AAM1212-51/53

ADSL2+ module of IES-1000

User's Guide

Version 3.53
4/2008
Edition 1

DEFAULT LOGIN	
IP Address	**http://192.168.1.1**
User Name	**admin**
Password	**1234**

www.zyxel.com

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the AAM1212 using the web configurator. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

Related Documentation

- Quick Start Guide
  The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.
- Web Configurator Online Help
  Embedded web help for descriptions of individual screens and supplementary information.
- Command Reference Guide
  The Command Reference Guide explains how to use the Command-Line Interface (CLI) and CLI commands to configure the AAM1212.

It is recommended you use the web configurator to configure the AAM1212.

- Supporting Disk
  Refer to the included CD for support documents.
- ZyXEL Web Site
  Please refer to www.zyxel.com for additional support documentation and product certifications.

User’s Guide Feedback

Help us help you. Send all User’s Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,
ZyXEL Communications Corp.,
6 Innovation Road II,
Science-Based Industrial Park,
Hsinchu, 300, Taiwan.

E-mail: techwriters@zyxel.com.tw

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your AAM1212.

Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

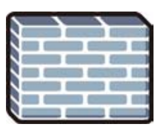
Syntax Conventions

- "AAM1212" refers to the AAM1212-51 for ADSL over POTS (Annex A) and the AAM1212-53 for ADSL over ISDN (Annex B). Differentiation is made where needed.
- The AAM1212 may be referred to as the "AAM1212", the "device" or the "system" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The AAM1212 icon is not an exact representation of your AAM1212.

Table 1 Common Icons

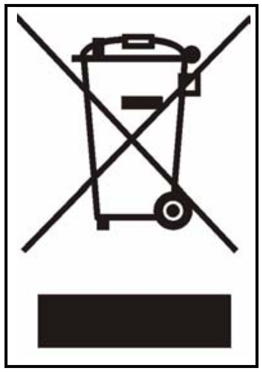
IES-1000 	Computer 	Notebook 
Server 	Telephone 	Wireless Signal 
Switch 	Router 	Internet Cloud 
Firewall 	Modem 	

Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- CAUTION: RISK OF EXPLOSION IF BATTERY (on the motherboard) IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS. Dispose them at the applicable collection point for the recycling of electrical and electronic equipment. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.



Contents Overview

Introduction **39**

Getting to Know the AAM1212 41
Installing and Removing the AAM1212 45
Front Panel 47
Introducing the Web Configurator 59
Initial Configuration 67
Home and Port Statistics Screens 73

Basic Settings **85**

System Information 87
General Setup 91
User Account 93
Switch Setup 97
IP Setup 103
ENET Port Setup 105
xDSL Port Setup 107
xDSL Profiles Setup 125
xDSL Line Data 139

Advanced **147**

VLAN 149
IGMP 157
Static Multicast 167
Multicast VLAN 169
Filtering 175
MAC Filter 177
Spanning Tree Protocol 179
Port Authentication 185
Port Security 189
DHCP Relay 191
DHCP Snoop 195
2684 Routed Mode 199
PPPoA to PPPoE 207
DSCP 213
TLS PVC 215
ACL 219
Downstream Broadcast 225

Syslog 227
Access Control 229
PPPoE Intermediate Agent 237
Maximum MTU Size 241
PVC Upstream Limit 243
OUI Filter 247

Routing Protocol 249

Static Routing 251
Alarm 253

Maintenance 259

Maintenance 261
Diagnostic 265
MAC Table 269
ARP Table 271

CLI Commands 273

Commands 275
Command Examples 313
Alarm Commands 323
DHCP Commands 331
IEEE 802.1Q Tagged VLAN Commands 341
MAC Commands 349
IGMP Commands 355
Packet Filter Commands 371
IP Commands 375
G.Bond Commands 381
Firmware and Configuration File Maintenance 383
SNMP 389
ADSL Commands 393
Virtual Channel Management 429
ACL Commands 455

Troubleshooting and Product Specifications 461

Troubleshooting 463
Product Specifications 473

Appendices and Index 477

Table of Contents

About This User's Guide 3

Document Conventions 4

Safety Warnings 6

Contents Overview 9

Table of Contents 11

List of Figures 27

List of Tables 35

Part I: Introduction 39

Chapter 1
Getting to Know the AAM1212 41

1.1 Overview 41
1.2 Applications 41
1.2.1 MTU Application 41
1.2.2 Curbside Application 42

Chapter 2
Installing and Removing the AAM1212 45

2.1 Installing the AAM1212 in the IES-1000 45
2.2 Removing the AAM1212 from the IES-1000 46

Chapter 3
Front Panel 47

3.1 Front Panel 47
3.1.1 Front Panel Ports 47
3.1.2 LEDs 48
3.1.3 Console Port 48
3.1.4 LAN Port (Ethernet) Connection 49
3.1.5 Notes About MDFs (Main Distribution Frames) 49
3.1.6 Telco-50 Cables 50
3.1.7 Telco-50 Connections 51
3.1.8 ADSL Connections 51

3.1.9 Typical MDF Scenarios 52

Chapter 4
Introducing the Web Configurator 59

4.1 Web Configurator Overview 59
4.2 Screen Privilege Levels 59
4.3 Accessing the Web Configurator 59
4.4 Navigation Panel 61
4.5 Changing Your Password 63
4.6 Saving Your Configuration 64
4.7 Logging Out of the Web Configurator 65

Chapter 5
Initial Configuration 67

5.1 Initial Configuration Overview 67
5.2 Initial Configuration 67

Chapter 6
Home and Port Statistics Screens 73

6.1 Home Screen 73
6.1.1 Ethernet Port Statistics Screen 74
6.1.2 DSL Port Statistics Screen 77
6.1.3 RMON Statistics Screen 79
6.1.4 RMON History Screen 81
6.1.5 RMON History Detail Screen 82

Part II: Basic Settings 85

Chapter 7
System Information 87

Chapter 8
General Setup 91

Chapter 9
User Account 93

9.1 User Account Screen 93
9.2 Authentication Screen 94

Chapter 10
Switch Setup 97

10.1 GARP Timer Setup 97
10.2 Switch Modes 97

10.2.1 Standalone Switch Mode 97
10.2.2 Port Isolation with Standalone Switch Mode Example 98
10.2.3 Daisychain Switch Mode 98
10.2.4 Port Isolation with Daisychain Switch Mode Example 99
10.3 Switch Setup Screen 99

Chapter 11
IP Setup..... 103

Chapter 12
ENET Port Setup 105

Chapter 13
xDSL Port Setup..... 107

13.1 ADSL Standards Overview 107
13.2 Downstream and Upstream 107
13.3 Profiles 108
13.4 Interleave Delay 108
13.4.1 Fast Mode 108
13.5 Configured Versus Actual Rate 108
13.6 Default Settings 109
13.7 xDSL Port Setup Screen 109
13.7.1 xDSL Port Setting Screen 111
13.8 Virtual Channels 115
13.8.1 Super Channel 115
13.8.2 LLC 116
13.8.3 VC Mux 116
13.8.4 Virtual Channel Profile 116
13.9 VC Setup Screen 116
13.10 Priority-based PVCs 120
13.11 PPVC Setup Screen 121
13.11.1 PPVC Setup Members Screen 122

Chapter 14
xDSL Profiles Setup..... 125

14.1 Port Profile Screen 125
14.2 ATM QoS 128
14.3 Traffic Shaping 128
14.3.1 ATM Traffic Classes 128
14.3.2 Traffic Parameters 129
14.4 Upstream Policing 131
14.5 VC Profile Screen 131
14.6 Alarm Profile Screen 133
14.7 IGMP Filtering 135

14.8 IGMP Filter Profile Screen 136

Chapter 15
xDSL Line Data........ 139

15.1 xDSL Line Rate Info Screen 139
15.2 xDSL Performance Screen 141
15.3 xDSL Line Data Screen 143

Part III: Advanced........ 147

Chapter 16
VLAN 149

16.1 Introduction to VLANs 149
16.2 Introduction to IEEE 802.1Q Tagged VLAN 149
16.2.1 Forwarding Tagged and Untagged Frames 150
16.3 VLAN Status Screen 150
16.4 Static VLAN Setting Screen 152
16.5 VLAN Port Setting Screen 153

Chapter 17
IGMP........ 157

17.1 IGMP 157
17.2 IP Multicast Addresses 157
17.2.1 IGMP Snooping 157
17.2.2 IGMP Proxy 158
17.3 IGMP Status Screen 159
17.4 IGMP Bandwidth Screen 160
17.4.1 Bandwidth Port Setup Screen 161
17.5 IGMP Setup Screen 162
17.6 IGMP Filter Setup Screen 164
17.7 IGMP Count Screen 164
17.8 IGMP Port Info Screen 165
17.9 IGMP Port Group Screen 166

Chapter 18
Static Multicast........ 167

18.1 Static Multicast 167
18.2 Static Multicast Screen 167

Chapter 19
Multicast VLAN........ 169

19.1 Multicast VLAN Overview 169
19.2 MVLAN Status Screen 169
19.3 MVLAN Setup Screen 170
19.4 MVLAN Group Screen 172

Chapter 20
Filtering........ 175

20.1 Packet Filter Screen 175

Chapter 21
MAC Filter........ 177

21.1 MAC Filter Introduction 177
21.2 MAC Filter Screen 177

Chapter 22
Spanning Tree Protocol........ 179

22.1 RSTP and STP 179
22.2 Spanning Tree Protocol Status Screen 181
22.3 Spanning Tree Protocol Screen 183

Chapter 23
Port Authentication........ 185

23.1 Introduction to Authentication 185
23.1.1 RADIUS 185
23.1.2 Introduction to Local User Database 185
23.2 RADIUS Screen 186
23.3 802.1x Screen 187

Chapter 24
Port Security........ 189

24.1 Port Security Overview 189
24.2 Port Security Screen 189

Chapter 25
DHCP Relay........ 191

25.1 DHCP Relay 191
25.2 DHCP Relay Agent Information Option (Option 82) 191
25.2.1 DHCP Relay Agent Circuit ID and Remote ID Sub-option Formats 191
25.3 DHCP Relay Screen 192

Chapter 26
DHCP Snoop........ 195

26.1 DHCP Snoop Overview 195

26.2 DHCP Snoop Screen 195
26.3 DHCP Snoop Status Screen 196
26.4 DHCP Counter Screen 197

Chapter 27
2684 Routed Mode 199

27.1 2684 Routed Mode 199
27.1.1 2684 Routed Mode Example 199
27.2 2684 Routed PVC Screen 201
27.3 2684 Routed Domain Screen 202
27.4 RPVC Arp Proxy Screen 204
27.5 2684 Routed Gateway Screen 205

Chapter 28
PPPoA to PPPoE 207

28.1 PPPoA to PPPoE Overview 207
28.2 PPPoA to PPPoE Screen 207
28.3 PPPoA to PPPoE Status Screen 210

Chapter 29
DSCP 213

29.1 DSCP Overview 213
29.2 DSCP Setup Screen 213
29.3 DSCP Map Screen 214

Chapter 30
TLS PVC 215

30.1 Transparent LAN Service (TLS) Overview 215
30.1.1 TLS Network Example 215
30.2 TLS PVC Screen 216

Chapter 31
ACL 219

31.1 Access Control Logic (ACL) Overview 219
31.1.1 ACL Profile Rules 219
31.1.2 ACL Profile Actions 220
31.2 ACL Setup Screen 220
31.3 ACL Profile Setup Screen 222
31.4 ACL Profile Map Screen 224

Chapter 32
Downstream Broadcast 225

32.1 Downstream Broadcast 225

32.2 Downstream Broadcast Screen 225

Chapter 33
Syslog 227

33.1 Syslog 227
33.2 SysLog Screen 227

Chapter 34
Access Control 229

34.1 Access Control Screen 229
34.2 Access Control Overview 229
34.3 SNMP 229
34.3.1 Supported MIBs 231
34.3.2 SNMP Traps 231
34.4 SNMP Screen 233
34.5 Service Access Control Screen 233
34.6 Remote Management Screen 234

Chapter 35
PPPoE Intermediate Agent 237

35.1 PPPoE Intermediate Agent Tag Format 237
35.2 PPPoE Intermediate Agent Screen 238

Chapter 36
Maximum MTU Size 241

36.1 Maximum MTU Size Screen 241

Chapter 37
PVC Upstream Limit 243

37.1 PVC Upstream Limit and Upstream VC Profiles 243
37.2 PVC Upstream Limit Screen 243

Chapter 38
OUI Filter 247

Part IV: Routing Protocol 249

Chapter 39
Static Routing 251

Chapter 40
Alarm 253

40.1 Alarm 253

40.2 Alarm Status Screen 253
40.3 Alarm Descriptions 254
40.4 Alarm Event Setup Screen 255
40.4.1 Edit Alarm Event Setup Screen 257
40.5 Alarm Port Setup Screen 258

Part V: Maintenance 259

Chapter 41
Maintenance 261

41.1 Maintenance Screen 261
41.2 Firmware Upgrade Screen 261
41.3 Restore Configuration Screen 262
41.4 Backing Up a Configuration File 262
41.5 Load Factory Defaults 263
41.6 Reboot System 263
41.7 Command Line FTP 264

Chapter 42
Diagnostic 265

42.1 Diagnostic Screen 265

Chapter 43
MAC Table 269

43.1 Introduction to MAC Table 269
43.2 MAC Table Screen 270

Chapter 44
ARP Table 271

44.1 Introduction to ARP Table 271
44.1.1 How ARP Works 271
44.2 ARP Table Screen 271

Part VI: CLI Commands 273

Chapter 45
Commands 275

45.1 Command Line Interface Overview 275
45.2 Command Privilege Levels 275
45.3 Saving Your Configuration 276

45.4 ADSL Command Input Values 276
45.5 Commands 276

Chapter 46
Command Examples........ 313

46.1 Command Examples Overview 313
46.2 Sys Commands 313
46.2.1 Log Show Command 313
46.3 Log Format 314
46.3.1 Log Messages 314
46.3.2 Log Clear Command 316
46.3.3 Info Show Command 316
46.4 Isolation Commands 317
46.4.1 Isolation Show Command 317
46.4.2 Isolation Enable Command 317
46.4.3 Isolation Disable Command 318
46.5 switch ouifilter Commands 318
46.5.1 switch ouifilter disable Command 318
46.5.2 switch ouifilter enable Command 318
46.5.3 switch ouifilter mode Command 318
46.5.4 switch ouifilter set Command 319
46.5.5 switch ouifilter show Command 319
46.6 Statistics Monitor Command 319
46.7 Statistics Port Command 320

Chapter 47
Alarm Commands 323

47.1 Alarm Commands 323
47.2 General Alarm Command Parameters 323
47.3 Alarm Show Command 323
47.4 Alarm Port Show Command 324
47.5 Alarm Port Set Command 325
47.6 Alarm Tablelist Command 325
47.7 Log Format 326
47.8 Alarm History Show Command 327
47.9 Alarm History Clear Command 328
47.10 Alarm XEdit Command 328
47.11 Alarm Cutoff Command 329
47.12 Alarm Clear Command 329

Chapter 48
DHCP Commands 331

48.1 DHCP Relay Commands 331

48.1.1 Show Command 331
48.1.2 Enable Command 332
48.1.3 Disable Command 332
48.1.4 Server Set Command 332
48.1.5 Server Delete Command 332
48.1.6 Server Active Command 333
48.1.7 Relaymode Command 333
48.2 DHCP Relay Option 82 (Agent Information) Sub-option 1 (Circuit ID) 334
48.2.1 Option 82 Sub-option 1 Enable Command 334
48.2.2 Option 82 Sub-option 1 Disable Command 334
48.2.3 Option 82 Sub-option 1 Set Command 334
48.3 DHCP Relay Option 82 (Agent Information) Sub-option 2 (Remote ID) 334
48.3.1 Option 82 Sub-option 2 Enable Command 335
48.3.2 Option 82 Sub-option 2 Disable Command 335
48.3.3 Option 82 Sub-option 2 Set Command 335
48.4 DHCP Snoop Commands 335
48.4.1 DHCP Snoop Enable Command 336
48.4.2 DHCP Snoop Disable Command 336
48.4.3 DHCP Snoop Flush Command 336
48.4.4 DHCP Snoop Show Command 337
48.4.5 DHCP Counter Statistics Command 337
48.4.6 DHCP Snoop Statistics Command 338

Chapter 49
IEEE 802.1Q Tagged VLAN Commands 341

49.1 Introduction to VLANs 341
49.2 IEEE 802.1Q Tagging Types 341
49.3 Filtering Databases 341
49.3.1 Static Entries (SVLAN Table) 341
49.4 IEEE VLAN1Q Tagged VLAN Configuration Commands 342
49.4.1 VLAN Port Show Command 342
49.4.2 VLAN PVID Command 342
49.4.3 VLAN Priority Command 343
49.4.4 VLAN Set Command 343
49.4.5 VLAN Frame Type Command 345
49.4.6 VLAN CPU Show Command 345
49.4.7 VLAN CPU Set Command 346
49.4.8 Configuring Management VLAN Example 346
49.4.9 VLAN Delete Command 347
49.5 VLAN Enable 347
49.6 VLAN Disable 347
49.6.1 VLAN Show Command 348

Chapter 50
MAC Commands 349

50.1 MAC Commands Overview 349
50.2 MAC Filter Commands 349
50.2.1 MAC Filter Show Command 349
50.2.2 MAC Filter Enable Command 350
50.2.3 MAC Filter Disable Command 350
50.2.4 MAC Filter Mode Command 350
50.2.5 MAC Filter Set Command 351
50.2.6 MAC Filter Delete Command 351
50.3 MAC Count Commands 352
50.3.1 MAC Count Show Command 352
50.3.2 MAC Count Enable Command 353
50.3.3 MAC Count Disable Command 353
50.3.4 MAC Count Set Command 354

Chapter 51
IGMP Commands 355

51.1 Multicast Overview 355
51.2 IGMP Snoop Commands 355
51.2.1 IGMP Snoop Show Command 355
51.2.2 IGMP Snoop Enable Command 355
51.2.3 IGMP Snoop Disable Command 356
51.3 IGMP Filter Commands 356
51.3.1 IGMP Filter Show Command 356
51.3.2 IGMP Filter Set Command 357
51.3.3 IGMP Filter Profile Set Command 357
51.3.4 IGMP Filter Profile Delete Command 358
51.3.5 IGMP Filter Profile Show Command 358
51.4 IGMP Bandwidth Commands 359
51.4.1 IGMP Bandwidth Default Command 359
51.4.2 IGMP Bandwidth Set Command 360
51.4.3 IGMP Bandwidth Delete Command 360
51.5 IGMP Bandwidth Port Commands 360
51.5.1 IGMP Bandwidth Port Disable Command 360
51.5.2 IGMP Bandwidth Port Enable Command 361
51.5.3 IGMP Bandwidth Port Set Command 361
51.5.4 IGMP Bandwidth Port Show Command 361
51.6 IGMP Count Limit Commands 362
51.6.1 IGMP Count Disable Command 362
51.6.2 IGMP Count Enable Command 363
51.6.3 IGMP Count Set Command 363
51.6.4 IGMP Count Show Command 364

51.7 IGMP Snoop Statistics Commands 364
51.7.1 IGMP Snoop Info Statistics Command 364
51.7.2 IGMP Group Statistics Command 365
51.7.3 IGMP Port Info Statistics Command 365
51.7.4 IGMP Port Group Statistics Command 366
51.8 Multicast VLAN Commands 366
51.8.1 Multicast VLAN Set Command 366
51.8.2 Multicast VLAN Delete Command 367
51.8.3 Multicast VLAN Disable Command 367
51.8.4 Multicast VLAN Enable Command 368
51.8.5 Multicast VLAN Show Command 368
51.8.6 Multicast VLAN Group Set Command 369
51.8.7 Multicast VLAN Group Delete Command 369
51.8.8 Multicast VLAN Group Show Command 369

Chapter 52
Packet Filter Commands 371

52.1 Packet Filter Commands 371
52.1.1 Packet Filter Show Command 371
52.1.2 Packet Filter Set Command 372
52.1.3 Packet Filter PPPoE Only Command 373

Chapter 53
IP Commands 375

53.1 IP Commands Introduction 375
53.2 IP Settings and Default Gateway 375
53.3 General IP Commands 376
53.3.1 Show 376
53.3.2 Ping Command 376
53.3.3 Route Set Command 377
53.3.4 Route Delete Command 377
53.3.5 Route Show Command 377
53.3.6 ARP Show Command 378
53.3.7 ARP Flush Command 378
53.4 Statistics IP Command 378

Chapter 54
G.Bond Commands 381

54.1 G.bond Commands 381
54.1.1 adsl gbond set Command 381
54.1.2 adsl gbond show Command 381
54.1.3 port gbond delete Command 382

Chapter 55
Firmware and Configuration File Maintenance 383

55.1 Firmware and Configuration File Maintenance Overview 383
55.2 Filename Conventions 383
55.3 Editable Configuration File 384
55.3.1 Editable Configuration File Backup 384
55.3.2 Edit Configuration File 385
55.3.3 Editable Configuration File Upload 386
55.4 Firmware File Upgrade 387

Chapter 56
SNMP 389

56.1 SNMP Commands 389
56.1.1 Get Community Command 389
56.1.2 Set Community Command 389
56.1.3 Trusted Host Set Command 390
56.1.4 Trap Community Command 390
56.1.5 Trap Destination Set Command 390
56.1.6 Show SNMP Settings Command 391

Chapter 57
ADSL Commands 393

57.1 DSL Port Commands 393
57.1.1 DSL Port Show Command 393
57.1.2 DSL Port Enable Command 393
57.1.3 DSL Port Disable Command 394
57.1.4 DSL Port Profile Show Command 394
57.1.5 DSL Port Profile Set Command 395
57.1.6 DSL Port Profile Delete Command 397
57.1.7 DSL Port Profile Map Command 397
57.1.8 DSL Port Name Command 398
57.1.9 DSL Port Tel Command 399
57.1.10 DSL Port Loopback Command 399
57.1.11 DSL Port Upstream PSD Command 400
57.1.12 DSL Port Downstream PSD Command 401
57.1.13 DSL Port Upstream Carrier Command 401
57.1.14 DSL Port Downstream Carrier0 Command 402
57.1.15 DSL Port Downstream Carrier1 Command 403
57.1.16 PMM Parameters Command 404
57.1.17 Impulse Noise Protection Command 406
57.1.18 Annex L Enable Command 406
57.1.19 Annex L Disable Command 407
57.1.20 Annex M Enable Command 407

57.1.21 Annex M Disable Command 408
57.1.22 Annex I Enable Command 408
57.1.23 Annex I Disable Command 408
57.2 DSL Port Statistics Commands 409
57.2.1 DSL Port Show Command 409
57.2.2 Linedata Command 409
57.2.3 Lineinfo Command 411
57.2.4 Lineperf Command 412
57.2.5 15 Minute Performance Command 413
57.2.6 1 Day Performance Command 415
57.2.7 Line Diagnostics Set Command 415
57.2.8 Line Diagnostics Get Command 416
57.2.9 Line Diagnostics Get 992.3 Command 418
57.2.10 SELT Diagnostic Set Command 420
57.2.11 SELT Diagnostic Get Command 421
57.2.12 Tone Diagnostics 992.3 Command 421
57.3 Alarm Profile Commands 423
57.3.1 Alarm Profile Show Command 423
57.3.2 Alarm Profile Set Command 424
57.3.3 Alarm Profile Delete Command 426
57.3.4 Alarm Profile Map Command 426
57.3.5 Alarm Profile Showmap Command 426

Chapter 58
Virtual Channel Management........ 429

58.1 Virtual Channel Management Overview 429
58.2 Virtual Channel Profile Commands 429
58.2.1 Show Virtual Channel Profile Command 429
58.2.2 Set Virtual Channel Profile Command 429
58.2.3 Delete Virtual Channel Profile Command 431
58.3 PVC Channels 431
58.3.1 PVC Show Command 432
58.3.2 PVC Set Command 432
58.3.3 PVC Delete Command 433
58.4 Priority-based PVCs 433
58.4.1 PPVC Set Command 434
58.4.2 PPVC Member Set Command 434
58.5 PPVC Member Delete Command 435
58.6 PPVC Member Show Command 436
58.6.1 PPVC Show Command 437
58.6.2 PPVC Delete Command 437
58.7 2684 Routed Mode Commands 438
58.7.1 2684 Routed Mode Example 439

58.7.2 RPVC Gateway Set Command 440
58.7.3 RPVC Gateway Show Command 440
58.7.4 RPVC Gateway Delete Command 441
58.7.5 RPVC Set Command 441
58.7.6 RPVC Show Command 442
58.7.7 RPVC Delete Command 443
58.7.8 RPVC Route Set Command 444
58.7.9 RPVC Route Show Command 444
58.7.10 RPVC Route Delete Command 445
58.7.11 RPVC ARP Agingtime Set Command 446
58.7.12 RPVC ARP Agingtime Show Command 446
58.7.13 RPVC ARP Show Command 447
58.7.14 RPVC ARP Flush Command 447
58.8 PPPoA to PPPoE (PAE) Commands 447
58.8.1 PAE PVC Delete Command 447
58.8.2 PAE PVC Set Command 448
58.8.3 PAE PVC Show Command 449
58.8.4 PAE PVC Session Command 449
58.8.5 PAE PVC Counter Command 450
58.9 Transparent LAN Service (TLS) Commands 451
58.9.1 TLS PVC Delete Command 451
58.9.2 TLS PVC Set Command 452
58.9.3 TLS PVC Show Command 452

Chapter 59
ACL Commands 455

59.1 ACL Profile Commands 455
59.1.1 ACL Profile Set Command 455
59.1.2 ACL Profile Delete Command 457
59.1.3 ACL Profile Show Map Command 457
59.1.4 ACL Profile Show Command 457
59.2 ACL Assignment Commands 458
59.2.1 ACL Assignment Set Command 458
59.2.2 ACL Assignment Delete Command 459
59.2.3 ACL Assignment Show Command 459

Part VII: Troubleshooting and Product Specifications 461

Chapter 60
Troubleshooting 463

60.1 The SYS LED Does Not Turn On 463

60.2 The ALM LED Is On 463
60.3 LAN Port LEDs Do Not Turn On 464
60.4 LAN Port Data Transmission 464
60.5 DSL Data Transmission 465
60.6 There Is No Voice on a DSL Connection 465
60.7 Testing Wiring 465
60.8 Local Server 467
60.9 Data Rate 468
60.10 Configured Settings 468
60.11 Password 468
60.12 System Lockout 468
60.13 SNMP 469
60.14 Telnet 469
60.15 Resetting the Defaults 469
60.15.1 Resetting the Defaults Via Command 470
60.15.2 Uploading the Default Configuration File 470
60.16 Recovering the Firmware 471

Chapter 61
Product Specifications 473

Part VIII: Appendices and Index 477

Appendix A Legal Information 479

Appendix B Customer Support 483

Index 489

List of Figures

Figure 1 MTU Application 42
Figure 2 Curbside Application 42
Figure 3 Installation: Push the AAM1212 into the IES-1000 45
Figure 4 Installation: Tighten Module Screws 46
Figure 5 Removal: Loosen Module Screws 46
Figure 6 Removal: Removing the AAM1212 from the IES-1000 46
Figure 7 Front Panel 47
Figure 8 Stacking Multiple IES-1000 Units 49
Figure 9 MDF Wiring 50
Figure 10 Telco-50 Cable with RJ-11 Connectors 51
Figure 11 Installation Overview 52
Figure 12 Installation Scenario A 53
Figure 13 One MDF for End-user and CO Connections 54
Figure 14 Installation Scenario B 55
Figure 15 Two Separate MDFs for End-user and CO Connections 56
Figure 16 Installation Scenario C 57
Figure 17 Login 60
Figure 18 Home 60
Figure 19 User Account 64
Figure 20 User Account 64
Figure 21 Logout 65
Figure 22 IP Setup 67
Figure 23 xDSL Port Setup 68
Figure 24 VC Setup 69
Figure 25 VC Setup, Delete 69
Figure 26 Select Ports 69
Figure 27 VC Setup 70
Figure 28 VC Setup 70
Figure 29 Select Ports 70
Figure 30 VC Setup 71
Figure 31 Config Save 71
Figure 32 Config Save, Save Successful 71
Figure 33 Home 73
Figure 34 Port Statistics (Ethernet) 75
Figure 35 Port Statistics (DSL) 78
Figure 36 Port Statistics (RMON) 80
Figure 37 Port Statistics (RMON History)) 82
Figure 38 Port Statistics (RMON History Detail)) 83

Figure 39 System Info 87
Figure 40 General Setup 91
Figure 41 User Account 93
Figure 42 Authentication 95
Figure 43 Port Isolation with Standalone Switch Mode Example 98
Figure 44 Port Isolation with Daisychain Switch Mode Example 99
Figure 45 Switch Setup 100
Figure 46 IP Setup 103
Figure 47 ENET Port Setup 105
Figure 48 xDSL Port Setup 109
Figure 49 Select Ports 110
Figure 50 xDSL Port Setting 112
Figure 51 VC Setup 117
Figure 52 Basic Setting, xDSL Port Setup, VC Setup, Delete 119
Figure 53 Select Ports 119
Figure 54 Select Ports 120
Figure 55 PPVC Setup 121
Figure 56 PPVC Setup, Edit 123
Figure 57 Port Profile 125
Figure 58 PCR, SCR and MBS in Traffic Shaping 130
Figure 59 TAT, CDVT and BT in Traffic Shaping 130
Figure 60 VC Profile 132
Figure 61 Alarm Profile 134
Figure 62 IGMP Filter Profile 136
Figure 63 xDSL Line Rate Info 139
Figure 64 xDSL Performance 141
Figure 65 xDSL Line Data 144
Figure 66 VLAN Status 151
Figure 67 Static VLAN Setting 152
Figure 68 VLAN Port Setting 154
Figure 69 Select Ports 155
Figure 70 IGMP Proxy Network Example 158
Figure 71 IGMP (Status) 159
Figure 72 IGMP Bandwidth 160
Figure 73 Bandwidth Port Setup 162
Figure 74 IGMP Setup 163
Figure 75 IGMP Count 164
Figure 76 IGMP Port Info 165
Figure 77 IGMP Port Group 166
Figure 78 Static Multicast 167
Figure 79 MVLAN Status 169
Figure 80 MVLAN Setup 171
Figure 81 MVLAN Group 172

Figure 82 Packet Filter 175
Figure 83 MAC Filter 177
Figure 84 STP Root Ports and Designated Ports 180
Figure 85 Spanning Tree Protocol Status 181
Figure 86 Spanning Tree Protocol 183
Figure 87 RADIUS Server 185
Figure 88 RADIUS 186
Figure 89 802.1x 187
Figure 90 Port Security 189
Figure 91 Select Ports 190
Figure 92 DHCP Relay Agent Circuit ID Sub-option Format 192
Figure 93 DHCP Relay Agent Remote ID Sub-option Format 192
Figure 94 DHCP Relay 192
Figure 95 DHCP Snoop 195
Figure 96 DHCP Snoop Status 196
Figure 97 DHCP Counter 197
Figure 98 2684 Routed Mode Example 200
Figure 99 2684 Routed PVC 201
Figure 100 2684 Routed Domain 203
Figure 101 RPVC Arp Proxy 204
Figure 102 2684 Routed Gateway 205
Figure 103 Mixed PPPoA-to-PPPoE Broadband Network Example 207
Figure 104 PPPoA to PPPoE 208
Figure 105 PPPoA to PPPoE Status 210
Figure 106 DSCP Setup 213
Figure 107 DSCP Map 214
Figure 108 Transparent LAN Service Network Example 216
Figure 109 TLS PVC 217
Figure 110 ACL Setup 221
Figure 111 ACL Profile Setup 222
Figure 112 ACL Profile Map 224
Figure 113 Downstream Broadcast 225
Figure 114 SysLog 227
Figure 115 Access Control 229
Figure 116 SNMP Management Model 230
Figure 117 SNMP 233
Figure 118 Service Access Control 234
Figure 119 Remote Management (Secured Client Setup) 235
Figure 120 PPPoE Intermediate Agent 239
Figure 121 Maximum MTU 241
Figure 122 PVC Upstream Limit 244
Figure 123 OUI Filter 247
Figure 124 Static Routing 251

Figure 125 Alarm Status 253
Figure 126 Alarm Event Setup 256
Figure 127 Alarm Event Setup Edit 257
Figure 128 Alarm Port Setup 258
Figure 129 Maintenance 261
Figure 130 Firmware Upgrade 261
Figure 131 Restore Configuration 262
Figure 132 Restore Default Configuration 263
Figure 133 Restore Factory Default Settings, Reboot 263
Figure 134 Reboot System 264
Figure 135 Diagnostic 265
Figure 136 MAC Table Filtering Flowchart 269
Figure 137 MAC Table 270
Figure 138 ARP Table 272
Figure 139 Log Show Command Example 313
Figure 140 Info Show Example 317
Figure 141 Isolation Show Example 317
Figure 142 Statistics Monitor Command Example 320
Figure 143 Statistics Port Command Example 321
Figure 144 Alarm Show Command Example 324
Figure 145 Alarm Port Show Command Example 325
Figure 146 Alarm Port Set Command Example 325
Figure 147 Alarm Tablelist Command Example 326
Figure 148 Alarm History Show Command Example 327
Figure 149 Alarm History Clear Command Example 328
Figure 150 Alarm Xedit Command Example 329
Figure 151 Show Command Example 331
Figure 152 DHCP Snoop Enable Command Example 336
Figure 153 DHCP Snoop Show Command Example 337
Figure 154 DHCP Counter Statistics Command Example 338
Figure 155 DHCP Snoop Statistics Command Example 338
Figure 156 VLAN Port Show Command Example 342
Figure 157 VLAN PVID Command Example 343
Figure 158 VLAN CPU Set Command Example 343
Figure 159 Modifying the Static VLAN Example 344
Figure 160 VLAN Frame Type Command Example 345
Figure 161 VLAN CPU Set Command Example 346
Figure 162 VLAN CPU Set Command Example 346
Figure 163 CPU VLAN Configuration and Activation Example 346
Figure 164 Deleting Default VLAN Example 347
Figure 165 VLAN Delete Command Example 347
Figure 166 VLAN Show Command Example 348
Figure 167 MAC Filter Show Command Example 349

Figure 168 MAC Filter Enable Command Example 350
Figure 169 MAC Filter Disable Command Example 350
Figure 170 MAC Filter Mode Command Example 351
Figure 171 MAC Filter Set Command Example 351
Figure 172 MAC Filter Delete Command Example 352
Figure 173 MAC Count Show Command Example 352
Figure 174 MAC Count Enable Command Example 353
Figure 175 MAC Count Disable Command Example 353
Figure 176 MAC Count Set Command Example 354
Figure 177 IGMP Snoop Show Command Example 355
Figure 178 IGMP Snoop Enable Command Example 356
Figure 179 IGMP Snoop Disable Command Example 356
Figure 180 IGMP Filter Show Command Example 357
Figure 181 IGMP Filter Set Command Example 357
Figure 182 IGMP Filter Profile Set Command Example 358
Figure 183 IGMP Filter Profile Delete Command Example 358
Figure 184 IGMP Filter Show Command Example 359
Figure 185 IGMP Bandwidth Port Show Command Example 362
Figure 186 IGMP Count Disable Command Example 363
Figure 187 IGMP Count Enable Command Example 363
Figure 188 IGMP Count Set Command Example 364
Figure 189 IGMP Count Show Command Example 364
Figure 190 IGMP Snoop Info Statistics Command Example 365
Figure 191 IGMP Group Statistics Command Example 365
Figure 192 IGMP Port Info Statistics Command Example 366
Figure 193 IGMP Port Group Statistics Command Example 366
Figure 194 Multicast VLAN Disable Command Example 368
Figure 195 Multicast VLAN Show Command Example 368
Figure 196 Multicast VLAN Group Set Command Example 369
Figure 197 Packet Filter Show Command Example 371
Figure 198 Packet Filter Set Command Example 373
Figure 199 Packet Filter PPPoE Only Command Example 373
Figure 200 IP Settings and Default Gateway Address Commands 375
Figure 201 IP Settings and Default Gateway Address Command Example 376
Figure 202 Route Show Command Example 378
Figure 203 ARP Show Command Example 378
Figure 204 Statistics IP Command Example 379
Figure 205 FTP Put Configuration File Example 383
Figure 206 FTP Get Configuration File Example 383
Figure 207 Example: Use an FTP Client to Connect to the AAM1212 384
Figure 208 Example: Enter the Management Password 385
Figure 209 Example: Get the Configuration File config-0 385
Figure 210 Example: Close FTP Client 385

Figure 211 Configuration File Example 386
Figure 212 Example: Use an FTP Client to Connect to the AAM1212 386
Figure 213 Example: Enter the Management Password 387
Figure 214 Example: Upload the Configuration File config-0 387
Figure 215 Example: Close FTP Client 387
Figure 216 Example: Use an FTP Client to Connect to the AAM1212 387
Figure 217 Example: Enter the Management Password 387
Figure 218 Example: Transfer the Firmware File 388
Figure 219 Example: Close FTP Client 388
Figure 220 DSL Port Show Command Example 393
Figure 221 DSL Profile Show Command Example 395
Figure 222 DSL Port Profile Set Command Example 1 397
Figure 223 DSL Port Profile Set Command Example 2 397
Figure 224 DSL Port Profile Delete Command Example 397
Figure 225 DSL Port Profile Delete Command Example 398
Figure 226 DSL Port Name Command Example 399
Figure 227 DSL Port Tel Command Example 399
Figure 228 DSL Port Loopback Command Example 400
Figure 229 DSL Port Upstream PSD Command Example 400
Figure 230 DSL Port Downstream PSD Command Example 401
Figure 231 DSL Port Upstream Carrier Command Example 402
Figure 232 DSL Port Upstream Carrier Command Display Example 402
Figure 233 DSL Port Downstream Carrier0 Command Example 1 403
Figure 234 DSL Port Downstream Carrier0 Command Display Example 403
Figure 235 DSL Port Downstream Carrier0 Command Example 2 403
Figure 236 DSL Port Downstream Carrier1 Command Example 1 404
Figure 237 DSL Port Downstream Carrier1 Command Example 2 404
Figure 238 DSL Port Downstream Carrier1 Command Display Example 404
Figure 239 PMM Parameters Command Example 406
Figure 240 Impulse Noise Protection Command Example 406
Figure 241 Annex L Enable Command Example 407
Figure 242 Annex L Disable Command Example 407
Figure 243 Annex M Enable Command Example 407
Figure 244 Annex M Disable Command Example 408
Figure 245 Annex I Enable Command Example 408
Figure 246 Annex I Disable Command Example 409
Figure 247 DSL Port Show Command Example 409
Figure 248 Linedata Command Example 410
Figure 249 Lineinfo Command Example 411
Figure 250 Lineperf Command Example 412
Figure 251 15 Minute Performance Command Example 414
Figure 252 1Day Performance Command Example 415
Figure 253 Line Diagnostics Set Command Example 416

Figure 254 Line Diagnostics Get Command Example 417
Figure 255 Line Diagnostics Get 992.3 Command Example 419
Figure 256 SELT Diagnostic Set Command Example 421
Figure 257 Line Diagnostics Get Command Example 421
Figure 258 Tone Diagnostics Command Example 422
Figure 259 Alarm Profile Show Command Example 424
Figure 260 Alarm Profile Set Command Example 425
Figure 261 Alarm Profile Delete Command Example 426
Figure 262 Alarm Profile Map Command Example 426
Figure 263 Alarm Profile Showmap Command Example 427
Figure 264 Set Virtual Channel Profile Command Example 1 430
Figure 265 Set Virtual Channel Profile Command Example 2 430
Figure 266 Set Virtual Channel Profile Command Example 3 431
Figure 267 Delete Virtual Channel Profile Command Example 431
Figure 268 PVC Set Command Example 433
Figure 269 PPVC Set Command Example 434
Figure 270 PPVC Member Set Command Example 435
Figure 271 PPVC Member Delete Command Example 436
Figure 272 PPVC Member Show Command Example 437
Figure 273 PPVC Show Command Example 437
Figure 274 PPVC Delete Command Example 438
Figure 275 2684 Routed Mode Example 439
Figure 276 2684 Routed Mode Commands Example 440
Figure 277 RPVC Gateway Set Command Example 440
Figure 278 RPVC Gateway Show Command Example 441
Figure 279 RPVC Gateway Delete Command Example 441
Figure 280 RPVC Set Command Example 442
Figure 281 RPVC Show Command Example 443
Figure 282 RPVC Delete Command Example 443
Figure 283 RPVC Route Set Command Example 444
Figure 284 RPVC Route Show Command Example 445
Figure 285 RPVC Route Delete Command Example 446
Figure 286 RPVC ARP Agingtime Command Example 446
Figure 287 RPVC ARP Agingtime Show Command Example 446
Figure 288 RPVC ARP Agingtime Show Command Example 447
Figure 289 PAE PVC Set Command Example 448
Figure 290 PAE PVC Show Command Example 449
Figure 291 PAE PVC Session Command Example 450
Figure 292 PAE PVC Counter Command Example 450
Figure 293 TLS PVC Set Command Example 452
Figure 294 ACL Profile Set Command Example 457
Figure 295 ACL Profile Show Map Command Example 457
Figure 296 ACL Profile Show Command Example 458

Figure 297 ACL Assignment Set Command Example 459
Figure 298 ACL Assignment Show Command Example 459
Figure 299 Testing In-house Wiring 466
Figure 300 Resetting the Switch Via Command 470
Figure 301 Example Xmodem Upload 471
Figure 302 Example Xmodem Upload 472

List of Tables

Table 1 Common Icons 5
Table 2 Front Panel Ports 47
Table 3 LEDs 48
Table 4 Navigation Panel Submenu Links 61
Table 5 Web Configurator Screens 61
Table 6 Home 73
Table 7 Port Statistics (Ethernet) 75
Table 8 Port Statistics (DSL) 78
Table 9 Port Statistics (RMON) 80
Table 10 Port Statistics (RMON History) 82
Table 11 Port Statistics (RMON History Detail) 83
Table 12 System Info 88
Table 13 General Setup 92
Table 14 User Account 93
Table 15 User Account 95
Table 16 Switch Setup 100
Table 17 IP Setup 103
Table 18 ENET Port Setup 105
Table 19 ADSL Standards Maximum Transfer Rates 107
Table 20 xDSL Port Setup 109
Table 21 xDSL Port Setting 112
Table 22 VC Setup 117
Table 23 IEEE 802.1p Priority to PPVC Mapping 120
Table 24 PPVC Setup 121
Table 25 PPVC Setup, Edit 123
Table 26 Port Profile 126
Table 27 VC Profile 132
Table 28 Alarm Profile 134
Table 29 IGMP Filter Profile 137
Table 30 xDSL Line Rate Info 139
Table 31 xDSL Performance 142
Table 32 xDSL Line Data 144
Table 33 VLAN Status 151
Table 34 Static VLAN Setting 153
Table 35 VLAN Port Setting 154
Table 36 IGMP (Status) 159
Table 37 IGMP Bandwidth 161
Table 38 Bandwidth Port Setup 162

Table 39 IGMP Setup 163
Table 40 IGMP Count 164
Table 41 IGMP Port Info 165
Table 42 IGMP Port Group 166
Table 43 Static Multicast 167
Table 44 MVLAN Status 170
Table 45 MVLAN Setup 171
Table 46 MVLAN Group 173
Table 47 Packet Filter 175
Table 48 MAC Filter 178
Table 49 Path Cost 179
Table 50 RSTP Port States 180
Table 51 Spanning Tree Protocol Status 182
Table 52 Spanning Tree Protocol 183
Table 53 RADIUS 186
Table 54 802.1x 188
Table 55 Port Security 189
Table 56 DHCP Relay 193
Table 57 DHCP Snoop 196
Table 58 DHCP Snoop Status 197
Table 59 DHCP Counter 197
Table 60 2684 Routed PVC 201
Table 61 2684 Routed Domain 203
Table 62 RPVC Arp Proxy 204
Table 63 2684 Routed Gateway 205
Table 64 PPPoA to PPPoE 208
Table 65 PPPoA to PPPoE Status 210
Table 66 DSCP Setup 213
Table 67 DSCP Map 214
Table 68 TLS PVC 217
Table 69 ACL Setup 221
Table 70 ACL Profile Setup 223
Table 71 ACL Profile Map 224
Table 72 Downstream Broadcast 225
Table 73 SysLog 227
Table 74 Access Control Summary 229
Table 75 SNMP Commands 230
Table 76 SNMPv2 Traps 231
Table 77 SNMP 233
Table 78 Service Access Control 234
Table 79 Remote Management (Secured Client Setup) 235
Table 80 PPPoE Intermediate Agent Vendor-specific Tag Format 237
Table 81 PPPoE Intermediate Agent Vendor-specific Tag Format 237

Table 82 PPPoE Intermediate Agent Remote ID Sub-option Format 237
Table 83 PPPoE Intermediate Agent Sub-option Format: TR-101 (VID on) 238
Table 84 PPPoE Intermediate Agent Sub-option Format: TR-101 (VID off) 238
Table 85 PPPoE Intermediate Agent 239
Table 86 Maximum MTU 241
Table 87 PVC Upstream Limit 244
Table 88 OUI Filter 247
Table 89 Static Routing 251
Table 90 Alarm Status 253
Table 91 Alarm Descriptions 254
Table 92 Alarm Event Setup 256
Table 93 Alarm Event Setup Edit 257
Table 94 Alarm Port Setup 258
Table 95 Diagnostic 266
Table 96 MAC Table 270
Table 97 ARP Table 272
Table 98 ADSL Command Input Values 276
Table 99 Commands 277
Table 100 Log Format 314
Table 101 Log Messages 314
Table 102 General Alarm Command Parameters 323
Table 103 Log Format 326
Table 104 Filename Conventions 384
Table 105 Line Performance Counters 413
Table 106 15 Minute Performance Counters 414
Table 107 Line Diagnostics Get Command 417
Table 108 Line Diagnostics Get 992.3 Command 419
Table 109 ToneDiag Command 422
Table 110 SYS LED Troubleshooting 463
Table 111 ALM LED Troubleshooting 463
Table 112 10/100 LED Troubleshooting 464
Table 113 Troubleshooting Data Transmission 464
Table 114 DSL Data Transmission Troubleshooting 465
Table 115 DSL Voice Troubleshooting 465
Table 116 Wiring Tests 466
Table 117 Testing In-house Wiring 467
Table 118 Troubleshooting a Local Server 467
Table 119 Troubleshooting the SYNC-rate 468
Table 120 Troubleshooting the AAM1212's Configured Settings 468
Table 121 Troubleshooting the SNMP Server 469
Table 122 Troubleshooting Telnet 469
Table 123 Device Specifications 473
Table 124 Wire Gauge Specifications 475

PART I
Introduction

Getting to Know the AAM1212 (41)
Installing and Removing the AAM1212 (45)
Front Panel (47)
Introducing the Web Configurator (59)
Initial Configuration (67)
Home and Port Statistics Screens (73)

1

Getting to Know the AAM1212

This chapter introduces the main features and applications of your AAM1212.

1.1 Overview

The AAM1212 (ADSL Access Module) is an ADSL multiplexer network module designed to be installed in the IES-1000 IP-based DSLAM chassis. The AAM1212 aggregates traffic from 12 ADSL lines to two Ethernet ports to connect ADSL subscribers to the Internet.

You can use the built-in web configurator to manage and configure the AAM1212. In addition, the AAM1212 can also be managed via Telnet, the console port, or third-party SNMP management.

See Chapter 61 on page 471 for a complete list of features.

1.2 Applications

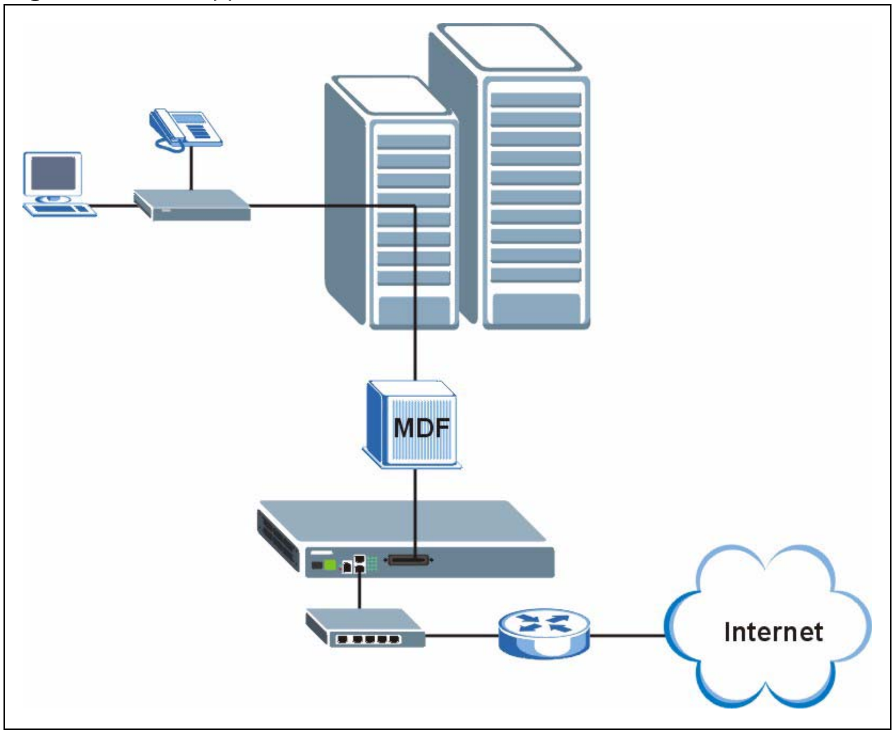
These are the main applications for the AAM1212:

- Provide Internet access and multimedia services for Multiple Tenant Units (MTU).
- Other applications include telemedicine, surveillance systems, remote servers systems, cellular base stations and high-quality teleconferencing.

1.2.1 MTU Application

The following diagram depicts a typical application of the AAM1212 with DSL modems in a large residential building or multiple tenant unit (MTU). This application leverages existing phone line wiring to provide Internet access to all tenants, and the tenants can continue to use the existing phone services.

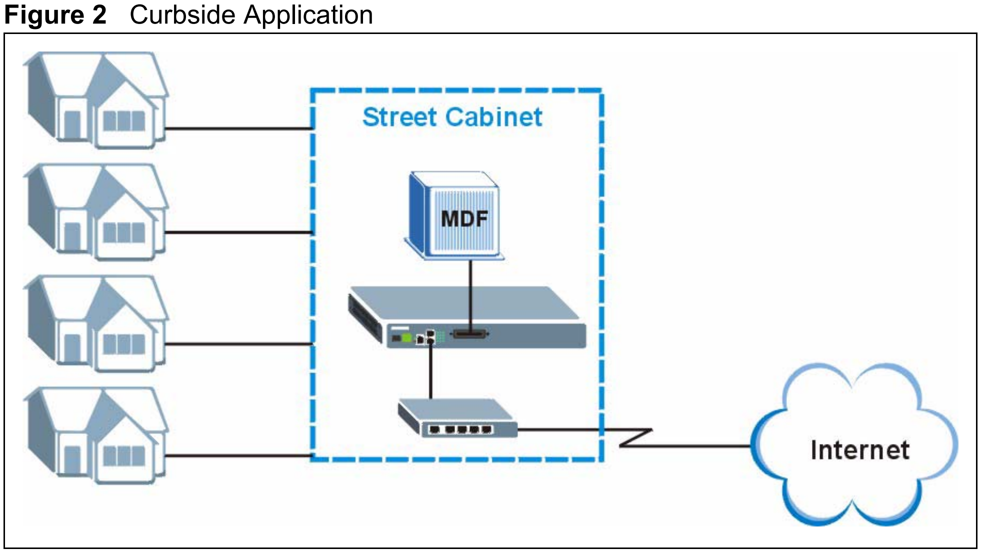
Figure 1 MTU Application



1.2.2 Curbside Application

The AAM1212 can be used by an Internet Service Provider (ISP) in a street cabinet to form a "mini POP (Point-of-Presence)" to provide broadband services to residential areas that are too far away from the ISP to avail of DSL services. Residents need a DSL modem, connected as shown in the previous figure.

