially defined when disabling this function.



Caution

Since you define this password as part of the process of disabling this function, Allied Telesis has no knowledge of it. You are responsible for keeping the password in a safe place. If it is lost, Allied Telesis does not have a way to help you recover it.

See "Disabling Factory Default Reset Feature" on page 342 for information about how to disable the factory default reset feature.

Disabling Factory Default Reset Feature

The factory default reset feature allows anyone to reset the switch to the factory default configuration. You may disable this feature. More details are available concerning "Password Protection of Factory Reset" on page 342.

To disable the factory default reset feature, perform the following procedure:

1. From the main menu on the left side of the page, select the **Tools** folder.
The **Tools** folder expands.

2. From the **Tools** folder, select **Reboot**.
The Factory Default Reset/Reboot Page is displayed. See Figure 133 on page 338.
3. Go to the Factory Default Reset section on the upper part of the page. You will find a field called **Factory Default Reset**. This selection allows you to reset the switch configuration to the factory default settings given in “MSTP Overview” on page 327 by using the **Reboot** procedures outlined in “Configure Factory Default Values” on page 340.
4. To disable the factory default reset feature, select **Disable** on the pull-down menu of the **Factory Default Reset** field.
The Factory Default Reset/Reboot Page changes to include fields for entering a password. See Figure 134.



Factory Default Reset

Factory Default Reset: (Maximum length is 12)

New Password:

Confirm Password:

Reboot

Reboot Type:

Note: System will reset in a few seconds after pressing Apply button.

Figure 134. Factory Default Reset/Reboot Page with Password Entry

5. In the **New Password** field, enter a password of up to 12 characters in length. It is case-sensitive. There is not a default password for this field.



Caution

Since you define this password as part of the process of disabling this function, Allied Telesis has no knowledge of it. You are responsible for keeping the password in a safe place. If it is lost, Allied Telesis does not have a way to help you recover it.

6. Re-enter the same password in the **Confirm Password** field.
7. Click **Apply**.
The following message is displayed:

*By clicking on Accept, the Factory Default Reset function will be Disabled on both the switch management software and the physical front panel ecoFriendly button. If you loose this password, ATI cannot recover it for you.
By Clicking on Cancel, the “Factory Default Reset” function will*

remain Enabled on both the switch management software and the physical front panel ecoFriendly button.

- Click **Accept** on the message.
The Factory Default Reset page changes and displays the Factory Default Reset feature as **Disabled**. See Figure 135.

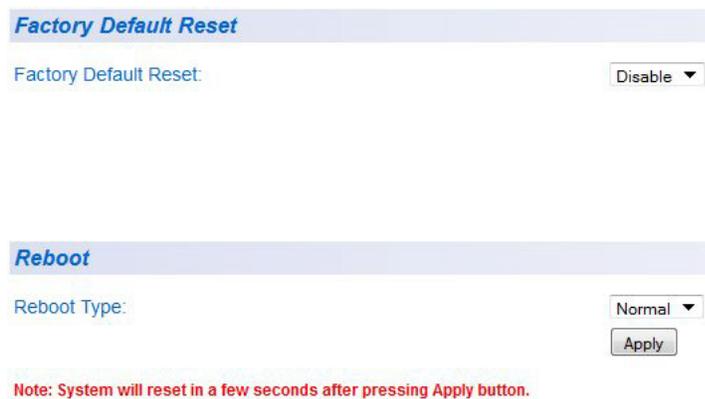


Figure 135. Factory Default Reset Disabled Page

- From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Enabling Factory Default Reset

If the Factory Default Reset feature is disabled and you choose to **Enable** it, perform the following procedure:

- From the main menu on the left side of the page, select the **Tools** folder.
The **Tools** folder expands.
- From the **Tools** folder, select **Reboot**.
The Factory Default Reset/Reboot Page is displayed. See Figure 135.
- Go to the Factory Default Reset section on the upper part of the page.
The **Factory Default Reset** field should be set to **Disable**.

Note

If the **Factory Default Reset** field is already set to **Enable**, you do not need to continue with this procedure.

- To enable the factory default reset feature, select **Enable** on the pull-down menu of the **Factory Default Reset** field.
The Factory Default Reset/Reboot Page changes to include a **Password** field for entering a password. See Figure 136 on page 345.

Factory Default Reset

Factory Default Reset: (Maximum length is 12)

Password:

Note: Enter P/W and click "Apply" to enable "Factory Default Reset" feature

Reboot

Reboot Type:

Note: System will reset in a few seconds after pressing Apply button.

Figure 136. Factory Default Reset/Reboot Page with Password Entry

5. Enter the same password that you defined when you previously set the **Factory Default Reset** field to **Disable**.
6. Click **Apply**.
The initial Factory Default Reset/Reboot Page is displayed with the **Factory Default Reset** field **Enabled**. See Figure 133 on page 338. In the Reboot section, the **Reboot Type** field now includes the options presented in its pull down menu for returning the switch configuration to the factory default values. See "Configure Factory Default Values" on page 340 for more information.
7. From the main menu on the left side of the page, select **Save Configuration to Flash** to permanently save your changes.

Chapter 29

Pinging a Remote System

This chapter provides the procedure for pinging a node on your network from the AT-GS950/10PS switch. This procedure is useful in determining whether an active link exists between the switch and another network device.

Note

The device you are pinging must be a member of the Default VLAN and within the same local area network as your switch. In other words, the port on the switch through which the node is communicating with the switch must be an untagged or tagged member of the Default VLAN.

To ping a network device, perform the following procedure:

1. From the main menu on the left side of the page, select the **Tools** folder.
The **Tools** folder expands.
2. From the **Tools** folder, select **Ping**.
The Ping Test Configuration Page is displayed. See Figure 137.

Ping Test Configuration

Destination IP Address: 192 . 168 . 1 . 7

Timeout Value: 3 Sec.(1-5)

Number of Ping Requests: 10 Times(1-10)

Start

Show Ping Result

Figure 137. Ping Test Configuration Page

3. Configure the following parameters:

Destination IP Address - The IP address of the node you want to ping in the xxx.xxx.xxx.xxx format.

Timeout Value - Specifies the length of time, in seconds, the

switch waits for a response before assuming that a ping has failed.

Number of Ping Requests - Specifies the number of ping requests you want the switch to perform.

4. Click **Start**.
5. To view the ping results, click **Show Ping Results**.
A sample Ping Test Results Page is displayed. See Figure 138.



Figure 138. Ping Test Results Page

The following information is displayed:

Destination IP Address - Indicates the IP address of the unit that receives the ping.

Pass - Indicates the percentage of times the ping passed.

Average Time - Indicates the time, in milliseconds, the ping was received.

6. Click **Back to Ping Test** to return to the Ping Test Configuration Page.

MSTP Overview

This appendix provides background information about the Multiple Spanning Tree Protocol (MSTP) and includes the following sections:

- ❑ “Overview” on page 350
- ❑ “Multiple Spanning Tree Instance (MSTI)” on page 352
- ❑ “General Guidelines” on page 355
- ❑ “VLAN and MSTI Associations” on page 356
- ❑ “Ports in Multiple MSTIs” on page 357
- ❑ “Multiple Spanning Tree Regions” on page 358
- ❑ “Associating VLANs to MSTIs” on page 363
- ❑ “VLANs Across Different Regions” on page 365
- ❑ “Summary of Guidelines” on page 367

Note

To configure the MSTP feature on the AT-GS950/10PS switch, go to “Multiple Spanning Tree Protocol” on page 79 for more information.

Overview

In the AT-GS950/10PS, 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 active protocol stops the loops by placing one or more bridge ports in a blocking state. See Chapter 4, “STP and RSTP” on page 61 for more information.

As explained in “Spanning Tree and VLANs” on page 68, 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. This can result in 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) feature. This spanning tree shares many of the same characteristics as RSTP in that 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.

Note

MSTP and RSTP cannot be enabled at the same time. If RSTP is enabled and you attempt to simultaneously enable MSTP, an error message will be displayed saying, “ERROR: Please disable RSTP before enabling MSTP.” Once RSTP is disabled, you may then enable MSTP.

The following sections describe some of the terms and concepts related to MSTP. If you are not familiar with spanning tree or RSTP, you should first review the Chapter 4, “STP and RSTP” on page 61.

Note

Do not activate MSTP on the AT-GS950/10PS switch without first familiarizing yourself with the following concepts and guidelines. Like STP and RSTP, you must activate this MSTP protocol on a switch and then configure the protocol parameters.

Note

The implementation of MSTP in the management software complies fully with the new IEEE 802.1s standard and should be interoperable with any other vendor's fully compliant 802.1s implementation.

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-GS950 switches. The switch can support up to 31 MSTIs at a time.

Before creating a MSTI, you first enable MSTP. Then you must assign the MSTI a unique number, referred to as the MSTI ID. The range is 1 to 31. After 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.

Resolving VLAN Fragmentation

Following are several examples of how MSTP can be applied.

Figure 139 illustrates two AT-GS950/10PS switches, each containing the two VLANs Sales and Production. The ports of each VLAN on each switch are connected with a direct link using untagged ports. If the switches were running STP or RSTP, one of these two 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 Figure 139, the link between the two ports of the Production VLAN is blocked, resulting in a loss of communications between the two parts of the Production VLAN.

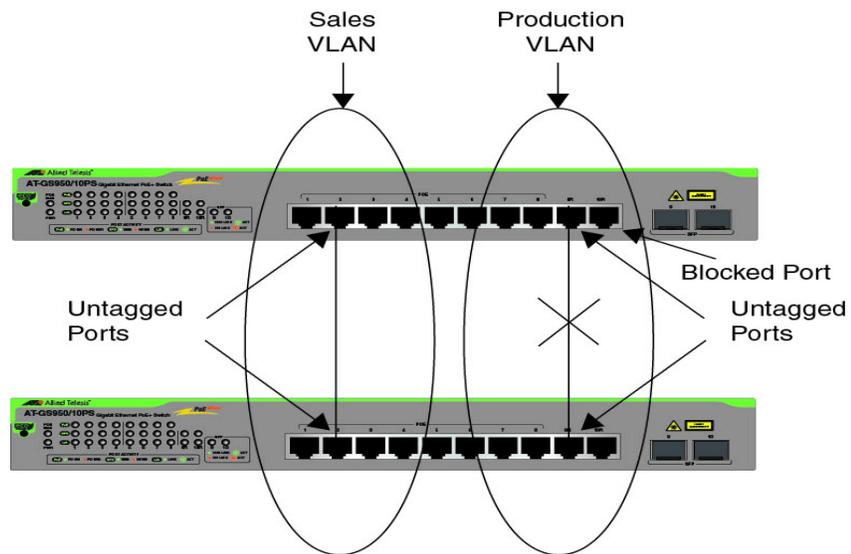


Figure 139. VLAN Fragmentation with STP or RSTP

Figure 140 on page 353 illustrates the same two AT-GS950/10PS 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.