Figure 2 Curbside Application



2

Installing and Removing the AAM1212

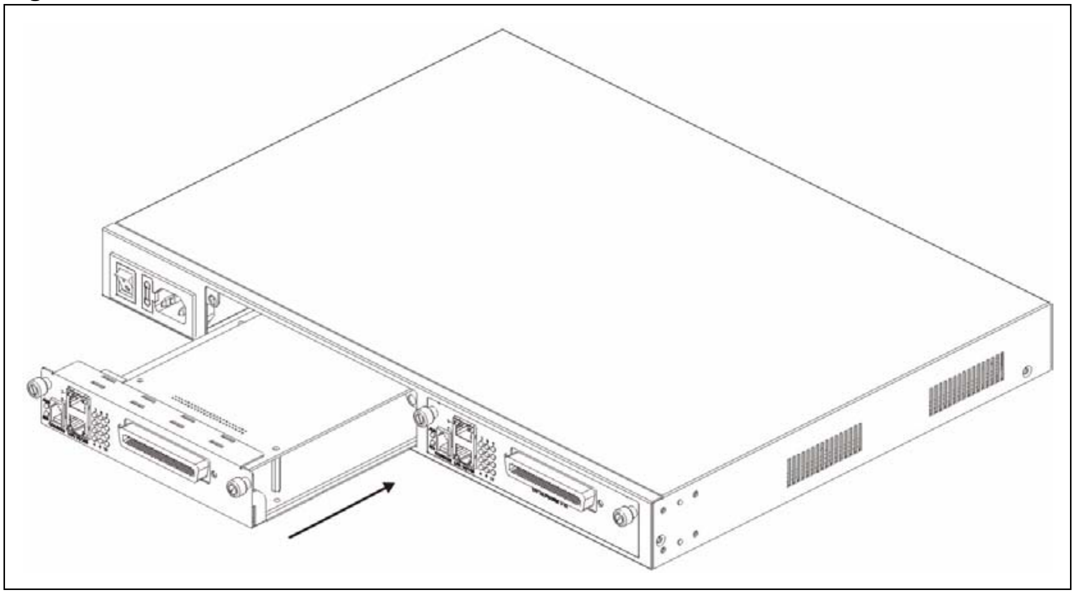
This chapter shows you how to install the AAM1212 in the IES-1000 and how to remove it.

2.1 Installing the AAM1212 in the IES-1000

1 Hold the AAM1212 with the network ports facing you.

2 Insert it into an empty slot on the front of the IES-1000. Push the AAM1212 into the IES-1000 until the front of the AAM1212 is flush with the IES-1000.

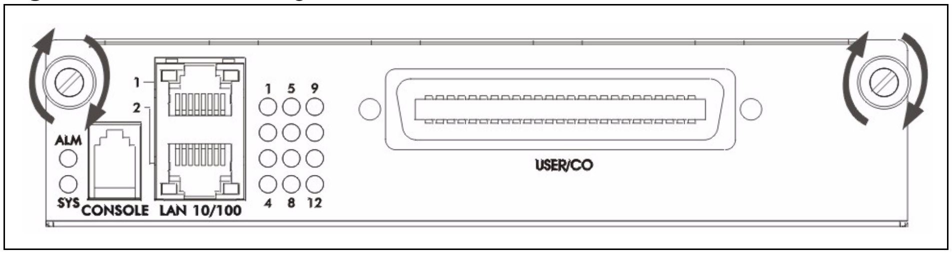
Figure 3 Installation: Push the AAM1212 into the IES-1000



Note: The front of the AAM1212 must be flush with the front of the IES-1000.

3 Turn the two screws on the front of the AAM1212 clockwise to secure the AAM1212 to the chassis as shown below.

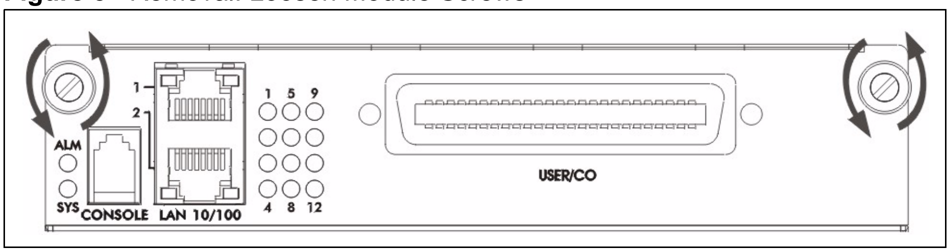
Figure 4 Installation: Tighten Module Screws



2.2 Removing the AAM1212 from the IES-1000

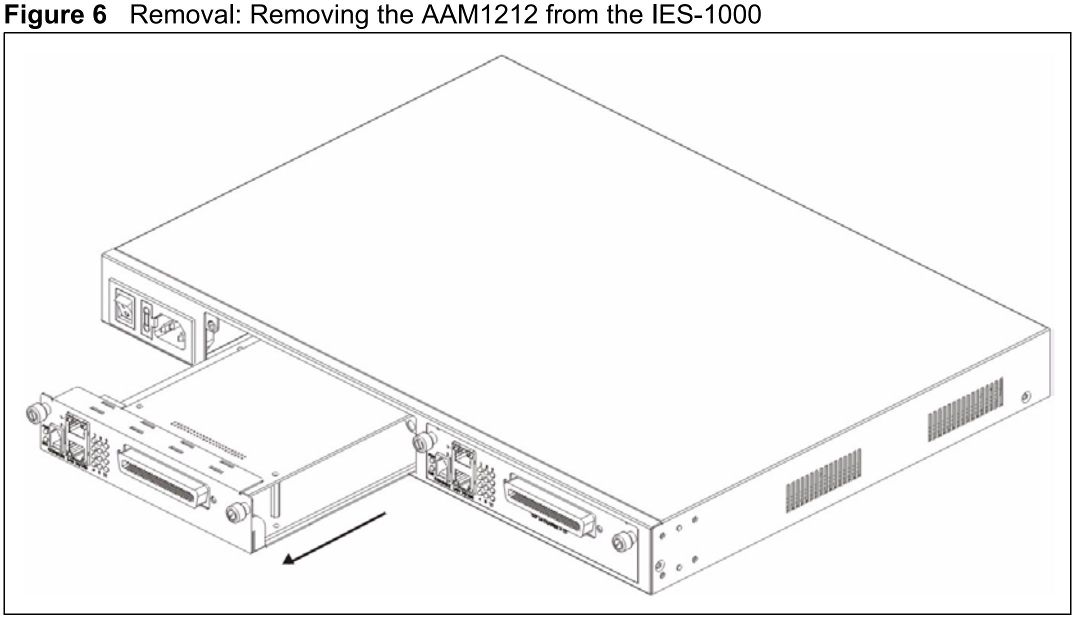
1 Turning the two screws that secure the module to the chassis counter-clockwise to loosen them.

Figure 5 Removal: Loosen Module Screws



2 Gently pull the AAM1212 out of the chassis as shown next.

Figure 6 Removal: Removing the AAM1212 from the IES-1000



3

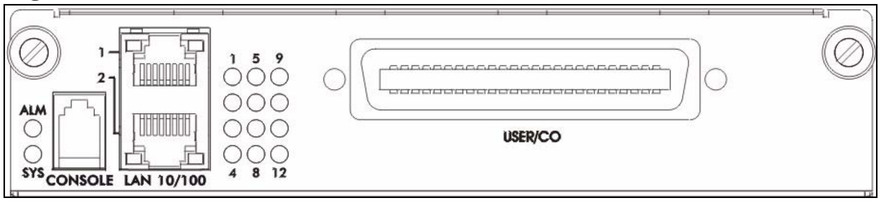
Front Panel

This chapter describes the front panel and rear panel of the AAM1212 and shows you how to make the hardware connections.

3.1 Front Panel

The figure below shows the front panel of the AAM1212.

Figure 7 Front Panel



3.1.1 Front Panel Ports

The following table describes the port labels on the front panel.

Table 2 Front Panel Ports

LABEL	DESCRIPTION
CONSOLE	Only connect this port if you want to configure the AAM1212 using the command line interface (CLI) via the console port.
LAN 10/100	Connect these ports to a computer, a hub, an Ethernet switch or router.
USER/CO	Connect the Telco-50 connector **USER** pins (14-25, 39-50) to subscribers respectively. Connect the Telco-50 connector **CO** pins (1-12, 26-37) to the telephone company for subscribers respectively.

3.1.2 LEDs

The following table describes the LED indicators on the AAM1212.

Table 3 LEDs

LED	COLOR	STATUS	DESCRIPTION
ALM	Red	On	The on board temperature is above a safe level.
		Off	The on board temperature is within a safe range.
SYS	Green	Blinking	The system is rebooting and performing self-diagnostic tests.
		On	The system is on and functioning properly.
		Off	The power is off or the system is not ready/malfunctioning.
LAN 10/100	Green	On	The link to a 10 Mbps Ethernet network is up.
		Off	The link to a 10 Mbps Ethernet network is down.
		Blinking	The 10 Mbps link is transmitting and receiving data.
	Orange	On	The link to a 100 Mbps Ethernet network is up.
		Off	The link to a 100 Mbps Ethernet network is down.
		Blinking	The 100 Mbps link is transmitting and receiving data.
1-12	Green	On	The DSL link is up.
		Blinking	The AAM1212 is initializing the DSL line.
		Off	The DSL link is down.

3.1.3 Console Port

For local management, you can use a computer with terminal emulation software configured to the following parameters:

- VT100 terminal emulation
- 9600 bps
- No parity, 8 data bits, 1 stop bit
- No flow control

Connect the male 9-pin end of the console cable to the console port of the AAM1212. Connect the female end to a serial port (COM1, COM2 or other COM port) of your computer.

3.1.3.1 Default Ethernet Settings

The factory default negotiation settings for the Ethernet ports on the AAM1212 are:

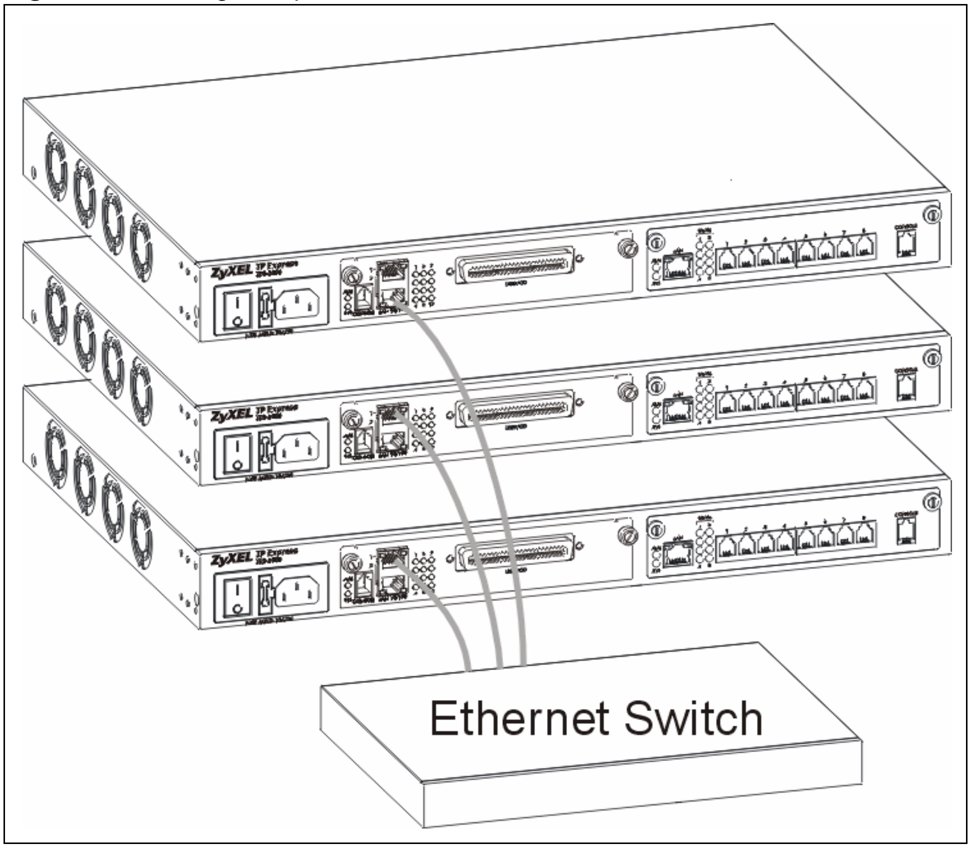
- Speed: Auto
- Duplex: Auto

3.1.4 LAN Port (Ethernet) Connection

Connect the LAN port of your AAM1212 to an Ethernet WAN switch using a straight-through Category 5 UTP (Unshielded Twisted Pair) cable with RJ-45 connectors.

You may stack multiple IES-1000 units up to the number of ports available on the Ethernet switch as shown next.

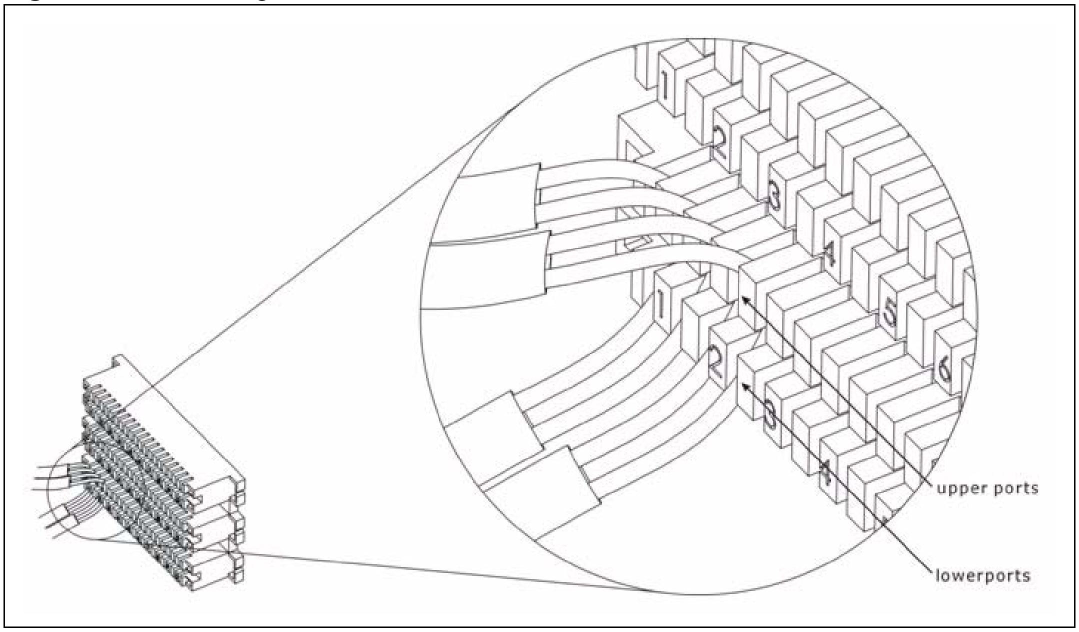
Figure 8 Stacking Multiple IES-1000 Units



3.1.5 Notes About MDFs (Main Distribution Frames)

An MDF is usually installed between end-users' equipment and the telephone company (CO) in a basement or telephone room. The MDF is the point of termination for the outside telephone company lines coming into a building and the telephone lines in the building.

Figure 9 MDF Wiring



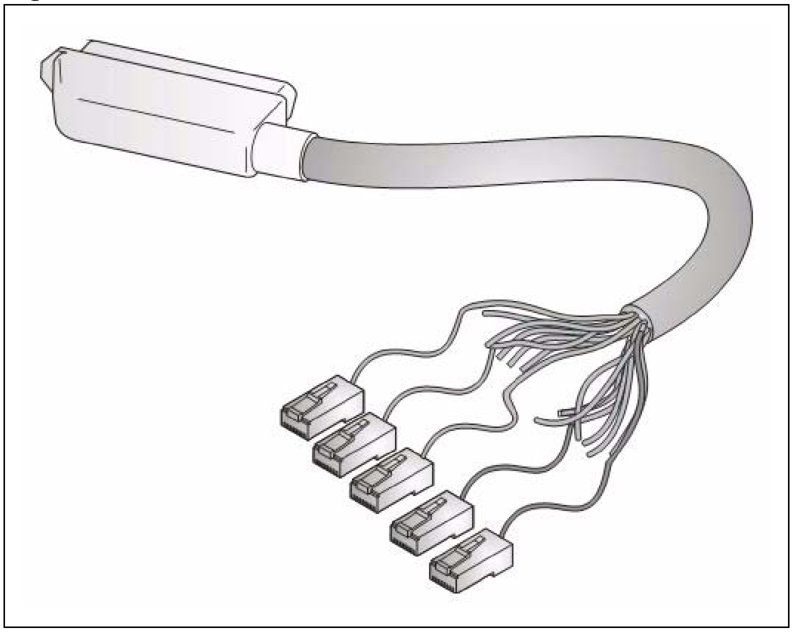
- Connect wiring from end-user equipment to the lower ports of an MDF using a telephone wire. Connect wiring from the telephone company to the upper ports of an MDF (see the previous figure).
- Some MDFs have surge protection circuitry built in between the two banks; thus, do not connect telephone wires from the telephone company directly to the AAM1212.
- Use a punch-down tool to seat telephone lines between MDF blocks.

3.1.6 Telco-50 Cables

Telco-50 cables are used for data and voice applications with MDFs (Main Distribution Frame), patch panels and distribution boxes. They can also be used as extension cables. Telco-50 cables are made up of 25 twisted-pair copper wires.

Connect a Telco-50 connector to one end of the cable (see the hardware specifications appendix for pin assignments) and connect the other end directly to an MDF; alternatively attach RJ-11 connectors and connect directly to DSL modem(s).

Figure 10 Telco-50 Cable with RJ-11 Connectors



3.1.7 Telco-50 Connections

The internal DSL splitters separate the voice signals from the DSL signals. They feed the DSL signals to the AAM1212 and divert the voice signals to the **CO** lines of the Telco-50 connector.

Connect the **CO** lines of the Telco-50 connector to the PBX or PSTN/ISDN switch.

Connect the **USER** lines of the Telco-50 connector to the subscribers' telephone wiring. In most multi-tenant unit applications, the USER pins connect to the subscribers' telephone wiring via Main Distribution Frame (MDF).

See the section on MDF scenarios and the pin assignments in the hardware specifications appendix for details on Telco-50 connections.

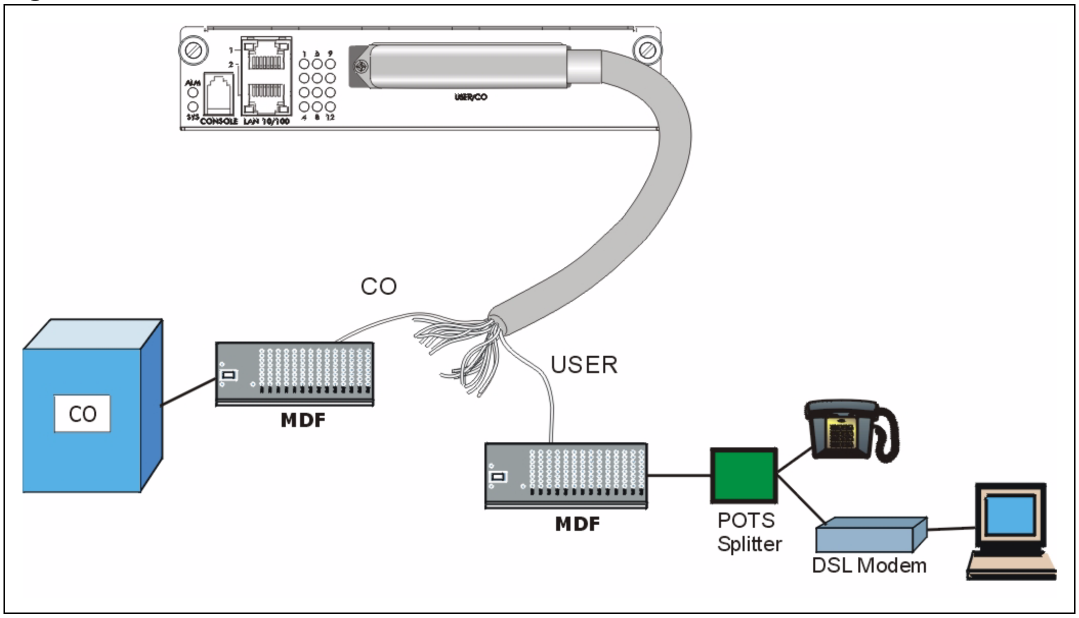
3.1.8 ADSL Connections

Connect the lines from the user equipment (ADSL modems) to the Telco-50 connector **USER** pins and the lines from the central office switch or PBX (Private Branch Exchange) to the Telco-50 connector **CO** pins. Make sure that the **USER** line and the **CO** lines are not shorted on the MDF (Main Distribution Frame).

The line from the user carries both the ADSL and the voice signals. For each line, the AAM1212 has a built-in splitter that separates the high frequency ADSL signal from the voice band signal and feeds the ADSL signal to the AAM1212, while the voice band signal is diverted to the CO port.

The following figure gives an overview on a possible installation scenario for the AAM1212. Data and voice signals can coexist on the same telephone wiring.

Figure 11 Installation Overview



Note: You can also attach RJ-11 connectors to the Telco-50 cable and connect directly to a DSL modem(s) or patch panel. This chapter discusses connections using MDFs.

3.1.9 Typical MDF Scenarios

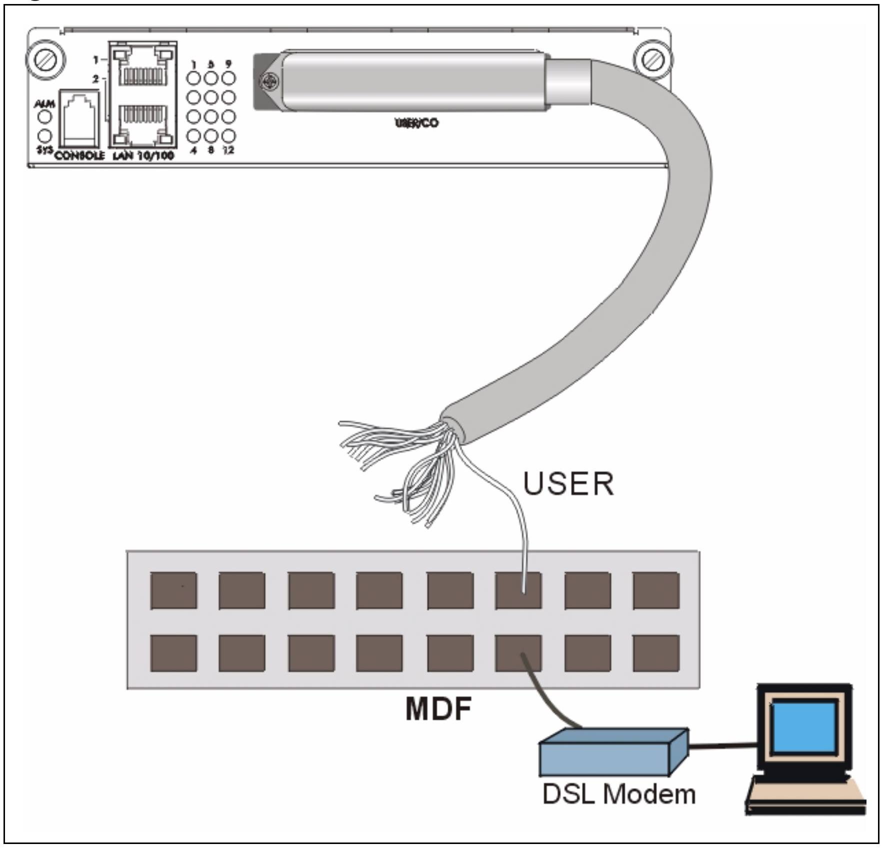
This section describes typical installation scenarios.

3.1.9.1 Installation Scenario A

You want to install the AAM1212 in an environment where there are no previously installed MDFs. There is no phone service and you want to install the AAM1212 for data-access only. No connections from the **CO** lines are necessary.

You may connect using an MDF or attach RJ-11 connectors to the non-AAM1212 end of the Telco-50 cable and then connect to DSL modems directly.

Figure 12 Installation Scenario A



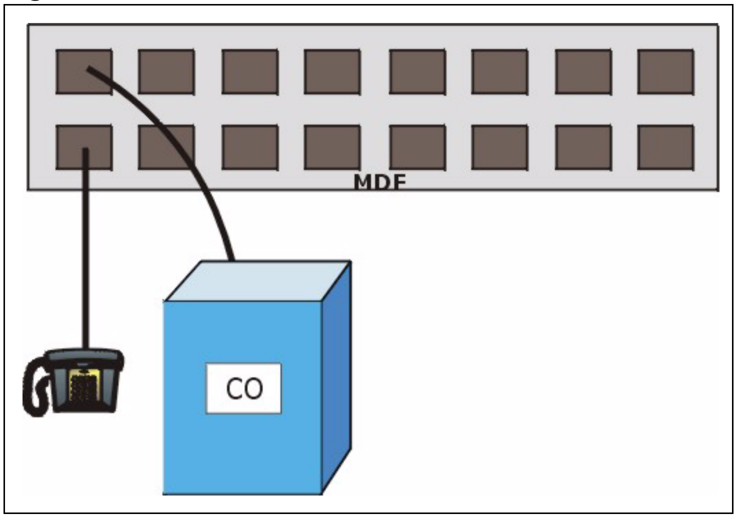
3.1.9.1.1 Procedure To Connect To An MDF

1. Connect the Telco-50 connector end of the cable to the Telco-50 connector.
2. Connect the USER wiring on the other end of the Telco-50 cable to the upper ports of the MDF using a punch-down tool.
3. Connect the telephone wiring from each end-user's DSL modem to the lower ports of the MDF.

3.1.9.2 Installation Scenario B

Phone service is available. There is one MDF from which end-users CO connections are made (see next figure).

Figure 13 One MDF for End-user and CO Connections

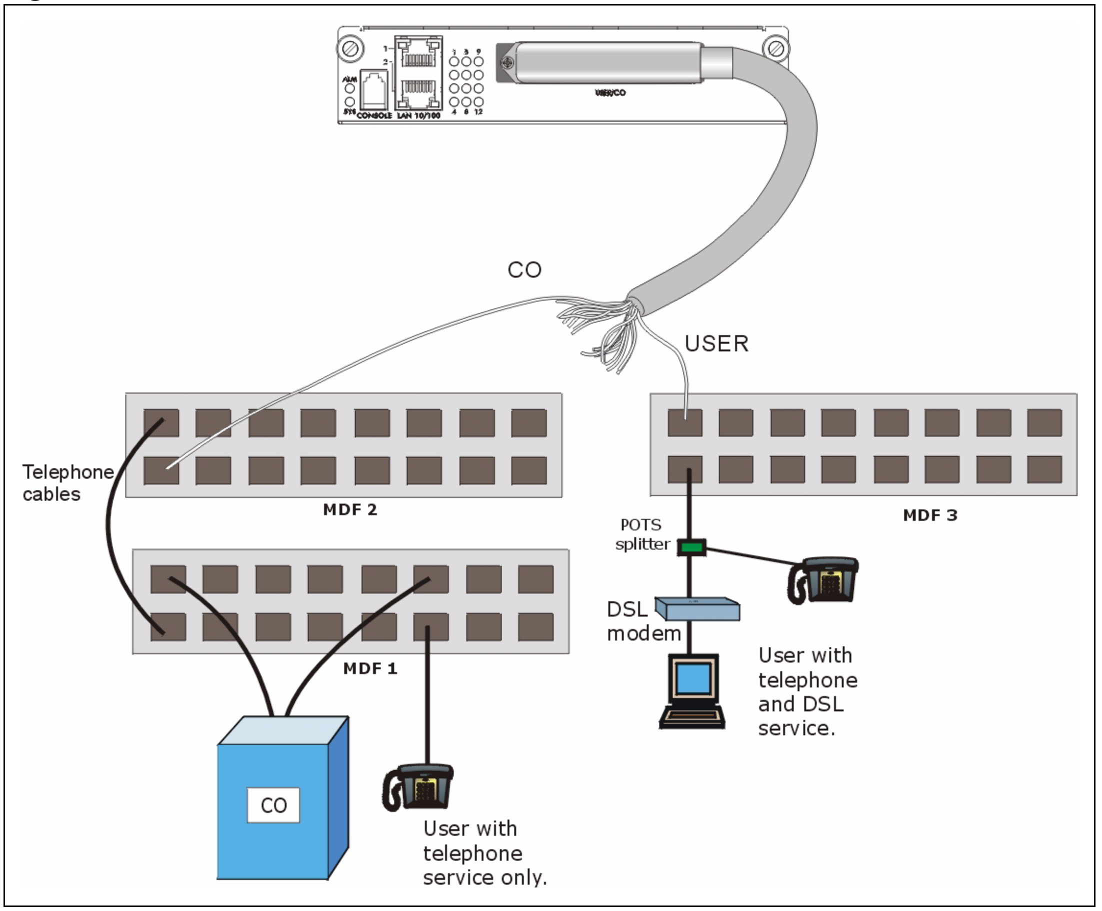


This installation scenario requires three MDFs. Please refer to the following figure for the connection schema.

- MDF 1 is the original MDF used for telephone connections only.
- MDF 2 is used for telephone connections only.
- MDF 3 is for ADSL service connections.

Note: Change the wiring (in the following figure) from MDF 1 to MDF 3 for telephone subscribers who want ADSL service.

Figure 14 Installation Scenario B



3.1.9.2.1 Procedure To Connect To MDFs

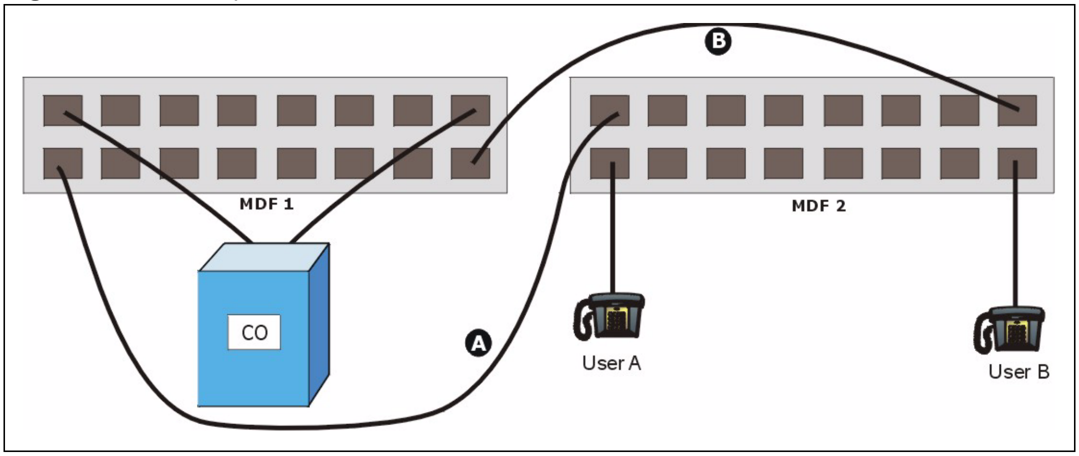
1. Connect the Telco-50 connector end of the cable to the Telco-50 connector.
2. Connect the **USER** wiring on the other end of the Telco-50 cable to the upper ports of MDF 3 using a punch-down tool.
3. Connect the telephone wiring from the end-user's DSL modem(s) to the lower ports of MDF 3.
4. Connect the **CO** wiring of the Telco-50 cable to the lower ports of MDF 2 using a punch-down tool.
5. Connect the upper ports of MDF 2 to the lower ports of MDF 1 using telephone wires.
6. Connect the upper ports of MDF 1 to the telephone company.
7. Telephone subscribers only (non-DSL subscribers) retain connections to the lower ports of MDF 1.
8. Change the wiring from MDF 1 to MDF 3 for telephone subscribers who want DSL service.

3.1.9.3 Installation Scenario C

Phone service is also available but there are two MDFs; one for end-user telephone line connections and the other one for CO telephone wiring connections (see the following figure).

Note: Users A and B have telephone (only) service.

Figure 15 Two Separate MDFs for End-user and CO Connections

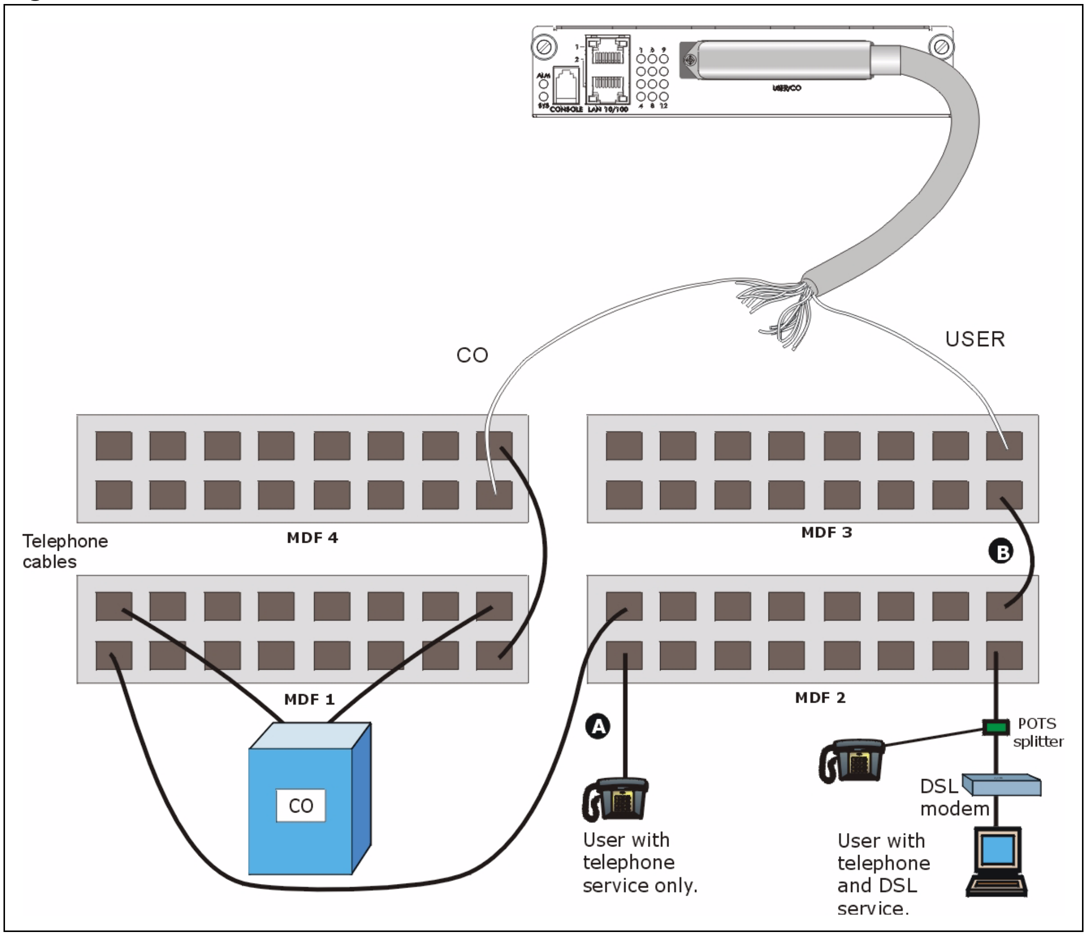


This installation scenario requires four MDFs. Please refer to the following figure for the DSL connection schema.

- MDFs 1 and 2 are the two original MDFs.
- MDFs 3 and 4 are two additional MDFs you need.

Note: User A still has telephone service only. User B now has telephone and DSL service (see the following figure).

Figure 16 Installation Scenario C



3.1.9.3.1 Procedure To Connect To MDFs

1 Connect the Telco-50 connector end of the cable to the Telco-50 connector.

2 Connect the **USER** wiring on the other end of the Telco-50 cable to the upper ports of MDF 3 using a punch-down tool.

3 Connect the lower ports of MDF 3 to the upper ports of MDF 2 for those users that want DSL service. (Users who want telephone service only, retain the original connection from the top port of MDF 2 to the bottom port of MDF 1.)

4 Connect the telephone wiring from the end-user's DSL equipment to the lower ports of MDF 2.

5 Connect the **CO** wiring of the Telco-50 cable to the lower ports of MDF 4 using a punch-down tool.

6 Connect the top ports of MDF 4 to the bottom ports of MDF 1 using telephone wires.

7 Connect the top ports of MDF 1 to the telephone company.

4

Introducing the Web Configurator

This chapter tells how to access and navigate the web configurator.

4.1 Web Configurator Overview

The web configurator allows you to use a web browser to manage the AAM1212.

4.2 Screen Privilege Levels

There is a high or low privilege level for each screen.

High privilege screens are only available to administrators with high privilege access. High privilege screens include things like creating administrator accounts, restarting the system, saving changes to the nonvolatile memory and resetting to factory defaults. Nonvolatile memory refers to the AAM1212's storage that remains even if the AAM1212's power is turned off. Administrators with high privilege access can use all screens including the lower privilege screens.

Administrators with the low privilege level are restricted to using only low privilege screens. Low privilege screens are read only.

4.3 Accessing the Web Configurator

Use Internet Explorer 6 and later versions with JavaScript enabled.

Use the following instructions to log on to the web configurator.

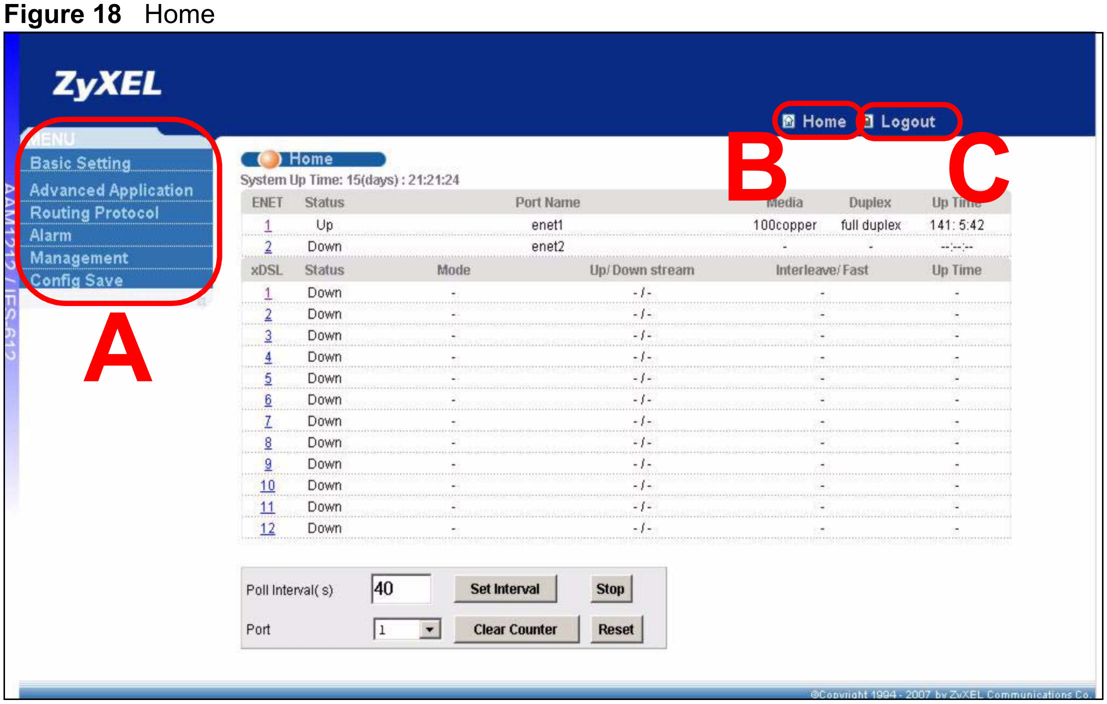
1 Launch your web browser, and enter the IP address of the AAM1212 (default: **192.168.1.1** is the factory default) in the **Location** or **Address** field. Press **Enter**. The **Login** screen appears.

Figure 17 Login

2 Type **admin** in the **User Name** field and your password (default: **1234**) in the **Password** field. Click **OK**. The main screen appears.

This is the web configurator's main screen.

Figure 18 Home



A - Click the menu items to open submenu links, and then click on a submenu link to open the screen in the main window. See Section 4.4 on page 61 for more information.

B - Click this to open the **Home** screen. (This is the same screen that is displayed above.) See Chapter 6 on page 73 for more information.

C - Click this to log out of the web configurator.

4.4 Navigation Panel

In the navigation panel, click a menu item to reveal a list of submenu links. Click a submenu link to go to the corresponding screen.

Table 4 Navigation Panel Submenu Links

BASIC SETTING	ADVANCED APPLICATION	ROUTING PROTOCOL
System Information General Setup User Account Switch Setup IP Setup ENET Port Setup xDSL Port Setup xDSL Profiles Setup xDSL Line Data G.bond	VLAN IGMP Static Multicast Multicast VLAN Filtering MAC Filter Spanning Tree Protocol Port Authentication Port Security DHCP Relay DHCP Snoop 2684 Routed Mode PPPoA to PPPoE DSCP TLS PVC ACL Downstream Broadcast SysLog Access Control PPPoE Intermediate Agent Maximum MTU Size PVC Upstream Limit OUI Filter	Static Routing
ALARM	**MANAGEMENT**	**CONFIG SAVE**
Alarm Status Alarm Event Setup Alarm Port Setup	Maintenance Diagnostic MAC Table ARP Table	Config Save

The following table briefly describes the functions of the screens that you open by clicking the navigation panel's sub-links.

Table 5 Web Configurator Screens

LABEL	DESCRIPTION
Basic Setting	
System Information	Use this screen to display general system and hardware monitoring information.

Table 5 Web Configurator Screens (continued)

LABEL	DESCRIPTION
General Setup	Use this screen to configure general identification information about the device and the time and date settings.
User Account	Use this screen to configure system administrator accounts.
Switch Setup	Use this screen to set up system-wide parameters such as MAC address learning and priority queues.
IP Setup	Use this screen to configure the system and management IP addresses and subnet masks.
ENET Port Setup	Use this screen to configure settings for the Ethernet ports.
xDSL Port Setup	Use these screens for configuring settings for individual DSL ports.
xDSL Profiles Setup	Use these screens for configuring profiles for the DSL ports.
xDSL Line Data	Use these screens for viewing DSL line operating values, bit allocation and performance counters.
G.bond	Use this screen to configure G.bond, letting subscribers connect to an ISP using data streams spread over multiple DSL lines.
Advanced Application	
VLAN	Use these screens for viewing and configuring the VLAN settings.
IGMP	Use these screens to view IGMP status information and configure IGMP settings and IGMP filters. You can also use these screens to set up bandwidth requirements by multicast group or port and to set up limits on the number of multicast groups to which a port can subscribe.
Static Multicast	Use this screen to configure static multicast entries.
Multicast VLAN	Use these screens to set up multicast VLANs that can be shared among different subscriber VLANs on the network.
Filtering	Use this screen to configure packet filtering.
MAC Filter	Use this screen to configure MAC filtering for each port.
Spanning Tree Protocol	Use these screens to display Rapid Spanning Tree Protocol (RSTP) information and configure RSTP settings.
Port Authentication	Use these screens to configure RADIUS and IEEE 802.1x security settings.
Port Security	Use this screen to limit the number of MAC address that can be learned on a port.
DHCP Relay	Use this screen to configure the DHCP relay settings.
DHCP Snoop	Use these screens to drop traffic from IP addresses not assigned by the DHCP server and to look at a summary of the DHCP packets on each port.
2684 Routed Mode	Use this screen to configure the AAM1212 to handle 2684 routed mode traffic.
PPPoA to PPPoE	Use this screen to enable PPPoA-to-PPPoE conversions on each port.
DSCP	Use this screen to set up DSCP on each port and to convert DSCP values to IEEE 802.1p values.
TLS PVC	Use this screen to set up Transparent LAN Service (VLAN stacking, Q-in-Q) on each port.
ACL	Use this screen to set up Access Control Logic profiles and to assign them to each PVC.
Downstream Broadcast	Use this screen to block downstream broadcast packets from being sent to specified VLANs on specified ports.

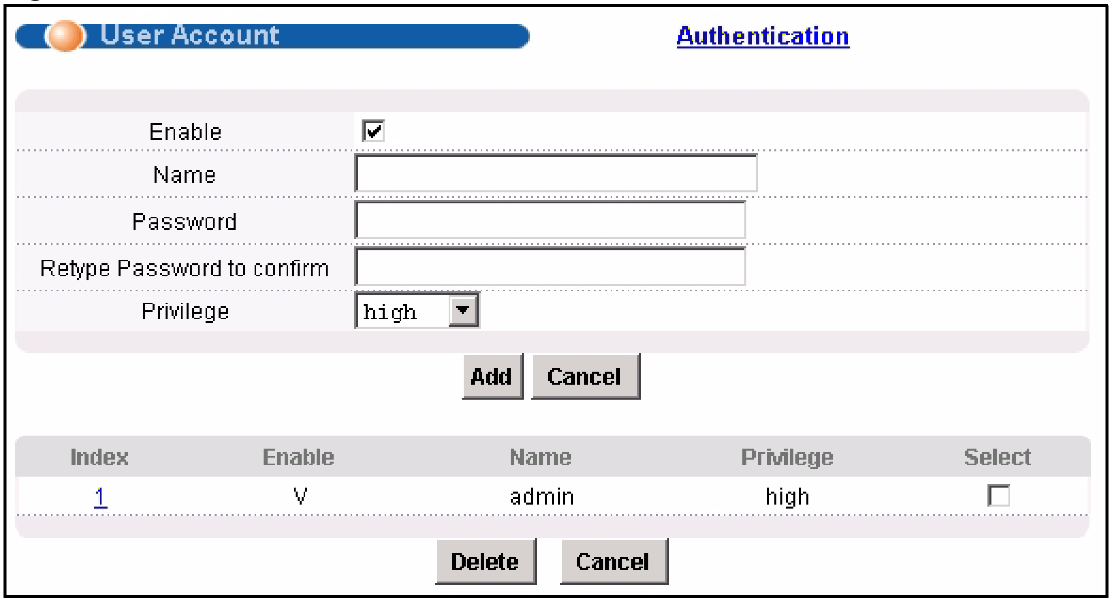
Table 5 Web Configurator Screens (continued)

LABEL	DESCRIPTION
SysLog	Use this screen to configure the syslog settings.
Access Control	Use this screen to configure service access control and configure SNMP and remote management.
PPPoE Intermediate Agent	Use this screen to insert line information into client PPPoE PADI (PPPoE Active Discovery Initialization) and PADR (PPPoE Active Discovery Request) packets.
Maximum MTU Size	Use this screen to configure the Maximum Transmission Unit (MTU) for the Ethernet interfaces. The Ethernet interfaces discard any packets larger than this.
PVC Upstream Limit	Use this screen to limit the transmission rate for upstream traffic by PVC.
OUI Filter	Use this screen to configure the AAM1212 to filter packets based on the OUI (Organizationally Unique Identifier) used in the MAC address to identify the manufacturer of a device.
Routing Protocol	
Static Routing	Use this screen to configure static routes. A static route defines how the AAM1212 should forward traffic by configuring the TCP/IP parameters manually.
Alarm	
Alarm Status	Use these screens to view the alarms that are currently in the system.
Alarm Event Setup	Use these screens to view and set the severity levels of the alarms and where the system is to send them.
Alarm Port Setup	Use this screen to set the alarm severity threshold for recording alarms on an individual port(s).
Management	
Maintenance	Use this screen to perform firmware and configuration file maintenance as well as restart the system.
Diagnostic	Use this screen to view system logs and test port(s).
MAC Table	Use this screen to view the MAC addresses of devices attached to what ports.
ARP Table	Use this screen to view the MAC address to IP address resolution table.
Config Save	
Config Save	Use this screen to save the device’s configuration into the nonvolatile memory (the AAM1212’s storage that remains even if the AAM1212’s power is turned off).

4.5 Changing Your Password

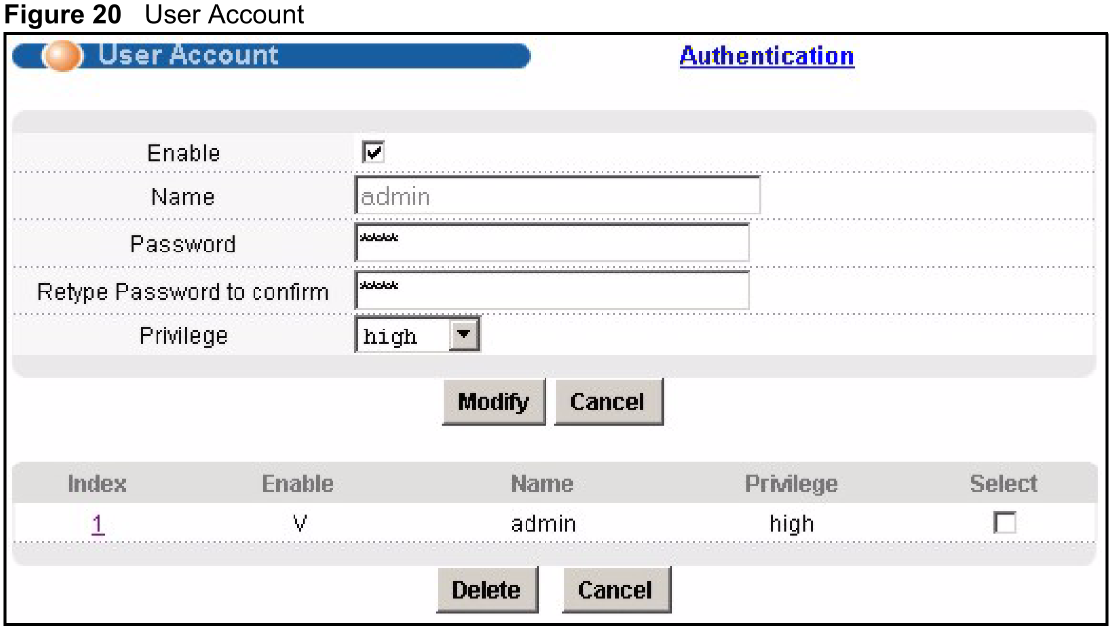
After you log in for the first time, it is recommended you change the default administrator password. Click **Basic Setting** and then **User Account** to display the **User Account** screen.

Figure 19 User Account



Click the index number **1** to edit the default administrator account settings.

Figure 20 User Account



Enter the new password in the **Password** and **Retype Password** to confirm fields, and click **Modify**. Do not forget to click **Config Save** before you exit the web configurator. See Section 4.6 on page 64.

4.6 Saving Your Configuration

Click **Apply** in a configuration screen when you are done modifying the settings in that screen to save your changes back to the run-time memory. Settings in the run-time memory are lost when the AAM1212's power is turned off.

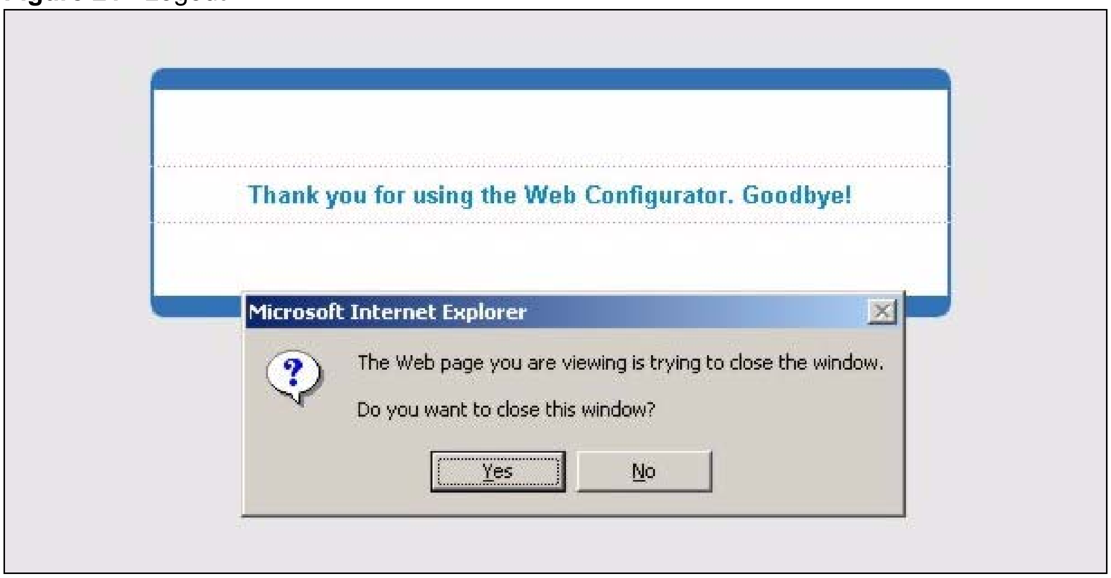
Click **Config Save** in the navigation panel to save your configuration to nonvolatile memory. Nonvolatile memory refers to the AAM1212's storage that remains even if the AAM1212's power is turned off.

Use **Config Save** when you are done with a configuration session.

4.7 Logging Out of the Web Configurator

Click **Logout** in any screen to exit the web configurator. You have to log in with your password again after you log out. This is recommended after you finish a management session both for security reasons and so you do not lock out other device administrators.

Figure 21 Logout



5

Initial Configuration

This chapter describes initial configuration for the AAM1212. See Chapter 61 on page 471 for various default settings of the AAM1212.

5.1 Initial Configuration Overview

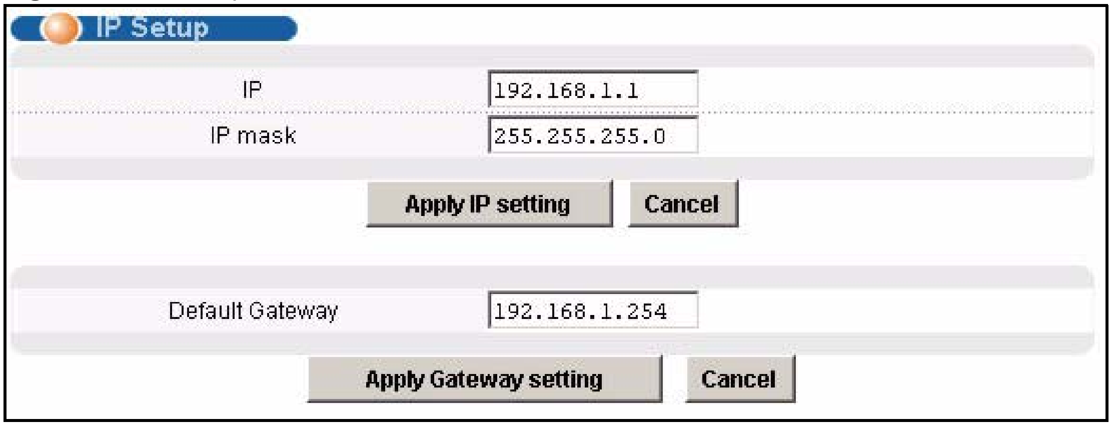
This chapter shows what you first need to do to provide service to DSL subscribers.

5.2 Initial Configuration

This chapter uses the web configurator for initial configuration. See the CLI chapters for information on the commands. Use Internet Explorer 6 and later versions with JavaScript enabled.

1 Log in to the web configurator. See Section 4.3 on page 59 for instructions.
2 In the navigation panel, click **Basic Setting**, **IP Setup**. The **IP Setup** screen appears.

Figure 22 IP Setup



3 Use this screen to change the IP address, subnet mask, and default gateway IP address for your network. Apply the settings.

If you change the IP address of the AAM1212, after you click **Apply IP setting**, you have to use the new IP address to log into the web configurator again.

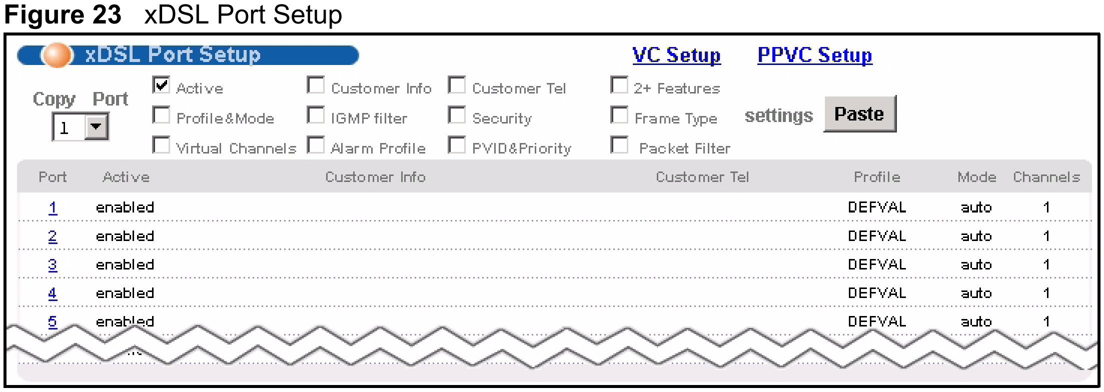
4 If your subscribers use VPI 0 and VCI 33 (the default for all of the DSL ports), go to step 13. Otherwise, use the following steps to change the VPI and VCI settings for all of the DSL ports.

First, you will delete the default virtual channel from all of the DSL ports. (You cannot edit it). Then, you will configure a new virtual channel for a port and copy it to the other DSL ports.

Adding another virtual channel without deleting the default virtual channel is not recommended since you cannot set the new channel to be the port's super channel. The super channel can forward frames belonging to multiple VLAN groups (that are not assigned to other channels). A channel that is not the super channel can only forward frames with a single VLAN ID (that is configured on that channel). In this case, the AAM1212 drops any frames received from the subscriber that are tagged with another VLAN ID.

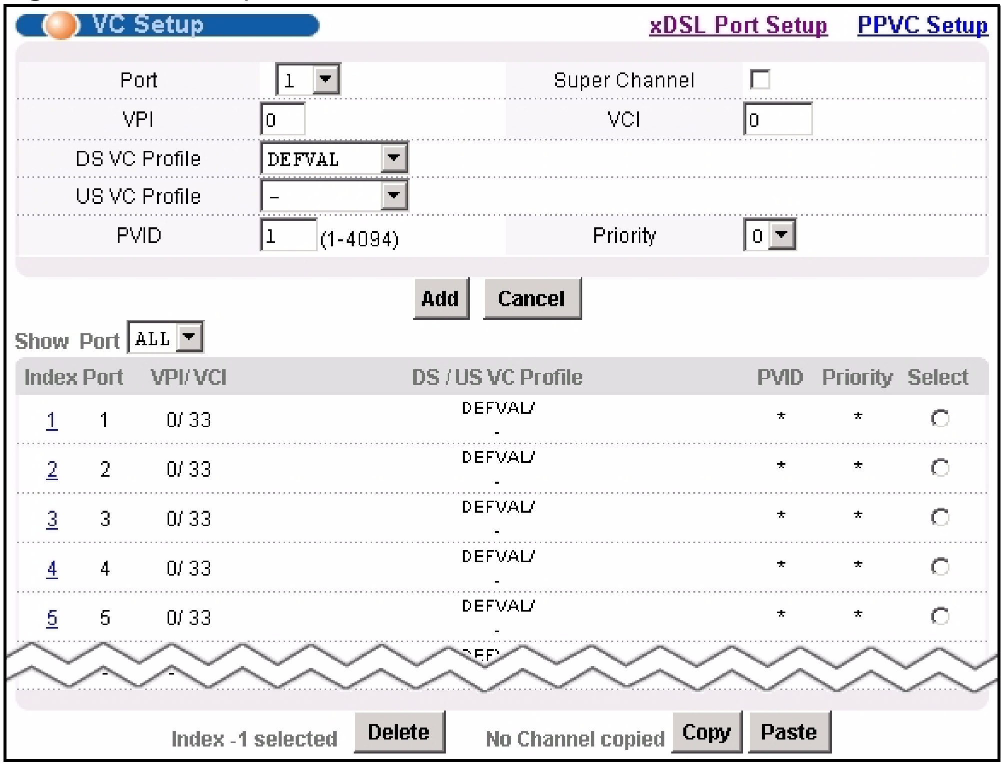
5 In the navigation panel, click **Basic Setting**, **xDSL Port Setup**. The **xDSL Port Setup** screen appears.

Figure 23 xDSL Port Setup



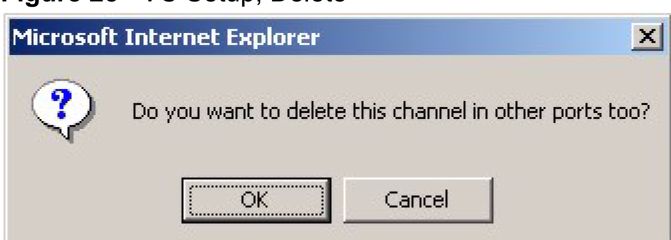
6 Click **VC Setup**. The following screen appears.

Figure 24 VC Setup



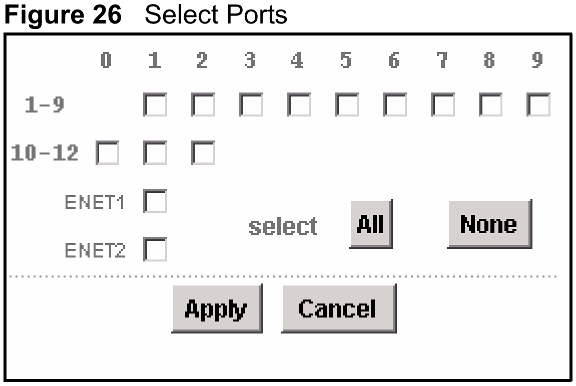
7 Select any virtual channel's **Select** radio button, and click **Delete**. The following screen appears.

Figure 25 VC Setup, Delete



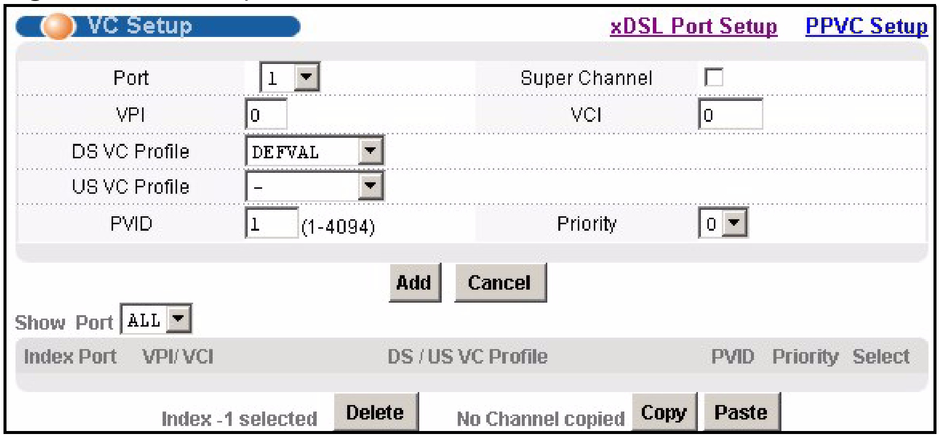
8 Click **OK**. The following screen appears.

Figure 26 Select Ports



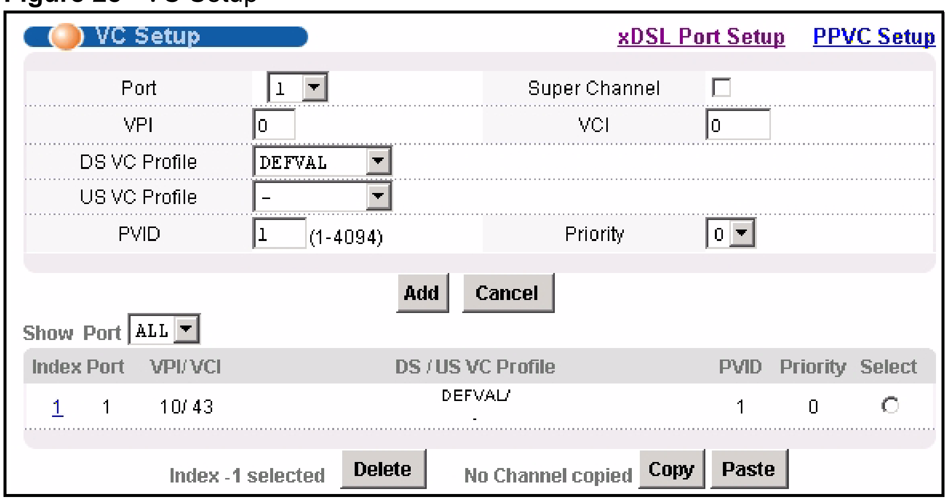
9 Click **All,** and then click **Apply**. The **VC Setup** screen is updated.

Figure 27 VC Setup



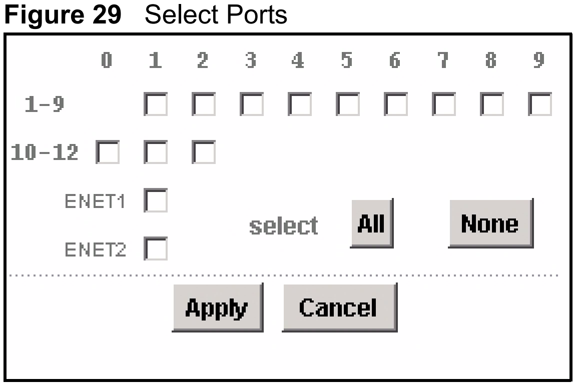
10 Select **Super Channel** to allow the channel to forward frames belonging to multiple VLAN groups (that are not assigned to other channels). Then, enter the VPI and VCI that you use. Leave the other default settings, and click **Add**. The **VC Setup** screen is updated.

Figure 28 VC Setup



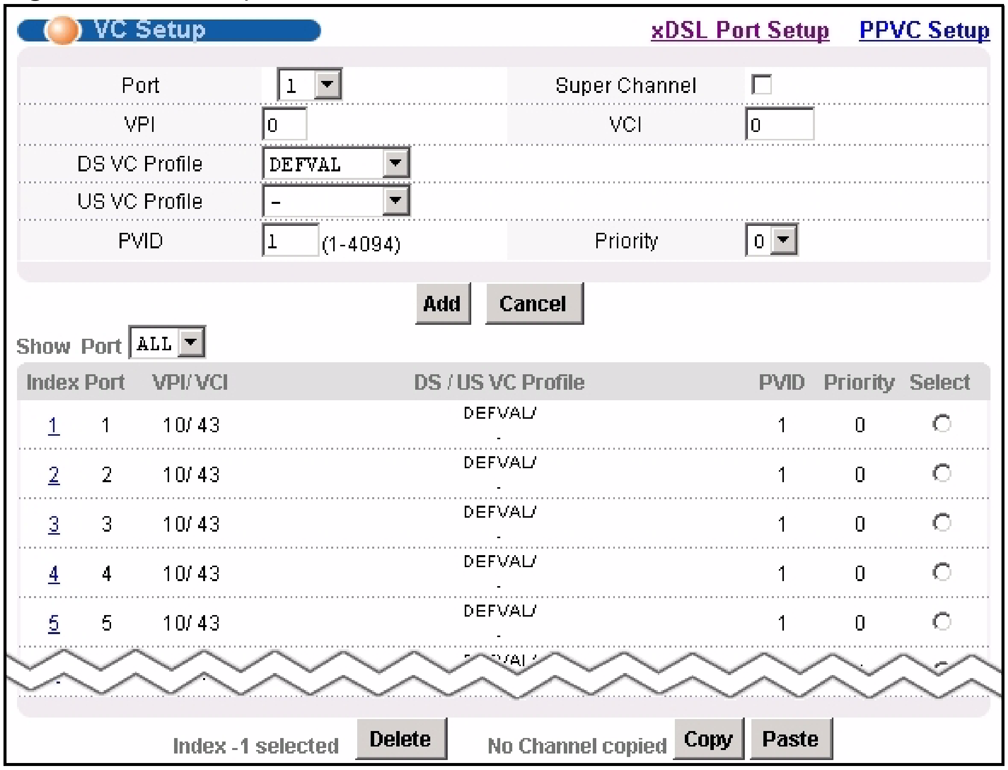
11 Select the new channel's **Select** radio button. Click **Copy**, and then click **Paste**. The following screen appears. The following screen appears.

Figure 29 Select Ports



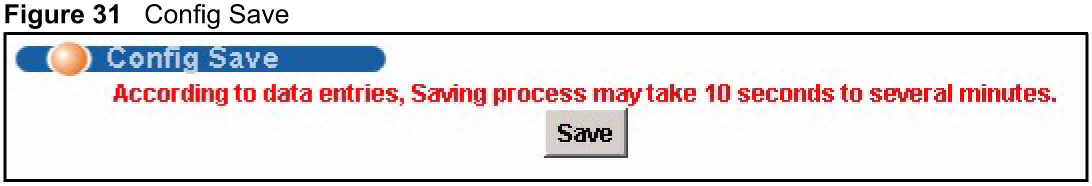
12 Click **All,** and then click **Apply**. The **VC Setup** screen is updated.

Figure 30 VC Setup



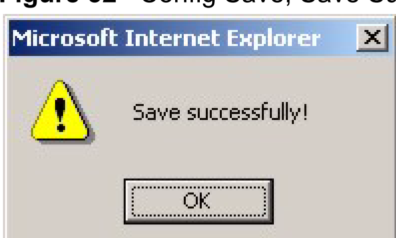
13 Click **Config Save**, **Config Save**. The **Config Save** screen appears.

Figure 31 Config Save



14 Click **Save**. The following screen should appear.

Figure 32 Config Save, Save Successful



You can now use the device (with the other settings set to the defaults) to provide service to DSL subscribers. See Chapter 61 on page 471 for information on other default settings.

6

Home and Port Statistics Screens

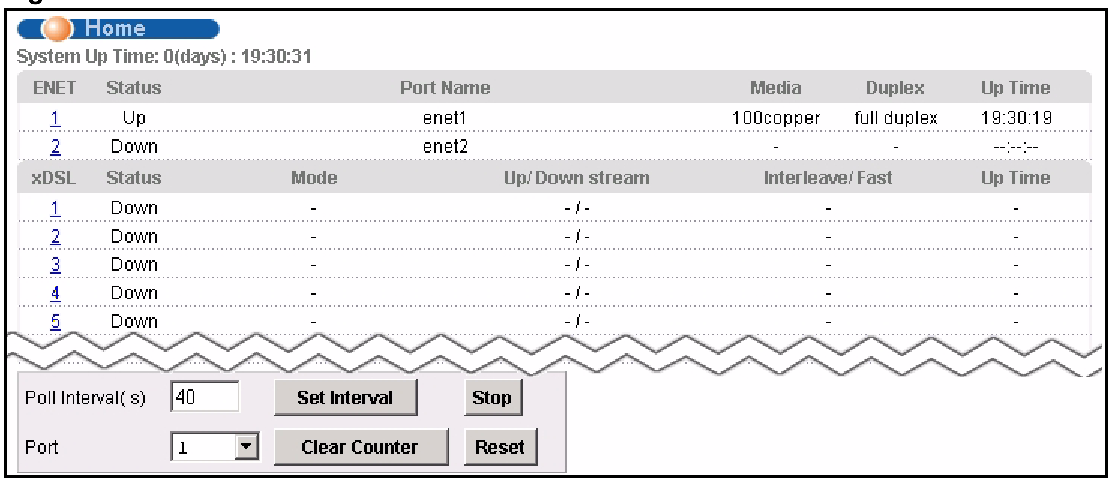
This chapter describes the **Home** (status), **Port Statistics**, and RMON screens.

6.1 Home Screen

The **Home** screen of the web configurator displays a port statistical summary with links to each port showing statistical details.

To open this screen, click **Home** in any web configurator screen.

Figure 33 Home



The following table describes the labels in this screen.

Table 6 Home

LABEL	DESCRIPTION
System up Time	This field shows how long the system has been running since the last time it was started.
	The following fields are related to the Ethernet ports.
ENET	This field displays the number of the Ethernet port. Click a port number to display that port's statistics screen. See Section 6.1.1 on page 74.
Status	This field displays whether the Ethernet port is connected (**Up**) or not (**Down**).
Port Name	This field displays the name of the Ethernet port.

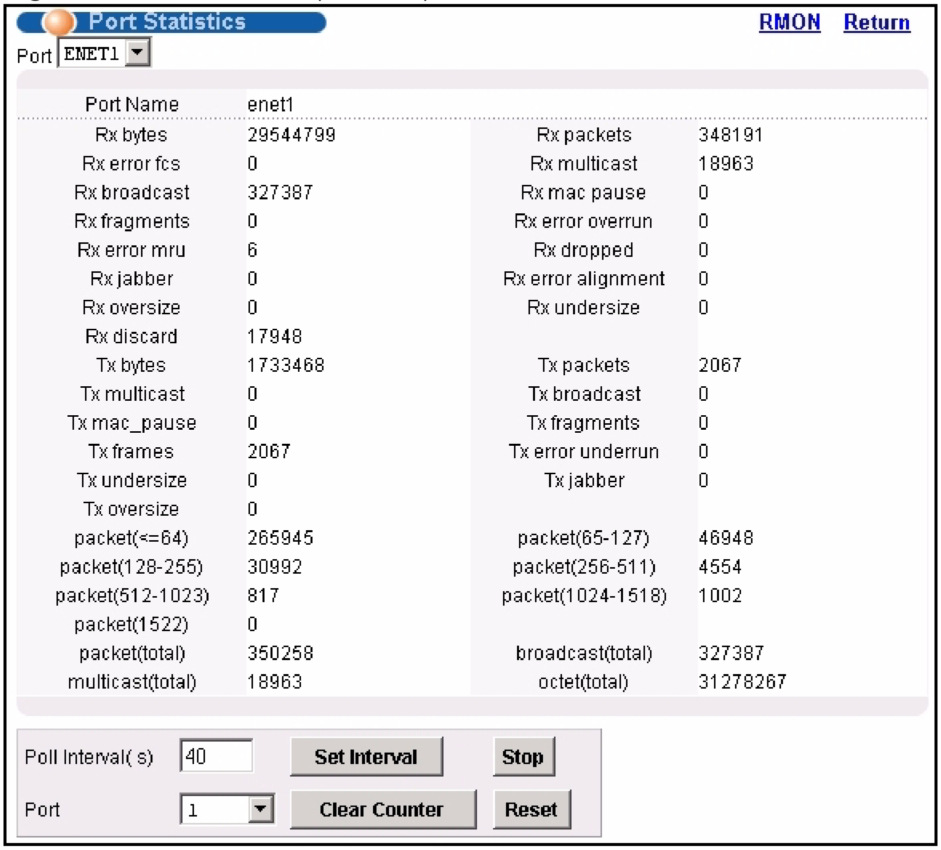
Table 6 Home (continued)

LABEL	DESCRIPTION
Media	This field displays the type of media that this Ethernet port is using for a connection. “**-**“ displays when the port is disabled or not connected.
Duplex	This field displays whether the port is using half or full-duplex communication. “**-**“ displays when the port is disabled or not connected.
Up Time	This field shows the total amount of time in hours, minutes and seconds the port’s connection has been up. “**--:--:--**“ displays when the port is disabled or not connected.
	The following fields are related to the xDSL ports.
xDSL	This identifies the xDSL port. Click a port number to display that port’s statistics screen. See Section 6.1.2 on page 77 for more information.
Status	This field shows whether the port is connected (**Up**) or not (**Down**).
Mode	This field shows which ADSL operational mode the port is set to use. “**-**“ displays when the port is not connected.
Up/Down stream	This field shows the number of kilobits per second that a port is set to transmit and receive.
Interleave/Fast	This field shows the port’s ADSL latency mode (fast or interleave).
Up Time	This field shows the total amount of time in hours, minutes and seconds the port’s connection has been up. “**-**“ displays when the port is not connected.
	The following fields and buttons apply to the whole screen.
Poll Interval(s) Set Interval	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to halt system statistic polling.
Port Clear Counter	Select a port from the **Port** drop-down list box and then click **Clear Counter** to erase the recorded statistical information for that port.
Reset	Click this to set the **Poll Interval(s)** and **Port** fields to their default values and to refresh the screen.

6.1.1 Ethernet Port Statistics Screen

Use this screen to display statistics about an Ethernet port. To open this screen, click an Ethernet port’s number in the **Home** screen.

Figure 34 Port Statistics (Ethernet)



The following table describes the labels in this screen.

Table 7 Port Statistics (Ethernet)

LABEL	DESCRIPTION
RMON	Click this to open the **RMON Statistics** screen.
Return	Click this to go back to the **Home** screen.
Port	Use this drop-down list box to select a port for which you wish to view statistics. This field identifies the port described in this screen.
Port Name	This field displays the name that you have configured for the port.
Rx bytes	This field shows the number of octets of Ethernet frames received that are from 0 to 1518 octets in size, counting the ones in bad packets, not counting framing bits but counting FCS (Frame Check Sequence) octets. An octet is an 8-bit binary digit (byte).
Rx packets	This field shows the number of packets received on this port (including multicast, unicast, broadcast and bad packets).
Rx error fcs	This field shows the number of frames received with an integral length of 64 to 1518 octets and containing a Frame Check Sequence error.
Rx multicast	This field shows the number of good multicast frames received of 64 to 1518 octets in length (for non VLAN) or 1522 octets (for VLAN), not including Broadcast frames. Frames with range or length errors are also not taken into account.
Rx broadcast	This field shows the number of good broadcast frames received of 64 to 1518 octets in length (for non VLAN) or 1522 octets (for VLAN), not including multicast frames. Frames with range or length errors are also not taken into account.

Table 7 Port Statistics (Ethernet) (continued)

LABEL	DESCRIPTION
Rx mac pause	This field shows the number of valid IEEE 802.3x Pause frames received on this port.
Rx fragments	This field shows the number of frames received that were less than 64 octets long, and contained an invalid FCS, including non-integral and integral lengths.
Rx error overrun	This field shows how many times an Ethernet transmitter overrun occurred.
Rx error mru	This field shows the number of received frames that were dropped due to exceeding the Maximum Receive Unit frame size.
Rx dropped	This field shows the number of received frames that were received into the AAM1212, but later dropped because of a lack of system resources.
Rx jabber	This field shows the number of frames received that were longer than 1518 octets (non VLAN) or 1522 octets (VLAN) and contained an invalid FCS, including alignment errors.
Rx error alignment	This field shows the number of frames received that were 64 to 1518 (non VLAN) or 1522 (VLAN) octets long but contained an invalid FCS and a non-integral number of octets.
Rx oversize	This field shows the number of frames received that were bigger than 1518 (non VLAN) or 1522 (VLAN) octets and contained a valid FCS.
Rx undersize	This field shows the number of frames received that were less than 64 octets long and contained a valid FCS.
Rx discard	This field shows the number of frames dropped based on packet filtering.
Tx bytes	This field shows the number of bytes that have been transmitted on this port. This includes collisions but not jam signal or preamble/SFD (Start of Frame Delimiter) bytes.
Tx packets	This field shows the number of packets transmitted on this port.
Tx multicast	This field shows the number of good multicast frames transmitted on this port (not including broadcast frames).
Tx broadcast	This field shows the number of broadcast frames transmitted on this port (not including multicast frames).
Tx mac_pause	This field shows the number of valid IEEE 802.3x Pause frames transmitted on this port.
Tx fragments	This field shows the number of transmitted frames that were less than 64 octets long, and with an incorrect FCS value.
Tx frames	This field shows the number of complete good frames transmitted on this port.
Tx error underrun	This field shows the number of outgoing frames that were less than 64 octets long.
Tx undersize	This field shows the number of frames transmitted that were less than 64 octets long and contained a valid FCS.
Tx jabber	This field shows the number of frames transmitted that were longer than 1518 octets (non VLAN) or 1522 octets (VLAN) and contained an incorrect FCS value.
Tx oversize	This field shows the number of frames transmitted that were bigger than 1518 octets (non VLAN) or 1522 (VLAN) and contained a valid FCS.
packet(<=64)	This field shows the number of frames received and transmitted (including bad frames) that were 64 octets or less in length (this includes FCS octets but excludes framing bits).
packet(65-127)	This field shows the number of frames received and transmitted (including bad frames) that were 65 to 127 octets in length (this includes FCS octets but excludes framing bits).

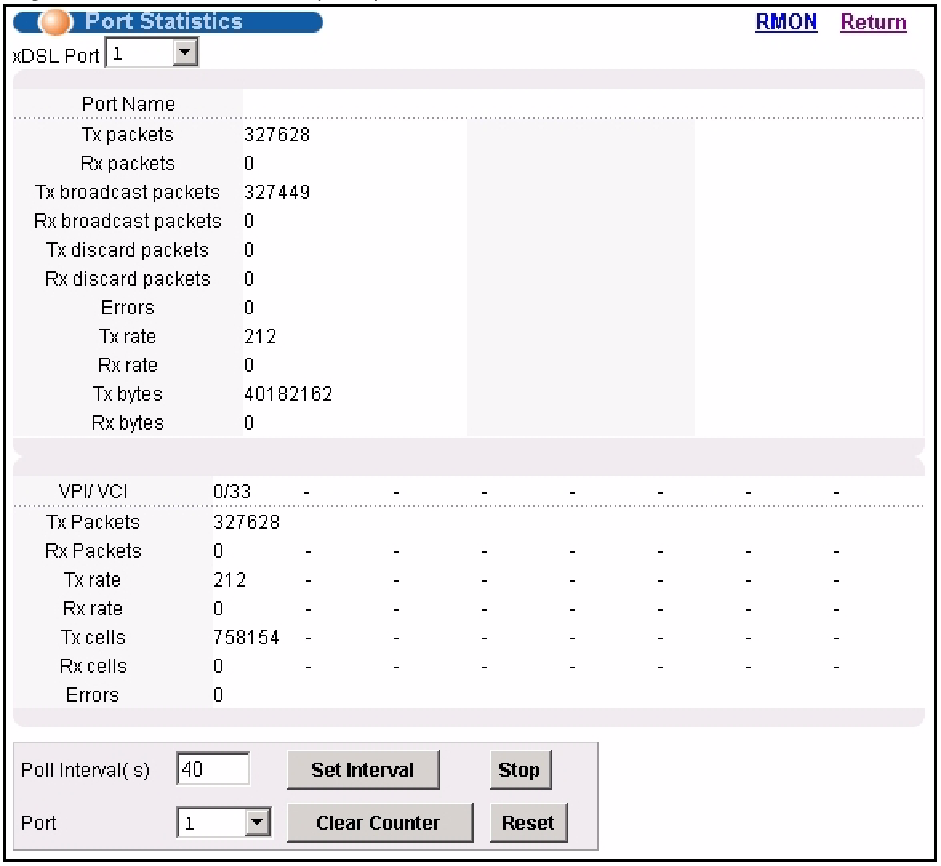
Table 7 Port Statistics (Ethernet) (continued)

LABEL	DESCRIPTION
packet(128-255)	This field shows the number of frames received and transmitted (including bad frames) that were 128 to 255 octets in length (this includes FCS octets but excludes framing bits).
packet(256-511)	This field shows the number of frames received and transmitted (including bad frames) that were 256 to 511 octets in length (this includes FCS octets but excludes framing bits).
packet(512-1023)	This field shows the number of frames received and transmitted (including bad frames) that were 512 to 1023 octets in length (this includes FCS octets but excludes framing bits).
packet(1024-1518)	This field shows the number of frames received and transmitted (including bad frames) that were 1024 to 1518 octets in length (this includes FCS octets but excludes framing bits).
packet(1522)	This field shows the number of frames received and transmitted (including bad frames) that were 1519 to 1522 octets in length (this includes FCS octets but excludes framing bits).
packet(total)	This field shows the total number of received and transmitted packets.
broadcast(total)	This field shows the total number of received and transmitted broadcast frames.
multicast(total)	This field shows the total number of received and transmitted multicast frames.
octet(total)	This field shows the total number of received and transmitted octets (unicast, multicast and broadcast).
Poll Interval(s) Set Interval	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to halt system statistic polling.
Port Clear Counter	Select a port from the **Port** drop-down list box and then click **Clear Counter** to erase the recorded statistical information for that port.
Reset	Click this to set the **Poll Interval(s)** and **Port** fields to their default values and to refresh the screen.

6.1.2 DSL Port Statistics Screen

Use this screen to display statistics about a DSL port. To open this screen, click a DSL port's number in the **Home** screen.

Figure 35 Port Statistics (DSL)



The following table describes the labels in this screen.

Table 8 Port Statistics (DSL)

LABEL	DESCRIPTION
RMON	Click this to open the **RMON Statistics** screen.
Return	Click this to go back to the **Home** screen.
xDSL Port	Use this drop-down list box to select a port for which you wish to view statistics. This field identifies the port described in this screen.
Port Name	This field displays the name that you have configured for the port. If you have not configured a name, it is blank.
Tx packets	This field shows the number of packets transmitted on this port.
Rx packets	This field shows the number of packets received on this port.
Tx broadcast packets	This field shows the number of broadcast packets transmitted on this port.
Rx broadcast packets	This field shows the number of broadcast packets received on this port.
Tx discard packets	This field shows the number of outgoing packets that were dropped on this port. The “Tx discard packets” counter always displays “0” because the AAM1212 does not discard packets that it sends.

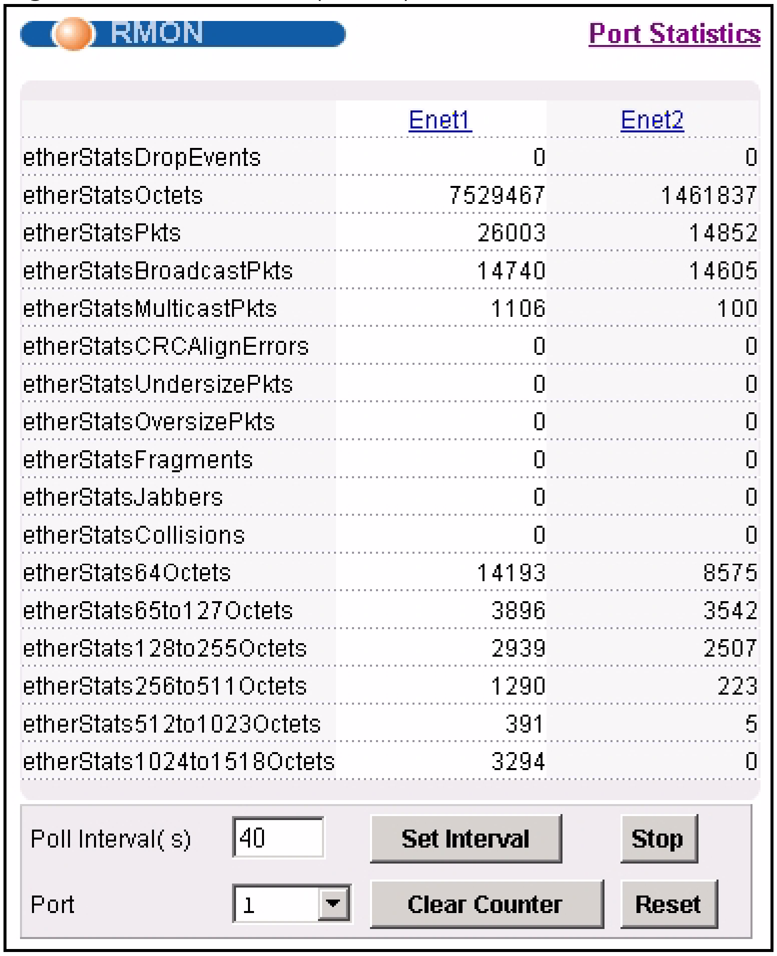
Table 8 Port Statistics (DSL) (continued)

LABEL	DESCRIPTION
Rx discard packets	This field shows the number of received packets that were dropped on this port. Some of the possible reasons for the discarding of received (rx) packets are: • The packet filter is enabled and the packets matched a packet filter. • The MAC filter is enabled and the AAM1212 dropped the packets according to the MAC filter's configuration. • The packets contained frames with an invalid VLAN ID.
Errors	This field shows the number of AAL5 frames received with CRC errors.
Tx rate	This field shows the number of kilobytes per second transmitted on this port.
Rx rate	This field shows the number of kilobytes per second received on this port.
Tx bytes	This field shows the number of bytes that have been transmitted on this port.
Rx bytes	This field shows the number of bytes that have been received on this port.
VPI/VCI	This field displays the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) of channels on this port.
Tx Packets	This field shows the number of packets transmitted on each channel.
Rx Packets	This field shows the number of packets received on each channel.
Tx rate	This field shows the number of bytes per second transmitted on each channel.
Rx rate	This field shows the number of bytes per second received on each channel.
Tx cells	This field shows the number of ATM cells transmitted on each channel.
Rx cells	This field shows the number of ATM cells received on each channel.
Errors	This field shows the number of error packets on each channel.
Poll Interval(s) Set Interval	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to halt system statistic polling.
Port Clear Counter	Select a port from the **Port** drop-down list box and then click **Clear Counter** to erase the recorded statistical information for that port.
Reset	Click this to set the **Poll Interval(s)** and **Port** fields to their default values and to refresh the screen.

6.1.3 RMON Statistics Screen

Use this screen to display RMON statistics about a port. To open this screen, click **RMON** in the **DSL Port Statistics** screen or **Ethernet Port Statistics** screen.

Figure 36 Port Statistics (RMON)



The following table describes the labels in this screen.

Table 9 Port Statistics (RMON)

LABEL	DESCRIPTION
Port Statistics	Click this to go back to the previous screen.
Enet1	Click this to look at the RMON history for this port.
Enet2	Click this to look at the RMON history for this port.
EtherStatsDropEvents	This field displays the total number of packets that were dropped on this port.
EtherStatsOctets	This field displays the total number of octets received/transmitted on this port.
EtherStatsPkts	This field displays the total number of good packets received/ transmitted on this port.
EtherStatsBroadcastPkts	This field displays the total number of broadcast packets received/ transmitted on this port.
EtherStatsMulticastPkts	This field displays the total number of multicast packets received/ transmitted on this port.
EtherStatsCRCAlignErrors	This field displays the total number of CRC (Cyclical Redundancy Check) alignment errors on this port.

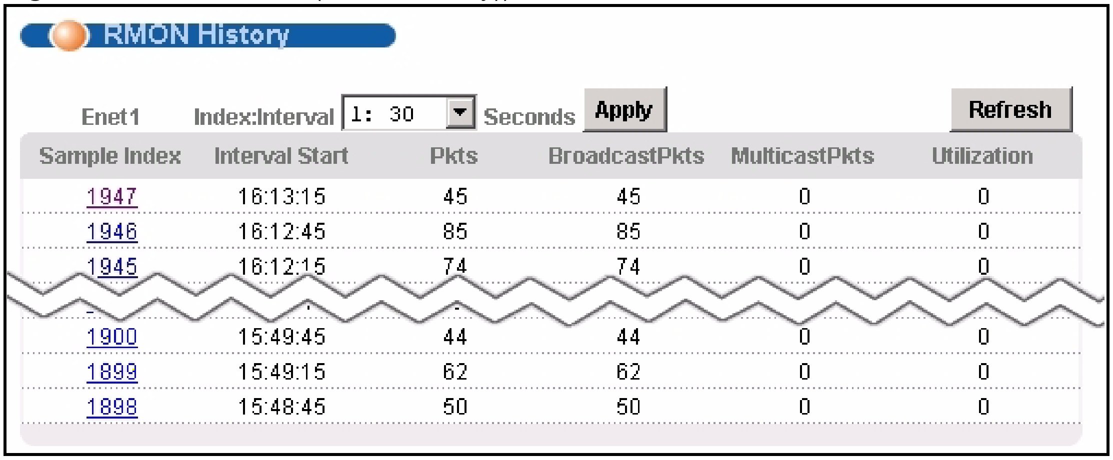
Table 9 Port Statistics (RMON) (continued)

LABEL	DESCRIPTION
EtherStatsUndersizePkts	This field displays the total number of packets that were too small received/transmitted on this port.
EtherStatsOversizePkts	This field displays the total number of packets that were too big received/transmitted on this port.
EtherStatsFragments	This is the number of frames received/transmitted that were less than 64 octets long, and contained an invalid FCS, including non-integral and integral lengths.
EtherStatsJabbers	This is the number of frames received/transmitted that were longer than 1518 octets (non VLAN) or 1522 octets (VLAN) and contained an invalid FCS, including alignment errors.
EtherStatsCollisions	This is the number of frames for which transmission failed due to excessive collisions. Excessive collision is defined as the number of maximum collisions before the retransmission count is reset.
EtherStats64Octets	This is the number of frames received/transmitted (including bad frames) that were 64 octets or less in length (this includes FCS octets but excludes framing bits).
EtherStats65to127Octets	This is the number of frames received/transmitted (including bad frames) that were 65 to 127 octets in length (this includes FCS octets but excludes framing bits).
EtherStats128to255Octets	This is the number of frames received and transmitted (including bad frames) that were 128 to 255 octets in length (this includes FCS octets but excludes framing bits).
EtherStats256to511Octets	This is the number of frames received/transmitted (including bad frames) that were 256 to 511 octets in length (this includes FCS octets but excludes framing bits).
EtherStats512to1023Octets	This is the number of frames received/transmitted (including bad frames) that were 512 to 1023 octets in length (this includes FCS octets but excludes framing bits).
EtherStats1024to1518Octets	This is the number of frames received/transmitted (including bad frames) that were 1024 to 1518 octets in length (this includes FCS octets but excludes framing bits).
Poll Interval(s) Set Interval	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to halt system statistic polling.
Port Clear Counter	Select a port from the **Port** drop-down list box and then click **Clear Counter** to erase the recorded statistical information for that port.
Reset	Click this to set the **Poll Interval(s)** and **Port** fields to their default values and to refresh the screen.

6.1.4 RMON History Screen

Use this screen to display general information (such as sample time) on history samples. To open this screen, click any port number in the **RMON Statistics** screen.

Figure 37 Port Statistics (RMON History))



The following table describes the labels in this screen.

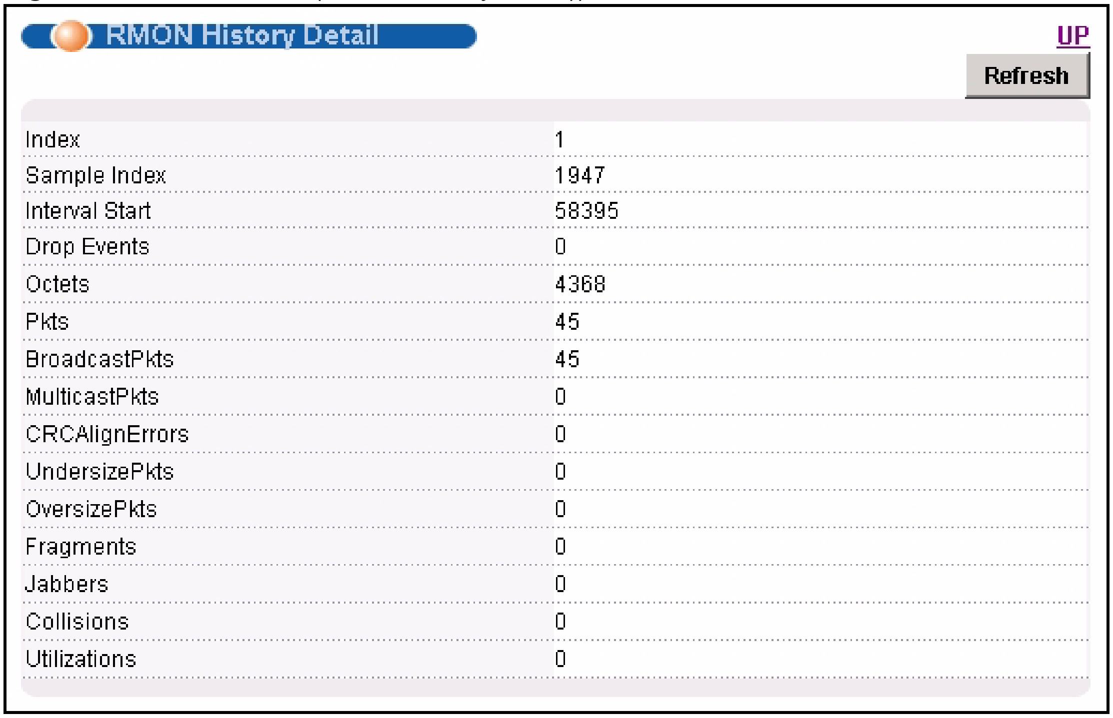
Table 10 Port Statistics (RMON History)

LABEL	DESCRIPTION
Index:Interval	Select the index of the sample interval and the desired data sampling time (in seconds).
Apply	Click this to use the selected data sampling time.
Refresh	Click this to update this screen.
Sample Index	This field display the sample number.
Interval Start	This field displays the data sampling time.
Pkts	This field displays the number of packets received or transmitted since the last sample time.
BroadcastPkts	This field displays the number of broadcast packets received or transmitted since the last sample time.
MulticastPkts	This field displays the number of multicast packets received/transmitted since the last sample time.
Utilization	This field displays the port utilization status.

6.1.5 RMON History Detail Screen

Use this screen to display detailed RMON history. To open this screen, click any index number in the **RMON History** screen.

Figure 38 Port Statistics (RMON History Detail))



The following table describes the labels in this screen.

Table 11 Port Statistics (RMON History Detail)

LABEL	DESCRIPTION
UP	Click this to return to the previous screen.
Refresh	Click this to update this screen.
Index	This field displays the index of the sample interval.
Sample Index	This field displays the sample number.
Interval Start	This field displays the data sampling time.
Drop Events	This field displays the total number of packets that were dropped in the sampling period.
Octets	This field displays the total number of octets received/transmitted in the sampling period.
Pkts	This field displays the total number of good packets received/transmitted in the sampling period.
BroadcastPkts	This field displays the total number of broadcast packets received/transmitted in the sampling period.
MulticastPkts	This field displays the total number of multicast packets received/transmitted in the sampling period.
CRCAlignErrors	This field displays the total number of CRC (Cyclical Redundancy Check) alignment errors in the sampling period.
UndersizePkts	This field displays the total number of packets that were too small received/ transmitted in the sampling period.
OversizePkts	This field displays the total number of packets that were too big received/ transmitted in the sampling period.

Table 11 Port Statistics (RMON History Detail) (continued)

LABEL	DESCRIPTION
Fragments	This is the number of frames received/transmitted that were less than 64 octets long, and contained an invalid FCS, including non-integral and integral lengths.
Jabbers	This is the number of frames received/transmitted that were longer than 1518 octets (non VLAN) or 1522 octets (VLAN) and contained an invalid FCS, including alignment errors.
Collisions	This is the number of frames for which transmission failed due to excessive collisions. Excessive collision is defined as the number of maximum collisions before the retransmission count is reset.
Utilizations	This field displays the port utilization status in the sampling period.

PART II
Basic Settings

System Information (87)
General Setup (91)
User Account (93)
Switch Setup (97)
IP Setup (103)
ENET Port Setup (105)
xDSL Port Setup (107)
xDSL Profiles Setup (125)
xDSL Line Data (139)

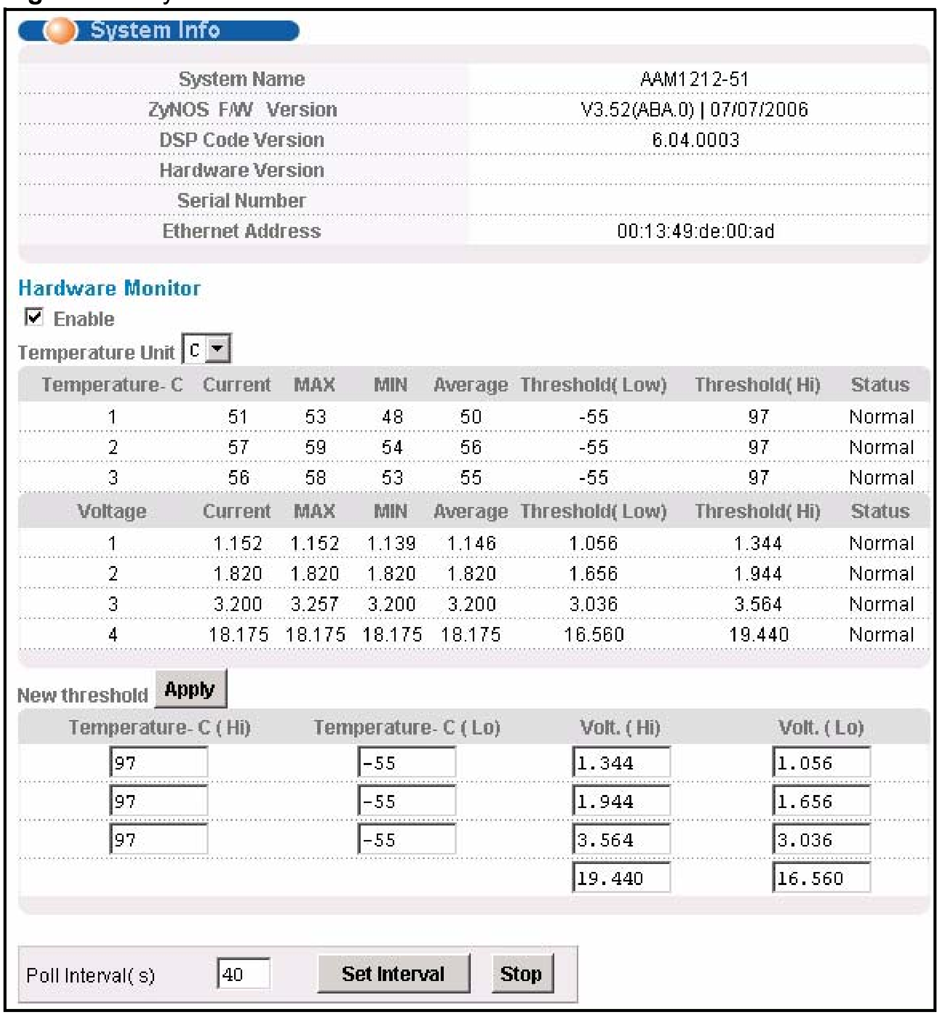
7

System Information

The **System Information** screen displays general device information (such as firmware version number) and hardware polling information (such as temperature status). You can check the firmware version number and monitor the hardware status in this screen.