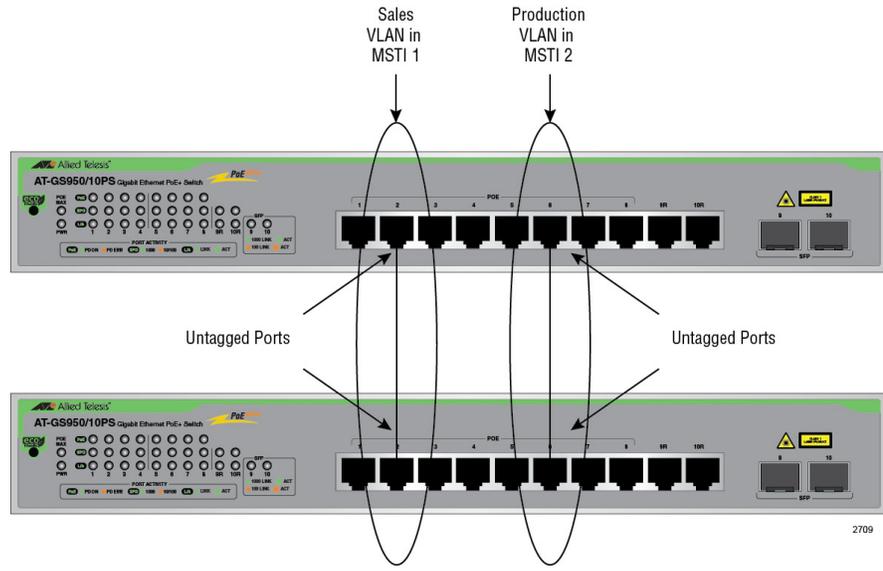


Figure 140. MSTP Example of Two Spanning Tree Instances

Multiple VLANs Assigned to an MSTI

A MSTI can contain more than one VLAN. This is illustrated in Figure 141 on page 354 where there are two AT-GS950/10PS 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.

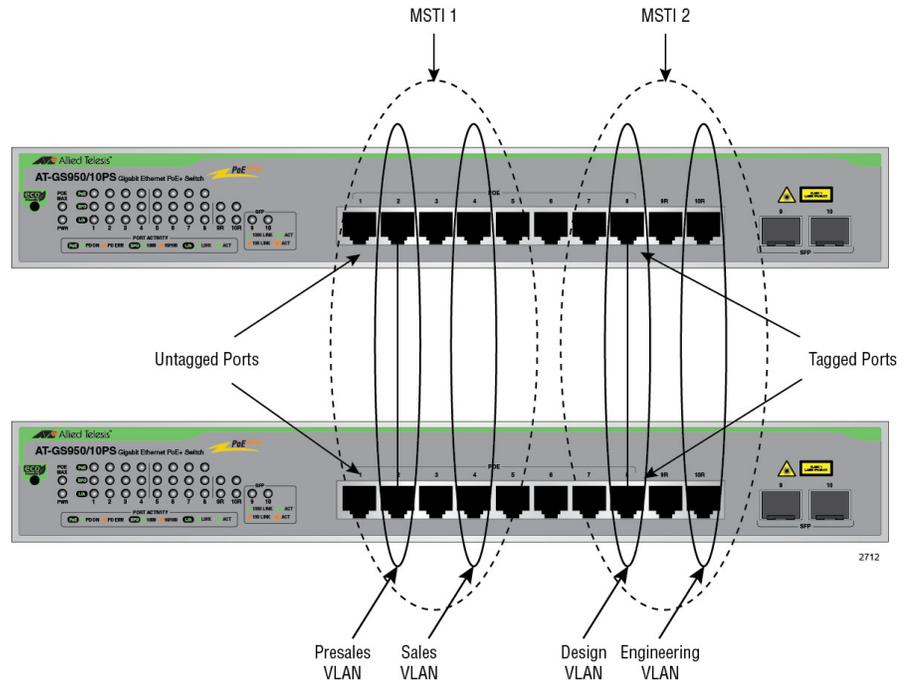


Figure 141. Multiple VLANs in a MSTI

In this example, because 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 141, the tagged link in MSTI 1 is carrying traffic for both the Presales and Sales VLANs between the two switches while the tagged link in MSTI 2 is carrying traffic for the Design and Engineering VLANs.

General Guidelines

Here are the guidelines for MSTIs:

- ❑ The AT-GS950/10PS switch can support up to 31 spanning tree instances, including the CIST.
- ❑ A MSTI can contain any number of VLANs.
- ❑ A VLAN can belong to only one MSTI at a time.
- ❑ A switch port can belong to more than one spanning tree instance at a time by being an untagged and tagged member of VLANs belonging to different MSTI's. This is possible because a port can be in different MSTP states for different MSTI's simultaneously. For example, a port can be in the MSTP blocking state for one MSTI and the forwarding state for another spanning tree instance. For further information, refer to "Ports in Multiple MSTIs," next.

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.

Ports in Multiple MSTIs

A port can be a member of more than one MSTI at a time if it is a tagged member of one or more VLANs assigned to different MSTI's. In this circumstance, a port might have to operate in different spanning tree states simultaneously, depending on the requirements of the MSTIs. For example, a port that belongs to two different VLANs in two different MSTIs might operate in the forwarding state in one MSTI and the blocking state in the other.

A port's MSTI parameter settings are divided into two groups. The first group is referred to as generic parameters. These are set just once on a port and apply to all the MSTI's where the port is a member. One of these parameters is the external path cost, which sets the operating cost of a port connected to a device outside its region. A port, even if it belongs to multiple MSTI's, can have only one external path cost. Another generic parameter designates a port as an edge port or a point-to-point port.

The second group of port parameters can be set differently for each MSTI in which a port is a member. One parameter, the internal path cost, specifies the operating cost of a port when it is connected to a bridge in the same MSTP region. The other parameter in this group sets the port priority, which acts as a tie breaker when two or more ports have equal costs to a regional root bridge.

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:

- ❑ Region name
- ❑ Region revision
- ❑ VLANs
- ❑ VLAN to MSTI ID associations

A *region name* is a name assigned to a region to identify it. You must assign each region exactly the same name for each bridge in that region; 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. Examples are Sales Region and Engineering Region.

The *region revision* is an arbitrary number assigned 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 important that each bridge in a region has the same region revision number. However, it is practically not important that you maintain this number.

The bridges of a particular region must also have the same VLANs. The names of the VLANs and the VIDs must be same on all bridges of a region.

Finally, each of the VLANs across the bridges must be associated to the same MSTI IDs.

If any of the above information is different on two bridges, MSTP does consider the bridges as residing in different regions.

Table 10 illustrates the concept of regions. It shows one MSTP region consisting of two AT-GS950/10PS 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.