To open this screen, click **Basic Setting**, **System Information**.

Figure 39 System Info



The following table describes the labels in this screen.

Table 12 System Info

LABEL	DESCRIPTION
System Name	This field displays the device's model name.
ZyNOS F/W Version	This field displays the version number of the device’s current firmware including the date created.
DSP Code Version	This field displays the Digital Signal Processor firmware version number. This is the modem code firmware.
Hardware Version	This is the version of the physical device hardware. This field may be blank.
Serial Number	This is the individual identification number assigned to the device at the factory. This field may be blank.
Ethernet Address	This field refers to the Ethernet MAC (Media Access Control) address of the device.
Hardware Monitor	
Enable	Select this check box to turn the hardware monitor on or clear it to turn the hardware monitor off.
Temperature Unit	Select **C** to display all temperature measurements in degrees Celsius. Select **F** to display all temperature measurements in degrees Fahrenheit.
Temperature	Each temperature sensor can detect and report the temperature. Temperature sensor 1 is near the DSL chipset. Temperature sensor 2 is near the central processing unit. Temperature sensor 3 is at the hardware monitor chip.
Current	This shows the current temperature at this sensor.
MAX	This field displays the maximum temperature measured at this sensor.
MIN	This field displays the minimum temperature measured at this sensor.
Average	This field displays the average temperature measured at this sensor.
Threshold (Low)	This field displays the lowest temperature limit at this sensor.
Threshold (Hi)	This field displays the highest temperature limit at this sensor.
Status	This field displays **Normal** for temperatures below the threshold and **Over** for those above.
Voltage(V)	The power supply for each voltage has a sensor that can detect and report the voltage.
Current	This is the current voltage reading.
MAX	This field displays the maximum voltage measured at this point.
MIN	This field displays the minimum voltage measured at this point.
Average	This field displays the average voltage measured at this sensor.
Threshold (Low)	This field displays the lowest voltage limit at this sensor.
Threshold (Hi)	This field displays the highest voltage limit at this sensor.
Status	**Normal** indicates that the voltage is within an acceptable operating range at this point; otherwise **Abnormal** is displayed.
	Use this section of the screen to configure the hardware monitor threshold settings.
New threshold Apply	Configure new threshold settings in the fields below and click **Apply** to use them.
Temperature (Hi)	Use these fields to configure the highest temperature limit at each sensor.

Table 12 System Info (continued)

LABEL	DESCRIPTION
Temperature (Lo)	Use these fields to configure the lowest temperature limit at each sensor.
Volt. (Hi)	Use these fields to configure the highest voltage limit at each sensor.
Volt. (Lo)	Use these fields to configure the lowest voltage limit at each sensor.
Poll Interval(s) Set Interval	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to halt statistic polling.

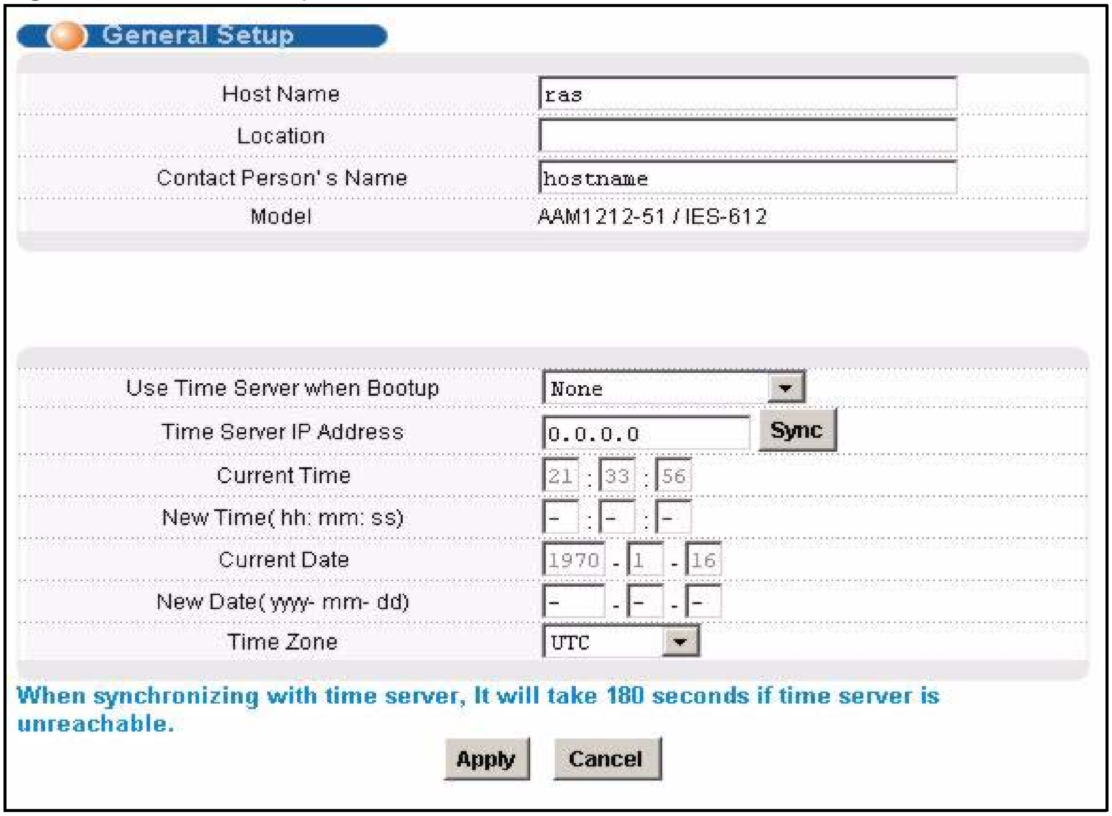
8

General Setup

The **General Setup** screen allows you to configure general device identification information. It also allows you to set the system time manually or get the current time and date from an external server when you turn on your device. The real time is then displayed in the logs.

To open this screen, click **Basic Setting**, **General Setup**.

Figure 40 General Setup



The following table describes the labels in this screen.

Table 13 General Setup

LABEL	DESCRIPTION
Host Name	Choose a descriptive name for identification purposes. This name consists of up to 31 ASCII characters; spaces are allowed.
Location	Enter the geographic location of your device. You can use up to 31 ASCII characters; spaces are allowed.
Contact Person's Name	Enter the name of the person in charge of this device. You can use up to 31 ASCII characters; spaces are allowed.
Model	This field displays your device type.
Use Time Server When Bootup	Select the time service protocol that the timeserver uses. Not all time servers support all protocols, so you may have to use trial and error to find a protocol that works. The main differences between them are the time format. When you select the **Daytime (RFC 867)** format, the switch displays the day, month, year and time with no time zone adjustment. When you use this format it is recommended that you use a Daytime timeserver within your geographical time zone. **Time (RFC-868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. **NTP (RFC-1305)** is similar to Time (RFC-868). **None** is the default value. Enter the time manually. Each time you turn on the device, the time and date will be reset to 2000-1-1 0:0.
Time Server IP Address	Enter the IP address of your timeserver. The device searches for the timeserver for up to 60 seconds.
Current Time	This field displays the time you open this menu (or refresh the menu).
New Time (hh:min:ss)	Enter the new time in hour, minute and second format. The new time then appears in the **Current Time** field after you click **Apply**.
Current Date	This field displays the date you open this menu.
New Date (yyyy-mm-dd)	Enter the new date in year, month and day format. The new date then appears in the **Current Date** field after you click **Apply**.
Time Zone	Select the time difference between UTC (Universal Time Coordinated, formerly known as GMT, Greenwich Mean Time) and your time zone from the drop-down list box.
Apply	Click **Apply** to save your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to start configuring the screen again.

9

User Account

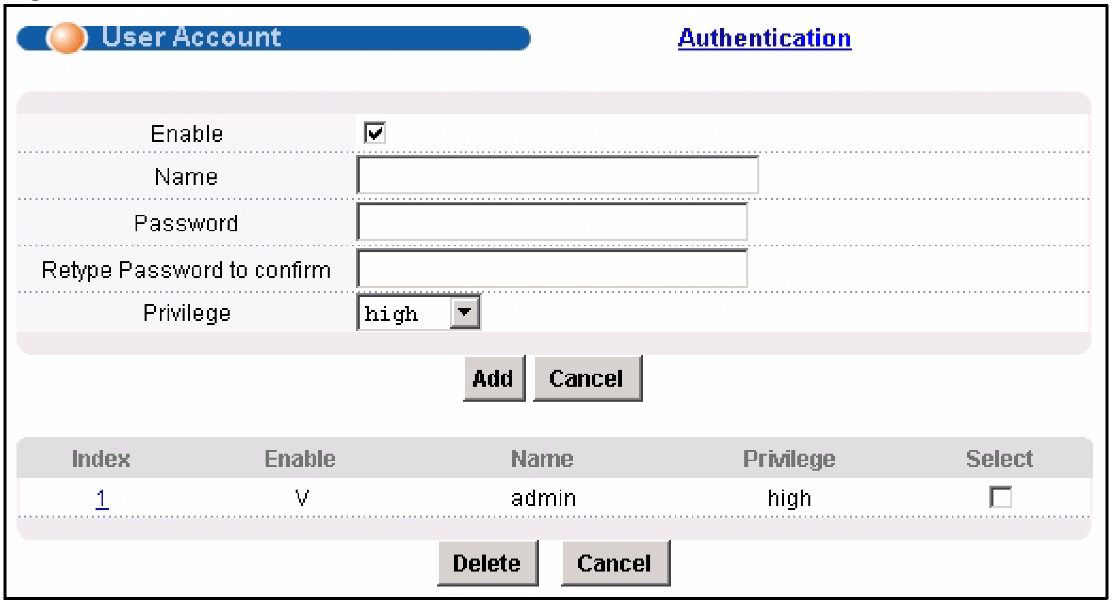
The **User Account** screens allows you to set up and configure system administrator accounts for the AAM1212. You can also configure the authentication policy for AAM1212 administrators. This is different from port authentication in Chapter 23 on page 185.

See Chapter 23 on page 185 for background information on authentication.

9.1 User Account Screen

To open this screen, click **Basic Setting**, **User Account**.

Figure 41 User Account



The following table describes the labels in this screen.

Table 14 User Account

LABEL	DESCRIPTION
Authentication	Click this to open the **Authentication** screen. See Section 9.2 on page 94.
Enable	Select this check box to turn on the administrator account.
Name	Enter a user name for the administrator account.

Table 14 User Account (continued)

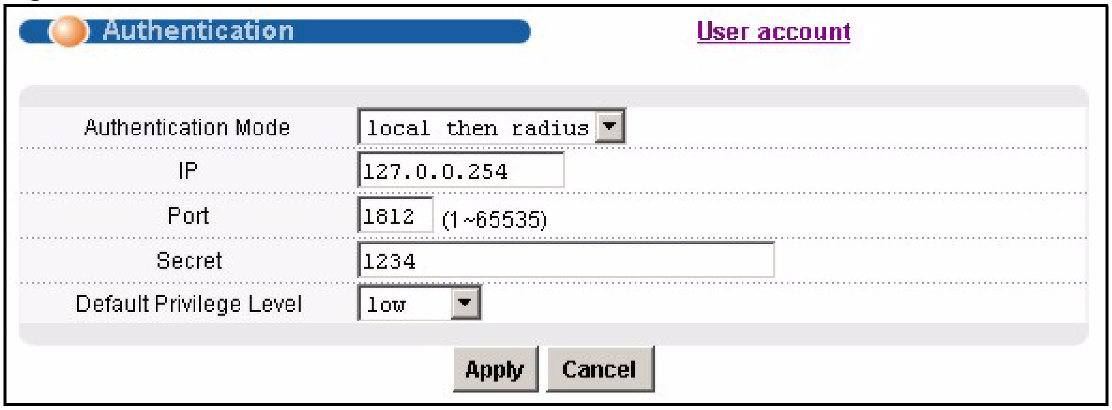
LABEL	DESCRIPTION
Password	Enter a password for the administrator account.
Retype Password to Confirm	Re-enter the administrator account's password to verify that you have entered it correctly.
Privilege	Select a privilege level to determine which screens the administrator can use. There is a high, medium or low privilege level for each command. Select **high** to allow the administrator to use all commands including the lower privilege commands. High privilege commands include things like creating administrator accounts, restarting the system and resetting the factory defaults. Select **middle** to allow the administrator to use middle or low privilege commands. Select **low** to allow the administrator to use only low privilege commands. Low privilege commands are read only.
Add	Click **Add** to save your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring the fields again.
Index	This field displays the number of the user account. Click an account's index number to use the top of the screen to edit it.
Enable	This field displays a "V " if you have the administrator account turned on. It displays a "-" if the administrator account is turned off.
Name	This field displays the administrator account's user name.
Privilege	This field displays the administrator account's access level (high, middle or low).
Select	Select this check box and click the **Delete** button to remove an administrator account.
Delete	Select an administrator account's check box and click this button to remove the administrator account.
Cancel	Click **Cancel** to start configuring the screen afresh.

9.2 Authentication Screen

Use this screen to set up the authentication policies and settings by which administrators can access the AAM1212.

To open this screen, click **Basic Setting**, **User Account**, **Authentication**.

Figure 42 Authentication



The following table describes the labels in this screen.

Table 15 User Account

LABEL	DESCRIPTION
User account	Click this to open the **User Account** screen. See Section 9.1 on page 93.
Authentication Mode	Select the process by which the AAM1212 authenticates administrators. **local** - Search the local database. You maintain this database in the **User Account** screen. **radius** - Check an external RADIUS database using the settings below. **local then radius** - Search the local database; if the user name is not found, check an external RADIUS database using the settings below.
IP	Enter the IP address of the external RADIUS server in dotted decimal notation.
Port	The default UDP port of the RADIUS server for authentication is **1812**. You need not change this value unless your network administrator instructs you to do so.
Secret	Specify a password (up to 31 alphanumeric characters) as the key to be shared between the external RADIUS server and the switch. This key is not sent over the network. This key must be the same on the external RADIUS server and the switch.
Default Privilege Level	Select the privilege level assigned to administrators in case the external RADIUS database does not provide one. The privilege level determines which screens the administrator can use. There is a high, medium or low privilege level for each command. You can also choose to deny access to the AAM1212. Select **high** to allow the administrator to use all commands including the lower privilege commands. High privilege commands include things like creating administrator accounts, restarting the system and resetting the factory defaults. Select **middle** to allow the administrator to use middle or low privilege commands. Select **low** to allow the administrator to use only low privilege commands. Low privilege commands are read only. Select **deny** to prevent the administrator from accessing the AAM1212.

10

Switch Setup

The **Switch Setup** screen allows you to set up and configure global device features.

10.1 GARP Timer Setup

GARP (Generic Attribute Registration Protocol) allows network devices to register and de-register attribute values with other GARP participants within a bridged LAN. GARP is a protocol that provides a generic mechanism for protocols that serve a more specific application, for example, GVRP (GARP VLAN Registration Protocol). GARP and GVRP are the protocols used to automatically register VLAN membership across switches.

Switches join VLANs by making a declaration. A declaration is made by issuing a **Join** message using GARP. Declarations are withdrawn by issuing a **Leave** message. A **Leave All** message terminates all registrations. GARP timers set declaration timeout values.

10.2 Switch Modes

The AAM1212 supports standalone and daisychain switch modes.

10.2.1 Standalone Switch Mode

"Standalone switch mode" relates to the AAM1212's operational behavior, not a standalone network topology. The standalone switch mode allows either or both of the AAM1212's Ethernet ports to connect to the backbone Ethernet network. You can also connect one of the AAM1212's Ethernet ports to the Ethernet network and the other to another AAM1212 (see Figure 43 on page 98 for an example). When the AAM1212 is in standalone mode, you can use it in a network topology that uses loops (you should also enable RSTP). You can have multiple AAM1212 connected on the same network and set both of them to use standalone mode in order to use them with a network topology that uses loops.

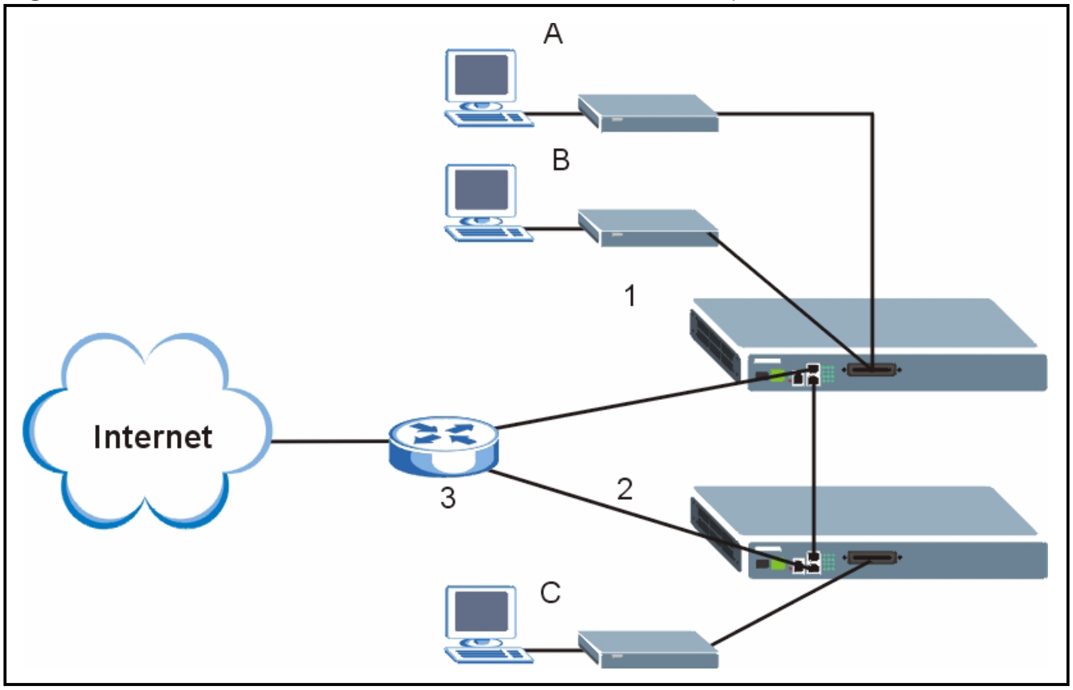
Standalone switch mode with port isolation enabled blocks communications between subscriber ports on an individual AAM1212. However, one AAM1212's subscribers can communicate with another AAM1212's subscribers if the two AAM1212's Ethernet ports are connected to each other (see Figure 43 on page 98 for an example). If you have multiple AAM1212 connected on the same network and set to standalone mode, they do not all need to have the same port isolation setting.

10.2.2 Port Isolation with Standalone Switch Mode Example

The following graphic shows AAM1212 **1** and **2** connected to each other and the Ethernet backbone switch (**3**) in a network topology that creates a loop. The AAM1212 are using the standalone switch mode and have RSTP enabled.

In this example, both AAM1212 have port isolation turned on. Communications between **A** and **B** must first go through another switch (**3** in the figure). However, **A** and **B** can communicate with **C** without their communications going through another switch or router.

Figure 43 Port Isolation with Standalone Switch Mode Example



10.2.3 Daisychain Switch Mode

Daisychain switch mode sets the AAM1212 to use Ethernet port one (ENET 1) as an uplink port to connect to the Ethernet backbone and Ethernet port two (ENET 2) to connect to another (daisychained or subtending) AAM1212. The daisychain switch mode is recommended for use in a network topology that does not have loops. When you daisychain multiple AAM1212 they must all be set to daisychain mode.

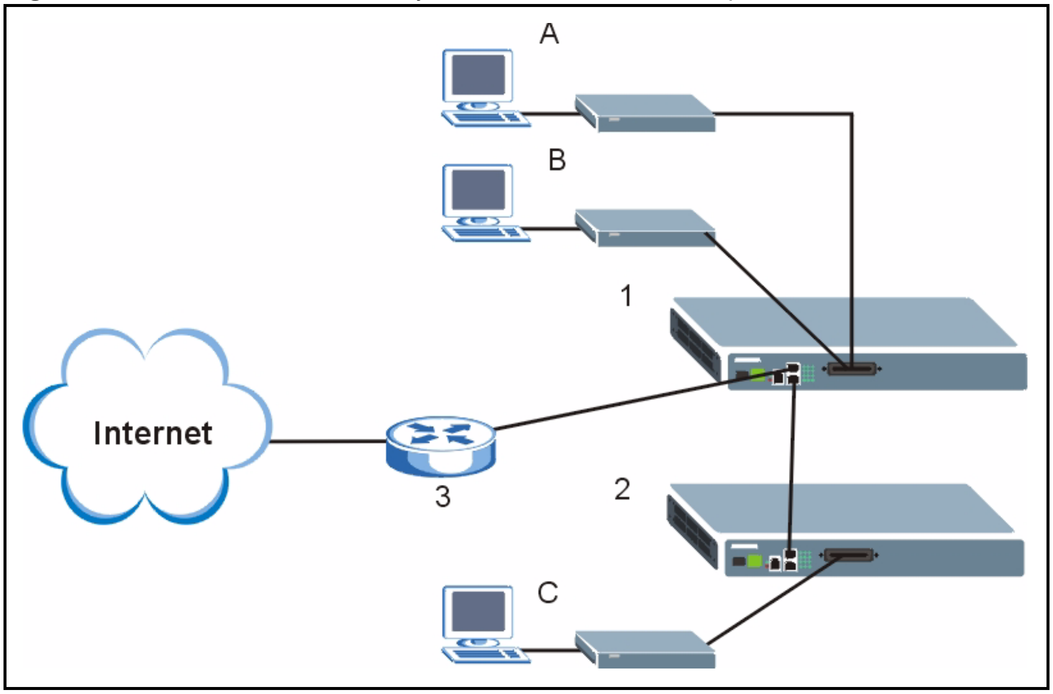
Daisychain switch mode with port isolation enabled blocks communications between subscriber ports on an individual AAM1212 and between the subscribers of any daisychained AAM1212 (see Figure 44 on page 99 for an example). Use the same port isolation setting on all AAM1212 that you set up in a daisychain.

10.2.4 Port Isolation with Daisychain Switch Mode Example

In the example below, the AAM1212 1 has its Ethernet port one (ENET 1) connected to the Ethernet backbone switch (**3**) and it's Ethernet port two (ENET2) connected to Ethernet port one (ENET 1) of the daisychained AAM1212 (**2**).

With port isolation turned on, communications between **A** and **B** must first go through another switch or router (**3** in the figure). **A** and **B** also cannot communicate with **C** without their communications going through another switch or router.

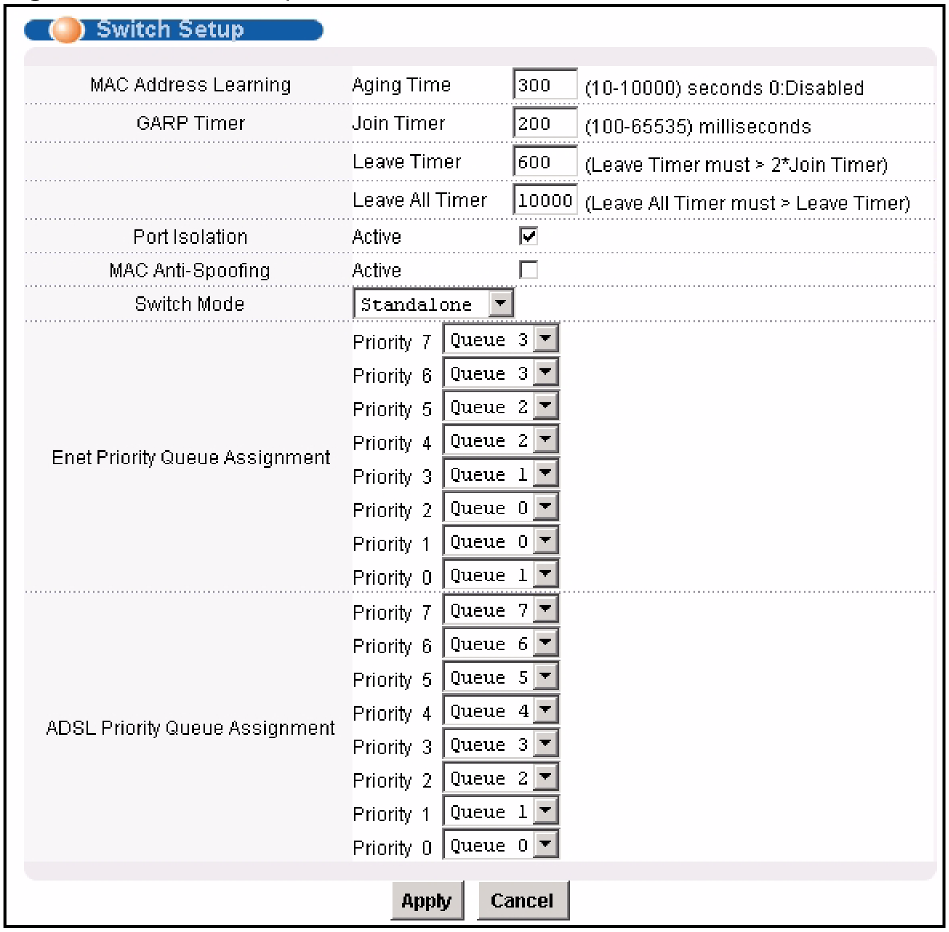
Figure 44 Port Isolation with Daisychain Switch Mode Example



10.3 Switch Setup Screen

To open this screen, click **Basic Setting**, **Switch Setup**.

Figure 45 Switch Setup



The following table describes the labels in this screen.

Table 16 Switch Setup

LABEL	DESCRIPTION
MAC Address Learning Aging Time	Enter a time from 10 to 10,000 seconds. This is how long all dynamically learned MAC addresses remain in the MAC address table before they age out (and must be relearned). Enter 0 to disable the aging out of MAC addresses.
	GARP Timer: Switches join VLANs by making a declaration. A declaration is made by issuing a Join message using GARP. Declarations are withdrawn by issuing a Leave message. A Leave All message terminates all registrations. GARP timers set declaration timeout values. Click here for more information on VLANs.
Join Timer	**Join Timer** sets the duration of the Join Period timer for GVRP in milliseconds. Each port has a Join Period timer. The allowed Join Time range is between 100 and 65535 milliseconds; the default is 200 milliseconds.
Leave Timer	**Leave Timer** sets the duration of the Leave Period timer for GVRP in milliseconds. Each port has a single Leave Period timer. Leave Time must be two times larger than Join Timer; the default is 600 milliseconds.
Leave All Timer	**Leave All Timer** sets the duration of the Leave All Period timer for GVRP in milliseconds. Each port has a single Leave All Period timer. Leave All Timer must be larger than Leave Timer.

Table 16 Switch Setup (continued)

LABEL	DESCRIPTION
Port Isolation Active	Turn on port isolation to block communications between subscriber ports. When you enable port isolation you do not need to configure the VLAN to isolate subscribers.
MAC Anti-Spoofing	Select this if you want the AAM1212 to generate an alarm and issue a SNMP trap when an existing MAC address appears on another port.
Switch Mode	Select **Standalone** to use both of the AAM1212's Ethernet ports (ENET 1 and ENET 2) as uplink ports. **Note:** Standalone mode is recommended for network topologies that use loops. Use **Daisychain** mode to cascade (daisychain) multiple AAM1212. The AAM1212 uses Ethernet port one (ENET 1) as an uplink port to connect to the Ethernet backbone and uses Ethernet port two (ENET 2) to connect to another (daisychained or subtending) AAM1212. **Note:** Daisychain mode is recommended for network topologies that do not use loops.
Priority Queue Assignment	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Frames without an explicit priority tag are given the default priority of the ingress port. Use the next two fields to configure the priority level-to-physical queue mapping. The device has 4 physical queues that you can map to the 8 priority levels for outgoing Ethernet traffic. The device has 8 physical queues that you can map to the 8 priority levels for outgoing DSL traffic. Traffic assigned to higher index queues gets through the device faster while traffic in lower index queues is dropped if the network is congested.
Priority Level	The following descriptions are based on the traffic types defined in the IEEE 802.1d standard (which incorporates IEEE 802.1p).
Priority 7	Typically used for network control traffic such as router configuration messages.
Priority 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Priority 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Priority 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Priority 3	Typically used for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay.
Priority 2	This is for "spare bandwidth".
Priority 1	This is typically used for non-critical "background" traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Priority 0	Typically used for best-effort traffic.
Apply	Click **Apply** to save your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

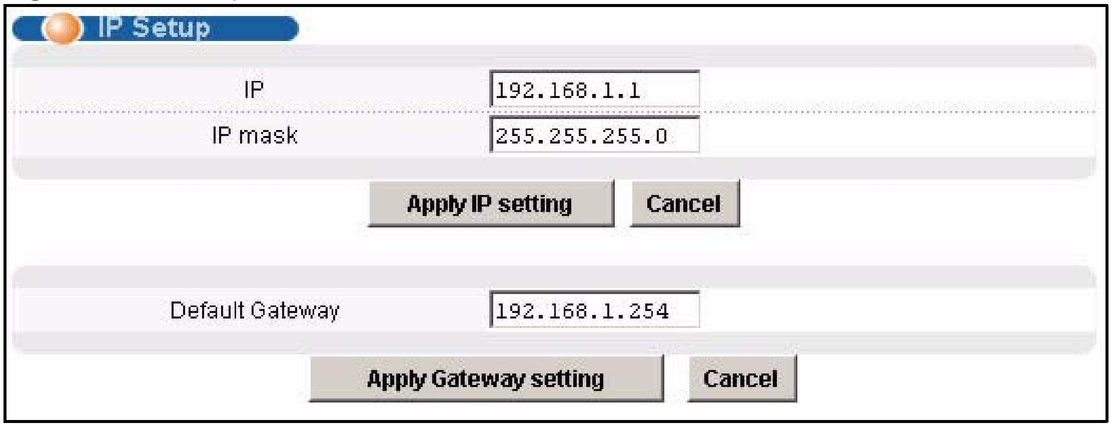
11

IP Setup

The **IP Setup** screen allows you to configure a device IP address, subnet mask and DNS (domain name server) for management purposes.

To open this screen, click **Basic Setting**, **IP Setup**.

Figure 46 IP Setup



The following table describes the labels in this screen.

Table 17 IP Setup

LABEL	DESCRIPTION
IP	Enter the IP address of your AAM1212 in dotted decimal notation for example 1.2.3.4.
IP Mask	Enter the IP subnet mask of your AAM1212 in dotted decimal notation for example 255.255.255.0.
Apply IP setting	Click **Apply IP setting** to save your changes to the device's IP address and/or subnet mask to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring the fields again.
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation.

Table 17 IP Setup (continued)

LABEL	DESCRIPTION
Apply Gateway setting	Click **Apply Gateway setting** to save your changes to the device’s IP address and/or subnet mask to the AAM1212’s volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring the fields again.

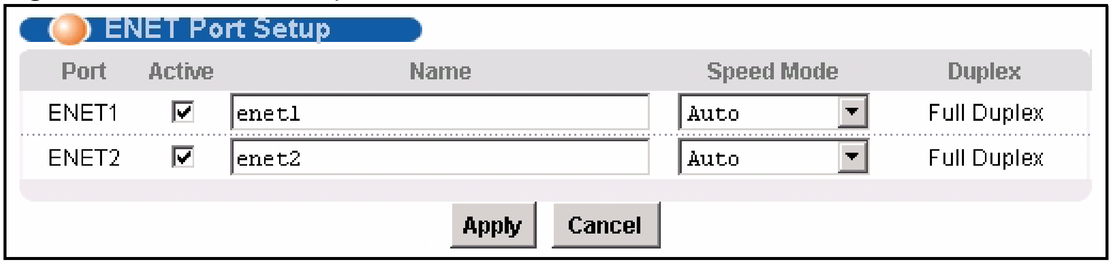
12

ENET Port Setup

The **ENET Port Setup** screen allows you to configure settings for the Ethernet ports.

To open this screen, click **Basic Setting**, **ENET Port Setup**.

Figure 47 ENET Port Setup



The following table describes the labels in this screen.

Table 18 ENET Port Setup

LABEL	DESCRIPTION
Port	This is the port index number.
Active	Select the check box to turn on the port. Clear it to disable the port.
Name	Enter a descriptive name that identifies this port. You can use up to 31 ASCII characters; spaces are allowed.
Speed Mode	Select the type of Ethernet connection for this port. When you don't use auto-negotiation, you must make sure that the settings of the peer Ethernet port are the same in order to connect. Select **Auto** (auto-negotiation) to have the AAM1212 automatically determine the type of connection that the Ethernet port has. When the peer Ethernet device has auto-negotiation turned on, the AAM1212 negotiates with the peer to determine the connection speed. If the peer Ethernet port does not have auto-negotiation turned on, the AAM1212 determines the connection speed by detecting the signal on the cable and using full duplex. Select **10 Copper** if the Ethernet port has a 10 MB electrical connection. Select **100 Copper** if the Ethernet port has a 100 MB electrical connection.
Duplex	The AAM1212 uses full duplex Ethernet connections by default.
Apply	Click **Apply** to save your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

13

xDSL Port Setup

This chapter explains how to configure settings for profiles and individual ADSL ports. It also covers how to configure virtual channels and virtual channel profiles.

13.1 ADSL Standards Overview

These are the ADSL standards and rates that the AAM1212 supports at the time of writing. The actual transfer rates will vary depending on what the subscriber's device supports, the line conditions and the connection distance.

Table 19 ADSL Standards Maximum Transfer Rates

STANDARD	MAXIMUM DOWNSTREAM	MAXIMUM UPSTREAM
G.dmt (AAM1212-51)	8160 Kbps	1024 Kbps
G.dmt Annex B (AAM1212-53)	8160 Kbps	1024 Kbps
ETSI (AAM1212-53)	8160 Kbps	1024 Kbps
ANSI T1.413 issue 2 (AAM1212-51)	8160 Kbps	1024 Kbps
ADSL2	12000 Kbps	1200 Kbps
ADSL2 Annex M (AAM1212-51)	12000 Kbps	2400 Kbps
ADSL2+	25000 Kbps	1200 Kbps
ADSL2+ Annex M (AAM1212-51)	25000 Kbps	2400 Kbps

13.2 Downstream and Upstream

Downstream refers to traffic going out from the AAM1212 to the subscriber's ADSL modem or router. Upstream refers to traffic coming into the AAM1212 from the subscriber's ADSL modem or router.

13.3 Profiles

A profile is a table that contains a list of pre-configured ADSL settings. Each ADSL port has one (and only one) profile assigned to it at any given time. You can configure multiple profiles, including profiles for troubleshooting. Profiles allow you to configure ADSL ports efficiently. You can configure all of the ADSL ports with the same profile, thus removing the need to configure the ADSL ports one-by-one. You can also change an individual ADSL port by assigning it a different profile.

For example, you could set up different profiles for different kinds of accounts (for example, economy, standard and premium). Assign the appropriate profile to an ADSL port and it takes care of a large part of the port's configuration maximum and minimum transfer rates. You still get to individually enable or disable each port, as well as configure its channels and operational mode.

13.4 Interleave Delay

Interleave delay is the wait (in milliseconds) that determines the size of a single block of data to be interleaved (assembled) and then transmitted. Interleave delay is used when transmission error correction (Reed- Solomon) is necessary due to a less than ideal telephone line. The bigger the delay, the bigger the data block size, allowing better error correction to be performed.

Reed-Solomon codes are block-based error correcting codes with a wide range of applications. The Reed-Solomon encoder takes a block of digital data and adds extra "redundant" bits. The Reed-Solomon decoder processes each block and attempts to correct errors and recover the original data.

13.4.1 Fast Mode

Fast mode means no interleaving takes place and transmission is faster (a "fast channel"). This would be suitable if you have a good line where little error correction is necessary.

13.5 Configured Versus Actual Rate

You configure the maximum rate of an individual ADSL port by modifying its profile (see Chapter 14 on page 125) or assigning the port to a different profile (see Section 13.7.1 on page 111). However, due to noise and other factors on the line, the actual rate may not reach the maximum that you specify.

Even though you can specify arbitrary numbers using the Edit Profile screen, the actual rate is always a multiple of 32 Kbps. If you enter a rate that is not a multiple of 32 Kbps, the actual rate will be the next lower multiple of 32Kbps. For instance, if you specify 60 Kbps for a port, the actual rate for that port will not exceed 32 Kbps, and if you specify 66 Kbps, the actual rate will not be over 64Kbps.

Regardless of a profile's configured upstream and downstream rates, the AAM1212 automatically limits the actual rates for each individual port to the maximum speeds supported by the port's ADSL operational mode. For example, if you configure a profile with a maximum downstream rate of 25000 Kbps, and apply it to a port set to use G.dmt, the AAM1212 automatically uses a maximum downstream rate of 8160 Kbps. This means that if you configure a profile with very high rates, you can still use it with any port. See Table 19 on page 107 for a list of the maximum rates supported by the different ADSL standards.

13.6 Default Settings

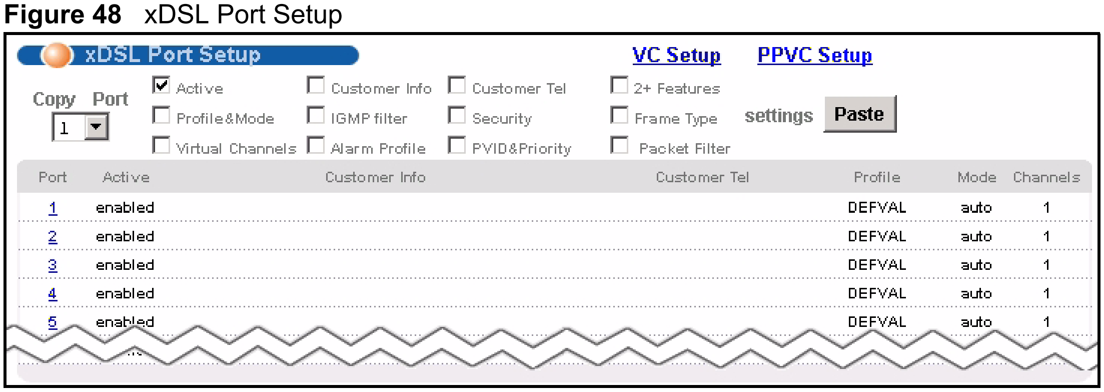
The default profile always exists and all of the ADSL ports use the default profile settings when the AAM1212 is shipped. The default profile's name is set to `DEFVAL_MAX`.

See Chapter 61 on page 471 for the settings of the default profile and ADSL port default settings.

13.7 xDSL Port Setup Screen

To open this screen, click **Basic Setting**, **xDSL Port Setup**.

Figure 48 xDSL Port Setup



The following table describes the labels in this screen.

Table 20 xDSL Port Setup

LABEL	DESCRIPTION
VC Setup	Click **VC Setup** to open the **VC Setup** screen where you can configure VC settings for the DSL ports (see Section 13.9 on page 116).
PPVC Setup	Click **PPVC Setup** to open the **PPVC Setup** screen where you can configure priority PVC settings for the DSL ports (see Section 13.11 on page 121).

Table 20 xDSL Port Setup (continued)

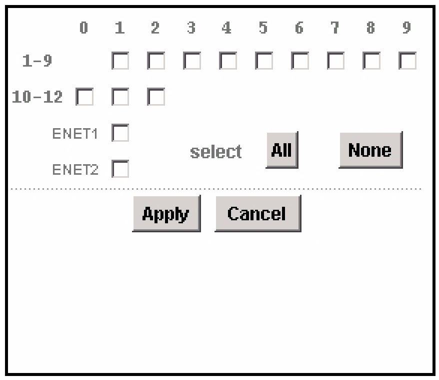
LABEL	DESCRIPTION
Copy Port Paste	Do the following to copy settings from one DSL port to another DSL port or ports. 1. Select the number of the DSL port from which you want to copy settings. 2. Select the settings that you want to copy. 3. Click **Paste** and the following screen appears. 4. Select to which ports you want to copy the settings. Use **All** to select every port. Use **None** to clear all of the check boxes. 5. Click **Apply** to paste the settings. **Figure 49** Select Ports 
Active	Select this check box to copy this port's active setting. This is configured in the **xDSL Port Setting** screen (see Section 13.7.1 on page 111).
Customer Info	Select this check box to copy this port's subscriber information. This is configured in the **xDSL Port Setting** screen (see Section 13.7.1 on page 111).
Customer Tel	Select this check box to copy this port's subscriber's telephone number. This is configured in the **xDSL Port Setting** screen (see Section 13.7.1 on page 111).
2+ Features	Select this check box to copy this port's ADSL2+ feature settings. These are configured in the **xDSL Port Setting** screen (see Section 13.7.1 on page 111).
Profile&Mode	Select this check box to copy this port's port profile settings and ADSL operational mode. The port profile settings are configured in the **xDSL Port Profile Setup** screens (see Chapter 14 on page 125). The ADSL operational mode is configured in the **xDSL Port Setting** screen (see Section 13.7.1 on page 111).
IGMP Filter	Select this check box to copy this port's IGMP filter settings. These are configured in the **IGMP Filter Profile** screen (see Section 14.8 on page 136).
Security	Select this check box to copy this port's security settings. This is configured in the **Port Security** screen (see Chapter 24 on page 189).
Frame Type	Select this check box to copy this port's allowed frame type. This is configured in the **Static VLAN Setting** screen (see Chapter 16 on page 149).
Virtual Channels	Select this check box to copy this port's virtual channel settings. These are configured in the **VC Setup** screen (see Section 13.9 on page 116).
Alarm Profile	Select this check box to copy this port's alarm profile. This is configured in the **Alarm Profile Setup** screen (see Section 14.6 on page 133).
PVID&Priority	Select this check box to copy this port's PVID and priority settings. These are configured in the **VLAN Port Setting** screen (see Chapter 16 on page 153).
Packet Filter	Select this check box to copy this port's packet filter settings. These are configured in the **Packet Filtering** screen (see Chapter 20 on page 175).
Paste	See **Copy Port**.

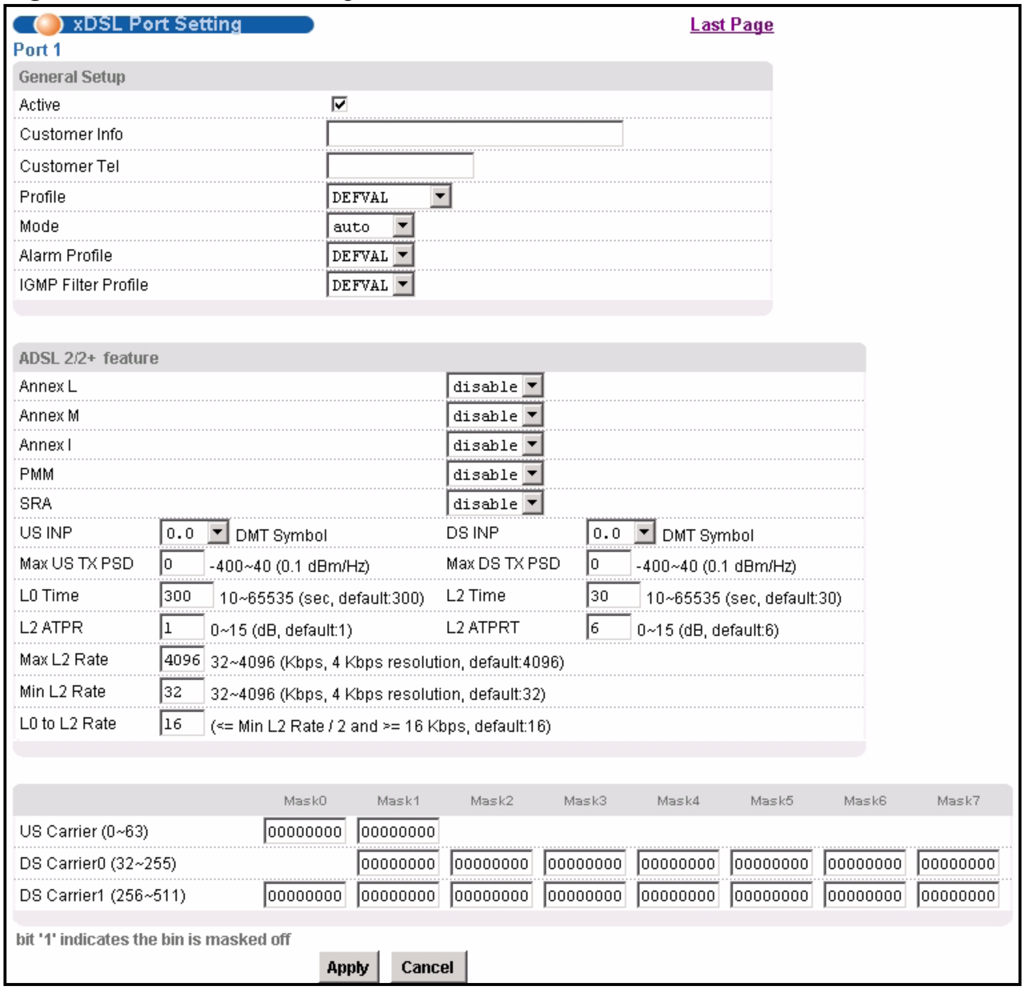
Table 20 xDSL Port Setup (continued)

LABEL	DESCRIPTION
Port	This field shows each ADSL port number.
Active	This field shows the active status of this port. The port may be **enabled** or **disabled**. This is configured in the **xDSL Port Setting** screen (see Section 13.7.1 on page 111).
Customer Info	This field shows the customer information provided for this port. This is configured in the **xDSL Port Setting** screen (see Section 13.7.1 on page 111).
Customer Tel	This field shows the customer telephone number provided for this port. This is configured in the **xDSL Port Setting** screen (see Section 13.7.1 on page 111).
Profile	This field shows which profile is assigned to this port. This is configured in the **xDSL Port Setting** screen (see Section 13.7.1 on page 111).
Mode	This field shows which ADSL operational mode the port is set to use. This is configured in the **xDSL Port Setting** screen (see Section 13.7.1 on page 111).
Channels	This field displays the number of PVCs (Permanent Virtual Circuits) that are configured for this port. This is configured in the **VC Setup** screen (see Section 13.9 on page 116).

13.7.1 xDSL Port Setting Screen

To open this screen, click **Basic Setting**, **xDSL Port Setup**, and then click a port's index number.

Figure 50 xDSL Port Setting



The following table describes the labels in this screen.

Table 21 xDSL Port Setting

LABEL	DESCRIPTION
Last Page	Click this to return to the previous screen.
General Setup	
Active	Select this check box to turn on this ADSL port.
Customer Info	Enter information to identify the subscriber connected to this ADSL port. You can use up to 31 printable ASCII characters (including spaces and hyphens).
Customer Tel	Enter information to identify the telephone number of the subscriber connected to this ADSL port. You can use up to 15 ASCII characters (including spaces and hyphens).
Profile	Select a profile of ADSL settings (such as the transfer rate, interleave delay and signal to noise ratio settings) to assign to this port. Use the **Port Profile** screen to configure port profiles (see Chapter 14 on page 125).
Mode	Select the port's ADSL operational mode. Select the mode that the subscriber's device uses or **auto** to have the AAM1212 automatically determine the mode to use. See Table 19 on page 107 for information on the individual ADSL modes.

Table 21 xDSL Port Setting (continued)

LABEL	DESCRIPTION
Alarm Profile	Select the port's alarm profile. The alarm profile defines alarm thresholds for the ADSL port. The AAM1212 sends an alarm trap and generates a syslog entry when the thresholds of the alarm profile are exceeded (see Section 14.6 on page 133).
IGMP Filter Profile	The IGMP filter profile defines which multicast groups a port can join. Select a profile of IGMP filter settings to assign to this port. Use the **IGMP Filter Profile** screen to configure IGMP filter profiles (see Section 14.8 on page 136).
ADSL2/2+ feature	These are features available with ADSL2/2+. The subscriber's ADSL device must also support the individual features in order to use them. At the time of writing these features have not been fully tested and their performance and interoperability cannot be guaranteed.
Annex L	This field is not available for the AAM1212-53. Enable Annex L to use reach extended ADSL2. This allows increased connection distances.
Annex M	This field is not available for the AAM1212-53. Enable Annex M to use double upstream mode. This has the upstream connection use tones 6 to 63.
Annex I	This field is not available for the AAM1212-53. Enable Annex I to use all digital mode. With Annex I, the ADSL connection uses the full spectrum of the physical line and the user can not use POTS or ISDN service. This increases the upstream data rate. **Note:** The subscriber cannot use POTS or ISDN services when you enable Annex I.
PMM	Enable the Power ManageMent (PMM) feature to reduce the amount of power used overall and reduce the instances of the connection going down. PMM increases or decreases the transmission power based on line conditions. PMM also decreases the number of service interruptions. Select **L2** to have the ADSL connection use power saving mode and reduce the rate when there is no traffic. The rate comes back up when there is traffic. Select **L3** to use both power management modes L2 and L3. L3 puts the ADSL connection to sleep mode. L0 power mode uses no power reduction. See the ITU-T G.992.3 standard for more on PMM and the power modes (states).
SRA	Enable Seamless Rate Adaptation (SRA) to have the AAM1212 automatically adjust the connection's data rate according to line conditions without interrupting service.
	Sudden spikes in the line's noise level (impulse noise) can cause errors and result in lost packets. Set the impulse noise protection minimum to have a buffer to protect the ADSL physical layer connection against impulse noise. This buffering causes a delay that reduces transfer speeds. It is recommended that you use a non-zero setting for real time traffic that has no error correction (like videoconferencing).
US INP	Set the minimum upstream (US) impulse noise protection setting.
DS INP	Set the minimum downstream (DS) impulse noise protection setting.
Max US TX PSD	Specify the maximum upstream transmit power. The unit of measure is 0.1 dBm/Hz; for example, to set the maximum upstream transmit power to -10 dBm/Hz, set this value to -100.
Max DS TX PSD	Specify the maximum downstream transmit power. The unit of measure is 0.1 dBm/Hz; for example, to set the maximum downstream transmit power to -10 dBm/Hz, set this value to -100.
L0 Time	Set the minimum time (in seconds) that the ADSL line must stay in L0 power mode before changing to the L2 power mode.

Table 21 xDSL Port Setting (continued)

LABEL	DESCRIPTION
L2 Time	Set minimum time (in seconds) that the ADSL line must stay in the L2 power mode before reducing the power again in the L2 power mode.
L2 ATPR	Set the maximum Aggregate Transmit Power Reduction (ATPR) in decibels (dB) that is permitted in a L2 power reduction. The system can gradually decrease the ADSL line transmission power while it is in the L2 power mode. This is the largest individual power reduction allowed in the L2 power mode.
L2 ATPRT	Set the maximum Aggregate Transmit Power Reduction Total (ATPRT) in decibels (dB) that is permitted in the L2 power mode. This is the total transmit power decrease that is allowed to occur in the L2 power mode.
Max L2 Rate	Set the maximum transfer rate (in Kilobits per second) that is permitted while the port is in the L2 power mode. The supported range is 32~4096 Kbps in 4 Kbps increments. If you enter a number that is not a multiple of 4, the system uses the next lower multiple of 4. If you enter 39, for example, the system will use 36.
Min L2 Rate	Set the minimum transfer rate (in Kilobits per second) that is permitted while the port is in the L2 power mode. The supported range is 32~4096 Kbps in 4 Kbps increments. If you enter a number that is not a multiple of 4, the system uses the next lower multiple of 4. If you enter 39, for example, the system will use 36.
L0 to L2 Rate	Set the down stream transfer rate (in Kilobits per second) that serves as the threshold for whether the port is to use the L0 or the L2 power mode. The system changes from L0 mode to L2 mode when the downstream transfer rate stays below this threshold for **L0 Time**. The system changes back from L2 mode to L0 mode when the downstream transfer rate goes above this threshold. This rate must be less than or equal to one half of the **Min L2 Rate** and at least 16 Kbps.
Use this part of the screen to mask carrier tones. Masking a carrier tone disables the use of that tone on the ADSL port. Do this to have the system not use an ADSL line’s tones that are known to have a high noise level. Each mask can use up to 8 hexadecimal digits (00000000~ffffffff). Each hexadecimal digit represents 4 tones. The hexadecimal digit is converted to binary and a '1' masks (disables) the corresponding tone. The most significant bit defines the lowest tone number in a mask.	
US Carrier	**Mask0** represents tones 0~31. **Mask1** represents tones 32~63. The most significant bit defines Tone 0. In other words, 0x00000001 means tone 31. For example, you could use 0xfffff000 to disable upstream carrier tones 0~19 and leave tones 20 ~ 31 enabled.
DS Carrier0 (32~255)	**Mask1** represents tones 32~63 **Mask2** represents tones 64~95 **Mask3** represents tones 96~127 **Mask4** represents tones 128~159 **Mask5** represents tones 160~191 **Mask6** represents tones 192~223 **Mask7** represents tones 224~255 For example, use 0x01000000 in **Mask2** to disable downstream carrier tone 71. Use 0x03000000 in **Mask2** to disable downstream carrier tones 70 and 71.

Table 21 xDSL Port Setting (continued)

LABEL	DESCRIPTION
DS Carrier1 (256~511)	**Mask0** represents tones 256~287 **Mask1** represents tones 288~319 **Mask2** represents tones 320~351 **Mask3** represents tones 352~383 **Mask4** represents tones 384~415 **Mask5** represents tones 416~447 **Mask6** represents tones 448~479 **Mask7** represents tones 480~511 For example, use 0x00001000 in **Mask1** to disable downstream carrier tone 307. Use 0x0000f000 in **Mask1** to disable downstream carrier tones 304 to 307.
Apply	Click **Apply** to save your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring the fields again.

13.8 Virtual Channels

Defining virtual channels (also called Permanent Virtual Circuits or PVCs) allows you to set priorities for different services or subscribers. You can define up to eight channels on each DSL port and use them for different services or levels of service. You set the PVID that is assigned to untagged frames received on each channel. You also set an IEEE 802.1p priority for each of the PVIDs. In this way you can assign different priorities to different channels (and consequently the services that get carried on them or the subscribers that use them).

For example, you want to give high priority to voice service on one of the ADSL ports.

Use the **Edit Static VLAN** screen to configure a static VLAN on the AAM1212 for voice on the port.

Use the **ADSL Edit Port Channel Setup** screen to:

- Configure a channel on the port for voice service.
- Set the channel to use the PVID of the static VLAN you configured.
- Assign the channel a high priority.

13.8.1 Super Channel

The AAM1212 forwards frames belonging to VLAN groups that are not assigned to specific channels to the super channel. Enable the super channel option to allow a channel forward frames belonging to multiple VLAN groups (that are not assigned to other channels). The super channel functions in the same way as the channel in a single channel environment. One port can have only one super channel.

13.8.2 LLC

LLC is a type of encapsulation where one VC (Virtual Circuit) carries multiple protocols with each packet header containing protocol identifying information. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol, for example, if charging heavily depends on the number of simultaneous VCs.

13.8.3 VC Mux

VC Mux is a type of encapsulation where, by prior mutual agreement, each protocol is assigned to a specific virtual circuit, for example, VC1 carries IP, VC2 carries IPX, and so on. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

13.8.4 Virtual Channel Profile

Virtual channel profiles allow you to configure the virtual channels efficiently. You can configure all of the virtual channels with the same profile, thus removing the need to configure the virtual channels one-by-one. You can also change an individual virtual channel by assigning it a different profile.

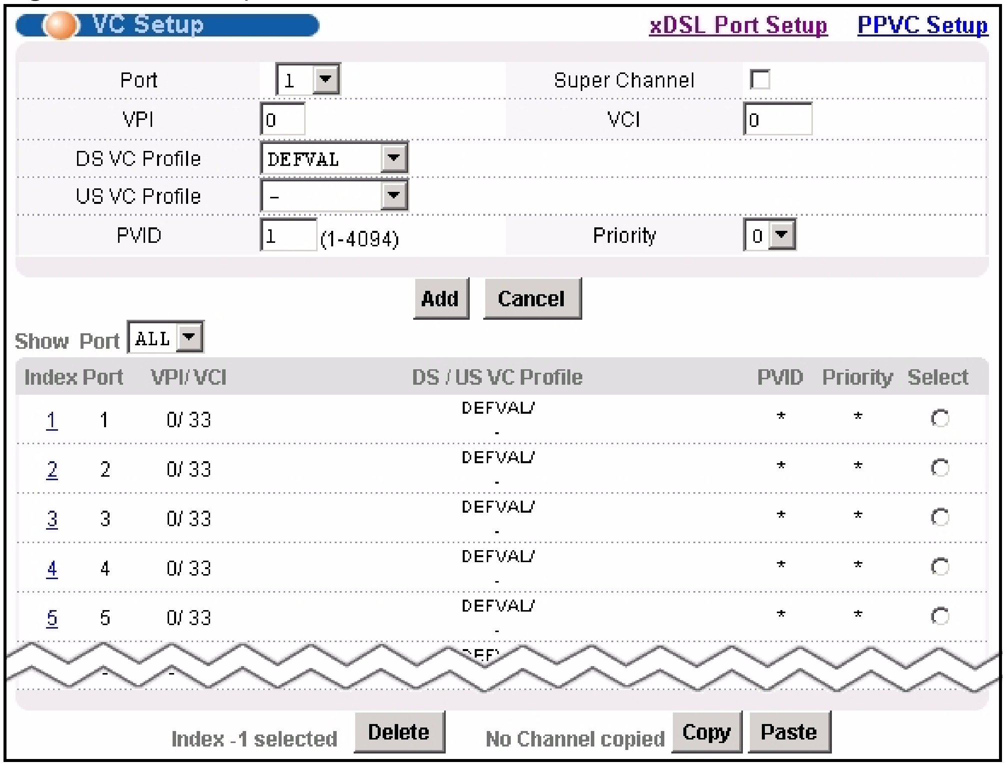
The AAM1212 provides two default virtual channel profiles: **DEFVAL** (for LLC encapsulation) and **DEFVAL_VC** (for VC encapsulation). By default, all virtual channels are associated to **DEFVAL**.

13.9 VC Setup Screen

Use this screen to view and configure a port’s channel (PVC) settings.

To open this screen, click **Basic Setting**, **xDSL Port Setup**, **VC Setup**.

Figure 51 VC Setup



The following table describes the labels in this screen.

Table 22 VC Setup

LABEL	DESCRIPTION
xDSL Port Setup	Click **xDSL Port Setup** to go to the screen where you can configure DSL port settings (see Section 13.7 on page 109).
PPVC Setup	Click **PPVC Setup** to open the **PPVC Setup** screen where you can configure priority PVC settings for the DSL ports (see Section 13.11 on page 121).
Port	Use this drop-down list box to select a port for which you wish to view or configure settings. This field is read-only once you click on a port number below.
Super Channel	The AAM1212 forwards frames belonging to VLAN groups that are not assigned to specific channels to the super channel. Enable the super channel option to have this channel forward frames belonging to multiple VLAN groups (that are not assigned to other channels). The super channel functions in the same way as the channel in a single channel environment.
VPI	Type the Virtual Path Identifier for a channel on this port.
VCI	Type the Virtual Circuit Identifier for a channel on this port.
DS VC Profile	Use the drop-down list box to select a VC profile to use for this channel's downstream traffic shaping.

Table 22 VC Setup (continued)

LABEL	DESCRIPTION
US VC Profile	Use the drop-down list box to select a VC profile to use for this channel's upstream traffic. The AAM1212 does not perform upstream traffic policing if you do not specify an upstream VC profile. **Note:** Upstream traffic policing should be used in conjunction with the ATM shaping feature on the subscriber's device. If the subscriber's device does not apply the appropriate ATM shaping, all upstream traffic will be discarded due to upstream traffic policing.
PVID	Type a PVID (Port VLAN ID) to assign to untagged frames received on this channel.
Priority	Use the drop-down list box to select the priority value (0 to 7) to add to incoming frames without a (IEEE 802.1p) priority tag. An asterisk (*) denotes a super channel.
Add Apply	Click this to add or save channel settings on the selected port. (The name of the button depends on whether or not you have clicked on a PVC number in the **Index** column.) This saves your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to start configuring the screen again.
Show Port	Select the number of an ADSL port for which to display VC settings (or display all of them).
Index	This field displays the number of the PVC. Click a PVC's index number to use the top of the screen to edit the PVC. **Note:** At the time of writing, you cannot edit the VPI and VCI. If you want to change them, add a new PVC with the desired settings. Then you can delete any unwanted PVCs.
Port	This field displays the number of the ADSL port on which the PVC is configured.
VPI/VCI	This field displays the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI). The VPI and VCI identify a channel on this port.
DS / US VC Profile	This shows which VC profile this channel uses for downstream traffic shaping. The VC profile for upstream policing also displays if the channel is configured to use one.
PVID	This is the PVID (Port VLAN ID) assigned to untagged frames or priority frames (0 VID) received on this channel. An asterisk (*) denotes a super channel.
Priority	This is the priority value (0 to 7) added to incoming frames without a (IEEE 802.1p) priority tag. An asterisk (*) denotes a super channel.

Table 22 VC Setup (continued)

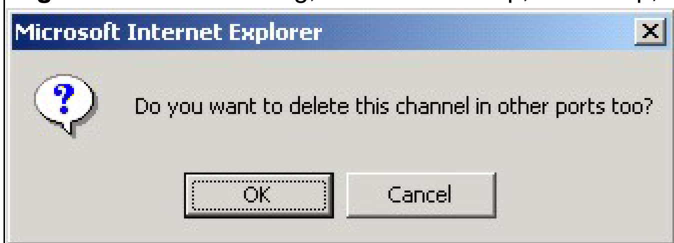
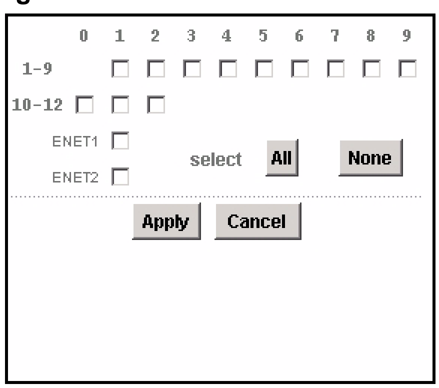
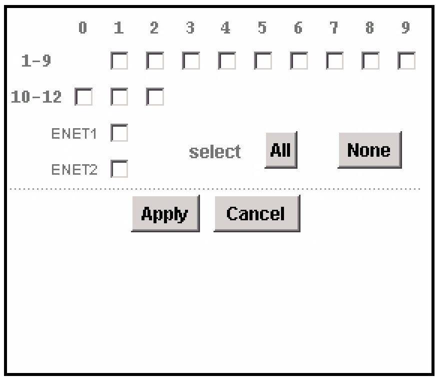
LABEL	DESCRIPTION
Select Delete	Do the following to remove one or more PVCs. **1** Select a PVC's **Select** radio button. **2** Click **Delete**. **3** Click **OK** if you want to remove the PVC from other ports. Click **Cancel** to only remove the one you selected. **Figure 52** Basic Setting, xDSL Port Setup, VC Setup, Delete  **4** If you clicked **OK**, the following screen appears. **5** Select to which ports you want to copy the settings. Use **All** to select every port. Use **None** to clear all of the check boxes. **6** Click **Apply** to delete the channels. **Figure 53** Select Ports 

Table 22 VC Setup (continued)

LABEL	DESCRIPTION
Select Copy Paste	Do the following to copy settings from one PVC to another port or ports. 1 Click the **Select** radio button of the PVC from which you want to copy settings. 2 Click **Paste**. 3 The following screen appears. 4 Select to which ports you want to copy the settings. Use **All** to select every port. Use **None** to clear all of the check boxes. 5 Click **Apply** to copy the settings. **Figure 54** Select Ports 

13.10 Priority-based PVCs

A PPVC (Priority-based PVC) allows you to give different priorities to PVCs that are members of the same VLAN.

The AAM1212 uses eight priority queues (also called levels) for the member PVCs. The system maps frames with certain IEEE 802.1p priorities to a PVC with a particular priority queue. The following table gives the factory default mapping.

Table 23 IEEE 802.1p Priority to PPVC Mapping

IEEE 802.1 PRIORITY	MAPS TO:	PPVC 0/33, PRIORITY QUEUE
7	->	level 7
6	->	level 6
5	->	level 5
4	->	level 4
3	->	level 3
2	->	level 2

Table 23 IEEE 802.1p Priority to PPVC Mapping (continued)

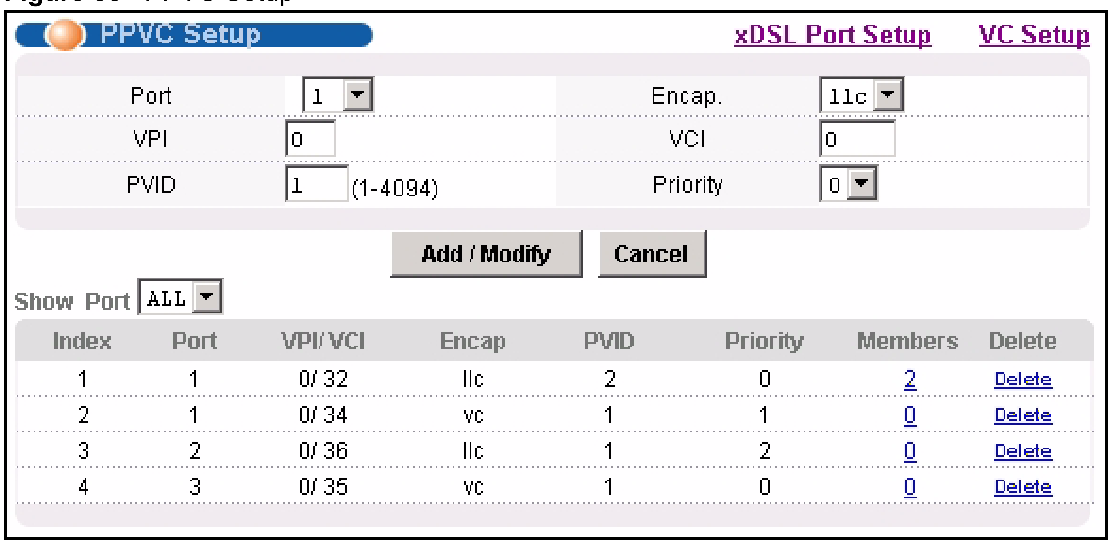
IEEE 802.1 PRIORITY	MAPS TO:	PPVC 0/33, PRIORITY QUEUE
1	->	level 1
0	>	level 0

13.11 PPVC Setup Screen

Use this screen to view and configure PPVCs.

To open this screen, click **Basic Setting**, **xDSL Port Setup**, **PPVC Setup**.

Figure 55 PPVC Setup



The following table describes the labels in this screen.

Table 24 PPVC Setup

LABEL	DESCRIPTION
xDSL Port Setup	Click **xDSL Port Setup** to go to the screen where you can configure DSL port settings (see Section 13.7 on page 109).
VC Setup	Click **VC Setup** to open the **VC Setup** screen where you can configure VC settings for the DSL ports (see Section 13.9 on page 116).
Port	Use this drop-down list box to select a port for which you wish to configure settings.
Encap.	Select the encapsulation type (**llc** or **vc**) for this PPVC.
VPI	Type the Virtual Path Identifier for this PPVC.
VCI	Type the Virtual Circuit Identifier for this PPVC. The AAM1212 uses this PVC channel internally. This PVC is not needed on the subscriber’s device. This PVC cannot overlap with any existing PVCs on this port.
PVID	Type a PVID (Port VLAN ID) to assign to untagged frames received on this PPVC.

Table 24 PPVC Setup (continued)

LABEL	DESCRIPTION
Priority	Use the drop-down list box to select the priority value (0 to 7) to add to incoming frames without a (IEEE 802.1p) priority tag.
Add / Modify	Click **Add / Modify** to save PPVC settings for a port. In order to change a port's PPVC settings, just select the port from the **Port** drop-down list box and then configure the settings you want. These settings replace the port's old settings when you click **Add / Modify**. Clicking **Add / Modify** saves your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to start configuring the screen again.
Show Port	Select the number of an ADSL port for which to display PPVC settings (or display all of them).
Index	This field displays the number of the PPVC.
Port	This field displays the number of the ADSL port on which the PPVC is configured.
VPI/VCI	This field displays the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI). The VPI and VCI identify a channel on this port. The AAM1212 uses this PVC channel internally. This PVC is not needed on the subscriber's device.
Encap	This field displays the PPVC's type of encapsulation (**llc** or **vc**).
PVID	This is the PVID (Port VLAN ID) assigned to untagged frames or priority frames (0 VID) received on this channel.
Priority	This is the priority value (0 to 7) added to incoming frames without a (IEEE 802.1p) priority tag.
Members	This field displays how many PVCs belong to this PPVC has. Click the number to open a screen where you can configure the PPVC's member PVCs.
Delete	Click **Delete** to remove a PPVC. Clicking **Delete** saves your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.

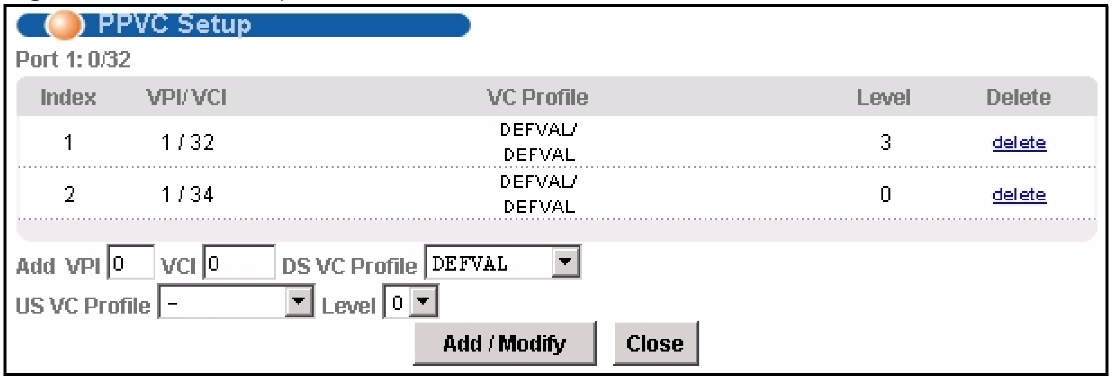
13.11.1 PPVC Setup Members Screen

Use this screen to add and remove member PVCs.

Note: The member PVCs must be created on the subscriber's device.

To open this screen, click **Basic Setting**, **xDSL Port Setup**, **PPVC Setup**. Then, click a PPVC's member number to open the **PPVC Setup Members** screen.

Figure 56 PPVC Setup, Edit



The following table describes the labels in this screen.

Table 25 PPVC Setup, Edit

LABEL	DESCRIPTION
Port	This is the port for which you are viewing or configuring settings.
Index	This field displays the number of the member PVC.
VPI/VCI	This field displays the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI). The VPI and VCI identify a channel on this port. The subscriber’s device must create this PVC.
VC Profile	This shows which VC profile this channel uses for downstream traffic shaping. The VC profile for upstream policing also displays if the channel is configured to use one.
Level	This field displays the number of the member PVC’s priority queue.
Delete	Click **Delete** to remove a member PVC from the PPVC. Clicking **Delete** saves your changes to the AAM1212’s volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Add	Use this section of the screen to add or modify a member PVC.
VPI	Type the Virtual Path Identifier for this member PVC.
VCI	Type the Virtual Circuit Identifier for this member PPVC. This PVC cannot overlap with any existing PVC’s on this port.
DS VC Profile	Use the drop-down list box to select a VC profile to use for this channel’s downstream traffic shaping.
US VC Profile	Use the drop-down list box to select a VC profile to use for this channel’s upstream traffic. The AAM1212 does not perform upstream traffic policing if you do not specify an upstream VC profile.
Level	Use the drop-down list box to select the priority queue (0 to 7) to add to use for the PVC. 7 is the highest level.

Table 25 PPVC Setup, Edit (continued)

LABEL	DESCRIPTION
Add / Modify	Click **Add / Modify** to save member PVC settings for a PPVC. In order to change a member PVC ‘s settings, just enter the PVC’s VPI and VCI, and configure the settings you want. These settings replace the PVC’s old settings when you click **Add / Modify**. Clicking **Add / Modify** saves your changes to the AAM1212’s volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Close	Click **Close** to exit the screen without saving your changes.

14

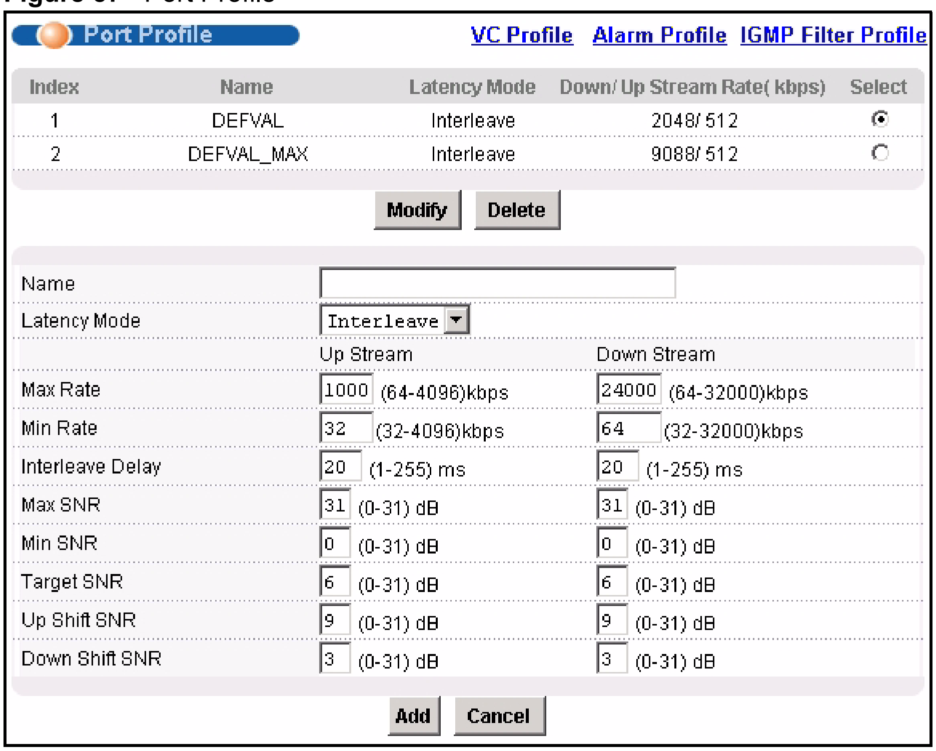
xDSL Profiles Setup

A profile is a list of settings that you define. Then you can assign them to one or more individual ports. For background information about many of these settings, see Chapter 13 on page 107.

14.1 Port Profile Screen

To open this screen, click **Basic Setting**, **xDSL Profiles Setup**.

Figure 57 Port Profile



The following table describes the labels in this screen.

Table 26 Port Profile

LABEL	DESCRIPTION
VC Profile	Click **VC Profile** to open the **VC Profile** screen where you can configure virtual channel profiles (see Section 14.5 on page 131).
Alarm Profile	Click **Alarm Profile** to open the **Alarm Profile** screen where you can configure limits that trigger an alarm when exceeded (see Section 14.6 on page 133)
IGMP Filter Profile	Click **IGMP Filter Profile** to open the **IGMP Filter Profile** screen where you can configure IGMP multicast filter profiles (see Section 14.8 on page 136).
Index	This is the port profile index number.
Name	These are the names of individual profiles. The DEFVAL profile always exists and all of the DSL ports have it assigned to them by default. You can use up to 31 ASCII characters; spaces are not allowed.
Latency Mode	This is the ADSL latency mode (**Fast** or **Interleave**) for the ports that belong to this profile.
Down/Up Stream Rate (kbps)	These are the maximum downstream and upstream transfer rates for the ports that belong to this profile.
Select Modify	Select a profile's **Select** radio button and click **Modify** to edit the profile.
Select Delete	Select a profile's **Select** radio button and click **Delete** to remove the profile.
	The rest of the screen is for profile configuration.
Name	When editing a profile, this is the name of this profile. When adding a profile, type a name (up to 31 characters) for the profile.
Latency Mode	This field sets the ADSL latency mode for the ports that belong to this profile. Select **Fast** mode to use no interleaving and have faster transmission (a "fast channel"). This would be suitable if you have a good line where little error correction is necessary. Select **Interleave** mode to use interleave delay when transmission error correction (Reed- Solomon) is necessary due to a less than ideal telephone line. See Section 13.4 on page 108 for more on interleave delay.
Up Stream	The following parameters relate to upstream transmissions.
Max Rate	Type a maximum upstream transfer rate (64 to 4096 Kbps) for this profile. Configure the maximum upstream transfer rate to be less than the maximum downstream transfer rate.
Min Rate	Type the minimum upstream transfer rate (32 to 4096 Kbps) for this port. Configure the minimum upstream transfer rate to be less than the maximum upstream transfer rate.
Interleave Delay	Configure this field when you set the **Latency Mode** field to **Interleave**. Type the number of milliseconds (1-255) of interleave delay to use for upstream transfers. It is recommended that you configure the same latency delay for both upstream and downstream.
Max SNR	Type the maximum upstream signal to noise margin (0-31 dB).
Min SNR	Type the minimum upstream signal to noise margin (0-31 dB). Configure the minimum upstream signal to noise margin to be less than or equal to the maximum upstream signal to noise margin.

Table 26 Port Profile (continued)

LABEL	DESCRIPTION
Target SNR	Type the target upstream signal to noise margin (0-31 dB). Configure the target upstream signal to noise margin to be greater than or equal to the minimum upstream signal to noise margin and less than or equal to the maximum upstream signal to noise margin.
Up Shift SNR	The upstream up shift signal to noise margin (0-31 dB). When the channel's signal to noise margin goes above this number, the device can attempt to use a higher transfer rate. Configure the upstream up shift signal to noise margin to be greater than or equal to the target upstream signal to noise margin and less than or equal to the maximum upstream signal to noise margin.
Down Shift SNR	The upstream down shift signal to noise margin (0-31 dB). When the channel's signal to noise margin goes below this number, the device shifts to a lower transfer rate. Configure the upstream down shift signal to noise margin to be less than or equal to the target upstream signal to noise margin and greater than or equal to the minimum upstream signal to noise margin.
Down Stream	The following parameters relate to downstream transmissions.
Max Rate	Type a maximum downstream transfer rate (64 to 32000 Kbps) bps for this port. Configure the maximum downstream transfer rate to be greater than the maximum upstream transfer rate.
Min Rate	Type the minimum downstream transfer rate (32 to 32000 Kbps) for this port. Configure the minimum downstream transfer rate to be less than the maximum downstream transfer rate.
Interleave Delay	Configure this field when you set the **Latency Mode** field to **interleave**. Type the number of milliseconds (1-255) of interleave delay to use for upstream transfers. It is recommended that you configure the same latency delay for both upstream and downstream.
Max SNR	Type the maximum downstream signal to noise margin (0-31 dB).
Min SNR	Type the minimum downstream signal to noise margin (0-31 dB). Configure the minimum downstream signal to noise margin to be less than or equal to the maximum downstream signal to noise margin.
Target SNR	Type the target downstream signal to noise margin (0-31 dB). Configure the target downstream signal to noise margin to be greater than or equal to the minimum downstream signal to noise margin and less than or equal to the maximum downstream signal to noise margin.
Up Shift SNR	The downstream up shift signal to noise margin (0-31 dB). When the channel's signal to noise margin goes above this number, the device can attempt to use a higher transfer rate. Configure the downstream up shift signal to noise margin to be greater than or equal to the target downstream signal to noise margin and less than or equal to the maximum downstream signal to noise margin.
Down Shift SNR	The downstream down shift signal to noise margin (0-31 dB). When the channel's signal to noise margin goes below this number, the device shifts to a lower transfer rate. Configure the downstream down shift signal to noise margin to be less than or equal to the target downstream signal to noise margin and greater than or equal to the minimum downstream signal to noise margin.
Add	Click **Add** to save your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to start configuring the screen again.

14.2 ATM QoS

ATM Quality of Service (QoS) mechanisms provide the best service on a per-flow guarantee. ATM network infrastructure was designed to provide QoS. It uses fixed cell sizes and built-in traffic management (see Section 14.3 on page 128). This allows you to fine-tune the levels of services on the priority of the traffic flow.

14.3 Traffic Shaping

Traffic shaping is an agreement between the carrier and the subscriber to regulate the average rate and fluctuations of data transmission over an ATM network. This agreement helps eliminate congestion, which is important for transmission of real time data such as audio and video connections.

Note: Traffic shaping controls outgoing (downstream) traffic, not incoming (upstream).

14.3.1 ATM Traffic Classes

These are the basic ATM traffic classes defined by the ATM Forum Traffic Management 4.0 Specification.

14.3.1.1 Constant Bit Rate (CBR)

Constant Bit Rate (CBR) is an ATM traffic class that provides fixed bandwidth. CBR traffic is generally time-sensitive (doesn't tolerate delay). CBR is used for connections that continuously require a specific amount of bandwidth. Examples of connections that need CBR would be high-resolution video and voice.

14.3.1.2 Variable Bit Rate (VBR)

The Variable Bit Rate (VBR) ATM traffic class is used with bursty connections. Connections that use the Variable Bit Rate (VBR) traffic class can be grouped into real time (rt-VBR) or non-real time (nrt-VBR) connections.

The rt-VBR (real-time Variable Bit Rate) type is used with bursty connections that require closely controlled delay and delay variation. An example of an rt-VBR connection would be video conferencing. Video conferencing requires real-time data transfers and the bandwidth requirement varies in proportion to the video image's changing dynamics.

The nrt-VBR (non real-time Variable Bit Rate) type is used with bursty connections that do not require closely controlled delay and delay variation. An example of an nrt-VBR connection would be non-time sensitive data file transfers.

14.3.1.3 Unspecified Bit Rate (UBR)

The Unspecified Bit Rate (UBR) ATM traffic class is similar to the ABR traffic class for bursty data transfers. However, while ABR gives subscribers a set amount of bandwidth, UBR doesn't guarantee any bandwidth and only delivers traffic when the network has spare bandwidth.

14.3.2 Traffic Parameters

These are the parameters that control the flow of ATM traffic.

14.3.2.1 Peak Cell Rate (PCR)

Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 832Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent on the line speed.

14.3.2.2 Sustained Cell Rate (SCR)

Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

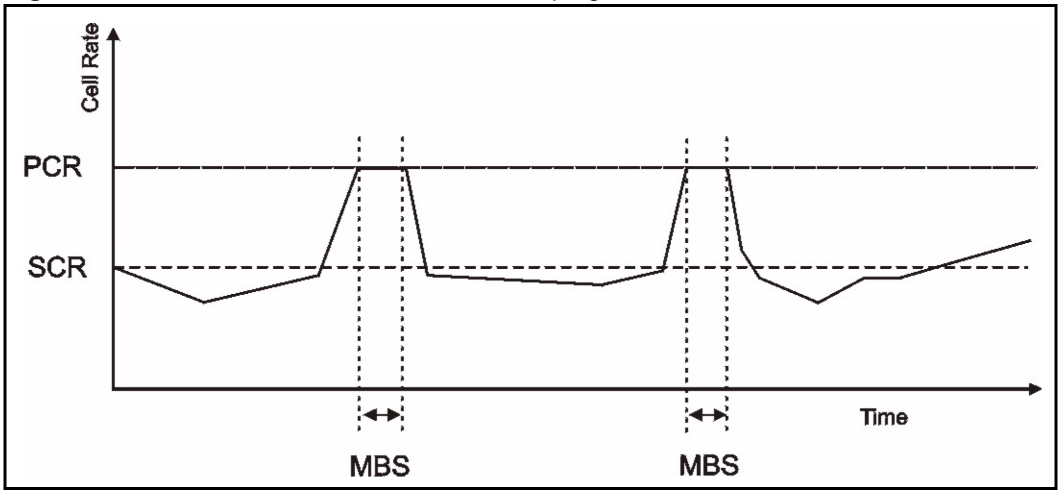
14.3.2.3 Maximum Burst Size (MBS)

Maximum Burst Size (MBS) is the maximum number of cells that can be sent at the PCR. After MBS is reached, cell rates fall below SCR until cell rate averages to the SCR again. At this time, more cells (up to the MBS) can be sent at the PCR again.

Note: If the PCR, SCR or MBS is set to the default of "0", the system will assign a maximum value that correlates to your upstream line rate.

The following figure illustrates the relationship between PCR, SCR and MBS.

Figure 58 PCR, SCR and MBS in Traffic Shaping



14.3.2.4 Cell Delay Variation Tolerance (CDVT)

Cell Delay Variation Tolerance (CDVT) is the accepted tolerance of the difference between a cell's transfer delay and the expected transfer delay. CDVT controls the time scale over which the PCR is enforced. CDVT is used to determine if a cell arrived too early in relation to PCR.

14.3.2.5 Burst Tolerance (BT)

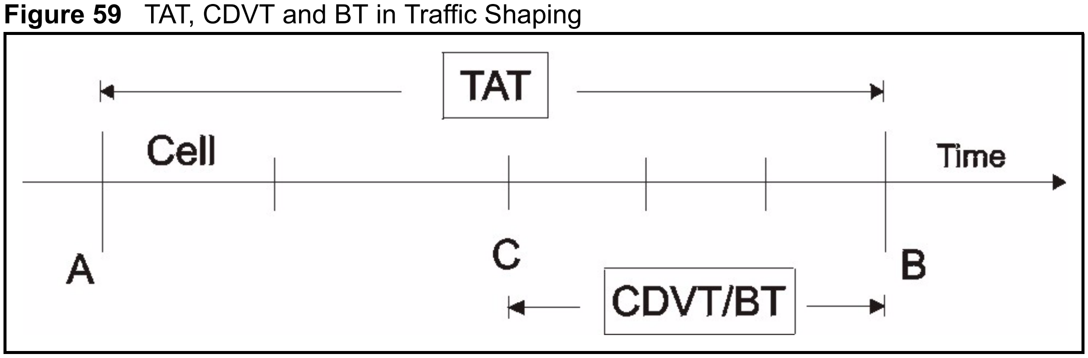
Burst Tolerance (BT) is the maximum number of cells that the port is guaranteed to handle without any discards. BT controls the time scale over which the SCR is enforced. BT is used to determine if a cell arrived too early in relation to SCR. Use this formula to calculate BT: (MBS – 1) x (1 / SCR – 1 / PCR) = BT.

14.3.2.6 Theoretical Arrival Time (TAT)

The Theoretical Arrival Time (TAT) is when the next cell (in an ATM connection's stream of cells) is expected to arrive. TAT is calculated based on the PCR or SCR.

The following figure illustrates the relationship between TAT, CDVT and BT. If a cell arrives at time A, then according to PCR or SCR, the next cell is expected to arrive at time B. If the next cell arrives earlier than time C, it is discarded or tagged for not complying with the TAT. Time C is calculated based on the CDVT or BT.

Figure 59 TAT, CDVT and BT in Traffic Shaping



14.4 Upstream Policing

Upstream policing is an agreement between the carrier and the subscriber to regulate the average rate and fluctuations of data transmission coming from the subscriber's device to the AAM1212.

Note: Upstream policing controls incoming (upstream) traffic, not outgoing (downstream).

The ATM traffic classes and parameters are identical with downstream shaping.

Upstream policing can control the upstream incoming traffic rate on specific PVCs. Upstream ATM cell traffic that violates the policing profile will be discarded. Traffic shaping must also be enabled on the subscriber's device in order to use upstream policing. If a subscriber attempts to enlarge his device's PVC shaping parameters in order to get more upstream traffic bandwidth, it will violate the AAM1212's upstream policing profile and the traffic will be discarded. Operators can use this feature to prevent subscribers from changing their device settings.

Note: Traffic shaping must also be enabled on the subscriber's device in order to use upstream policing.

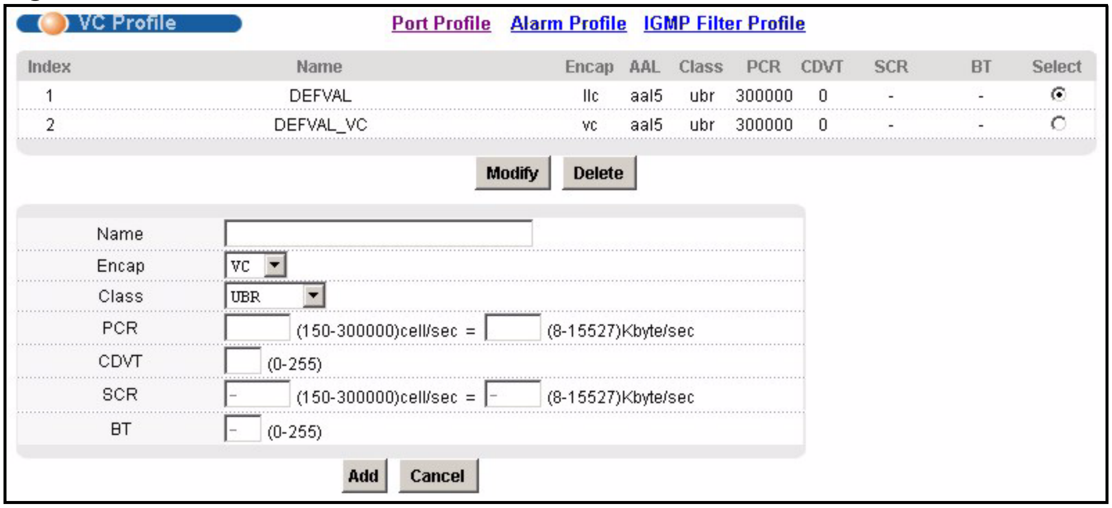
Note that since the AAM1212 uses ATM QoS, if the subscriber device's upstream shaping rate is larger than the AAM1212's upstream policing rate, some ATM cells will be discarded. In the worst case, none of the Ethernet packets from the CPE will be able to be reassembled from AAL5, so no packets from the subscriber's device can be received by the AAM1212.

The upstream policing feature can be enabled/disabled per PVC. No matter which ATM traffic class is used for the PVC's upstream traffic (CBR, VBR, or UBR), the AAM1212 will drop any upstream traffic that violates the specified ATM VC profile.

14.5 VC Profile Screen

To open this screen, click **Basic Setting**, **xDSL Profiles Setup**, **VC Profile**.

Figure 60 VC Profile



The following table describes the labels in this screen.

Table 27 VC Profile

LABEL	DESCRIPTION
Port Profile	Click **Port Profile** to configure port profiles and assign them to individual ports (see Section 14.1 on page 125).
Alarm Profile	Click **Alarm Profile** to open the **Alarm Profile** screen where you can configure limits that trigger an alarm when exceeded (see Section 14.6 on page 133)
IGMP Filter Profile	Click **IGMP Filter Profile** to open the **IGMP Filter Profile** screen where you can configure IGMP multicast filter profiles (see Section 14.8 on page 136).
Index	This is the number of the VC profile.
Name	This name identifies the VC profile.
Encap	This field displays the profile's type of encapsulation (**llc** or **vc**).
AAL	This field displays the ATM adaptation layer used by the VC profile. **aal5** - The VC profile uses ATM adaptation layer 5.
Class	This field displays the type of ATM traffic class: **cbr** (constant bit rate), **vbr** (real-time variable bit rate), **nrt-vbr** (non-real time variable bit rate) or **ubr** (unspecified bit rate).
PCR	This is the Peak Cell Rate (PCR), the maximum number of cells that the sender can send per second.
CDVT	This field displays the accepted tolerance of the difference between a cell's transfer delay and the expected transfer delay.
SCR	The Sustained Cell Rate (SCR) sets the average cell rate (long-term) in cells per second that can be transmitted. SCR applies with the **vbr** traffic class.
BT	Burst Tolerance (BT) is the maximum number of cells that the port is guaranteed to handle without any discards. BT applies with the **vbr** traffic class.
Select Modify	Select a VC profile's **Select** radio button and click **Modify** to edit the VC profile
Delete	Select a VC profile's **Select** radio button and click **Delete** to remove the VC profile
	The rest of the screen is for PVC configuration.

Table 27 VC Profile (continued)

LABEL	DESCRIPTION
Name	When editing a profile, this is the name of this profile. When adding a profile, type a name for the profile. You can use up to 31 ASCII characters; spaces are not allowed.
Encap	Select the encapsulation type (**LLC** or **VC**) for this port.
Class	Select **CBR** (constant bit rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select **UBR** (unspecified bit rate) for applications that are non-time sensitive, such as e-mail. Select **VBR** (real time variable bit rate) or **NRT-VBR** (non real time variable bit rate) for bursty traffic and bandwidth sharing with other applications.
PCR	The Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. PCR applies with all of the ATM traffic classes. You can type a number of (ATM) cells per second in the first field or type a number of kilobytes per second in the second field to have the system automatically compute the number of ATM cells per second.
CDVT	Cell Delay Variation Tolerance (CDVT) is the accepted tolerance of the difference between a cell's transfer delay and the expected transfer delay. CDVT applies with all of the ATM traffic classes. Type the CDVT here.
SCR	The Sustained Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. SCR applies with the **VBR** traffic classes. You can type a number of (ATM) cells per second in the first field or type a number of kilobytes per second in the second field to have the system automatically compute the number of ATM cells per second.
BT	Burst Tolerance (BT) sets a maximum number of cells that the port is guaranteed to handle without any discards. Type the BT here. BT applies with the **VBR** traffic classes.
Add	Click **Add** to save your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to start configuring the screen again.

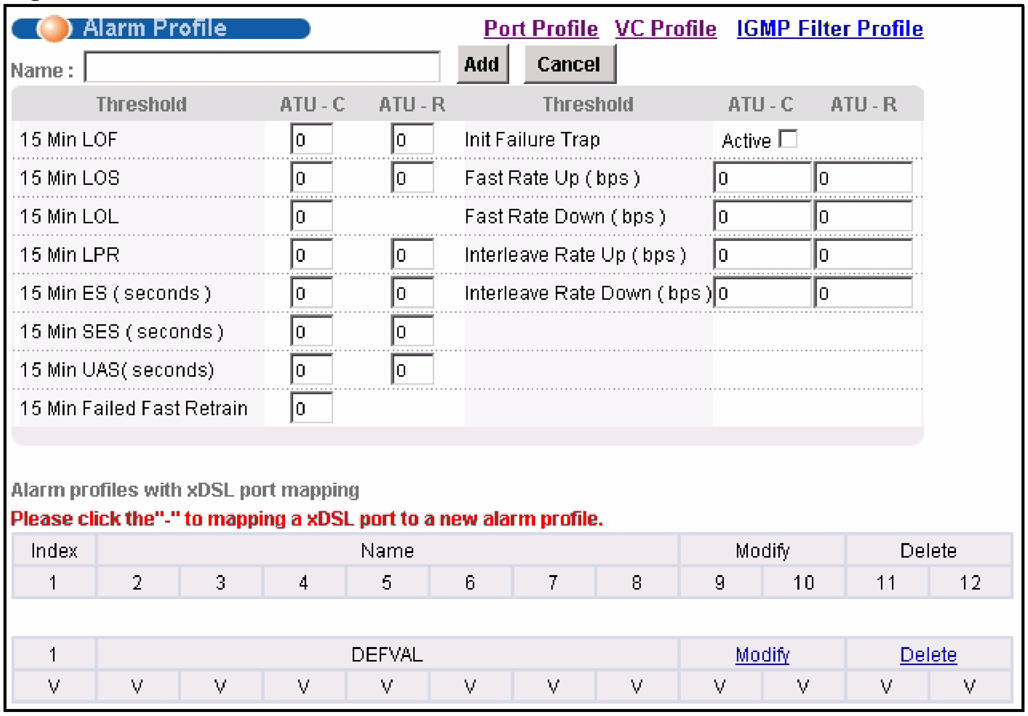
14.6 Alarm Profile Screen

Alarm profiles define ADSL port alarm thresholds. The AAM1212 sends an alarm trap and generates a syslog entry when the thresholds of the alarm profile are exceeded.

To open this screen, click **Basic Setting**, **xDSL Profiles Setup**, **Alarm Profile**.

Use the top part of the screen (with the **Add** and **Cancel** buttons) to add or edit alarm profiles. The rest of the screen displays the configured alarm profiles.

Figure 61 Alarm Profile



The following table describes the labels in this screen.

Table 28 Alarm Profile

LABEL	DESCRIPTION
Port Profile	Click **Port Profile** to open the **Port Profile** screen (see Section 14.1 on page 125). Use the **Port Profile** screen to configure profiles of ADSL port settings (such as the transfer rate, interleave delay and signal to noise ratio settings).
VC Profile	Click **VC Profile** to open the **VC Profile** screen where you can configure virtual channel profiles (see Section 14.5 on page 131).
IGMP Filter Profile	Click **IGMP Filter Profile** to open the **IGMP Filter Profile** screen where you can configure IGMP multicast filter profiles (see Section 14.8 on page 136).
Name	This field is read-only if you click **Modify** to edit a port profile. Type a name to identify the alarm profile (you cannot change the name of the DEFVAL profile). You can use up to 31 ASCII characters; spaces are not allowed.
Add	Click **Add** to save your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to start configuring the screen again.
Threshold	Specify limits for the individual performance counters. The AAM1212 sends an alarm trap and generates a syslog entry when one of these thresholds is exceeded. A value of 0 disables the alarm threshold.
ATU-C	These fields are for traffic coming from the subscriber's device to the AAM1212.
ATU-R	These fields are for traffic going from the AAM1212 to the subscriber's device.
15 Min LOF	This field sets the limit for the number of Loss Of Frame seconds that are permitted to occur within 15 minutes.

Table 28 Alarm Profile (continued)

LABEL	DESCRIPTION
15 Min LOS	This field sets the limit for the number of Loss Of Signal seconds that are permitted to occur within 15 minutes.
15 Min LOL	This field sets the limit for the number of Loss Of Link seconds that are permitted to occur within 15 minutes.
15 Min LPR	This field sets the limit for the number of Loss of Power seconds (on the ATUR) that are permitted to occur within 15 minutes.
15 Min ES (seconds)	This field sets the limit for the number of Errored Seconds that are permitted to occur within 15 minutes.
15 Min SES (seconds)	This field sets the limit for the number of Severely Errored seconds that are permitted to occur within 15 minutes.
15 Min UAS (seconds)	This field sets the limit for the number of UnAvailable seconds that are permitted to occur within 15 minutes.
15 Min Failed Fast Retrain	This field sets the limit for the number of failed fast retrains that are permitted within 15 minutes.
Init Failure Trap	Select **Active** to trigger an alarm for an initialization failure trap.
Fast Rate Up (bps)	Specify a rate in kilobits per second (kbps). If a fast mode connection’s upstream transmission rate increases by more than this number, then a trap is sent.
Fast Rate Down (bps)	Specify a rate in kilobits per second (kbps). If a fast mode connection’s downstream transmission rate decreases by more than this number, then a trap is sent.
Interleave Rate Up (bps)	Specify a rate in kilobits per second (kbps). If an interleave mode connection’s upstream transmission rate increases by more than this number, then a trap is sent.
Interleave Rate Down (bps)	Specify a rate in kilobits per second (kbps). If an interleave mode connection’s upstream transmission rate decreases by more than this number, then a trap is sent.
Alarm profiles with xDSL port mapping	After you add an alarm profile, you can click a port number’s “-“ symbol to map the xDSL port to that alarm profile. The port’s “V” symbol in the alarm profile where it was previously mapped changes to “-“.
Modify	Click **Modify** to edit a profile.
Delete	Click **Delete** to remove a profile.

14.7 IGMP Filtering

With the IGMP filtering feature, you can limit the multicast channel number of IGMP groups a subscriber on a port can join. This allows you to control the distribution of multicast services (such as content information distribution) based on service plans and types of subscription.

You can set the device to filter the multicast group join reports on a per-port basis by configuring an IGMP filtering profile and associating the profile to a port.

14.8 IGMP Filter Profile Screen

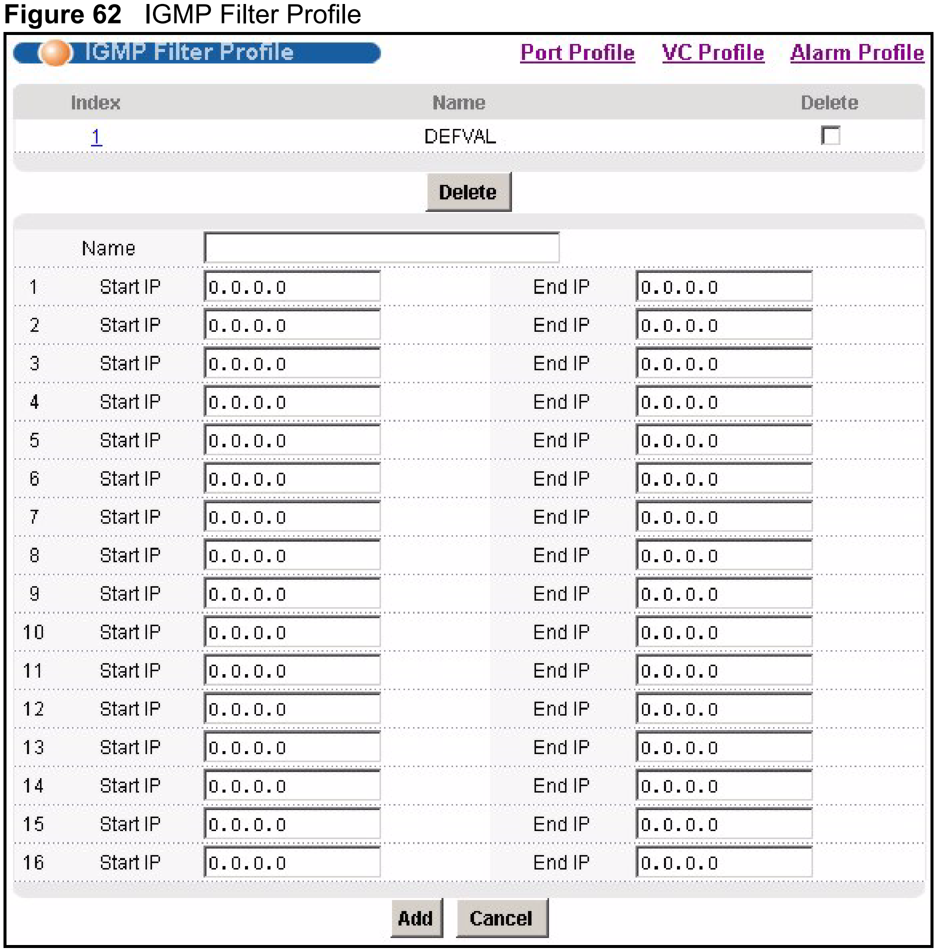
You can use the IGMP filter profiles to control access to a service that uses a specific multicast group (like a SIP server for example). Configure an IGMP filter profile that allows access to that multicast group. Then assign the IGMP filter profile to ADSL ports that are allowed to use the service.