Table 10. MSTP Region

Configuration Name: Marketing Region, Revision Level 1	
Switch 1	Switch 2
MSTI ID 1: VLAN: Sales (VID 2) VLAN: Presales (VID 3)	MSTI ID 1: VLAN: Sales (VID 2) VLAN: Presales (VID 3)
MSTI ID 2: VLAN: Accounting (VID 4)	MSTI ID 2: VLAN: Accounting (VID 4)

The AT-GS950/10PS switch determines regional boundaries by examining the MSTP BPDUs received on the ports. A port that receives a MSTP BPDU 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. 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 Bridge 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 select the increment that represents the desired MSTI priority value according to Table 11.

Table 11. Regional Bridge Priority Value Increments

Bridge Priority Selections	
0	32768
4096	36864
8192	40960
12288	45056
16384	49152
20480	53248
24576	57344
28672	61440

MST Region Guidelines

Following are several points to remember about regions.

- A network can contain any number of regions and a region can contain any number of AT-GS950/10PS switches.
- The AT-GS950/10PS 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 Bridge 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 DefaultVLAN 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.

MSTP uses CIST to form the spanning tree of an entire bridged network 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, selects the root bridge for the entire bridged network. If the AT-GS950/10PS 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 the AT-GS950/10PS switch running MSTP receives STP BPDUs, the port only sends STP BPDU packets. If a port receives RSTP BPDUs, the port sends MSTP BPDUs because RSTP can process MSTP BPDUs.

A port connected to a bridge running STP or RSTP is considered to be 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.

Associating VLANs to MSTIs

When you are using Multiple Spanning Tree, Allied Telesis recommends that you assign each VLANs to one of the existing MSTIs on a switch. You should not leave any VLAN unassigned 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 information identifying the Multiple Spanning Tree instance that is associated with the port transmitting the BPDU packet. By default, all ports of the AT-GS950/10PS switch belong to the CIST instance. So the CIST identification is always included in the BPDU. If the port is also a member of a VLAN that has been assigned to a MSTI, that information is included in the BPDU too.

This is illustrated in Figure 142. Port 1 in switch A is a member of the Default VLAN and has been assigned to MSTI ID 10 and port 8 is a member of VLAN 3 assigned to MSTI ID 10. The BPDUs transmitted by port 8 to switch B indicate that the port is a member of both CIST 0 and MSTI 15, while the BPDUs from port 1 indicate the port is a member of the CIST 0 and MSTI 10.

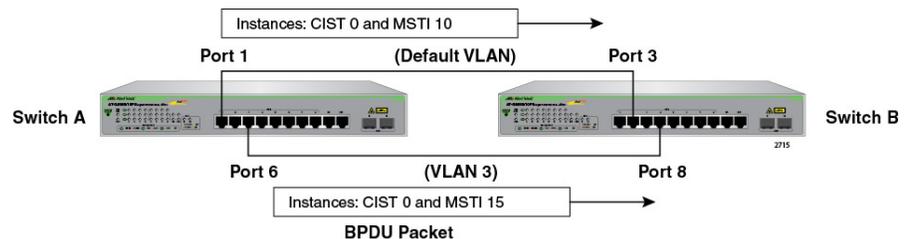


Figure 142. CIST and VLAN Guideline - Example 1

At first glance, it might appear that because 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 because both ports on switch A belong to different MSTIs, switch B determines that no loop exists.

A problem can arise, however, if you assign some VLANs to MSTIs while leaving others assigned only to CIST. Figure 143 on page 364 illustrates the issue. The network is the similar as the previous example. The primary difference is that the VLAN 2 containing port 1 on Switch A has not been assigned to a MSTI, and only belongs to CIST (MSTI ID 0).

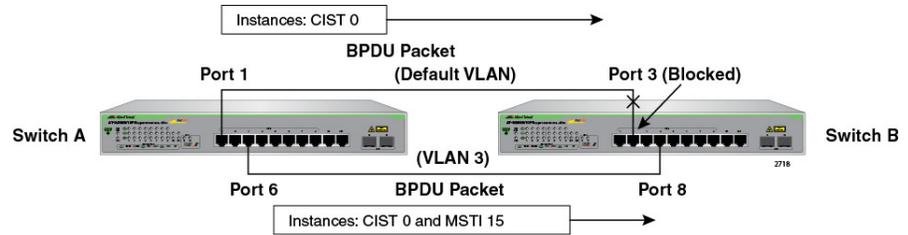


Figure 143. CIST and VLAN Guideline - Example 2

When port 3 on switch B receives a BPDU, the switch notes the port sending the packet belongs only to CIST 0. Therefore, switch B uses CIST 0 in determining whether a loop exists. The result would be that the switch detects a loop because the other port is also receiving BPDU packets from CIST 0. Switch B would block port 3 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 helps to ensure that loop detection is based on MSTI, not CIST.

VLANs Across Different Regions

Special consideration needs to be taken into account when you connect 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 144. The example shows two switches, each residing in a different region. Port 7 in switch A is a boundary port. It is an untagged member of the Accounting VLAN, which has been associated with MSTI 4. Port 6 is a tagged and untagged member of two different VLANs, both associated to MSTI 12.

If both switches were a part of the same region, there would be no problem because the ports reside in different spanning tree instances. However in this example, the switches are part of different regions and MSTIs do not cross regions. Consequently, the result is that spanning tree would determine that a loop exists between the regions, Switch B would block a port and the Accounting VLAN would be disabled between the two regions.