The **DEFVAL** IGMP filter profile is assigned to all of the ADSL ports by default. It allows a port to join all multicast IP addresses (224.0.0.0~239.255.255.255). If you want to allow an ADSL subscriber access to only specific IGMP multicast groups, use the **IGMP Filter Profile** screen to configure a different profile and then assign it to the subscriber's ADSL port in the **XDSL Port Setting** screen (see Section 13.7.1 on page 111).

To open this screen, click **Basic Setting**, **xDSL Profiles Setup**, **IGMP Filter Profile**.

The top of the screen displays the configured IGMP filter profiles. Use the bottom part of the screen (with the **Add** and **Cancel** buttons) to add or edit alarm profiles.

Figure 62 IGMP Filter Profile



The following table describes the labels in this screen.

Table 29 IGMP Filter Profile

LABEL	DESCRIPTION
Port Profile	Click **Port Profile** to configure port profiles and assign them to individual ports (see Section 14.1 on page 125).
VC Profile	Click **VC Profile** to open the **VC Profile** screen where you can configure virtual channel profiles (see Section 14.5 on page 131).
Alarm Profile	Click **Alarm Profile** to open the **Alarm Profile** screen where you can configure limits that trigger an alarm when exceeded (see Section 14.6 on page 133)
Index	This is the number of the IGMP filter profile. Click a profile's index number to edit the profile. You cannot edit the **DEFVAL** profile.
Name	This name identifies the IGMP filter profile.
Delete	Select the **Delete** check box and click **Delete** to remove an IGMP filter profile. You cannot delete the **DEFVAL** profile.
Name	Type a name to identify the IGMP filter profile (you cannot change the name of the DEFVAL profile). You can use up to 31 ASCII characters; spaces are not allowed.
Start IP	Enter the starting multicast IP address for a range of multicast IP addresses to which you want this IGMP filter profile to allow access.
End IP	Enter the ending multicast IP address for a range of IP addresses to which you want this IGMP filter profile to allow access. If you want to add a single multicast IP address, enter it in both the **Start IP** and **End IP** fields.
Add	Click **Add** to save your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to start configuring the screen again.

15

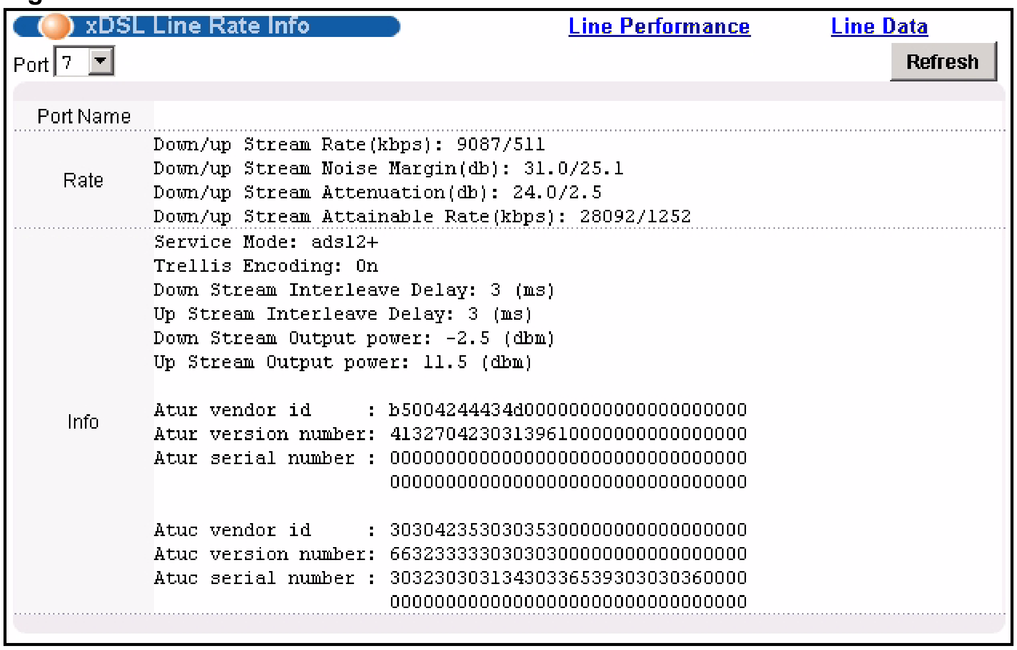
xDSL Line Data

15.1 xDSL Line Rate Info Screen

This screen displays an ADSL port's line operating values. Information obtained prior to training to steady state transition will not be valid or will be old information.

To open this screen, click **Basic Setting**, **xDSL Line Data**.

Figure 63 xDSL Line Rate Info



The following table describes the labels in this screen.

Table 30 xDSL Line Rate Info

LABEL	DESCRIPTION
Line Performance	Click **Line Performance** to display an ADSL port's line performance counters (see Section 15.2 on page 141).
Line Data	Click **Line Data** to display an ADSL port's line bit allocation (see Section 15.3 on page 143).
Port	Use this drop-down list box to select a port for which you wish to view information.

Table 30 xDSL Line Rate Info (continued)

LABEL	DESCRIPTION
Refresh	Click **Refresh** to display updated information.
Port Name	This section displays the name of the port.
Rate	The rate fields display the transmission rates. “Line Down” indicates that the ADSL port is not connected to a subscriber.
Down/up Stream Rate	These are the rates (in Kbps) at which the port has been sending and receiving data.
Down/up Stream Noise Margin	These are the DSL line’s downstream and upstream noise margins. Measured in decibels (dB).
Down/up Stream Attenuation	These are the reductions in amplitude of the downstream and upstream DSL signals. Measured in decibels (dB).
Down/up Stream Attainable Rate	These are the highest theoretically possible transfer rates (in Kbps) at which the port could send and receive data.
Info	
Service Mode	This field displays the ADSL standard that the port is using: G.dmt (AAM1212-51), G.dmt Annex B (AAM1212-53), ETSI (AAM1212-53), G.lite, ANSI T1.413 issue 2 (AAM1212-51), ADSL2, or ADSL2+.
Trellis Encoding	This field displays whether Trellis encoding is turned on or off. Trellis encoding helps to reduce the noise in ADSL transmissions. Trellis may reduce throughput but it makes the connection more stable.[A]
Down Stream Interleave Delay	This field displays the number of milliseconds of interleave delay for downstream transmissions.
Up Stream Interleave Delay	This field displays the number of milliseconds of interleave delay for upstream transmissions.
Down Stream Output Power	This field displays the amount of power that this port is using to transmit to the subscriber’s ADSL modem or router. The total output power of the transceiver varies with the length and line quality. The farther away the subscriber’s ADSL modem or router is or the more interference there is on the line, the more power is needed.
Up Stream Output Power	This field displays the amount of power that the subscriber’s ADSL modem or router is using to transmit to this port. The total output power of the transceiver varies with the length and line quality. The farther away the subscriber’s ADSL modem or router is or the more interference there is on the line, the more power is needed.
Info Atur Info Atuc	The **Info Atur** fields show data acquired from the ATUR (ADSL Termination Unit – Remote), in this case the subscriber’s ADSL modem or router, during negotiation/provisioning message interchanges. This information can help in identifying the subscriber’s ADSL modem or router. The **Info Atuc** fields show data acquired from the ATUC (ADSL Termination Unit – Central), in this case AAM1212, during negotiation/provisioning message interchanges. The vendor ID, vendor version number and product serial number are obtained from vendor ID fields (see ITU-T G.994.1) or R-MSGS1 (see T1.413).

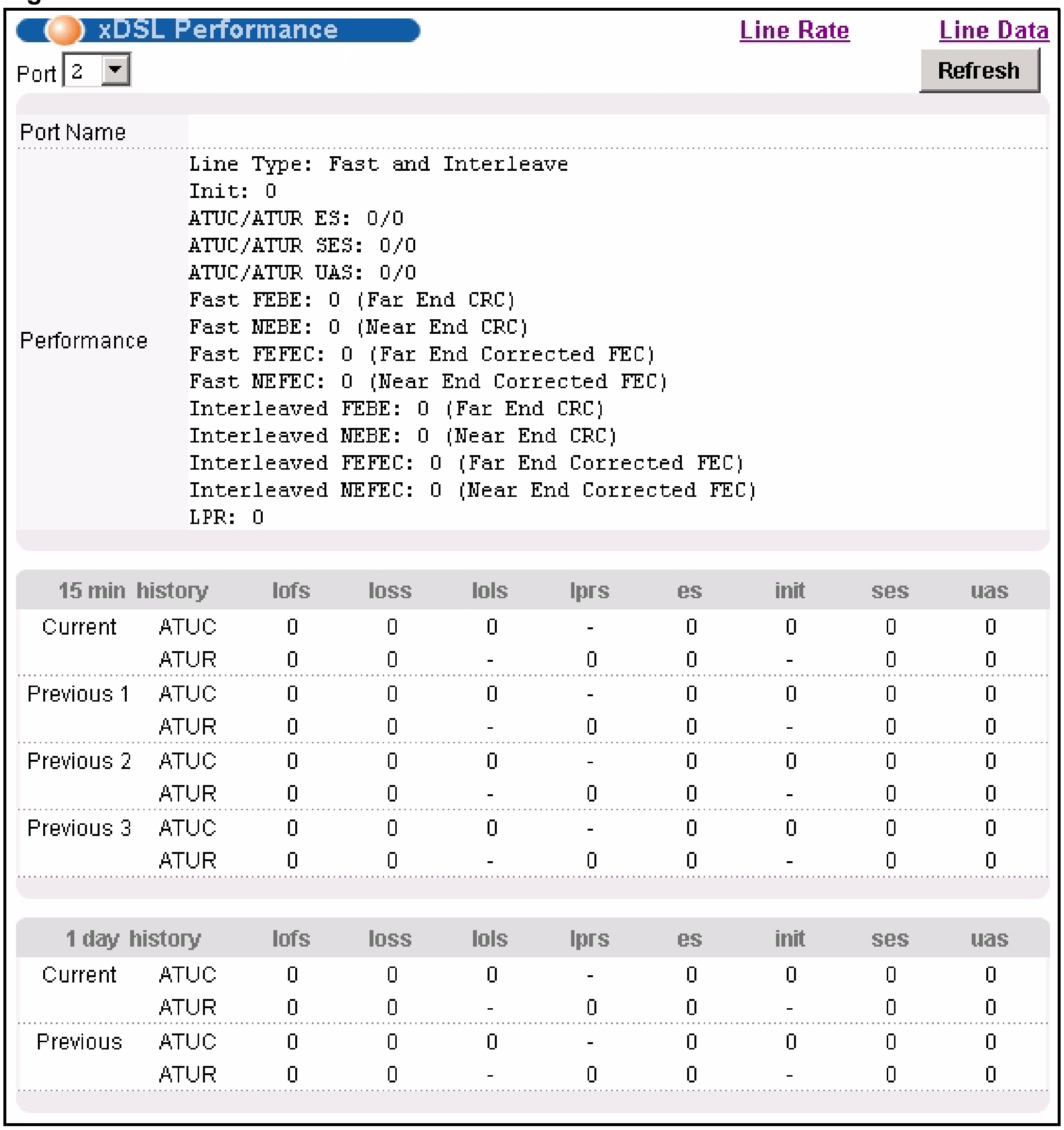
A. At the time of writing, the AAM1212 always uses Trellis coding.

15.2 xDSL Performance Screen

These counters display line performance data that has been accumulated since the system started. The definitions of near end/far end are always relative to the ATU-C (ADSL Termination Unit-Central Office). ATU-C refers to downstream traffic from the AAM1212. ATU-R (ADSL Termination Unit-Remote) refers to upstream traffic from the subscriber.

To open this screen, click **Basic Setting**, **xDSL Line Data**, **Line Performance**.

Figure 64 xDSL Performance



The following table describes the labels in this screen.

Table 31 xDSL Performance

LABEL	DESCRIPTION
Line Rate	Click **Line Rate** to display an ADSL port's line operating values (see Section 15.1 on page 139).
Line Data	Click **Line Data** to display an ADSL port's line bit allocation (see Section 15.3 on page 143).
Port	Use this drop-down list box to select a port for which you wish to view information.
Refresh	Click **Refresh** to display updated information.
Port Name	This section displays the name of the port.
Performance (since last link up)	
Line Type	"Fast" stands for non-interleaved (fast mode) and "Interleaved" stands for interleaved mode.
Init	This field displays the number of link-ups and link-downs.
ATUC/ATUR ES	The Number of Errored Seconds transmitted (downstream) or received (upstream) on this ADSL port.
ATUC/ATUR SES	The Number of Severely Errored Seconds transmitted (downstream) or received (upstream) on this ADSL port. Severely errored seconds contained 30% or more errored blocks or at least one defect. This is a subset of the **Down/Up Stream ES**.
ATUC/ATUR UAS	The downstream or upstream number of UnAvailable Seconds.
Fast FEBE	In fast mode, the number of Far End Block Errors (Far End Cyclic Redundancy Checks).
Fast NEBE	In fast mode, the number of Near End Block Errors (Near End Cyclic Redundancy Checks).
Fast FEFEC	In fast mode, the Far End number of ADSL frames repaired by Forward Error Correction.
Fast NEFEC	In fast mode, the Near End number of ADSL frames repaired by Forward Error Correction.
Interleaved FEBE	In interleaved mode, the number of Far End Block Errors (Far End Cyclic Redundancy Checks).
Interleaved NEBE	In interleaved mode, the number of Near End Block Errors (Near End Cyclic Redundancy Checks).
Interleaved FEFEC	In interleaved mode, the Far End number of ADSL frames repaired by Forward Error Correction.
Interleaved NEFEC	In interleaved mode, the Near End number of ADSL frames repaired by Forward Error Correction.
LPR	This is the number of times that the subscriber's ADSL device has experienced a Loss of Power (been off).
15 min, 1day history	This section of the screen displays line performance statistics for the current and previous 15-minute periods, as well as for the current and previous 24 hours.
lofs	The number of Loss Of Frame Seconds that have occurred within the period.
loss	The number of Loss Of Signal Seconds that have occurred within the period.
lols	The number of Loss Of Link Seconds that have occurred within the period.

Table 31 xDSL Performance (continued)

LABEL	DESCRIPTION
lprs	The number of Loss of Power Seconds that have occurred within the period.
es	The number of Errored Seconds that have occurred within the period.
init	The number of successful initializations that have occurred within the period.
ses	The number of Severely Errored Seconds that have occurred within the period.
uas	The number of UnAvailable Seconds that have occurred within the period.

15.3 xDSL Line Data Screen

This screen displays an ADSL port’s line bit allocation.

Discrete Multi-Tone (DMT) modulation divides up a line’s bandwidth into tones. This screen displays the number of bits transmitted for each tone. This can be used to determine the quality of the connection, whether a given sub-carrier loop has sufficient margins to support ADSL transmission rates, and possibly to determine whether certain specific types of interference or line attenuation exist. See the ITU-T G.992.1 recommendation for more information on DMT.

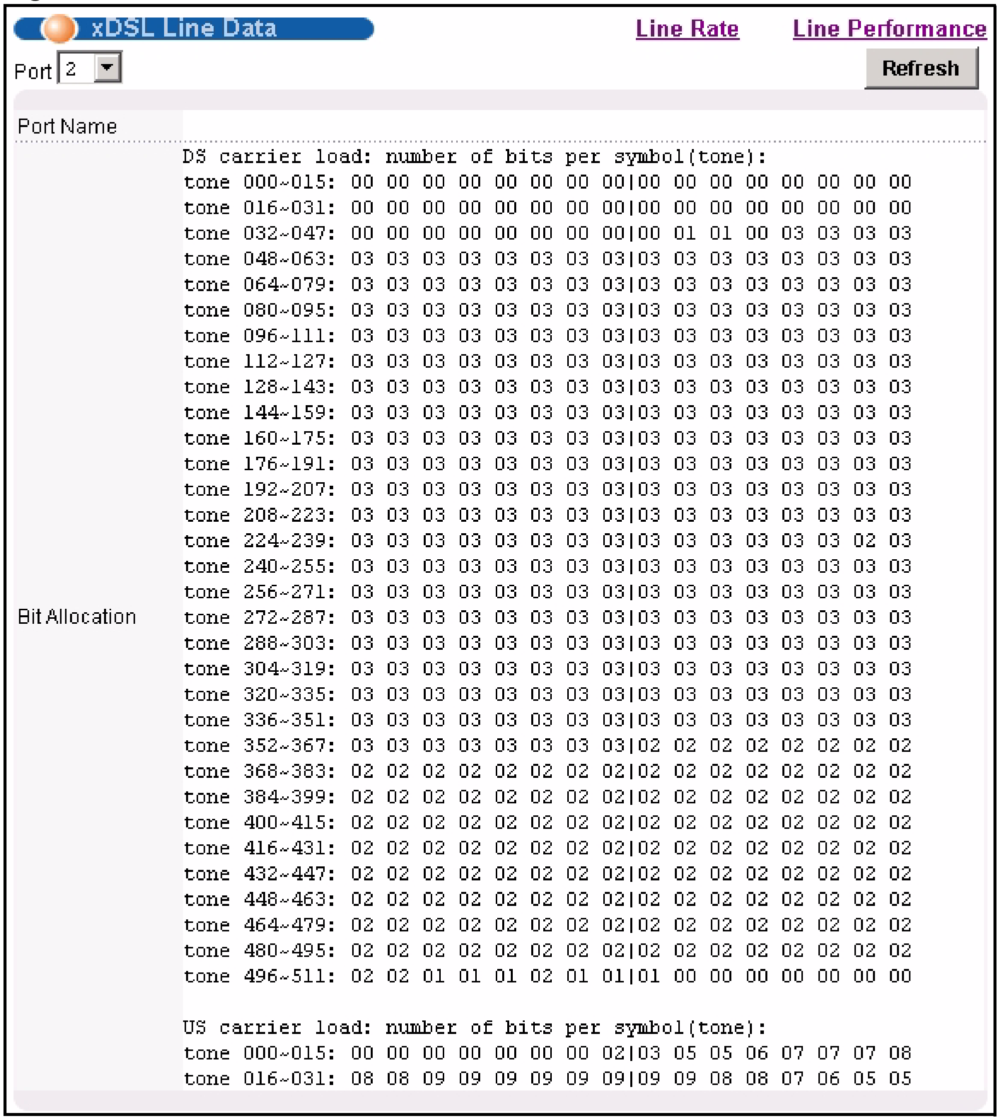
The better (or shorter) the line, the higher the number of bits transmitted for a DMT tone. The maximum number of bits that can be transmitted per DMT tone is 15.

The bit allocation contents are only valid when the link is up.

To open this screen, click **Basic Setting**, **xDSL Line Data**, **Line Data**.

In the screen shown, the downstream channel is carried on tones 48 to 255 and the upstream channel is carried on tones 16 to 31 (space is left between the channels to avoid interference).

Figure 65 xDSL Line Data



The following table describes the labels in this screen.

Table 32 xDSL Line Data

LABEL	DESCRIPTION
Line Rate	Click **Line Rate** to display an ADSL port's line operating values (see Section 15.1 on page 139).
Line Performance	Click **Line Performance** to display an ADSL port's line performance counters (see Section 15.2 on page 141).
Port	Use this drop-down list box to select a port for which you wish to view information.
Refresh	Click **Refresh** to display updated information.

Table 32 xDSL Line Data (continued)

LABEL	DESCRIPTION
Port Name	This section displays the name of the port.
Bit Allocation	“DS carrier load” displays the number of bits transmitted per DMT tone for the downstream channel (from the AAM1212 to the subscriber’s DSL modem or router). “US carrier load” displays the number of bits received per DMT tone for the upstream channel (from the subscriber’s DSL modem or router to the AAM1212).

PART III Advanced

VLAN (149)
IGMP (157)
Static Multicast (167)
Multicast VLAN (169)
Filtering (175)
MAC Filter (177)
Spanning Tree Protocol (179)
Port Authentication (185)
Port Security (189)
DHCP Relay (191)
DHCP Snoop (195)
2684 Routed Mode (199)
PPPoA to PPPoE (207)
DSCP (213)
TLS PVC (215)
ACL (219)
Downstream Broadcast (225)
Syslog (227)
Access Control (229)
PPPoE Intermediate Agent (237)
Maximum MTU Size (241)
PVC Upstream Limit (243)
OUI Filter (247)

16
VLAN

This chapter shows you how to configure IEEE 802.1Q tagged VLANs.

16.1 Introduction to VLANs

A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Devices on a logical network belong to one group. A device can belong to more than one group. With VLAN, a device cannot directly talk to or hear from devices that are not in the same group(s); the traffic must first go through a router.

In MTU (Multi-Tenant Unit) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network resources of another on the same LAN, thus a user will not see the printers and hard disks of another user in the same building.

VLAN also increases network performance by limiting broadcasts to a smaller and more manageable logical broadcast domain. In traditional switched environments, all broadcast packets go to each and every individual port. With VLAN, all broadcasts are confined to a specific broadcast domain.

Note that a VLAN is unidirectional, it only governs outgoing traffic.

16.2 Introduction to IEEE 802.1Q Tagged VLAN

Tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges - they are not confined to the device on which they were created. The VLANs can be created statically by hand or configured dynamically using GVRP.[1] The VLAN ID associates a frame with a specific VLAN and provides the information that devices need to process the frame across the network. A tagged frame is four bytes longer than an untagged frame and contains two bytes of TPID (Tag Protocol Identifier, residing within the type/length field of the Ethernet frame) and two bytes of TCI (Tag Control Information, starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 (2^{12}) VLANs. Note that user priority and VLAN

1. GVRP (GARP VLAN Registration Protocol) defines a way for switches to automatically configure switches in a VLAN network.

ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

TPID 2 Bytes	User Priority 3 Bits	CFI 1 Bit	VLAN ID 12 bits

The AAM1212 handles up to 4094 VLANs (VIDs 1-4094). The device accepts incoming frames with VIDs 1-4094.

16.2.1 Forwarding Tagged and Untagged Frames

Each port on the device is capable of passing tagged or untagged frames. To forward a frame from an 802.1Q VLAN-aware switch to an 802.1Q VLAN-unaware switch, the AAM1212 first decides where to forward the frame and then strips off the VLAN tag. To forward a frame from an 802.1Q VLAN-unaware switch to an 802.1Q VLAN-aware switch, the AAM1212 first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID. The default PVID is VLAN 1 for all ports, but this can be changed.

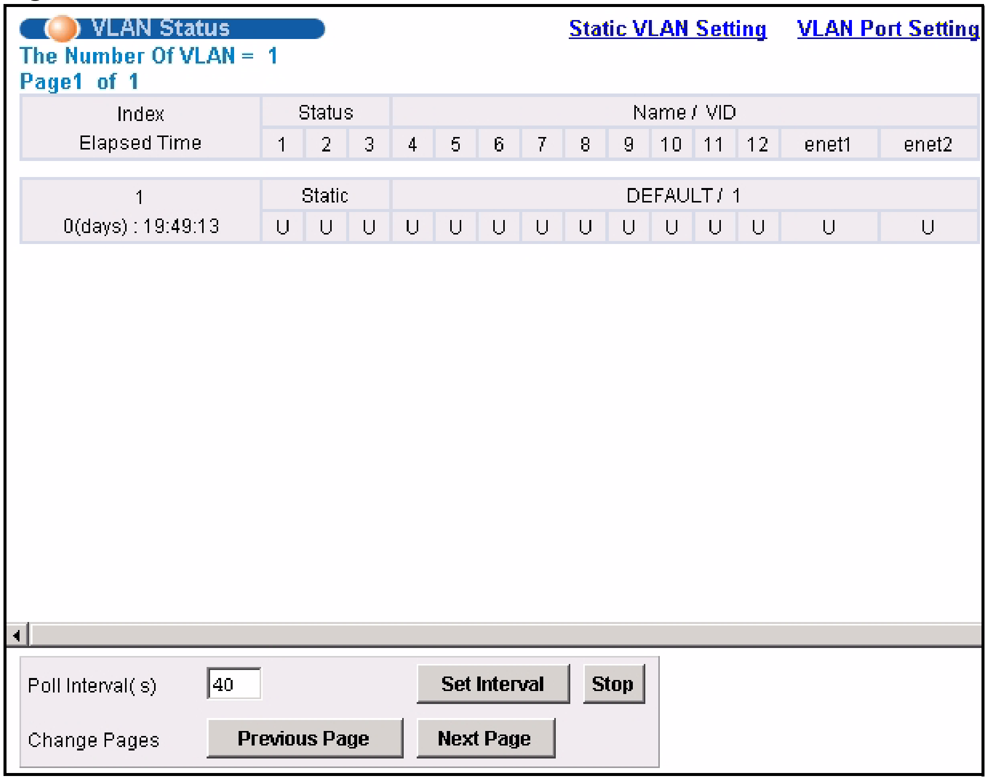
The egress (outgoing) port(s) of a frame is determined on the combination of the destination MAC address and the VID of the frame. For a unicast frame, the egress port (based on the destination MAC address) must be a member of the VID, also; otherwise, the frame is blocked. For a broadcast frame, it is duplicated only on ports (except the ingress port itself) that are members of the VID, thus confining the broadcast to a specific domain.

Whether to tag an outgoing frame depends on the setting of the egress port on a per-VLAN, per-port basis (recall that a port can belong to multiple VLANs). If the tagging on the egress port is enabled for the VID of a frame, then the frame is transmitted as a tagged frame; otherwise, it is transmitted as an untagged frame.

16.3 VLAN Status Screen

To open this screen, click **Advanced Application**, **VLAN**.

Figure 66 VLAN Status



The following table describes the labels in this screen.

Table 33 VLAN Status

LABEL	DESCRIPTION
Static VLAN Setting	Click **Static VLAN Setting** to configure ports to dynamically join a VLAN group or permanently assign ports to a VLAN group or prohibit ports from joining a VLAN group (see Section 16.4 on page 152).
VLAN Port Setting	Click **VLAN Port Setting** to specify Port VLAN IDs (PVIDs). See Section 16.5 on page 153.
The Number of VLAN	This is the number of VLANs configured on the AAM1212.
Page X of X	This identifies which page of VLAN status information is displayed and how many total pages of VLAN status information there are.
	The first table displays the names of the fields. The subsequent tables show the settings of the VLANs.
Index	This is the VLAN index number.
Name / VID	The name identifies an individual VLAN. The vid is the PVID, the Port VLAN ID assigned to untagged frames or priority-tagged frames received on this port.
1~12, enet1, enet2	These columns display the VLAN's settings for each port. A tagged port is marked as **T**, an untagged port is marked as **U** and ports not participating in a VLAN are marked as "**–**".
Elapsed Time	This field shows how long it has been since a normal VLAN was registered or a static VLAN was set up.
Status	This field shows that this VLAN was added to the AAM1212 statically, that is, added as a permanent entry.

Table 33 VLAN Status (continued)

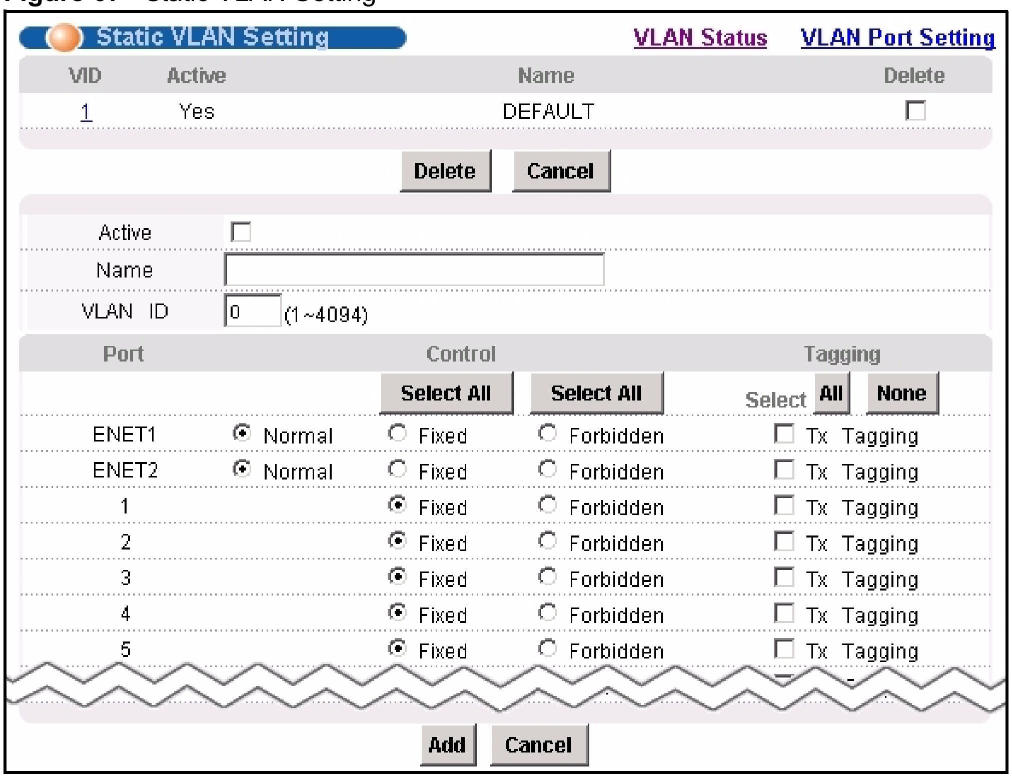
LABEL	DESCRIPTION
Poll Interval(s) Set Interval	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to halt polling statistics.
Previous Page Next Page	Click one of these buttons to show the preceding/following screen if the information cannot be displayed in one screen.

16.4 Static VLAN Setting Screen

You can assign a port to be a member of a VLAN group or prohibit a port from joining a VLAN group in this screen. This is an IEEE 802.1Q VLAN.

To open this screen, click **Advanced Application**, **VLAN**, **Static VLAN Setting**.

Figure 67 Static VLAN Setting



The following table describes the labels in this screen.

Table 34 Static VLAN Setting

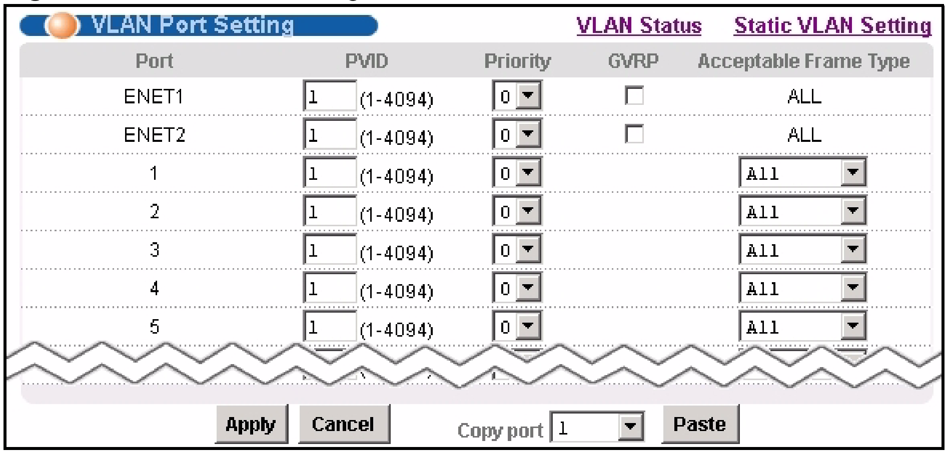
LABEL	DESCRIPTION
VLAN Status	Click **VLAN Status** to see which of the AAM1212's ports are members of which VLANs (see Section 16.3 on page 150)
VLAN Port Setting	Click **VLAN Port Setting** to specify Port VLAN IDs (PVIDs). See Section 16.5 on page 153.
VID	This field displays the ID number of the VLAN group. Click the number to edit the VLAN settings.
Active	This field indicates whether the VLAN settings are enabled (**Yes**) or disabled (**No**).
Name	This field displays the descriptive name for this VLAN group.
Delete	Select the check boxes of the rule(s) that you want to remove in the **Delete** column and then click the **Delete** button. You cannot delete a VLAN if any PVIDs are set to use the VLAN or the VLAN is the CPU (management) VLAN.
Cancel	Click **Cancel** to clear the **Delete** check boxes.
Active	Select this check box to enable the VLAN. You cannot disable a VLAN if any PVIDs are set to use the VLAN or the VLAN is the CPU (management) VLAN.
Name	Enter a descriptive name for this VLAN group for identification purposes. Spaces are not allowed.
VLAN ID	Enter the VLAN ID for this static VLAN entry; the valid range is between 1 and 4094.
Port	The port numbers identify the AAM1212's ports.
Control	Select **Fixed** for the port to be a permanent member of this VLAN group. Use the **Select All** button to include every port. Select **Forbidden** if you want to prohibit the port from joining this VLAN group. Use the **Select All** button to include every port.
Tagging	Select **TX Tagging** if you want the port to tag all outgoing frames transmitted with this VLAN ID. Use the **All** button to include every port. Use the **None** button to clear all of the ports check boxes.
Add	Click **Add** to save your settings. The VLAN then displays in the summary table at the top of the screen. Clicking **Add** saves your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring the fields afresh.

16.5 VLAN Port Setting Screen

Use this screen to specify port VLAN IDs and to set whether or not Ethernet ports propagate VLAN information to other devices.

To open this screen, click **Advanced Application**, **VLAN**, **VLAN Port Setting**.

Figure 68 VLAN Port Setting

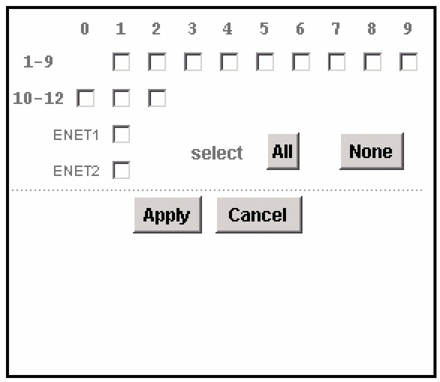


The following table describes the labels in this screen.

Table 35 VLAN Port Setting

LABEL	DESCRIPTION
VLAN Status	Click **VLAN Status** to see which of the AAM1212's ports are members of which VLANs (see Section 16.3 on page 150).
Static VLAN	Click **Static VLAN** to configure ports to dynamically join a VLAN group or permanently assign ports to a VLAN group or prohibit ports from joining a VLAN group (see Section 16.4 on page 152).
Port	The port numbers identify the AAM1212's ports.
PVID	Type the Port VLAN ID (PVID) from 1 to 4094. The AAM1212 assigns the PVID to untagged frames or priority frames (0 VID) received on this port.
Priority	Select an IEEE 802.1p priority to assign to untagged frames or priority frames (0 VID) received on this port.
GVRP	Select this check box if the AAM1212 should use GVRP to automatically register and configure VLAN membership.
Acceptable Frame Type	Select **All** to have the port accept both tagged and untagged incoming frames. [A] Select **Tag Only** to have the port only accept incoming frames that have a VLAN tag.
Apply	Click **Apply** to save your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.

Table 35 VLAN Port Setting (continued)

LABEL	DESCRIPTION
Cancel	Click **Cancel** to begin configuring this screen afresh.
Copy port Paste	Do the following to copy settings from one port to another port or ports. 1. Select the number of the port from which you want to copy settings. 2. Click **Paste** and the following screen appears. 3. Select to which ports you want to copy the settings. Use **All** to select every port. Use **None** to clear all of the check boxes. 4. Click **Apply** to paste the settings. **Figure 69** Select Ports 

A. At the time of writing, the **VLAN Acceptable Frame Type** field is read-only for the Ethernet ports. The AAM1212 accepts both tagged and untagged incoming frames on the Ethernet ports.

17

IGMP

This chapter describes the **IGMP** screens.

17.1 IGMP

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender to 1 recipient) or Broadcast (1 sender to everybody on the network). Multicast delivers IP packets to just a group of hosts on the network.

IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group - it is not used to carry user data. See RFC 1112 and RFC 2236 for information on IGMP versions 1 and 2, respectively.

17.2 IP Multicast Addresses

In IPv4, a multicast address allows a device to send packets to a specific group of hosts (multicast group) in a different sub-network. A multicast IP address represents a traffic receiving group, not individual receiving devices. IP addresses in the Class D range (224.0.0.0 to 239.255.255.255) are used for IP multicasting. Certain IP multicast numbers are reserved by IANA for special purposes (see the IANA web site for more information).

17.2.1 IGMP Snooping

A layer-2 switch can passively snoop on IGMP Query, Report and Leave (IGMP version 2) packets transferred between IP multicast routers/switches and IP multicast hosts to learn the IP multicast group membership. It checks IGMP packets passing through it, picks out the group registration information, and configures multicasting accordingly. IGMP snooping allows the AAM1212 to learn multicast groups without you having to manually configure them.

The AAM1212 forwards multicast traffic destined for multicast groups (that it has learned from IGMP snooping or that you have manually configured) to ports that are members of that group. The AAM1212 discards multicast traffic destined for multicast groups that it does not know. IGMP snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your device.

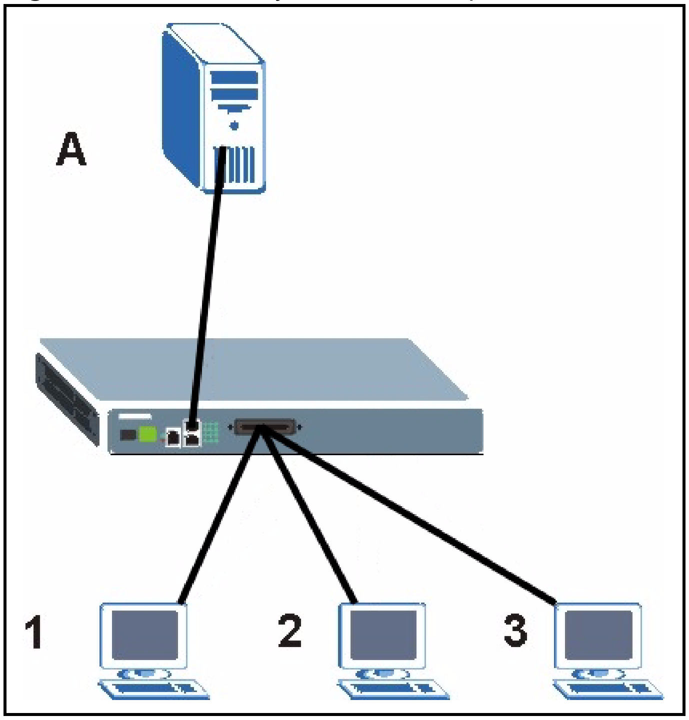
17.2.2 IGMP Proxy

To allow better network performance, you can use IGMP proxy instead of a multicast routing protocol in a simple tree network topology.

In IGMP proxy, an upstream interface is the port that is closer to the source (or the root of the multicast tree) and is able to receive multicast traffic. There should only be one upstream interface (also known as the query port) for one query VLAN on the AAM1212. A downstream interface is a port that connects to a host (such as a computer).

The following figure shows a network example where A is the multicast source while computers 1, 2 and 3 are the receivers. In the figure A is connected to the upstream interface and 1, 2 and 3 are connected to the downstream interface.

Figure 70 IGMP Proxy Network Example



The AAM1212 will not respond to IGMP join and leave messages on the upstream interface. The AAM1212 only responds to IGMP query messages on the upstream interface. The AAM1212 sends IGMP query messages to the hosts that are members of the query VLAN.

The AAM1212 only sends an IGMP leave messages via the upstream interface when the last host leaves a multicast group.

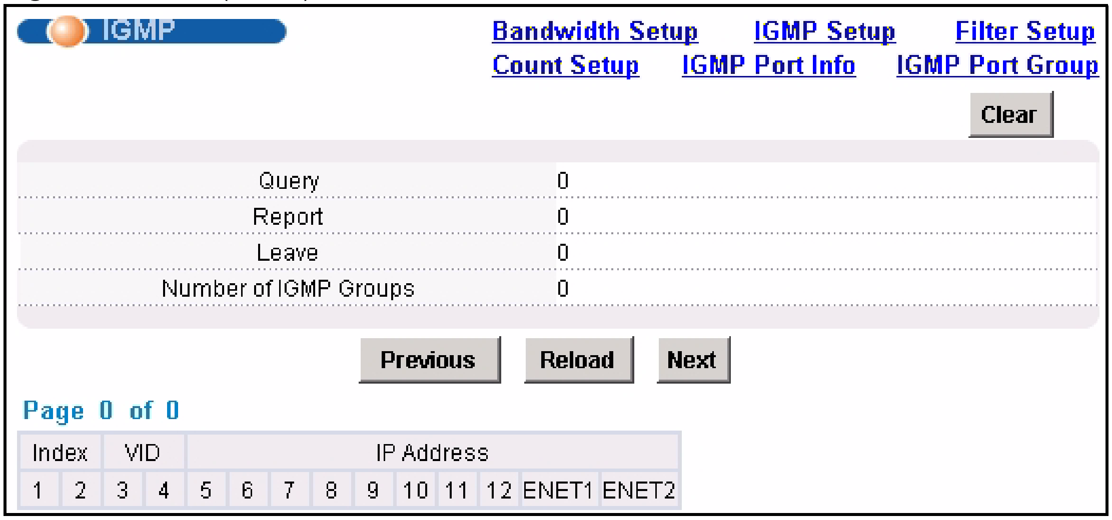
In daisychain mode, Ethernet interface 1 is set as the upstream interface and Ethernet interface 2 and the DSL ports are set as downstream interfaces.

17.3 IGMP Status Screen

Use this screen to view current IGMP information.

To open this screen, click **Advanced Application**, **IGMP**.

Figure 71 IGMP (Status)



The following table describes the labels in this screen.

Table 36 IGMP (Status)

LABEL	DESCRIPTION
Bandwidth Setup	Click **Bandwidth Setup** to open the **IGMP Bandwidth** screen where you can set up bandwidth requirements for multicast channels (see Section 17.4 on page 160). You can also open the **Bandwidth Port Setup** screen to set up multicast bandwidth requirements for selected ports (see Section 17.4.1 on page 161).
IGMP Setup	Click **IGMP Setup** to open the **IGMP Setup** screen where you can configure IGMP settings (see Section 17.5 on page 162).
Filter Setup	Click **Filter Setup** to open the **IGMP Filter Profile** screen where you can configure IGMP multicast filter profiles (see Section 17.6 on page 164).
Count Setup	Click **Count Setup** to open the **IGMP Count** screen where you can limit the number of IGMP groups a subscriber on a port can join (see Section 17.7 on page 164).
IGMP Port Info	Click **IGMP Port Info** to open the **IGMP Port Info** screen where you can look at the current number of IGMP-related packets received on each port (see Section 17.8 on page 165).
IGMP Port Group	Click **IGMP Port Group** to open the **IGMP Port Group** screen where you can look at the current list of multicast groups each port has joined (see Section 17.9 on page 166).
Clear	Click **Clear** to delete the information the AAM1212 has learned about multicast groups. This resets every counter in this screen.
Query	This is the total number of Query packets received.
Report	This is the total number of Report packets received.
Leave	This is the total number of Leave packets received.

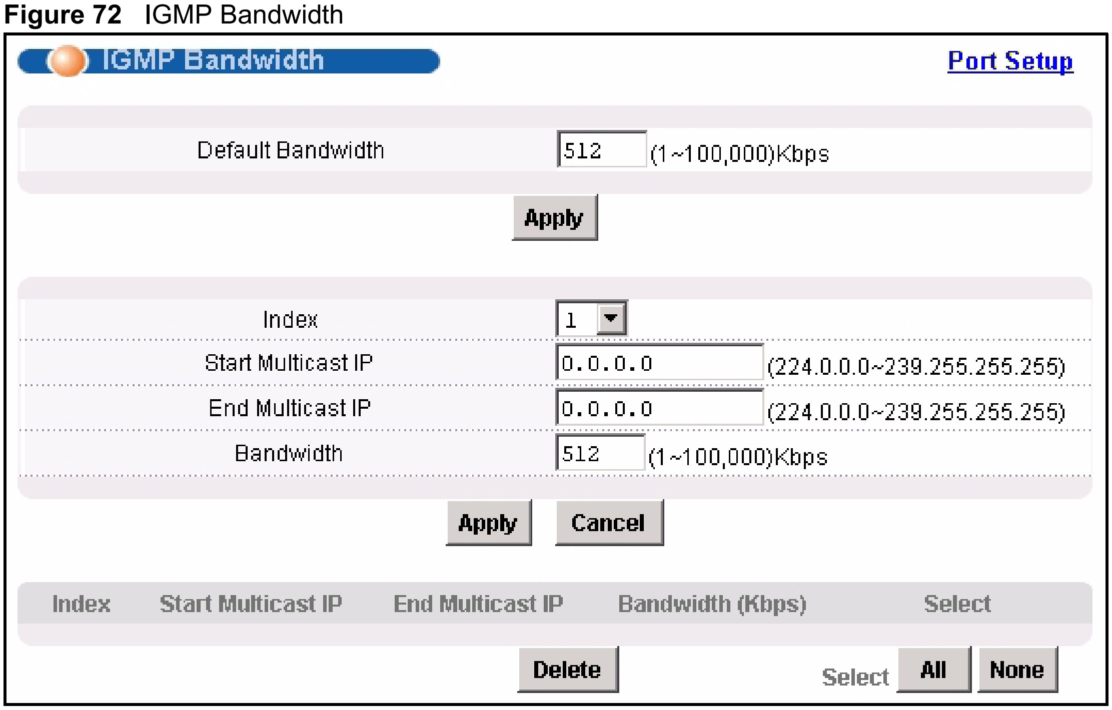
Table 36 IGMP (Status) (continued)

LABEL	DESCRIPTION
Number of IGMP Groups	This is how many IGMP groups the AAM1212 has identified on the local network.
Previous Next	Click one of these buttons to show the previous/next screen if all of the information cannot be seen in one screen.
Reload	Click this button to refresh the screen.
Page X of X	This identifies which page of information is displayed and the total number of pages of information.
	The first table displays the names of the fields. The subsequent tables show the settings of the IGMP groups.
Index	This is the IGMP group index number.
VID	The VID is the VLAN ID on which the IGMP group is created.
IP Address	This is the IP address of an IP multicast group member.
1~12, enet1, enet2	These columns indicate whether or not each port is a member of the IGMP snooping group.

17.4 IGMP Bandwidth Screen

Use this screen to set up bandwidth requirements for multicast channels. To open this screen, click **Advanced Application**, **IGMP**, **Bandwidth Setup**.

Figure 72 IGMP Bandwidth



The following table describes the labels in this screen.

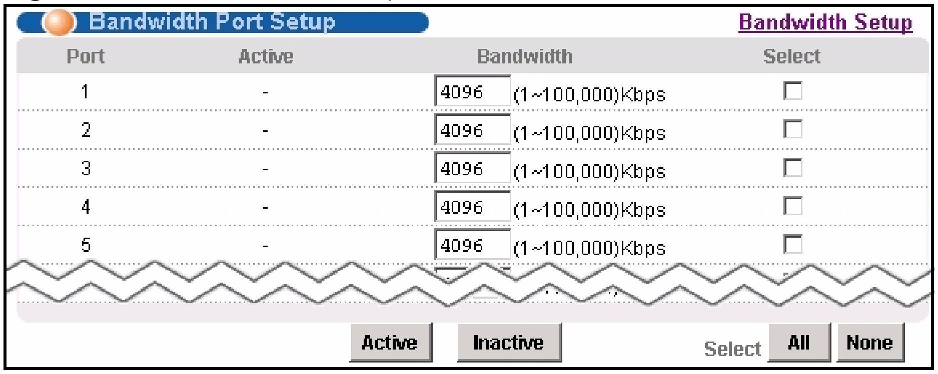
Table 37 IGMP Bandwidth

LABEL	DESCRIPTION
Port Setup	Click **Port Setup** to open the **Bandwidth Port Setup** screen where you can set up multicast bandwidth requirements on specified ports (see Section 17.4.1 on page 161).
Default Bandwidth	Enter the default bandwidth for multicast channels for which you have not configured bandwidth requirements.
Apply	Click **Apply** to save your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Index	Select a unique number for this setting. If you select a number that is already used, the new setting overwrites the old one when you click **Apply**.
Start Multicast IP	Enter the beginning of the multicast range.
End Multicast IP	Enter the end of the multicast range. For one multicast address, enter the start of the multicast range again.
Bandwidth	Enter the bandwidth requirement for the specified multicast range.
Apply	Click **Apply** to save the filter settings. The settings then display in the summary table at the bottom of the screen. Clicking **Apply** saves your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring the fields afresh.
	This table shows the multicast range settings.
Index	This field displays the number that identifies this setting.
Start Multicast IP	This field displays the beginning of the multicast range.
End Multicast IP	This field displays the end of the multicast range.
Bandwidth	This field displays the allowed bandwidth for the specified multicast range.
Select	Select this, and click **Delete** to remove the setting.
Delete	Click this to remove the selected settings.
Select All	Click this to select all entries in the table.
Select None	Click this to un-select all entries in the table.

17.4.1 Bandwidth Port Setup Screen

Use this screen to set up multicast bandwidth requirements for specific ports. To open this screen, click **Advanced Application**, **IGMP**, **Bandwidth Setup, Port Setup**.

Figure 73 Bandwidth Port Setup



The following table describes the labels in this screen.

Table 38 Bandwidth Port Setup

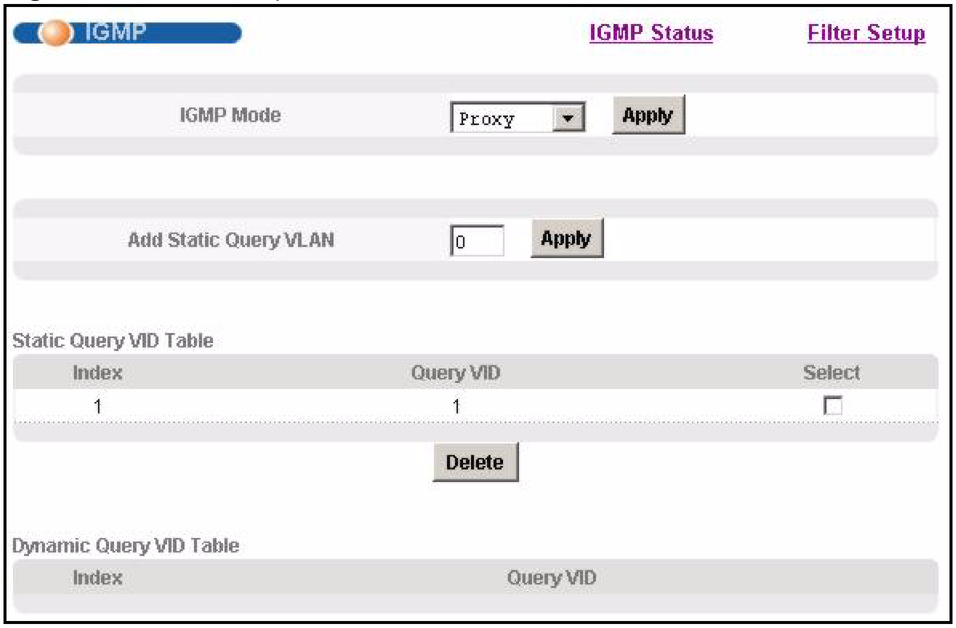
LABEL	DESCRIPTION
Bandwidth Setup	Click **Bandwidth Setup** to open the **IGMP Bandwidth** screen where you can set up bandwidth requirements for multicast channels (see Section 17.4 on page 160).
Port	This field shows each DSL port number.
Active	This field shows whether or not multicast bandwidth requirements are enabled on this port. “V” displays if it is enabled and “-“ displays if it is disabled.
Bandwidth	Enter the maximum acceptable multicast bandwidth for this port. This has no effect if bandwidth requirements are disabled.
Select	Select this, and click **Active** or **Inactive** to enable or disable the specified multicast bandwidth requirements on this port.
Active	Click this to enable the specified multicast bandwidth requirements on the selected port.
Inactive	Click this to disable the specified multicast bandwidth requirements on the selected port.
Select All	Click this to select all entries in the table.
Select None	Click this to un-select all entries in the table.