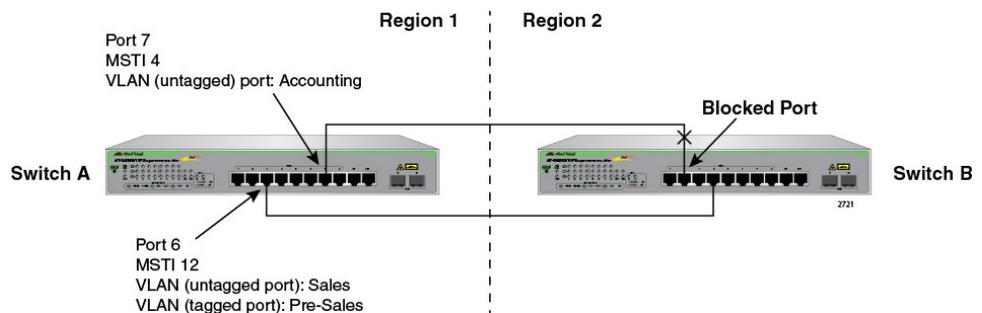


Figure 144. Spanning Regions - Example 1

There are several ways to address this issue. One is to configure only one MSTP region for each subnet in your network. This will eliminate the potential situation of a loop and blocked port(s) between multiple regions.

Another approach is to configure multiple regions in a subnet and group the VLANs that need to span two or more regions into the same MSTI. If other VLANs also exist that do not span multiple regions, they can be assigned to other MSTIs within their respective region.

Here is an example. Assume that you have two regions that contain the following VLANs:

Region 1 VLANs
 Accounting
 Sales
 Pre-Sales
 Marketing
 Product Management
 Project Management

Region 2 VLANs
 Accounting
 Sales
 Pre-Sales
 Technical Support
 Software Engineering
 Hardware Engineering

The two regions share three VLANs: Accounting, Sales, and Presales. You can group these three VLANs into the same MSTI in each region. For instance, for Region 1 you might group the three VLANs in MSTI 12 and in Region 2 you could group them into MSTI 6. After they are grouped, you can connect the VLANs across the regions using a link of untagged/tagged ports as shown in Figure 145.

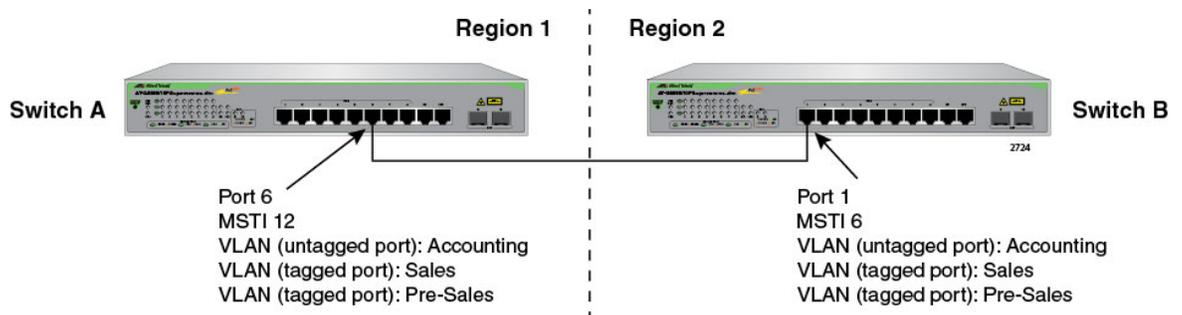


Figure 145. Spanning Regions without Blocking

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 contains a few new ones:

- The AT-GS950/10PS switch can support up to 32 multiple 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 switch port can belong to more than one spanning tree instance at a time. This allows you to assign a port as an untagged and tagged member of VLANs that belong to different MSTIs. What makes this possible is a port's ability to be in different MSTP states for different MSTIs simultaneously. For example, a port can be in the MSTP blocking state for one MSTI and the forwarding state for another spanning tree instance.
- A network can contain any number of regions and a region can contain any number of AT-GS950/10PS switches.
- The AT-GS950/10PS 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 is associated with another MSTI ID. However, in determining network loops, MSTI takes precedence over CIST. (This is explained more in "Associating VLANs to MSTIs" on page 363.)

Appendix B

AT-GS950/10PS Default Parameters

Table 12 lists the factory default settings for the AT-S110 Management software on the AT-GS950/10PS switch. The Parameters reflect the fields found on each web page.

Table 12. AT-S110 Management Software Default Settings

Parameter	AT-GS950/10PS Default Setting	Specifications
System/Management		
System Description	AT-GS950/10PS	-
System Object ID	1.3.6.1.4.1.207.1.4.199	-
System Name	none	0 - 15 characters
System Location	none	0 - 30 characters
System Contact	none	0 - 30 characters
System/IP Setup		
IP Address	192.168.1.1	IPv4 address in xxx.xxx.xxx.xxx hex format; except 127.0.0.1
Subnet Mask	255.255.255.0	IPv4 address in xxx.xxx.xxx.xxx hex format; except 127.0.0.1
Default Gateway Address	0.0.0.0	IPv4 address in xxx.xxx.xxx.xxx hex format; except 127.0.0.1
DHCP Mode (Client)	Disabled	Enabled/Disabled
System/IP Access List		
IP Restriction Status	Disabled	Enabled/Disabled
IP address	none	IPv4 address in xxx.xxx.xxx.xxx hex format; except 127.0.0.1

Table 12. AT-S110 Management Software Default Settings (Continued)

Parameter	AT-GS950/10PS Default Setting	Specifications
IP address entries	10 entries	10 entries
System/Administration		
User Name	manager	1 - 12 characters
Password	friend	1 - 12 characters
System/User Interface		
SNMP Agent	Enabled	Enabled/Disabled
Web Server Status	Enabled	Enabled/Disabled
Web Idle Timeout	10 Minutes	3 - 60 Minutes
System/System Time		
Clock Mode	Local Time	SNTP/Local Time
Date Setting(YYYY:MM:DD)	2009/1/1	-
Time Setting(HH:MM:SS)	1:00:00	-
SNTP Primary Server	0:0:0:0	IPv4 address in xxx.xxx.xxx.xxx format
SNTP Secondary Server	0:0:0:0	IPv4 address in xxx.xxx.xxx.xxx format
SNTP Poll Interval	1 Minute	1 - 60 Minutes
Time Zone	(GMT +09:00)Osaka, Sapporo, Tokyo	GMT -12:00 to GMT +13:00
Daylight Savings Time Status	Disabled	Enabled/Disabled
From (Month:Day:HH:MM)	January:01:00:00	-

Table 12. AT-S110 Management Software Default Settings (Continued)

Parameter	AT-GS950/10PS Default Setting	Specifications
To (Month:Day:HH:MM)	January:01:00:00	-
DST Offset	1 hr	-
System/SSL Settings		
SSL Settings	Disabled	Enabled/Disabled
System/DHCP Auto Configuration Settings		
Auto Configuration State	Disabled	Enabled/Disabled
System/System Log Configuration		
Syslog Status	Disabled	Enabled/Disabled
Time Stamp	Enabled	Enabled/Disabled
Messages Buffered Size	50	1 - 200
Syslog Server IP	0.0.0.0	IPv4 address in xxx.xxx.xxx.xxx format
Facility	local0	local0 - local 7
Logging Level	info	0 - Emergency level 1 - Alert level 2 - Critical level 3 - Error level 4 - Debug level 5 - Notification level 6 - Informational level 7 - Debug
Physical Interface		
Port	All, 1 - 10	-

Table 12. AT-S110 Management Software Default Settings (Continued)

Parameter	AT-GS950/10PS Default Setting	Specifications
Trunk	-	-
Type	1000TX	-
Link Status	Down	Up/Down
Admin Status	Enabled	Enabled/Disabled
Mode	Auto	Auto/10Half/10Full/100Half/100Full/1000Full
Jumbo	Enabled	Enabled/Disabled
Flow Control	Disabled	Enabled/Disabled
EAP Pass	Disabled	Enabled/Disabled
BPDU	Enabled	Enabled/Disabled
Bridge/Spanning Tree/RSTP		
Global RSTP Status	Disabled	Enabled/Disabled
Protocol Version	RSTP	STP - Compatible/RSTP
Bridge Priority	0x8000	0x0000-0xF000, step:0x1000
Bridge Hello Time	2 seconds	1 - 10 seconds
Bridge Maximum Age	20 seconds	6 - 40 seconds
Bridge Forward Delay	15 seconds	4 - 30 seconds
Port STP Status	Disabled	Enabled/Disabled
Port Priority	2	0 - 240, 16 steps
Port Path Cost	2	1 - 200,000,000
Admin/OperEdge	False	True/False
Admin/OperPtoP	False	True/False
Migration	False	True/False
Bridge/Spanning Tree/MSTP		
Global MSTP Status	Disabled	Enabled/Disabled
Maximum MST Instances	31	1 - 31

Table 12. AT-S110 Management Software Default Settings (Continued)

Parameter	AT-GS950/10PS Default Setting	Specifications
Bridge Priority	32768	0 - 61440
Region Name	MAC Address of AT-GS950/10PS switch	-
Region Revision	0	0 - 65535
Dynamic Path Cost Calculation	True	True/False
Bridge Maximum Age	20 Seconds	6 - 40 Seconds
Bridge Forward Delay	15 Seconds	4 - 30 Seconds
Maximum Hop Count	20	6 - 40
Transient Hold Count	3	1 - 10
MSTP Instance ID	none	1 - 31
Mapped VLAN	none	-
Path Cost	20000	1 - 200,000,000
Priority	128	0 - 240, 16 steps
PointToPoint Status	Auto	Auto/ForceTrue/ForceFalse
Edge Port	False	True/False
MSTP Status	Enable	Enable/Disable
Protocol Migration	False	True/False
Hello Time	2	1 - 9 seconds
AutoEdge Status	True	True/False

Table 12. AT-S110 Management Software Default Settings (Continued)

Parameter	AT-GS950/10PS Default Setting	Specifications
Restricted Role	False	True/False
Restricted TCN	False	True/False
Port State	Ignore	Enable/Disable/Ignore
Bridge/Trunk Config/Trunking		
Trunk Status	Disabled	Active/Passive/Manual/Disabled
Bridge/Trunk Config/LACP Group Status		
System Priority	32768	32768
System ID	MAC Address of AT-GS950/10PS switch	-
Port Priority	0	0 - 255
Bridge/Mirroring		
Mirroring Status	Disabled	Enabled/Disabled
Mirroring Port	-	All, 1 - 10
Ingress Mirrored Port	All, 1 - 10	All, 1 - 10
Egress Mirrored Port	All, 1 - 10	All, 1 - 10
Bridge/Loopback Detection		
State	Disabled	Enabled/Disabled
Interval	2 seconds	1 - 32767 seconds
Recover Time	60 seconds	0 or 60 - 1000000
Port	All, 1 - 10	-
Loopback Detection State	Disabled	Enabled/Disabled

Table 12. AT-S110 Management Software Default Settings (Continued)

Parameter	AT-GS950/10PS Default Setting	Specifications
Bridge/Static Unicast		
802.1Q VLAN	-	ID 1 - 4000
Port-Based VLAN Index	-	ID 1 - 52
MAC Address	none	xx:xx:xx:xx:xx:xx hex format
Port Member	-	All, 1 - 10
Bridge/Static Multicast		
802.1Q VLAN	-	ID 1 - 4000
Port-Based VALN Index	-	ID 1 - 52
Group MAC Address	none	01:00:5E:00:01:00 - 01:00:5E:7F:FF:FF
Group Member	-	All, 1 - 10
Static Multicast group number	256 entries (shared with IGMP Snooping)	-
Bridge/IGMP Snooping		
IGMP Snooping Status	Disabled	Enabled/Disabled
IGMP Snooping Age-Out Timer	280 seconds	280 - 420 seconds
Bridge/Storm Control		
Storm Control DLF	Disabled	Enabled/Disabled
Storm Control Broadcast Control Status	Disabled	Enabled/Disabled
Storm Control Multicast Control Status	Disabled	Enabled/Disabled

Table 12. AT-S110 Management Software Default Settings (Continued)