17.5 IGMP Setup Screen

Use this screen to configure your IGMP settings.

To open this screen, click **Advanced Application**, **IGMP**, **IGMP Setup**.

Figure 74 IGMP Setup



The following table describes the labels in this screen.

Table 39 IGMP Setup

LABEL	DESCRIPTION
IGMP Status	Click **IGMP Status** to open the **IGMP Setup** screen where you can view current IGMP information (see Section 17.3 on page 159).
Filter Setup	Click **Filter Setup** to open the **IGMP Filter Profile** screen where you can configure IGMP multicast filter profiles (see Section 17.6 on page 164).
IGMP Mode	Select **Proxy** to have the device use IGMP proxy. Select **Snooping** to have the device passively learn multicast groups. Select **Disable** to have the device use neither IGMP proxy nor snooping.
Apply	Click **Apply** to save your IGMP mode settings. Clicking **Apply** saves your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Add Static Query VLAN	Enter a VLAN ID in this field and click **Apply** to create a static query VLAN.
Static Query VID Table	This displays the static IGMP query VLANs already configured on the AAM1212.
Index	This is the index number of an existing static IGMP query VLAN on the AAM1212.
Query VID	This is the static IGMP query VLAN's VLAN ID.
Select	Click this to select an entry in the static query VLAN table.
Delete	Select a static query VLAN and click this to remove it from the table.
Dynamic Query VID Table	This section displays the list of dynamic query VLANs.

Table 39 IGMP Setup (continued)

LABEL	DESCRIPTION
Index	This is the dynamic IGMP query VLAN.
Query VID	This is the dynamic IGMP query VLAN's VLAN ID.

17.6 IGMP Filter Setup Screen

To open this screen, click **Advanced Application**, **IGMP**, **Filter Setup**. This screen is discussed in Section 14.7 on page 135.

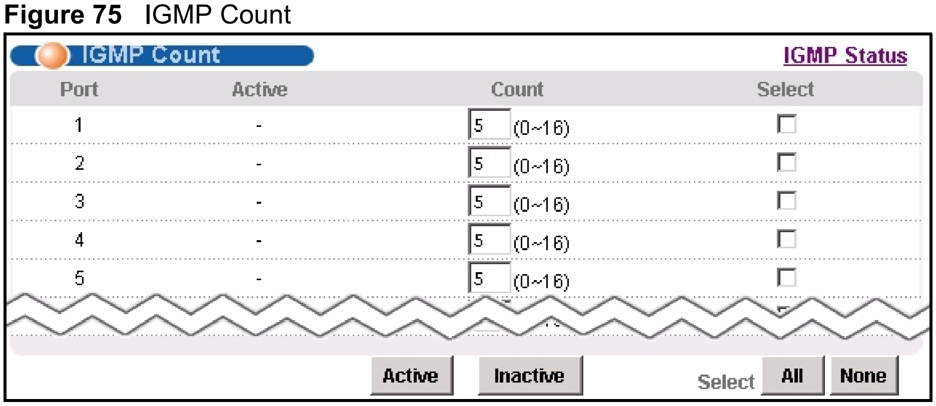
17.7 IGMP Count Screen

Use this screen to limit the number of IGMP groups a subscriber on a port can join. This allows you to control the distribution of multicast services (such as content information distribution) based on service plans and types of subscription.

IGMP count is useful for ensuring the service quality of high bandwidth services like video or Internet Protocol television (IPTV). IGMP count can limit how many channels (IGMP groups) the subscriber connected to a DSL port can use at a time. If each channel requires 4~5 Mbps of download bandwidth, and the subscriber's connection supports 11 Mbps, you can use IGMP count to limit the subscriber to using just 2 channels at a time. This also effectively limits the subscriber to using only two IPTVs with the DSL connection.

To open this screen, click **Advanced Application**, **IGMP**, **Count Setup**.

Figure 75 IGMP Count



The following table describes the labels in this screen.

Table 40 IGMP Count

LABEL	DESCRIPTION
IGMP Status	Click **IGMP Status** to open the **IGMP Setup** screen where you can view current IGMP information (see Section 17.3 on page 159).
Port	This field shows each DSL port number.

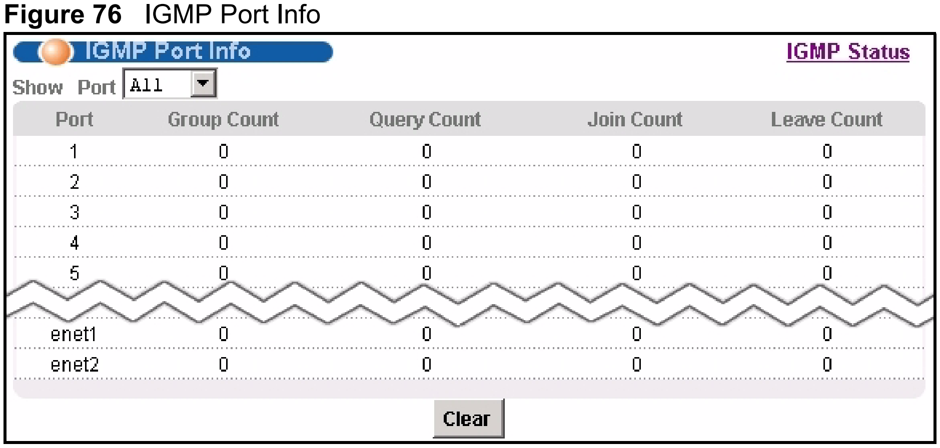
Table 40 IGMP Count (continued)

LABEL	DESCRIPTION
Active	This field shows whether or not the IGMP count limit is enabled on this port. “V” displays if it is enabled and “-“ displays if it is disabled.
Count	Enter the maximum number of IGMP groups a subscriber on this port can join. This has no effect if the IGMP count limit is disabled.
Select	Select this, and click **Active** or **Inactive** to enable or disable the specified IGMP count limit on this port.
Active	Click this to enable the specified IGMP count limits on the selected ports.
Inactive	Click this to disable the specified IGMP count limits on the selected ports.
Select All	Click this to select all entries in the table.
Select None	Click this to un-select all entries in the table.

17.8 IGMP Port Info Screen

Use this screen to display the current number of IGMP-related packets received on each port. To open this screen, click **Advanced Application**, **IGMP**, **IGMP Port Info**.

Figure 76 IGMP Port Info



The following table describes the labels in this screen.

Table 41 IGMP Port Info

LABEL	DESCRIPTION
IGMP Status	Click **IGMP Status** to open the **IGMP Setup** screen where you can view current IGMP information (see Section 17.3 on page 159).
Show Port	Select a port for which you wish to view information.
Port	This field shows each port number.
Group Count	This is the total number of Group packets received on this port.
Query Count	This is the total number of Query packets received on this port.
Join Count	This is the total number of Join packets received on this port.

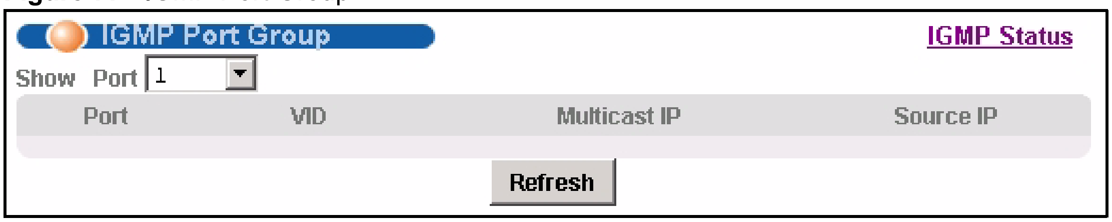
Table 41 IGMP Port Info (continued)

LABEL	DESCRIPTION
Leave Count	This is the total number of Leave packets received on this port.
Clear	Click **Clear** to delete the information the AAM1212 has learned about multicast groups. This resets every counter in this screen.

17.9 IGMP Port Group Screen

Use this screen to display the current list of multicast groups each port joins. To open this screen, click **Advanced Application**, **IGMP**, **IGMP Port Group**.

Figure 77 IGMP Port Group



The following table describes the labels in this screen.

Table 42 IGMP Port Group

LABEL	DESCRIPTION
IGMP Status	Click **IGMP Status** to open the **IGMP Setup** screen where you can view current IGMP information (see Section 17.3 on page 159).
Show Port	Select a port for which you wish to view information.
Port	This field shows each port number.
VID	This field shows the associated VLAN ID.
Multicast IP	This field shows the IP address of the multicast group joined by this port.
Source IP	This field shows the IP address of the client that joined the multicast group on this port.
Refresh	Click **Refresh** to display updated information.

18

Static Multicast

This chapter describes the **Static Multicast** screen.

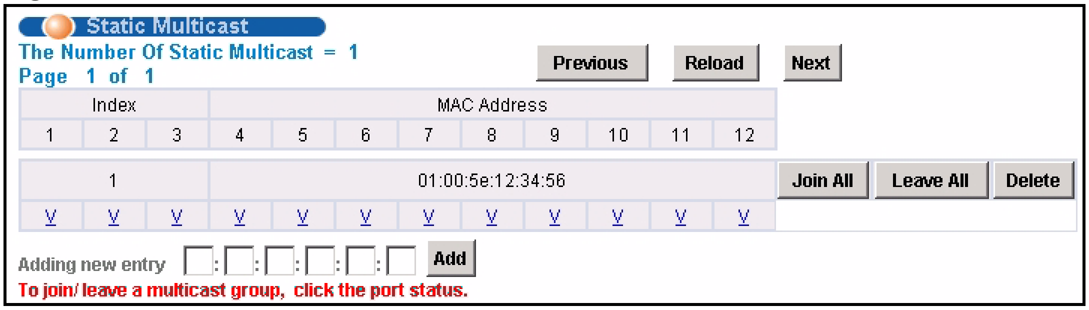
18.1 Static Multicast

Use static multicast to allow incoming frames based on multicast MAC address(es) that you specify. This feature can be used in conjunction with IGMP snooping/proxy to allow multicast MAC address(es) that are not learned by IGMP snooping or IGMP proxy. Use static multicast to pass routing protocols, such as RIP and OSPF.

18.2 Static Multicast Screen

To open this screen, click **Advanced Application**, **Static Multicast**.

Figure 78 Static Multicast



The following table describes the labels in this screen.

Table 43 Static Multicast

LABEL	DESCRIPTION
The Number of Static Multicast	This is the number of static multicast entries configured on the AAM1212.
Page X of X	This identifies which page of information is displayed and the total number of pages of information.
Previous Next	Click one of these buttons to show the previous/next screen if all status information cannot be seen in one screen.
Reload	Click this button to refresh the screen.

Table 43 Static Multicast (continued)

LABEL	DESCRIPTION
	The first table displays the names of the fields. The subsequent tables show the settings of the IGMP groups.
Index	This is the static multicast group index number.
MAC Address	This is the multicast MAC address.
1~12	These fields display the static multicast group membership status of the DSL ports. “V” displays for members and “-“ displays for non-members. Click a DSL port’s status to change it (clicking a “V” changes it to “-“ and vise versa).
Join All	Click **Join All** to make all of the DSL ports members of the static multicast group.
Leave All	Click **Leave All** to remove all of the DSL ports from the static multicast group.
Delete	Click **Delete** to remove a static multicast group.
Adding new entry Add	Type a multicast MAC address in the field, and click the **Add** button to create a new static multicast entry. Multicast MAC addresses must be `01:00:5E:xx:xx:xx`, where `x` is a “don’t care” value. For example, `01:00:5E:10:10:10` is a valid multicast MAC address. Clicking **Add** saves your changes to the AAM1212’s volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.

19 Multicast VLAN

This chapter describes the **Multicast VLAN** screens.

19.1 Multicast VLAN Overview

Multicast VLAN allows one single multicast VLAN to be shared among different subscriber VLANs on the network. This improves bandwidth utilization by reducing multicast traffic in the subscriber VLANs and simplifies multicast group management.

When the AAM1212 forwards traffic to a subscriber port, it tries to forward traffic to a normal PVC with the same VLAN ID. If this PVC does not exist, the AAM1212 uses the super channel instead. This applies to all downstream traffic, not just multicast traffic.

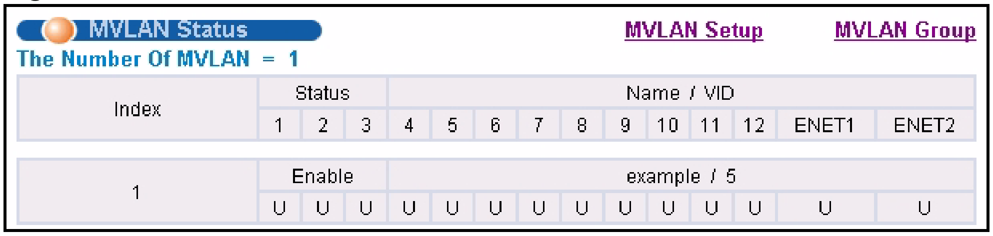
It is suggested to use a super channel for multicast VLAN. If a normal PVC is used and the multicast VLAN ID is not the same as the PVC's VID, the AAM1212 does not forward traffic to this PVC even if the subscriber's port has joined the multicast VLAN.

Since the AAM1212 might change the subscriber's VLAN ID to the multicast VLAN ID, both the subscriber's port and the Ethernet port should join the multicast VLAN.

19.2 MVLAN Status Screen

Use this screen to look at a summary of all multicast VLAN on the AAM1212. To open this screen, click **Advanced Application**, **Multicast VLAN**.

Figure 79 MVLAN Status


MVLAN Status

MVLAN Setup

MVLAN Group

The Number Of MVLAN = 1

Index	Status			Name / VID										
	1	2	3	4	5	6	7	8	9	10	11	12	ENET1	ENET2
1	Enable			example / 5										
	U	U	U	U	U	U	U	U	U	U	U	U	U	U

The following table describes the labels in this screen.

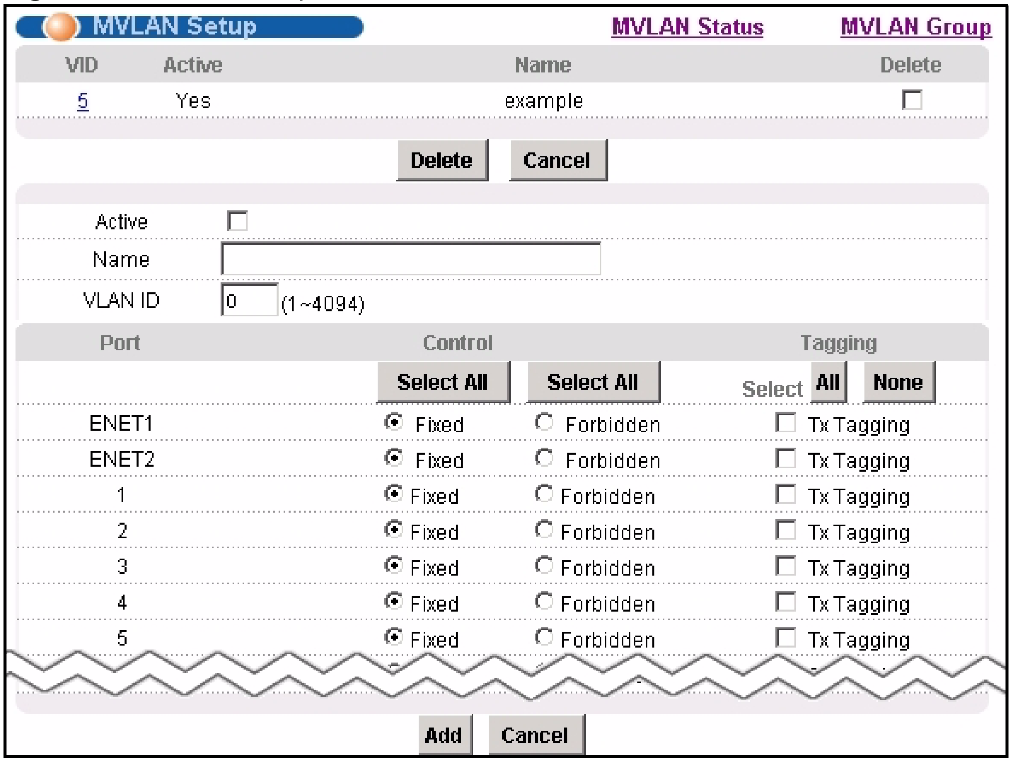
Table 44 MVLAN Status

LABEL	DESCRIPTION
MVLAN Setup	Click **MVLAN Setup** to open the **MVLAN Setup** screen where you can configure basic settings and port members for each multicast VLAN (see Section 19.3 on page 170).
MVLAN Group	Click **MVLAN Group** to open the **MVLAN Group** screen where you can configure ranges of multicast IP addresses for each multicast VLAN (see Section 19.4 on page 172).
The Number of MVLAN	This is the number of multicast VLAN configured on the AAM1212.
	The first table displays the names of the fields. The subsequent tables show the settings for each multicast VLAN.
Index	This is a sequential value and is not associated with this multicast VLAN.
Name / VID	This field shows the name and VLAN ID of this multicast VLAN.
1~12 ENET1-2	These fields display whether or not each port is a member of this multicast VLAN. “V” displays for members and “-“ displays for non-members. You can change these settings in the **MVLAN Setup** screen.
Status	This field shows whether this multicast VLAN is active (**Enable**) or inactive (**Disable**).

19.3 MVLAN Setup Screen

Use this screen to configure basic settings and port members for each multicast VLAN. To open this screen, click **Advanced Application**, **Multicast VLAN, MVLAN Setup**.

Figure 80 MVLAN Setup



The following table describes the labels in this screen.

Table 45 MVLAN Setup

LABEL	DESCRIPTION
MVLAN Status	Click **MVLAN Status** to open the **MVLAN Status** screen where you can view a summary of all multicast VLAN on the AAM1212 (see Section 19.2 on page 169).
MVLAN Group	Click **MVLAN Group** to open the **MVLAN Group** screen where you can configure ranges of multicast IP addresses for each multicast VLAN (see Section 19.4 on page 172).
VID	This field shows the VLAN ID of each multicast VLAN. Click it to edit its basic settings and port members in the fields below.
Active	This field shows whether this multicast VLAN is active (**Yes**) or inactive (**No**).
Name	This field shows the name of this multicast VLAN.
Delete	Select the check boxes of the rule(s) that you want to remove in the **Delete** column and then click the **Delete** button. You cannot delete a VLAN if any PVIDs are set to use the VLAN or the VLAN is the CPU (management) VLAN.
Cancel	Click **Cancel** to begin configuring the fields afresh.
Active	Select this if you want the multicast VLAN to be active. Clear this if you want the multicast VLAN to be inactive.
Name	Enter a descriptive name for the multicast VLAN. The name can be 1-31 printable ASCII characters long. Spaces are not allowed.
VLAN ID	Enter the VLAN ID of the multicast VLAN; the valid range is between 1 and 4094.

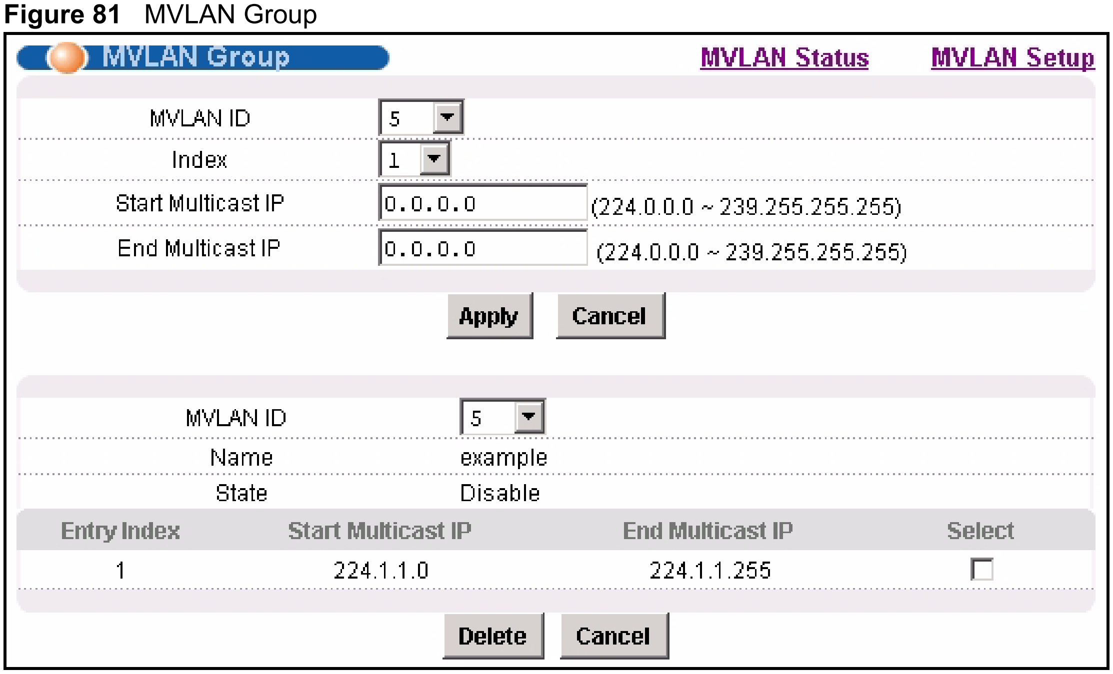
Table 45 MVLAN Setup (continued)

LABEL	DESCRIPTION
Port	This field displays each port number.
Control	Select **Fixed** for the port to be a permanent member of this multicast VLAN. Use the **Select All** button to include every port. Select **Forbidden** if you want to prohibit the port from joining this multicast VLAN. Use the **Select All** button to include every port.
Tagging	Select **TX Tagging** if you want the port to tag all outgoing frames transmitted with this VLAN ID. Use the **All** button to include every port. Use the **None** button to clear all of the ports check boxes.
Add	Click **Add** to save your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring the fields afresh.

19.4 MVLAN Group Screen

Use this screen to configure ranges of multicast IP addresses for each multicast VLAN. To open this screen, click **Advanced Application**, **Multicast VLAN, MVLAN Group**.

Figure 81 MVLAN Group



The following table describes the labels in this screen.

Table 46 MVLAN Group

LABEL	DESCRIPTION
MVLAN Status	Click **MVLAN Status** to open the **MVLAN Status** screen where you can view a summary of all multicast VLAN on the AAM1212 (see Section 19.2 on page 169).
MVLAN Setup	Click **MVLAN Setup** to open the **MVLAN Setup** screen where you can configure basic settings and port members for each multicast VLAN (see Section 19.3 on page 170).
MVLAN ID	Select the VLAN ID of the multicast VLAN for which you want to configure a range of multicast IP addresses.
Index	Select the index number of the multicast VLAN group (the range of multicast IP addresses) you want to configure for this multicast VLAN. If you want to change the current settings, select an index number that already exists. If you want to add a new multicast VLAN group, select an index number that does not exist.
Start Multicast IP	Enter the beginning of the range of multicast IP addresses. The IP address must be a valid multicast IP address, between 224.0.0.0 and 239.255.255.255.
End Multicast IP	Enter the end of the range of multicast IP addresses. The IP address must be a valid multicast IP address, between 224.0.0.0 and 239.255.255.255.
Apply	Click **Apply** to save your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring the fields afresh.
MVLAN ID	Select the VLAN ID of the multicast VLAN for which you want to look at or remove the multicast IP addresses currently added to it.
Name	This field displays the name of this multicast VLAN.
State	This field shows whether this multicast VLAN is active (**Enable**) or inactive (**Disable**).
Entry Index	This field displays the index number of each multicast VLAN group (the range of multicast IP addresses) configured for this multicast VLAN.
Start Multicast IP	This field displays the beginning of this range of multicast IP addresses.
End Multicast IP	This field displays the end of this range of multicast IP addresses.
Select	Select this, and click **Delete** to remove the multicast VLAN group.
Delete	Click this to remove the selected multicast VLAN groups.
Cancel	Click **Cancel** to begin configuring the fields afresh.

20

Filtering

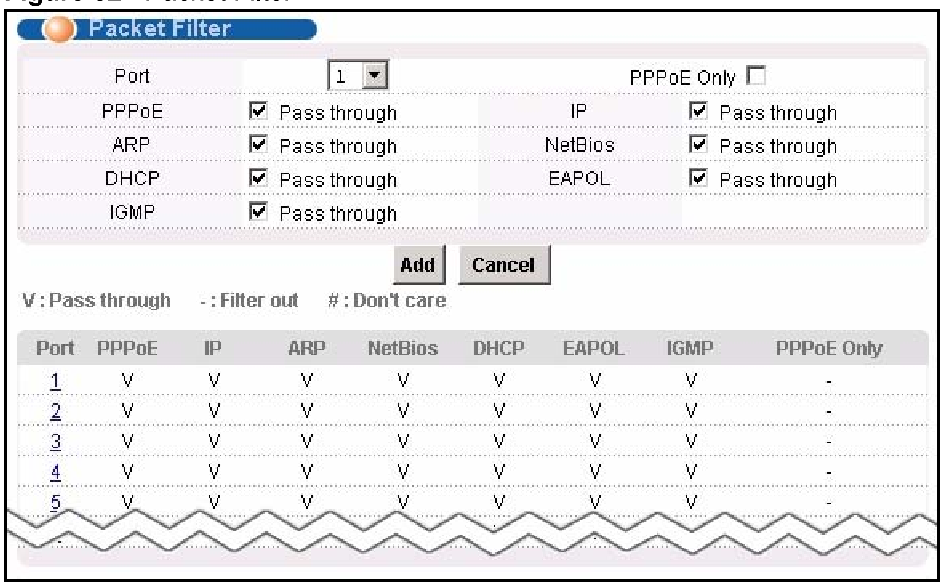
This chapter describes how to configure the **Packet Filter** screen.

20.1 Packet Filter Screen

Use this screen to set which types of packets the AAM1212 accepts on individual DSL ports.

To open this screen, click **Advanced Application**, **Filtering**.

Figure 82 Packet Filter



The following table describes the labels in this screen.

Table 47 Packet Filter

LABEL	DESCRIPTION
Port	Use this drop-down list box to select a DSL port for which you wish to configure packet type filtering. This box is read-only after you click on one of the port numbers in the table below.
PPPoE Only	Select this to allow only PPPoE traffic. This will gray out the check boxes for other packet types and the system will drop any non-PPPoE packets.

Table 47 Packet Filter (continued)

LABEL	DESCRIPTION
	Select the check boxes of the types of packets to accept on the DSL port. When you clear one of these check boxes, the field label changes to **Filter Out** and the system drops the corresponding type of packets
PPPoE Pass through	Point-to-Point Protocol over Ethernet relies on PPP and Ethernet. It is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as a single DSL line, wireless device or cable modem.
IP Pass through	Internet Protocol. The underlying protocol for routing packets on the Internet and other TCP/IP-based networks.
ARP Pass through	Address Resolution Protocol is a protocol for mapping an Internet Protocol address (IP address) to a physical computer address that is recognized in the local network.
NetBios Pass through	NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to find other computers.
DHCP Pass through	Dynamic Host Configuration Protocol automatically assigns IP addresses to clients when they log on. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses, for a period of time, which means that past addresses are “recycled” and made available for future reassignment to other systems.
EAPOL Pass through	EAP (Extensible Authentication Protocol, RFC 2486) over LAN. EAP is used with IEEE 802.1x to allow additional authentication methods (besides RADIUS) to be deployed with no changes to the access point or the wireless clients.
IGMP Pass through	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
Add Apply	Click **Add** or **Apply** to save the filter settings. The settings then display in the summary table at the bottom of the screen. Clicking **Add** or **Apply** saves your changes to the AAM1212’s volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring the fields afresh.
	This table shows the DSL port packet filter settings.
Port	These are the numbers of the DSL ports. Click this number to edit the port’s filter settings in the section at the top.
PPPoE, IP, ARP, NetBios, DHCP, EAPOL, IGMP, PPPoE Only	These are the packet filter settings for each port. “V” displays for the packet types that the AAM1212 is to accept on the port. “-“ displays for packet types that the AAM1212 is to reject on the port (packet types that are not listed are accepted). When you select **PPPoE Only**,”**#**” appears for all of the packet types. With **PPPoE Only**, the AAM1212 rejects all packet types except for PPPoE (packet types that are not listed are also rejected).

21

MAC Filter

This chapter introduces the MAC filter.

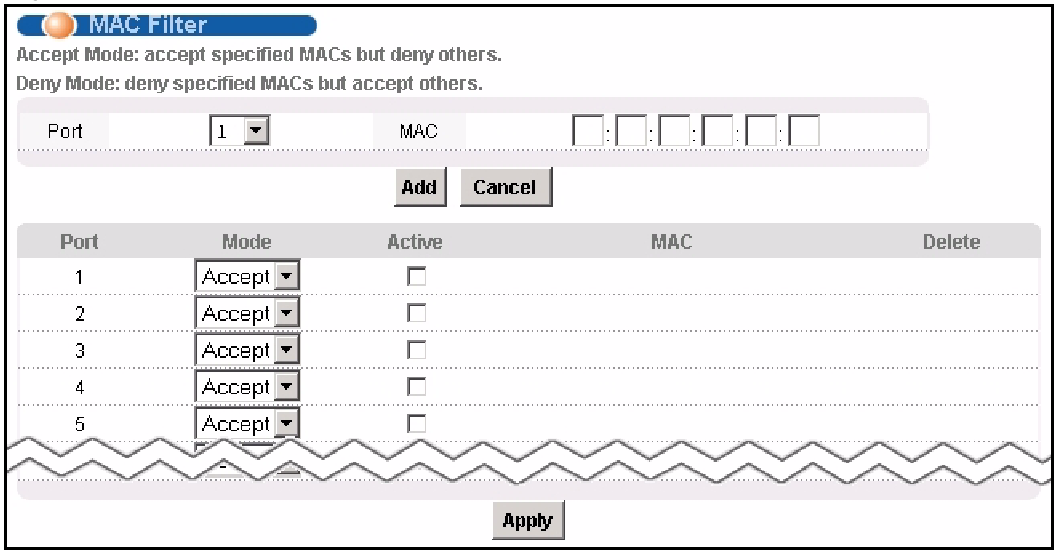
21.1 MAC Filter Introduction

Use the MAC filter to control from which MAC (Media Access Control) addresses frames can (or cannot) come in through a port.

21.2 MAC Filter Screen

To open this screen, click **Advanced Application**, **MAC Filter**.

Figure 83 MAC Filter



The following table describes the labels in this screen.

Table 48 MAC Filter

LABEL	DESCRIPTION
Port	Use this drop-down list box to select a DSL port for which you wish to configure MAC filtering.
MAC	Type a device’s MAC address in hexadecimal notation (xx:xx:xx:xx:xx:xx, where x is a number from 0 to 9 or a letter from a to f) in this field. The MAC address must be a valid MAC address.
Add	Click **Add** to save your changes to the AAM1212’s volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Port	These are the numbers of the DSL ports.
Mode	Select **Accept** to only allow frames from MAC addresses that you specify and block frames from other MAC addresses. Select **Deny** to block frames from MAC addresses that you specify and allow frames from other MAC addresses.
Active	Select this check box to turn on MAC filtering for a port.
MAC	This field lists the MAC addresses that are set for this port.
Delete	Click **Delete** to remove a MAC address from the list.
Apply	Click **Apply** to save your changes to the AAM1212’s volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.

22

Spanning Tree Protocol

This chapter introduces the Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP).

22.1 RSTP and STP

RSTP adds rapid reconfiguration capability to STP. The AAM1212 supports RSTP and the earlier STP. RSTP and STP detect and break network loops and provide backup links between switches, bridges or routers. They allow a device to interact with other RSTP or STP-aware devices in your network to ensure that only one path exists between any two stations on the network. The Integrated Ethernet Switch uses RSTP by default but can still operate with STP switches (although without RSTP's benefits).

The root bridge is the base of the spanning tree; it is the bridge with the lowest identifier value (MAC address). Path cost is the cost of transmitting a frame onto a LAN through that port. It is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost, as illustrated in the following table.

Table 49 Path Cost

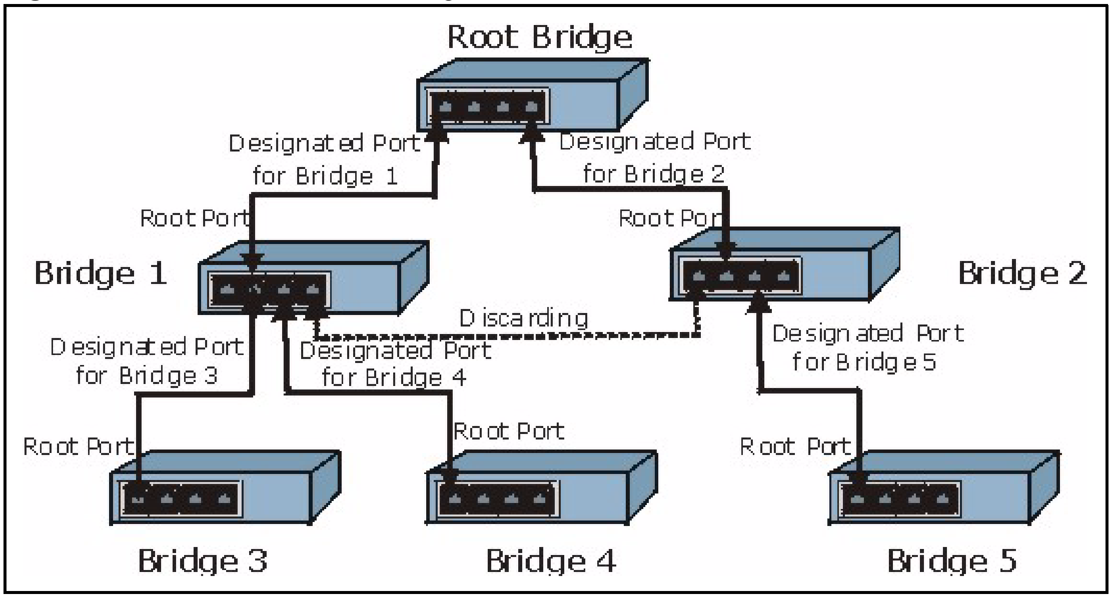
	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	4Mbps	250	100 to 1000	1 to 65535
Path Cost	10Mbps	100	50 to 600	1 to 65535
Path Cost	16Mbps	62	40 to 400	1 to 65535
Path Cost	100Mbps	19	10 to 60	1 to 65535
Path Cost	1Gbps	4	3 to 10	1 to 65535
Path Cost	10Gbps	2	1 to 5	1 to 65535

On each bridge, the root port is the port through which this bridge communicates with the root. It is the port on this Integrated Ethernet Switch with the lowest path cost to the root (the root path cost). If there is no root port, then this Integrated Ethernet Switch has been accepted as the root bridge of the spanning tree network.

For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.

After a bridge determines the lowest cost-spanning tree with RSTP, it enables the root port and the ports that are the designated ports for the connected LANs, and disables all other ports that participate in RSTP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

Figure 84 STP Root Ports and Designated Ports



RSTP-aware devices exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed.

In RSTP, the devices send BPDUs every Hello Time. If an RSTP-aware device does not get a Hello BPDU after three Hello Times pass (or the Max Age), the device assumes that the link to the neighboring bridge is down. This device then initiates negotiations with other devices to reconfigure the network to re-establish a valid network topology.

In STP, once a stable network topology has been established, all devices listen for Hello BPDUs transmitted from the root bridge. If an STP-aware device does not get a Hello BPDU after a predefined interval (Max Age), the device assumes that the link to the root bridge is down. This device then initiates negotiations with other devices to reconfigure the network to re-establish a valid network topology.

RSTP assigns three port states to eliminate packet looping while STP assigns five (see Table 50 on page 180). A device port is not allowed to go directly from blocking state to forwarding state so as to eliminate transient loops.

Table 50 RSTP Port States

RSTP PORT STATE	STP PORT STATE	DESCRIPTION
Discarding	Disabled	RSTP or STP is disabled (default).
Discarding	Blocking	In RSTP, BPDUs are discarded. In STP, only configuration and management BPDUs are received and processed.

Table 50 RSTP Port States (continued)

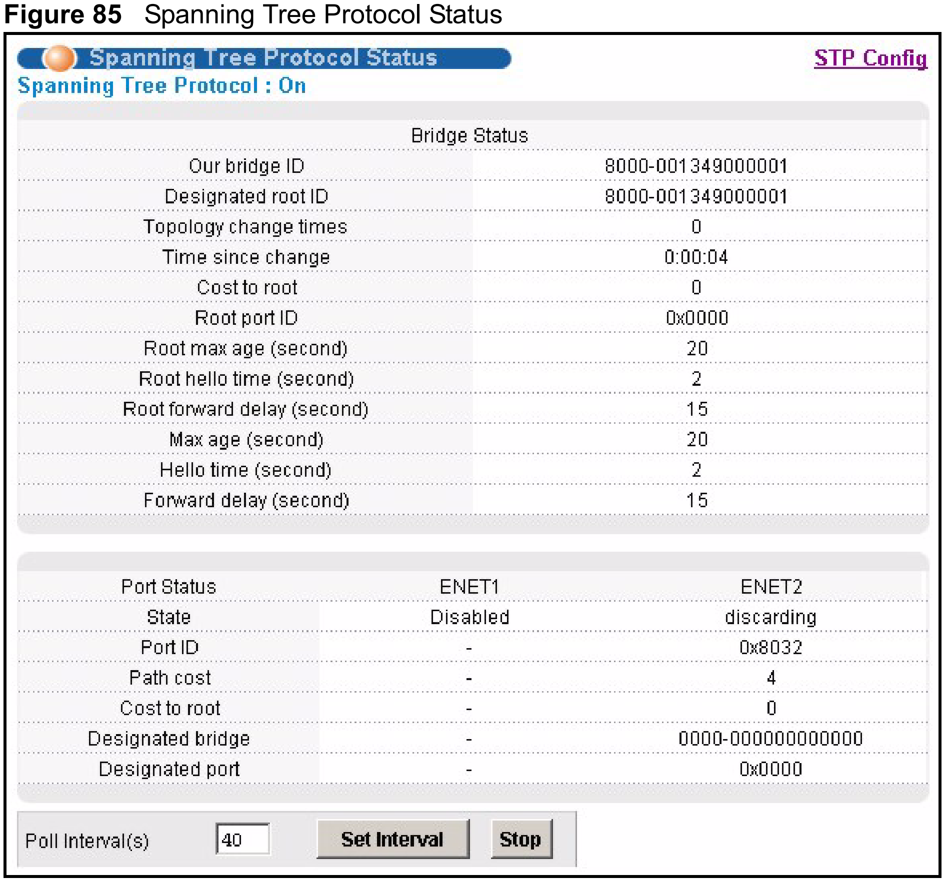
RSTP PORT STATE	STP PORT STATE	DESCRIPTION
Discarding	Listening	In RSTP, BPDUs are discarded. In STP, all BPDUs are received and processed.
Learning	Learning	All BPDUs are received and processed. Information frames are submitted to the learning process but not forwarded.
Forwarding	Forwarding	All BPDUs are received and processed. All information frames are received and forwarded.

See the IEEE 802.1w standard for more information on RSTP. See the IEEE 802.1D standard for more information on STP.

22.2 Spanning Tree Protocol Status Screen

To open this screen, click **Advanced Application**, **Spanning Tree Protocol**.

Figure 85 Spanning Tree Protocol Status



The following table describes the labels in this screen.

Table 51 Spanning Tree Protocol Status

LABEL	DESCRIPTION
STP Config	Click **STP Config** to modify the AAM1212's STP settings (see Section 22.3 on page 183).
Spanning Tree Protocol	This field displays **On** if STP is activated. Otherwise, it displays **Off**.
Bridge Status	If STP is activated, the following fields appear. If STP is not activated, **Disabled** appears.
Our bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same in **Designated root ID** if the AAM1212 is the root switch.
Designated root ID	This is the unique identifier for the root bridge, consisting of bridge priority plus MAC address. This ID is the same in **Our bridge ID** if the AAM1212 is the root switch.
Topology change times	This is the number of times the spanning tree has been reconfigured.
Time since change	This is the time since the spanning tree was last reconfigured.
Cost to root	This is the path cost from the root port on this switch to the root switch.
Root port ID	This is the priority and number of the port on the switch through which this switch must communicate with the root of the Spanning Tree. "0x0000" displays when this device is the root switch.
Root max age (second)	This is the maximum time (in seconds) the root switch can wait without receiving a configuration message before attempting to reconfigure.
Root hello time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines **Hello Time, Max Age** and **Forwarding Delay**.
Root forward delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding).
Max age (second)	This is the maximum time (in seconds) the AAM1212 can wait without receiving a configuration message before attempting to reconfigure.
Hello time (second)	This is the time interval (in seconds) at which the AAM1212 transmits a configuration message. The root bridge determines **Hello Time, Max Age** and **Forwarding Delay**.
Forward delay (second)	This is the time (in seconds) the AAM1212 will wait before changing states (that is, listening to learning to forwarding).
Port Status	This identifies the AAM1212's ports that support the use of STP. If STP is activated, the following fields appear. If STP is not activated, **Disabled** appears.
State	This field displays the port's RSTP (or STP) state. With RSTP, the state can be **discarding**, **learning** or **forwarding**. With STP, the state can be **disabled**, **blocking**, **listening**, **learning**, or **forwarding**. **Disabled** appears when RSTP has not been turned on for the individual port or the whole device.
Port ID	This is the priority and number of the port on the switch through which this switch must communicate with the root of the Spanning Tree. "0x0000" displays when this device is the root switch.
Path cost	This is the path cost from this port to the root switch.

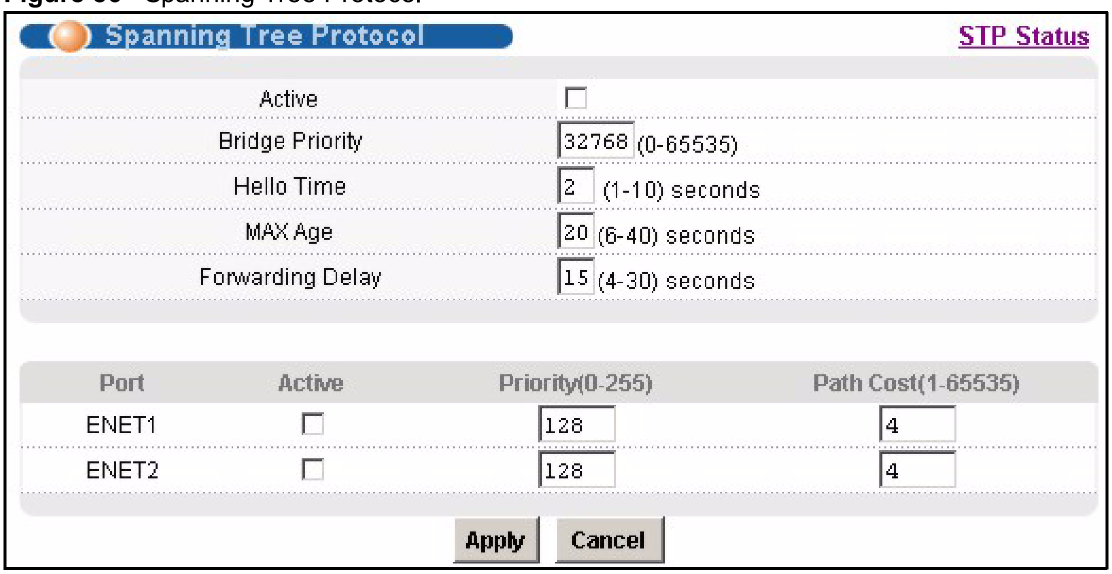
Table 51 Spanning Tree Protocol Status (continued)

LABEL	DESCRIPTION
Cost to root	This is the path cost from the root port on this switch to the root switch.
Designated bridge	This is the unique identifier for the bridge that has the lowest path cost to reach the root bridge, consisting of bridge priority plus MAC address.
Designated port	This is the port on the designated bridge that has the lowest path cost to reach the root bridge, consisting of bridge priority.
Poll Interval(s) Set Interval	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking **Set Interval**.
Stop	Click **Stop** to halt STP statistic polling.

22.3 Spanning Tree Protocol Screen

To open this screen, click **Advanced Application**, **Spanning Tree Protocol**, **STP Config**.

Figure 86 Spanning Tree Protocol



The following table describes the labels in this screen.

Table 52 Spanning Tree Protocol

LABEL	DESCRIPTION
STP Status	Click **STP Status** to display the AAM1212's STP status (see Section 22.2 on page 181).
Active	Select this check box to turn on RSTP. **Note:** It is recommended that you only use STP when you use the AAM1212 in standalone mode with a network topology that has loops.

Table 52 Spanning Tree Protocol (continued)

LABEL	DESCRIPTION
Bridge Priority	Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. The allowed range is 0 to 61440. The lower the numeric value you assign, the higher the priority for this bridge. Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
MAX Age	This is the maximum time (in seconds) a switch can wait without receiving a BPDU before attempting to reconfigure. All switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the switch ports attached to the network. The allowed range is 6 to 40 seconds.
Forwarding Delay	This is the maximum time (in seconds) a switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: **Note:** 2 * (Forward Delay - 1) >= Max Age >= 2 * (Hello Time + 1)
Port	This field identifies the Ethernet port.
Active	Select this check box to activate STP on this port.
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and default value is 128.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is assigned according to the speed of the bridge. The slower the media, the higher the cost.
Apply	Click **Apply** to save your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

23

Port Authentication

This chapter describes the 802.1x authentication method and RADIUS server connection setup.

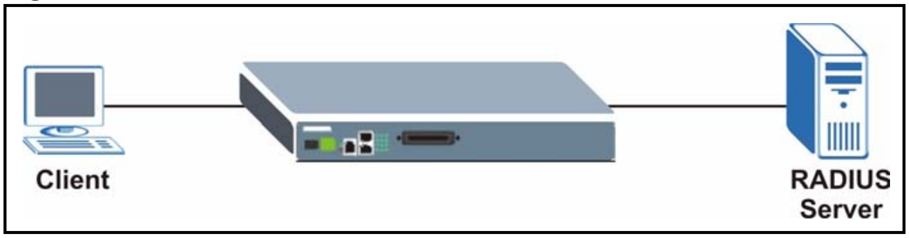
23.1 Introduction to Authentication

IEEE 802.1x is an extended authentication protocol[2] that allows support of RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile management on a network RADIUS server.

23.1.1 RADIUS

RADIUS (Remote Authentication Dial-In User Service) authentication is a popular protocol used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS authentication allows you to validate an unlimited number of users from a central location.

Figure 87 RADIUS Server



23.1.2 Introduction to Local User Database

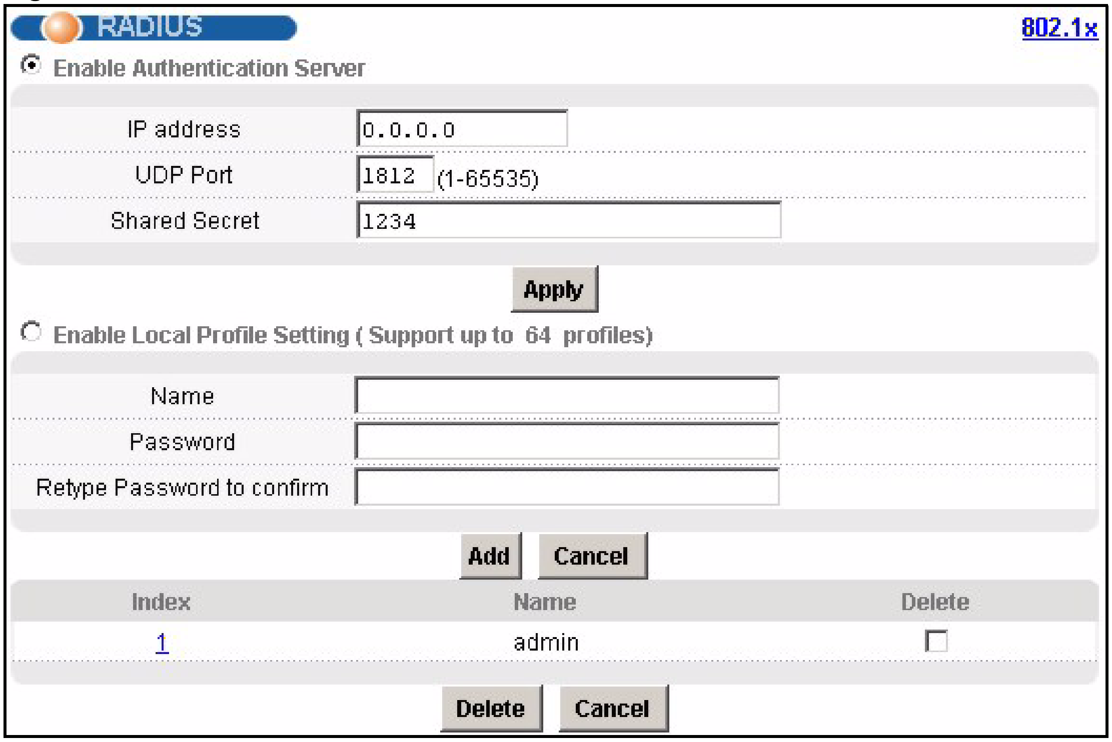
By storing user profiles locally on the AAM1212, your AAM1212 is able to authenticate users without interacting

2. At the time of writing, Windows XP of the Microsoft operating systems supports 802.1x. See the Microsoft web site for information on other Windows operating system support. For other operating systems, see its documentation. If your operating system does not support 802.1x, then you may need to install 802.1x client software.

23.2 RADIUS Screen

To open this screen, click **Advanced Application**, **Port Authentication**.

Figure 88 RADIUS



The following table describes the labels in this screen.

Table 53 RADIUS

LABEL	DESCRIPTION
802.1x	Click **802.1x** to configure individual port authentication settings (see Section 23.3 on page 187).
Enable Authentication Server	Select this check box to have the AAM1212 use an external RADIUS server to authenticate users.
IP Address	Enter the IP address of the external RADIUS server in dotted decimal notation.
UDP Port	The default port of the RADIUS server for authentication is **1812**. You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 31 alphanumeric characters) as the key to be shared between the external RADIUS server and the switch. This key is not sent over the network. This key must be the same on the external RADIUS server and the switch.
Apply	Click **Apply** to save your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Enable Local Profile Setting	Select this check box to have the AAM1212 use its internal database of user names and passwords to authenticate users.