Parameter	AT-GS950/10PS Default Setting	Specifications
Storm Control Threshold	Low	High (2500 pps) Medium (1000 pps) Low (500 pps) @ Packet size = 1518 Bytes
Ingress Rate Limiting Bandwidth	64Kbps X rate limit	where rate limit (1 - 15625)
Ingress Rate Limiting Status	Disabled	Enabled/Disabled
Egress Rate Limiting Bandwidth	64Kbps X rate limit	where rate limit (1 - 15625)
Egress Rate Limiting Status	Disabled	Enabled/Disabled
VLAN Mode	All ports - 802.1Q Tagged VLAN	802.1Q Tagged VLAN or Port-Based VLAN on any port
Tagged VLAN ID	none	2 - 4000
Tagged VLAN Name	none	0 - 32 characters
Tagged Management VLAN	Enabled on DefaultVLAN Disabled on all other VLANs	Always Enabled on Default/VLAN Enabled/Disabled on all other VLANs
Port-Based VLAN Index	none	1 - 52
Port-Based VLAN Name	none	0 - 32 characters
Port-Based Port	Not Member	Group Member or Not Member for each port
Port Settings PVID	1	1 - 4000
Port Settings Acceptable Frame Types	All	All/Tagged/Untagged and Priority Tagged
Port Settings Ingress Filtering	Enabled	Enabled/Disabled
Forwarding Table Learning Mode	IVL	IVL/SVL
Private VLAN Source Port	1	All, 1 - 10

Table 12. AT-S110 Management Software Default Settings (Continued)

Parameter	AT-GS950/10PS Default Setting	Specifications
Private VLAN Forwarding Ports	All, 1 - 10	All, 1 - 10
Bridge/GVRP		
GVRP Status	Disabled	Enabled/Disabled
Dynamic Vlan Status	Enabled	Enabled/Disabled
Restricted VLAN Registration	Disabled	Enabled/Disabled
GarpJoinTime	200 milli-seconds	10 - 1073741810 milli-seconds
GarpLeaveTime	600 milli-seconds	30 - 2147483630 milli-seconds
GarpLeaveAllTime	10000 milli-seconds	40 - 2147483640 milli-seconds
Bridge/QoS		
QoS Status	Disabled	Enabled/Disabled
Queue for Traffic Classes	0	0 - 3
Port Priority	0	0 - 7
DSCP Mapping/ Queue	0	0 - 3
Scheduling Algorithm	Strict Priority	Strict Priority/Weighted RoundRobin
SNMP/View Table		
View Name	ReadWrite	-
Subtree OID	1	-
OID Mask	1	-
View Type	included	included/excluded
SNMP/Group Access Table		
Group Name	ReadOnly/ReadWrite	-
Read View Name	ReadWrite	-
Write View	None	-
Notify View Name	ReadWrite	-

Table 12. AT-S110 Management Software Default Settings (Continued)

Parameter	AT-GS950/10PS Default Setting	Specifications
Security Model	v1	v1/v2c/v3
Security Level	NoAuthNoPriv	NoAuthNoPriv/AuthNoPriv/AuthPriv
SNMP User/Group		
User Name	Enabled	Enabled/Disabled
Group Name	10 entries	-
SNMP Version	v1	v1/v2c/v3
encrypted	not checked	not checked/checked
Auth-Protocol	MD5	MD5/SHA
Password	none	-
Priv-Protocol	DES	DES/none
Password	none	-
SNMP/Community Table		
Community Name	none	-
User Name (View Policy)	none	-
SNMP/Trap Management		
Trap	Enabled	Enabled/Disabled
Host IP Address	0.0.0.0	IPv4 address in xxx.xxx.xxx.xxx format
SNMP Version	v1	v1/v2c/v3NoAuthNoPriv/v3AuthNoPriv/v3AuthPriv
Community Name/ User Name	none	-
Access Control Configuration		
Classifier Index	none	1 - 65535
Source MAC Address	none	xx:xx:xx:xx:xx:xx hex format
Source MAC Mask Length	none	1 - 48

Table 12. AT-S110 Management Software Default Settings (Continued)

Parameter	AT-GS950/10PS Default Setting	Specifications
Destination MAC Address	none	xx:xx:xx:xx:xx:xx hex format
Destination MAC Mask Length	none	1 - 48
VLAN ID	none	0 - 4000
802.1p Priority	none	0 - 7
Ether Type	none	0000 - FFFF (Hex)
DSCP	none	0 - 63
Protocol	none	1 - 255
Source IP Address	none	IPv4 address in xxx.xxx.xxx.xxx hex format;
Source IP Mask Length	none	1 - 32
Destination IP Address	none	IPv4 address in xxx.xxx.xxx.xxx hex format;
Destination IP Mask Length	none	1 - 32
Source Layer 4 Port	none	1 - 65535
Destination Layer 4 Port	none	1 - 65535
Profile Action Index	none	1 - 72
Policed DSCP	none	0 - 63
Policed-CoS	none	0 - 7
In-Profile Action Index	none	1 - 65535
In-Profile Action Deny/Permit	Permit	Permit/Deny
Out-Profile Action Index	none	1 - 65535
Out-Profile Action Deny/Permit	Permit	Permit/Deny
Out-Profile Action Committed Rate	none	64 - 1000000 kbps/unit

Table 12. AT-S110 Management Software Default Settings (Continued)

Parameter	AT-GS950/10PS Default Setting	Specifications
Out-Profile Action Burst Size	16K	16K/32K/64K
Port List Index	none	1 - 65535
Port List	none	Any combination of ports 1 - 10
Authentication Method	RADIUS	RADIUS/Local
Port Number	port 1	ports 1 - 10
NAS ID	Nas1	1 - 16 characters
Authentication Method	RADIUS	RADIUS/Local
Port Number	port 1	ports 1 - 10
Policy Index	none	1 - 65535
Classifier Index	none	1 - 65535
Policy Sequence	none	1 - 64
RMON		
RMON Status	Disable	Disable/Enable
Statistics Index	none	1 - 65535
Statistics Port	none	-
Statistics Owner	none	-
History Index	none	1 - 65535
History Port	none	-
History Buckets Requested	none	1 - 50
History Interval	none	1 - 3600 seconds
History Owner	none	-
Alarms Index	none	1 - 65535
Alarms Interval	none	1 to 2147483647 seconds
Alarms Variable	none	-
Alarms Sample Type	Absolute value	Absolute value/Delta value

Table 12. AT-S110 Management Software Default Settings (Continued)

Parameter	AT-GS950/10PS Default Setting	Specifications
Alarms Rising Threshold	none	1 to 2147483647 seconds
Alarms Falling Threshold	none	1 to 2147483647 seconds
Alarms Rising Event Index	none	1 - 65535
Alarms Falling Event Index	none	1 - 65535
Alarms Owner	none	-
Event Index	Nas1	1 - 65535
Event Description	none	-
Event Type	None	None/Log/SNMP Trap/Log and Trap
Event Community	none	-
Event Owner	none	-
Voice VLAN		
Voice VLAN	Disabled	Enabled/Disabled
VLAN ID	1	-
Aging Time	1 Hour	1 - 120 Hours
COS	0	0 - 7
Auto-Detection	Disabled	Enabled/Disabled
User defined OUI - Description	none	-
User defined OUI - Telephone	none	xx:xx:xx:xx:xx:xx hex format
Security		
Port Access Control NAS ID	Nas1	1 - 23 characters
Port Access Control	Disabled	Disabled/Enabled

Table 12. AT-S110 Management Software Default Settings (Continued)

Parameter	AT-GS950/10PS Default Setting	Specifications
Port Access Control Authentication Method	Local	Local/Radius
Dial-In User Name	none	1 - 23 characters
Dial-In User Password	none	1 - 23 characters
Dial-In User Dynamic VLAN	none	1 - 4000 where 0 means ignore
RADIUS Server IP	0.0.0.0	IPv4 address in xxx.xxx.xxx.xxx hex format;
RADIUS Server Port	1812	1 - 65535
RADIUS Accounting Port	1813	1 - 65535
RADIUS Shared Secret	none	1 - 20 characters
Destination MAC Filter MAC Address	none	Rule: 1. Not support Multicast Mac address (01:xx:xx:xx:xx:xx) 2. Not support VRRP Mac address (00:00:5E:xx:xx:xx) 3. First 4 bit must be zero 4. Address cannot be all zero 5. Cannot add CPU MAC 6. Up to 128 MAC Address entries
DHCP Snooping		
General Setting DHCP Snooping	Disabled	Enabled/Disabled
General Setting Pass Through Option 82	Disabled	Enabled/Disabled
General Setting Verify MAC Address	Enabled	Enabled/Disabled
General Setting Backup Database	Disabled	Enabled/Disabled

Table 12. AT-S110 Management Software Default Settings (Continued)

Parameter	AT-GS950/10PS Default Setting	Specifications
General Setting Database Update Interval	1200	600 - 86400
General Setting DHCP Option 82 Insertion	Disabled	Enabled/Disabled
VLAN Settings VLAN ID	none	1 - 4000
Trusted Interfaces - Trust	Disabled	Enabled/Disabled
Binding Database MAC Address	none	xx:xx:xx:xx:xx:xx hex format
Binding Database IP Address	none	IPv4 address in xxx.xxx.xxx.xxx hex format;
Binding Database VLAN	none	-
Binding Database Port	port 1	All, 1 - 10
Binding Database Type	Dynamic	Dynamic/Static
Binding Database Lease Time	none	10 - 4,294,967,295 seconds
LLDP		
LLDP	Disabled	Enabled/Disabled
Message TX Hold Multiplier	4	2 - 10
Message TX Interval	30	5 - 32768
LLDP Reinit Delay	2	1 - 10
LLDP TX Delay	2	1 - 8192
Global Settings Port State	Enabled	Enabled/Disabled
Statistics Chart		

Table 12. AT-S110 Management Software Default Settings (Continued)

Parameter	AT-GS950/10PS Default Setting	Specifications
Traffic Comparison Statistics	Inbound Octet Rate (Bytes/s)	25 statistics
Traffic Comparison Auto Refresh	5 seconds	5/10/15/30 seconds
Traffic Comparison Color	Green	12 colors
Error Group Port	1	ports 1 - 10
Error Group Auto Refresh	5 seconds	5/10/15/30 seconds
Error Group Color	Green	12 colors
Historical Status Statistics	Inbound Octet Rate (Bytes/s)	12 statistics
Historical Status Auto Refresh	5 seconds	5/10/15/30 seconds
Historical Status Port	1	ports 1 - 10
Historical Status Color	Green	12 colors
Tools		
Firmware Upgrade via HTTP Firmware File	none	-
Firmware Upgrade via TFTP TFTP Server IP	0.0.0.0	IPv4 address in xxx.xxx.xxx.xxx hex format; except 127.0.0.1
Firmware Upgrade via TFTP Image File Name	none	1 - 30 characters (special characters are dependent on OS file name limitation)
Firmware Upgrade via TFTP Retry Count	5	1 - 20

Table 12. AT-S110 Management Software Default Settings (Continued)

Parameter	AT-GS950/10PS Default Setting	Specifications
Configuration File Upload/Download via HTTP Select File	none	-
Configuration File Upload/Download via TFTP TFTP Server IP	0.0.0.0	IPv4 address in xxx.xxx.xxx.xxx hex format; except 127.0.0.1
Configuration File Upload/Download via TFTP Config File Name	none	1 - 39 characters (special characters are dependent on OS file name limitation)
Cable Diagnostics Port	1	ports 1 - 10
LED ECO Mode	Disable	Enable/Disable
Reboot Factory Default Reset	Enable	Enabled/Disabled
Reboot selection	Normal	Normal/Factory Default/Factory Default Except IP
Ping - Destination IP Address	0.0.0.0	IPv4 address in xxx.xxx.xxx.xxx hex format
Ping - Timeout Value	3 seconds	1 - 5 seconds
Ping - Number of Ping Requests	10	1 - 10 times