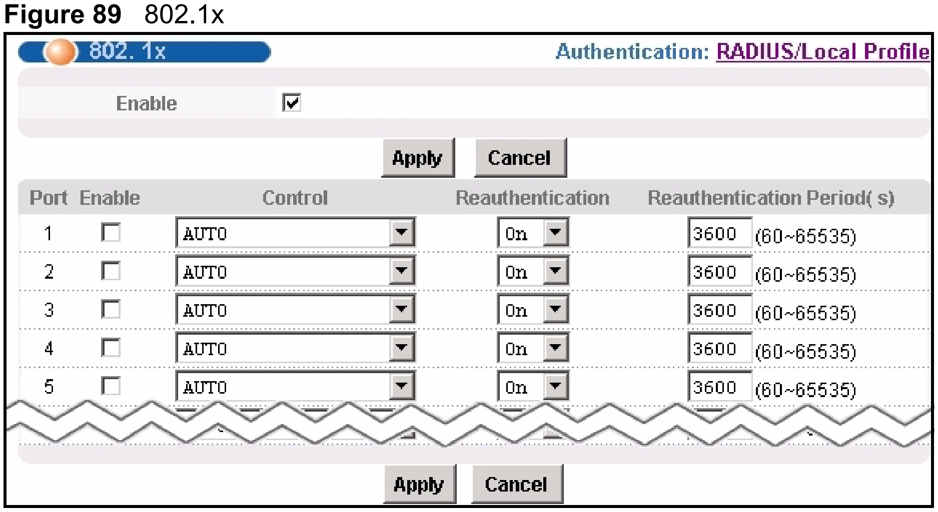
Table 53 RADIUS (continued)

LABEL	DESCRIPTION
Name	Type the user name of the user profile.
Password	Type a password up to 31 characters long for this user profile.
Retype Password to confirm	Type the password again to make sure you have entered it properly.
Add	Click **Add** to save your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
	This table displays the configured user profiles.
Index	These are the numbers of the user profiles. Click this number to edit the user profile.
Name	This is the user name of the user profile.
Delete	Select a user profile's **Delete** check box and click **Delete** to remove the user profile.
Cancel	Click **Cancel** to begin configuring this screen afresh and clear any selected **Delete** check boxes.

23.3 802.1x Screen

To open this screen, click **Advanced Application**, **Port Authentication**, **802.1x**.

Figure 89 802.1x



The following table describes the labels in this screen.

Table 54 802.1x

LABEL	DESCRIPTION
RADIUS/Local Profile	Click this link to configure the RADIUS server or local profile settings (see Section 23.2 on page 186).
Enable	Select this check box to turn on IEEE 802.1x authentication on the switch.
Apply	Click **Apply** to save your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Port	This field displays a port number.
Enable	Select this check box to turn on IEEE 802.1x authentication on this port.
Control	Select **AUTO** to authenticate all subscribers before they can access the network through this port. Select **FORCE AUTHORIZED** to allow all connected users to access the network through this port without authentication. Select **FORCE UNAUTHORIZED** to deny all subscribers access to the network through this port.
Reauthentication	Specify if a subscriber has to periodically re-enter his or her username and password to stay connected to the port.
Reauthentication Period(s)	Specify how often a client has to re-enter his or her username and password to stay connected to the port.
Apply	Click **Apply** to save your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

24

Port Security

This chapter shows you how to set up port security.

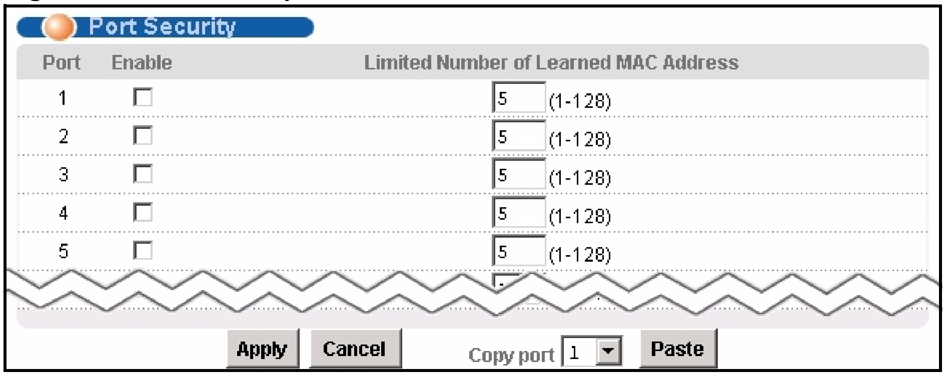
24.1 Port Security Overview

Port security allows you to restrict the number of MAC addresses that can be learned on a port.

24.2 Port Security Screen

To open this screen, click **Advanced Application**, **Port Security**.

Figure 90 Port Security

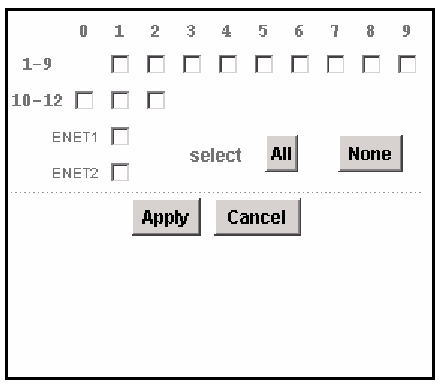


The following table describes the labels in this screen.

Table 55 Port Security

LABEL	DESCRIPTION
Port	This field displays a port number.
Enable	Select this check box to restrict the number of MAC addresses that can be learned on the port. Clear this check box to not limit the number of MAC addresses that can be learned on the port.

Table 55 Port Security (continued)

LABEL	DESCRIPTION
Limited Number of Learned MAC Address	Specify how many MAC addresses the AAM1212 can learn on this port. The range is 1~128. **Note:** If you also use MAC filtering on a port, it is recommended that you set this limit to be equal to or greater than the number of MAC filter entries you configure.
Apply	Click **Apply** to save your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Copy port Paste	Do the following to copy settings from one port to another port or ports. 1. Select the number of the port from which you want to copy settings. 2. Click **Paste** and the following screen appears. 3. Select to which ports you want to copy the settings. Use **All** to select every port. Use **None** to clear all of the check boxes. 4. Click **Apply** to paste the settings. **Figure 91** Select Ports 

25

DHCP Relay

This chapter shows you how to set up DHCP relays for each VLAN.

25.1 DHCP Relay

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a DHCP server. You can configure the AAM1212 to relay DHCP requests to one or more DHCP servers and the server's responses back to the clients. You can specify default DHCP servers for all VLAN, and you can specify DHCP servers for each VLAN.

25.2 DHCP Relay Agent Information Option (Option 82)

The AAM1212 can add information to DHCP requests that it relays to a DHCP server. This helps provide authentication about the source of the requests. You can also specify additional information for the AAM1212 to add to the DHCP requests that it relays to the DHCP server. Please see RFC 3046 for more details.

25.2.1 DHCP Relay Agent Circuit ID and Remote ID Sub-option Formats

The DHCP relay agent information feature adds an Agent Information field to the option 82 field of the DHCP headers of DHCP request frames that the AAM1212 relays to a DHCP server. The Agent Information field that the AAM1212 adds contains an "Agent Circuit-ID sub-option" that includes the port number, VLAN ID and optional information about the port where the DHCP request was received.

The following figure shows the format of the Agent Circuit ID sub-option. The 1 in the first field identifies this as an Agent Circuit ID sub-option. The length N gives the total number of octets in the Agent Information Field. If the configuration request was received on a DSL port, a 2-byte Port No field specifies the ingress port number (the first byte is always 0, the second byte is in hexadecimal format). The next field is 2 bytes and displays the DHCP request packet's VLAN ID. The last field (A) can range from 0 to 24 bytes and is optional information (that you specify) about this relay agent.

Figure 92 DHCP Relay Agent Circuit ID Sub-option Format

1	N	Port No	VLAN ID	A

The Agent Information field that the AAM1212 adds also contains an "Agent Remote-ID sub-option" of information that you specify.

The following figure shows the format of the Agent Remote ID sub-option. The 2 in the first field identifies this as an Agent Remote ID sub-option. The length N gives the total number of octets in the Agent Information Field. Then there is the number of the port (in plain text format) upon which the DHCP client request was received. The next field (B in the figure) is 0 to 23 bytes of optional information that you specify. This is followed by the name and telephone number configured for the DSL port. The port number, optional information (B in the figure), DSL name and DSL telephone number fields are separated by forward slashes.

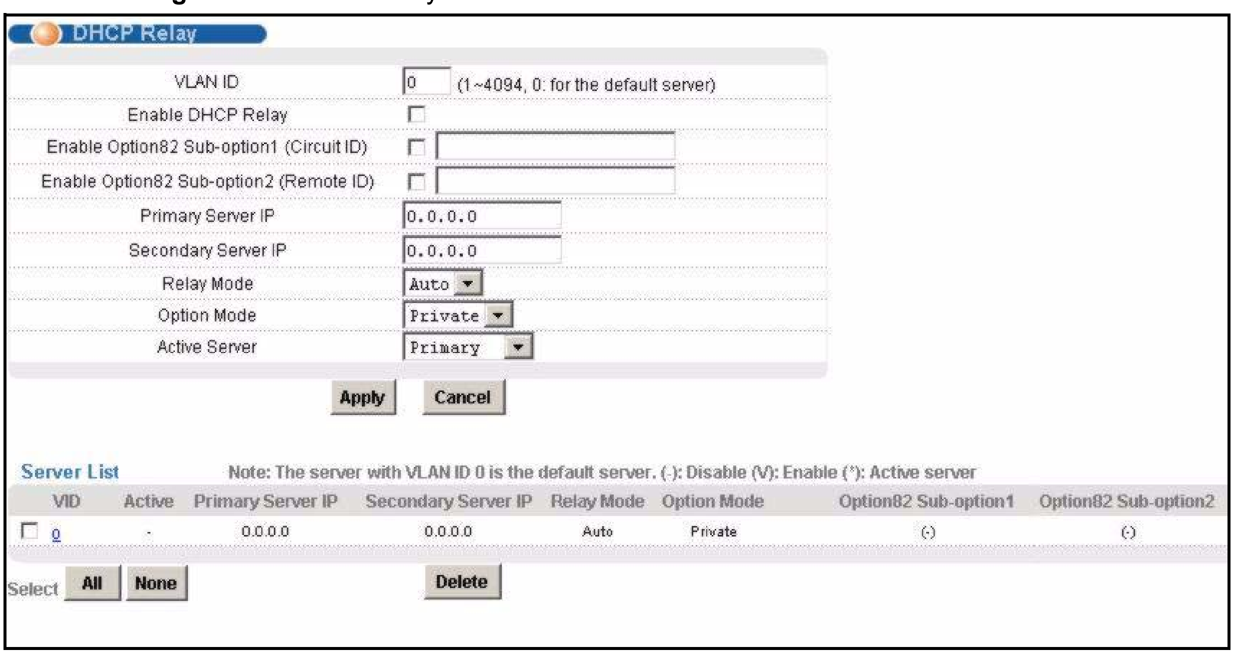
Figure 93 DHCP Relay Agent Remote ID Sub-option Format

2	N	Port Number	/	B	/	Name	/	Telephone

25.3 DHCP Relay Screen

To open this screen, click **Advanced Application**, **DHCP Relay**.

Figure 94 DHCP Relay



The following table describes the labels in this screen.

Table 56 DHCP Relay

LABEL	DESCRIPTION
VLAN ID	Enter the ID of the VLAN served by the specified DHCP relay(s). Enter 0 to set up the IP address(es) of the default DHCP relay(s).
Enable DHCP Relay:	Enable DHCP relay to have the AAM1212 relay DHCP requests to a DHCP server and the server's responses back to the clients.
Enable Option 82 sub option 1 (Circuit ID)	Select this to have the AAM1212 add the originating port numbers to DHCP requests in the selected VLAN regardless of whether the DHCP relay is on or off. In the field next to the check box, you can also specify up to 23 English keyboard characters of additional information for the AAM1212 to add to the DHCP requests that the AAM1212 relays to a DHCP server. Examples of information you could add would be the system name of the AAM1212 or the ISP's name.
Enable Option 82 sub option 2 (Circuit ID)	Select this to have the AAM1212 add the sub-option 2 (Remote ID) to DHCP requests in the selected VLAN regardless of whether the DHCP relay is on or off. In the field next to the check box, you can also specify up to 23 English keyboard characters of additional information for the AAM1212 to add to the DHCP requests that it relays to a DHCP server.
Primary Server IP	Enter the IP address of one DHCP server to which the switch should relay DHCP requests for the selected VLAN.
Secondary Server IP	Enter the IP address of a second DHCP server to which the switch should relay DHCP requests for the selected VLAN. Enter 0.0.0.0 if there is only one DHCP relay for the selected VLAN.
Relay Mode	Specify how the AAM1212 relays DHCP requests. **Auto** - The AAM1212 routes DHCP requests to the active server for each VLAN. **Both** - The AAM1212 routes DHCP requests to the primary and secondary server for each VLAN, regardless of which one is active.
Option Mode	Select which method (**Private** or **TR-101**) to use to encode PPPoE line information in PPPoE discover packets.
Active Server	This field has no effect if the **Relay Mode** is **Both**. If the **Relay Mode** is **Auto**, select which DHCP server (**Primary** or **Secondary**) to which the AAM1212 should relay DHCP requests for the selected VLAN.
Apply	Click **Apply** to save your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Server List	This section lists the DHCP servers that are already set up for each VLAN. An asterisk in parentheses (*) indicates which DHCP server is active for each VLAN.
VLAN ID	This field displays the ID of the VLAN served by the specified DHCP relay(s).
Active	
Primary Server IP	This field displays the IP address of one DHCP server to which the switch should relay DHCP requests.
Secondary Server IP	This field displays the IP address of a second DHCP server to which the switch should relay DHCP requests. This field is 0.0.0.0 if the primary server is the only DHCP relay.

Table 56 DHCP Relay (continued)

LABEL	DESCRIPTION
Relay Mode	This field displays how the AAM1212 relays DHCP requests for the selected VLAN. **Auto** - The AAM1212 routes DHCP requests to the active server for the VLAN. **Both** - The AAM1212 routes DHCP requests to the primary and secondary server for the VLAN, regardless of which one is active.
Option Mode	This field displays which method (**Private** or **TR-101**) is used to encode PPPoE line information in PPPoE discover packets.
Option 82 sub option 1	This field displays whether or not the AAM1212 adds the originating port numbers (and any additional information) to DHCP requests in the selected VLAN.
Option 82 sub option 2	This field displays whether or not the AAM1212 adds the sub-option 2 (and any additional information) to DHCP requests in the selected VLAN.
Select Delete	Select the check box in the **Select** column for an entry, and click **Delete** to remove the entry.
Select All	Click this to select all entries in the **Server List**.
Select None	Click this to un-select all entries in the **Server List**.

26

DHCP Snoop

This chapter shows you how to set up DHCP snooping settings on the subscriber ports.

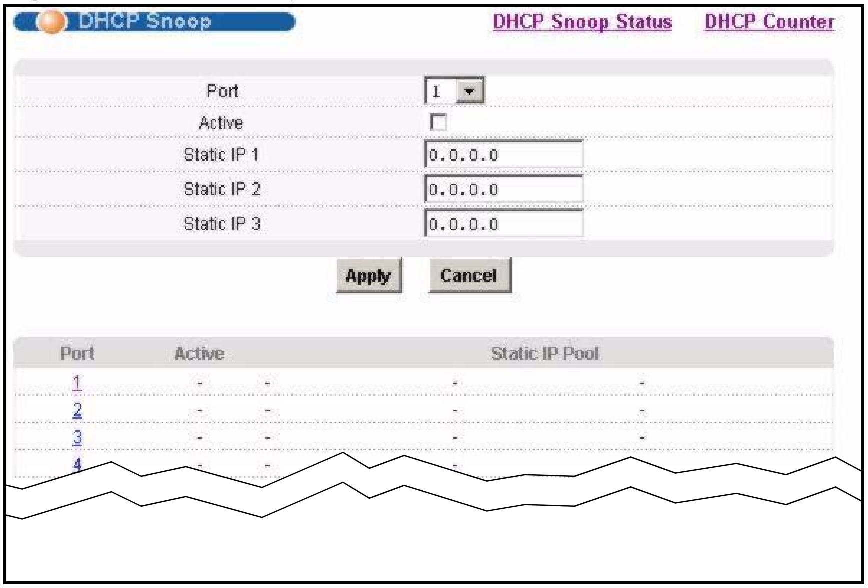
26.1 DHCP Snoop Overview

DHCP snooping prevents clients from assigning their own IP addresses. The AAM1212 can store every (DSL port, MAC address, IP address) tuple offered by the DHCP server. Then, it only forwards packets from clients whose MAC address and IP address are recorded. Packets from unknown IP addresses are dropped.

26.2 DHCP Snoop Screen

Use this screen to activate or deactivate DHCP snooping on each port. To open this screen, click **Advanced Application**, **DHCP Snoop**.

Figure 95 DHCP Snoop



The following table describes the labels in this screen.

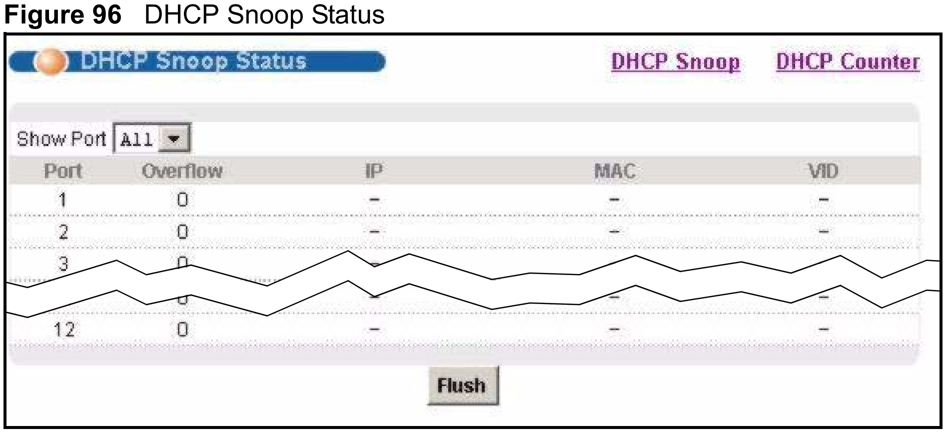
Table 57 DHCP Snoop

LABEL	DESCRIPTION
DHCP Snoop Status	Click **DHCP Snoop Status** to open the screen where you can look at or clear the current DHCP snooping table on each port (see Section 26.3 on page 196).
DHCP Counter	Click **DHCP Counter** to open the screen where you can look at a summary of the DHCP packets on each port (see Section 26.4 on page 197).
Port	Select a port from the drop-down list.
Active	Select to enable DHCP snooping on this port.
Static IP 1~3	These fields are only effective when DHCP snooping is active. Enter up to three IP addresses for which the AAM1212 should forward packets, even if the IP address is not assigned by the DHCP server. The AAM1212 drops packets from other unknown IP addresses on this port. To delete an existing IP address, enter **0.0.0.0**.
Port	This field displays each DSL port number.
Apply	Click **Apply** to save your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Active	This field displays whether DHCP snooping is active ("V") or inactive ("-") on this port.
Static IP Pool	These fields display IP addresses for which the AAM1212 should forward packets, even if the IP address is not assigned by the DHCP server. **0.0.0.0** is a blank value.

26.3 DHCP Snoop Status Screen

Use this screen to look at or to clear the DHCP snooping table on each port. To open this screen, click **Advanced Application**, **DHCP Snoop, DHCP Snoop Status**.

Figure 96 DHCP Snoop Status



The following table describes the labels in this screen.

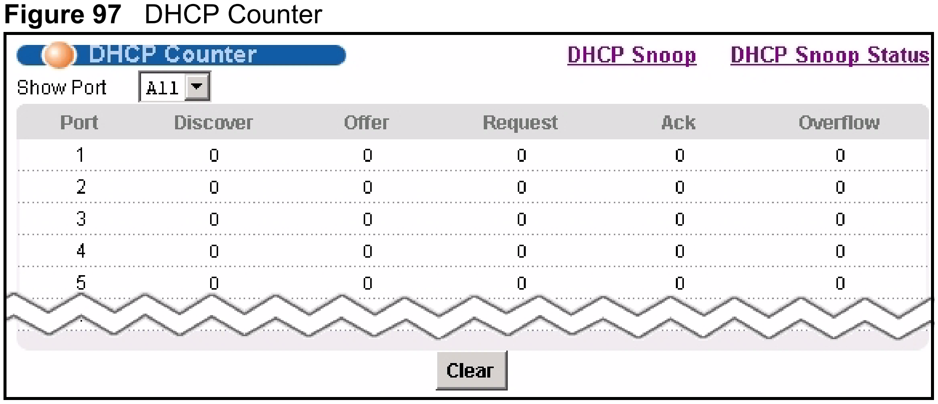
Table 58 DHCP Snoop Status

LABEL	DESCRIPTION
DHCP Snoop	Click **DHCP Snoop** to open the screen where you can activate or deactivate DHCP snooping on each port (see Section 26.2 on page 195).
DHCP Counter	Click **DHCP Counter** to open the screen where you can look at a summary of the DHCP packets on each port (see Section 26.4 on page 197).
Show Port	Select a port for which you wish to view information.
Port	This field displays the selected DSL port number(s).
Overflow	The DHCP server can assign up to 32 IP addresses at one time to each port. This field displays the number of requests from DHCP clients above this limit.
IP	This field displays the IP address assigned to a client on this port.
MAC	This field displays the MAC address of a client on this port to which the DHCP server assigned an IP address.
VID	This field displays the VLAN ID, if any, on the DHCP Request packet.
Flush	Click **Flush** to remove all of the entries from the DHCP snooping table for the selected port(s).

26.4 DHCP Counter Screen

Use this screen to look at a summary of the DHCP packets on each port. To open this screen, click **Advanced Application**, **DHCP Snoop, DHCP Counter**.

Figure 97 DHCP Counter



The following table describes the labels in this screen.

Table 59 DHCP Counter

LABEL	DESCRIPTION
DHCP Snoop	Click **DHCP Snoop** to open the screen where you can activate or deactivate DHCP snooping on each port (see Section 26.2 on page 195).
DHCP Snoop Status	Click **DHCP Snoop Status** to open the screen where you can look at or clear the current DHCP snooping table on each port (see Section 26.3 on page 196).

Table 59 DHCP Counter (continued)

LABEL	DESCRIPTION
Show Port	Select a port for which you wish to view information.
Port	This field displays the selected DSL port number(s).
Discover	This field displays the number of DHCP Discover packets on this port.
Offer	This field displays the number of DHCP Offer packets on this port.
Request	This field displays the number of DHCP Request packets on this port.
Ack	This field displays the number of DHCP Acknowledge packets on this port.
Overflow	The DHCP server can assign up to 32 IP addresses at one time to each port. This field displays the number of requests from DHCP clients above this limit.
Clear	Click **Clear** to delete the information the AAM1212 has learned about DHCP packets. This resets every counter in this screen.

27

2684 Routed Mode

This chapter shows you how to set up 2684 routed mode service.

27.1 2684 Routed Mode

Use the 2684 (formerly 1483) routed mode to have the AAM1212 add MAC address headers to 2684 routed mode traffic from a PVC that connects to a subscriber device that uses 2684 routed mode. You also specify the gateway to which the AAM1212 sends the traffic and the VLAN ID tag to add. See RFC-2684 for details on routed mode traffic carried over AAL type 5 over ATM.

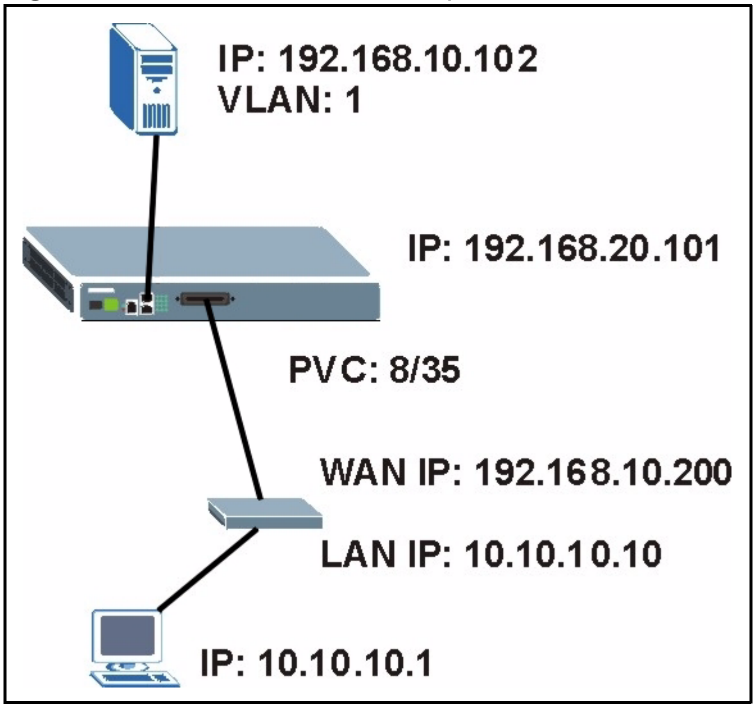
- Use the 2684 Routed PVC Screen to configure PVCs for 2684 routed mode traffic.
- Use the 2684 Routed Domain Screen to configure domains for 2684 routed mode traffic. The domain is the range of IP addresses behind the subscriber's device (the CPE or Customer Premises Equipment). This includes the CPE device's LAN IP addresses and the IP addresses of the LAN computers.
- Use the RPVC Arp Proxy Screen to view the Address Resolution Protocol table of IP addresses of CPE devices using 2684 routed mode and configure how long the device is to store them.
- Use the 2684 Routed Gateway Screen to configure gateway settings.
- For upstream traffic: Since the subscriber's device will not send out a MAC address, after the AAM1212 reassembles the Ethernet packets from the AAL5 ATM cells, the AAM1212 will append the routed mode gateway's MAC address and the AAM1212's MAC address as the destination/source MAC address.
- For downstream traffic: When the AAM1212 sees the destination IP address is specified in the RPVC (or RPVC domain), the AAM1212 will strip out the MAC header and send them to the corresponding RPVC.

27.1.1 2684 Routed Mode Example

The following figure shows an example 2684 routed mode set up. The gateway server uses IP address 192.168.10.102 and is in VLAN 1. The AAM1212 uses IP address 192.168.20.101. The subscriber's device (the CPE) is connected to DSL port 1 on the AAM1212 and the 2684 routed mode traffic is to use the PVC identified by VPI 8 and VCI 35. The CPE device's

WAN IP address is 192.168.10.200. The routed domain is the LAN IP addresses behind the CPE device. The CPE device's LAN IP address is 10.10.10.10 and the LAN computer's IP address is 10.10.10.1. This includes the CPE device's LAN IP addresses and the IP addresses of the LAN computers.

Figure 98 2684 Routed Mode Example



Note the following.

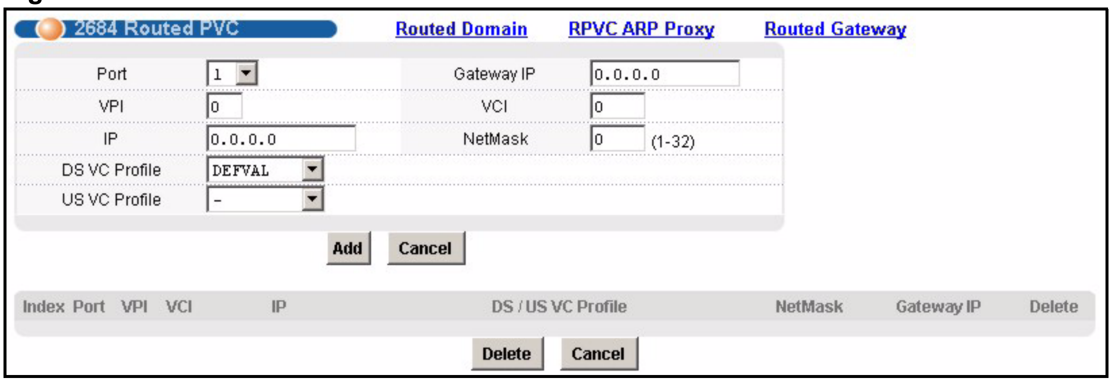
- The CPE device's WAN IP (192.168.10.200 in this example) must be in the same subnet as the gateway's IP address (192.168.10.102 in this example).
- The AAM1212's management IP address can be any IP address, it doesn't have any relationship to the WAN IP address or routed gateway IP address.
- The AAM1212's management IP address should not be in the same subnet as the one defined by the WAN IP address and netmask of the subscriber's device. It is suggested that you set the netmask of the subscriber's WAN IP address to 32 to avoid this problem.
- The AAM1212's management IP address should not be in the same subnet range of any RPVC and RPVC domain. It will make the AAM1212 confused if the AAM1212 receives a packet with this IP as destination IP.
- The AAM1212's management IP address also should not be in the same subnet as the one defined by the LAN IP address and netmask of the subscriber's device. Make sure you assign the IP addresses properly.
- In general deployment, the computer must set the CPE device's LAN IP address (10.10.10.10 in this example) as its default gateway.
- The subnet range of any RPVC and RPVC domain must be unique.

27.2 2684 Routed PVC Screen

Use this screen to configure PVCs for 2684 routed mode traffic.

To open this screen, click **Advanced Application**, **2684 Routed Mode**.

Figure 99 2684 Routed PVC



The following table describes the labels in this screen.

Table 60 2684 Routed PVC

LABEL	DESCRIPTION
Routed Domain	Click **Routed Domain** to open this screen where you can configure domains for 2684 routed mode traffic (see Section 27.3 on page 202).
RPVC ARP Proxy	Click **RPVC ARP Proxy** to go to the screen where you can view the Address Resolution Protocol table of IP addresses of CPE devices using 2684 routed mode and configure how long the device is to store them (see Section 27.4 on page 204).
Routed Gateway	Click **Routed Gateway** to go to the screen where you can configure gateway settings (see Section 27.5 on page 205).
Port	Use this drop-down list box to select a port for which you wish to configure settings.
Gateway IP	Enter the IP address of the gateway to which you want to send the traffic that the system receives from this PVC. Enter the IP address in dotted decimal notation.
VPI	Type the Virtual Path Identifier for this routed PVC.
VCI	Type the Virtual Circuit Identifier for this routed PVC.
IP	Enter the subscriber's CPE WAN IP address in dotted decimal notation.
NetMask	The bit number of the subnet mask of the subscriber's WAN IP address. To find the bit number, convert the subnet mask to binary and add all of the 1's together. Take "255.255.255.0" for example. 255 converts to eight 1's in binary. There are three 255's, so add three eights together and you get the bit number (24). Make sure that the routed PVC's subnet does not include the AAM1212's IP address.
DS VC Profile	Use the drop-down list box to select a VC profile to use for this channel's downstream traffic shaping.
US VC Profile	Use the drop-down list box to select a VC profile to use for this channel's upstream traffic. The AAM1212 does not perform upstream traffic policing if you do not specify an upstream VC profile.

Table 60 2684 Routed PVC (continued)

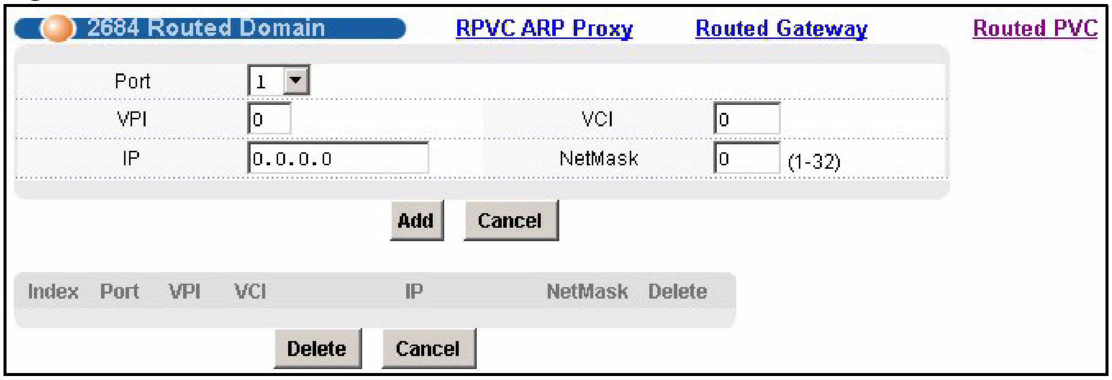
LABEL	DESCRIPTION
Add	Click **Add** to save your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to start configuring the screen again.
Index	This field displays the number of the routed PVC.
Port	This field displays the number of the DSL port on which the routed PVC is configured.
VPI	This field displays the Virtual Path Identifier (VPI) The VPI and VCI identify a channel on this port.
VCI	This field displays the Virtual Circuit Identifier (VCI). The VPI and VCI identify a channel on this port.
IP	This field displays the subscriber's IP address.
DS / US VC Profile	This shows which VC profile this channel uses for downstream traffic shaping. The VC profile for upstream policing also displays if the channel is configured to use one.
NetMask	This field displays the bit number of the subnet mask of the subscriber's IP address.
Gateway IP	This field displays the IP address of the gateway to which you want to send the traffic that the system receives from this PVC.
Delete	Select an entry's **Delete** check box and click **Delete** to remove the entry. Clicking **Delete** saves your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to start configuring the screen again.

27.3 2684 Routed Domain Screen

Use this screen to configure domains for 2684 routed mode traffic. The domain is the range of IP addresses behind the subscriber's device (the CPE). This includes the CPE device's LAN IP addresses and the IP addresses of the LAN computers.

To open this screen, click **Advanced Application**, **2684 Routed Mode**, **Routed Domain**.

Figure 100 2684 Routed Domain



The following table describes the labels in this screen.

Table 61 2684 Routed Domain

LABEL	DESCRIPTION
RPVC ARP Proxy	Click **RPVC ARP Proxy** to go to the screen where you can view the Address Resolution Protocol table of IP addresses of CPE devices using 2684 routed mode and configure how long the device is to store them (see Section 27.4 on page 204).
Routed Gateway	Click **Routed Gateway** to go to the screen where you can configure gateway settings (see Section 27.5 on page 205).
Routed PVC	Click **Routed PVC** to go to the screen where you can configure routed PVC settings (see Section 27.2 on page 201).
Port	Use this drop-down list box to select a port for which you wish to configure settings.
VPI	Type the Virtual Path Identifier for this routed PVC.
VCI	Type the Virtual Circuit Identifier for this routed PVC.
IP	Enter the subscriber's CPE LAN IP address in dotted decimal notation.
NetMask	The bit number of the subnet mask of the subscriber's IP address. To find the bit number, convert the subnet mask to binary and add all of the 1's together. Take "255.255.255.0" for example. 255 converts to eight 1's in binary. There are three 255's, so add three eights together and you get the bit number (24).
Add	Click **Add** to save your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to start configuring the screen again.
Index	This field displays the number of the routed PVC.
Port	This field displays the number of the DSL port on which the routed PVC is configured.
VPI	This field displays the Virtual Path Identifier (VPI) The VPI and VCI identify a channel on this port.
VCI	This field displays the Virtual Circuit Identifier (VCI). The VPI and VCI identify a channel on this port.
IP	This field displays the subscriber's IP address.
NetMask	This field displays the bit number of the subnet mask of the subscriber's LAN IP address.

Table 61 2684 Routed Domain (continued)

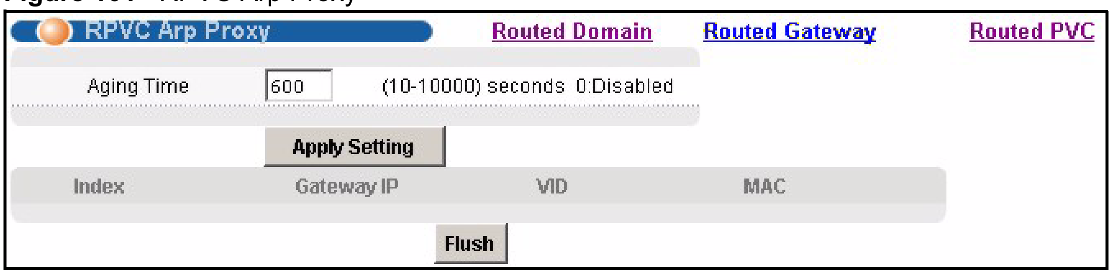
LABEL	DESCRIPTION
Delete	Select an entry's **Delete** check box and click **Delete** to remove the entry. Clicking **Delete** saves your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to start configuring the screen again.

27.4 RPVC Arp Proxy Screen

Use this screen to view the Address Resolution Protocol table of IP addresses of CPE devices using 2684 routed mode and configure how long the device is to store them.

To open this screen, click **Advanced Application**, **2684 Routed Mode**, **RPVC ARP Proxy**.

Figure 101 RPVC Arp Proxy



The following table describes the labels in this screen.

Table 62 RPVC Arp Proxy

LABEL	DESCRIPTION
Routed Domain	Click **Routed Domain** to open this screen where you can configure domains for 2684 routed mode traffic (see Section 27.3 on page 202).
Routed Gateway	Click **Routed Gateway** to go to the screen where you can configure gateway settings (see Section 27.5 on page 205).
Routed PVC	Click **Routed PVC** to go to the screen where you can configure routed PVC settings (see Section 27.2 on page 201).
Aging Time	Enter a number of seconds (10~10000) to set how long the device keeps the Address Resolution Protocol table's entries of IP addresses of CPE devices using 2684 routed mode. Enter 0 to disable the aging time.
Apply Setting	Click **Apply Setting** to save your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Index	This field displays the number of the IP address entry.
Gateway IP	This field displays the IP address of the gateway to which the device sends the traffic that it receives from this entry's IP address.

Table 62 RPVC Arp Proxy (continued)

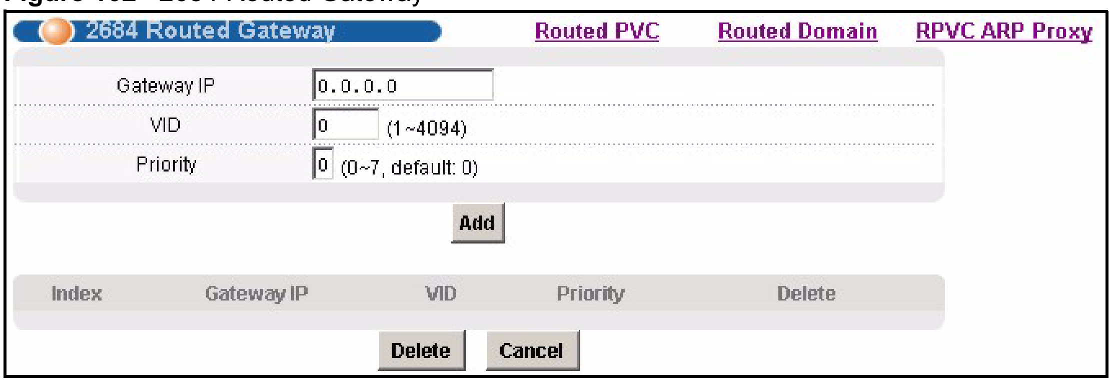
LABEL	DESCRIPTION
VID	This field displays the VLAN Identifier that the device adds to Ethernet frames that it sends to this gateway.
MAC	This field displays the subscriber's MAC (Media Access Control) address.
Flush	Click **Flush** to remove all of the entries from the ARP table.

27.5 2684 Routed Gateway Screen

Use this screen to configure gateway settings.

To open this screen, click **Advanced Application**, **2684 Routed Mode**, **Routed Gateway**.

Figure 102 2684 Routed Gateway



The following table describes the labels in this screen.

Table 63 2684 Routed Gateway

LABEL	DESCRIPTION
Routed PVC	Click **Routed PVC** to go to the screen where you can configure routed PVC settings (see Section 27.2 on page 201).
Routed Domain	Click **Routed Domain** to open this screen where you can configure domains for 2684 routed mode traffic (see Section 27.3 on page 202).
RPVC ARP Proxy	Click **RPVC ARP Proxy** to go to the screen where you can view the Address Resolution Protocol table of IP addresses of CPE devices using 2684 routed mode and configure how long the device is to store them (see Section 27.4 on page 204).
Gateway IP	Enter the IP address of the gateway to which you want to send the traffic that the system receives from this PVC. Enter the IP address in dotted decimal notation.
VID	Specify a VLAN Identifier to add to Ethernet frames that the system routes to this gateway.
Priority	Select the IEEE 802.1p priority (0~7) to add to the traffic that you send to this gateway.

Table 63 2684 Routed Gateway (continued)

LABEL	DESCRIPTION
Add	Click **Add** to save your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Index	This field displays the number of the gateway entry.
Gateway IP	This field displays the IP address of the gateway.
VID	This field displays the VLAN Identifier that the system adds to Ethernet frames that it sends to this gateway.
Priority	This field displays the IEEE 802.1p priority (0~7) that is added to traffic sent to this gateway.
Delete	Select an entry's **Delete** check box and click **Delete** to remove the entry. Clicking **Delete** saves your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to start configuring the screen again.

28

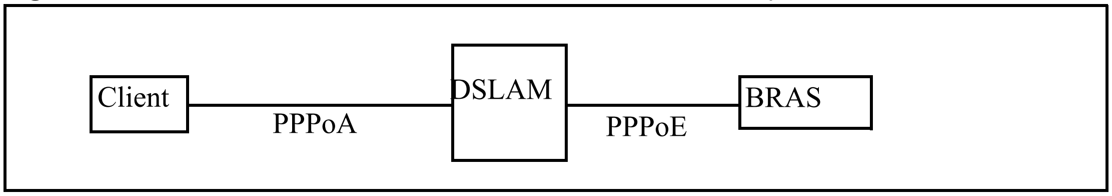
PPPoA to PPPoE

This chapter shows you how to set up the AAM1212 to convert PPPoA frames to PPPoE traffic and vice versa.

28.1 PPPoA to PPPoE Overview

Before migrating to an Ethernet infrastructure, a broadband network might consist of PPPoA connections between the CPE devices and the DSLAM and PPPoE connections from the DSLAM to the Broadband Remote Access Server (BRAS). The following figure shows a network example.

Figure 103 Mixed PPPoA-to-PPPoE Broadband Network Example



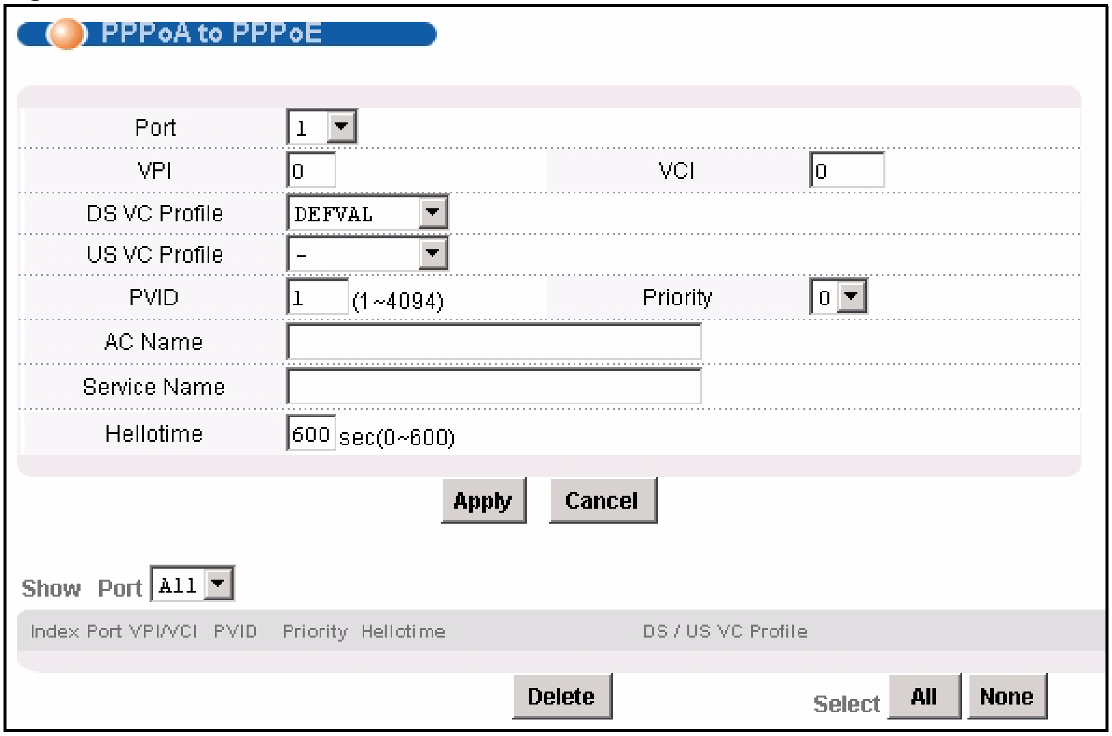
In order to allow communication between the end points (the CPE devices and the BRAS), you need to configure the DSLAM (the AAM1212) to translate PPPoA frames to PPPoE packets and vice versa.

When PPPoA packets are received from the CPE, the ATM headers are removed and the AAM1212 adds PPPoE and Ethernet headers before sending the packets to the BRAS. When the AAM1212 receives PPPoE packets from the BRAS, PPPoE and Ethernet headers are stripped and necessary PVC information (such as encapsulation type) is added before forwarding to the designated CPE.

28.2 PPPoA to PPPoE Screen

Use this screen to set up PPPoA to PPPoE conversions on each port. This conversion is set up by creating a PAE PVC. See Chapter 13 on page 120 for background information about creating PVCs. To open this screen, click **Advanced Application**, **PPPoA to PPPoE**.

Figure 104 PPPoA to PPPoE



The following table describes the labels in this screen.

Table 64 PPPoA to PPPoE

LABEL	DESCRIPTION
Port	Use this drop-down list box to select a port for which you wish to set up PPPoA to PPPoE conversions. This field is read-only once you click on a port number below.
VPI	Type the Virtual Path Identifier for a channel on this port.
VCI	Type the Virtual Circuit Identifier for a channel on this port.
DS VC Profile	Use the drop-down list box to select a VC profile to use for this channel's downstream traffic shaping.
US VC Profile	Use the drop-down list box to select a VC profile to use for this channel's upstream traffic. The AAM1212 does not perform upstream traffic policing if you do not specify an upstream VC profile. **Note:** Upstream traffic policing should be used in conjunction with the ATM shaping feature on the subscriber's device. If the subscriber's device does not apply the appropriate ATM shaping, all upstream traffic will be discarded due to upstream traffic policing.
PVID	Type a PVID (Port VLAN ID) to assign to untagged frames received on this channel. **Note:** Make sure the VID is not already used for multicast VLAN or TLS PVC.

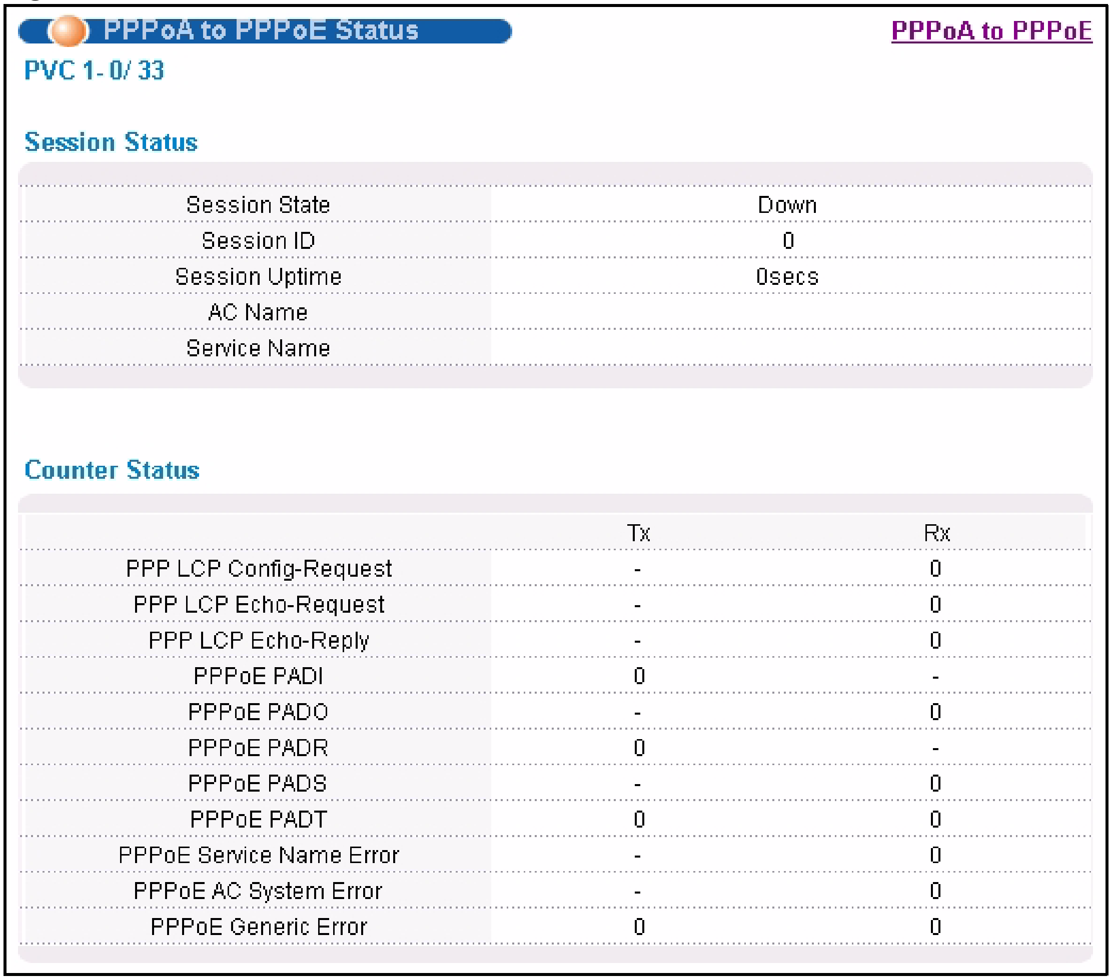
Table 64 PPPoA to PPPoE (continued)

LABEL	DESCRIPTION
Priority	Use the drop-down list box to select the priority value (0 to 7) to add to incoming frames without a (IEEE 802.1p) priority tag.
AC Name	This field is optional. Specify the hostname of a remote access concentrator if there are two access concentrators (or BRAS) on the network or if you want to allow PAE translation to the specified access concentrator. In this case, the AAM1212 checks the AC name field in the BRAS's reply PDU. If there is a mismatch, the AAM1212 drops this PDU. (This is not recorded as an **PPPoE AC System Error** in the **PPPoA to PPPoE Status** screen, however.)
Service Name	This field is optional. Specify the name of the service that uses this PVC. This must be a service name that you configure on the remote access concentrator.
Hellotime	Specify the timeout, in seconds, for the PPPoE session. Enter 0 if there is no timeout.
Apply	Click this to add or save channel settings on the selected port. This saves your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to start configuring the screen again.
Show Port	Select which DSL port(s) for which to display PPPoA to PPPoE conversion settings.
Index	This field displays the number of the PVC. Click a PVC's index number to open the screen where you can look at the current status of this PPPoA-to-PPPoE conversion. (See Section 28.3 on page 210.) **Note:** At the time of writing, you cannot edit the VPI and VCI. If you want to change them, add a new PVC with the desired settings. Then, delete any unwanted PVCs.
Port	This field displays the number of the DSL port on which the PVC is configured.
VPI/VCI	This field displays the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI). The VPI and VCI identify a channel on this port.
PVID	This is the PVID (Port VLAN ID) assigned to untagged frames or priority frames (0 VID) received on this channel.
Priority	This is the priority value (0 to 7) added to incoming frames without a (IEEE 802.1p) priority tag.
Hellotime	This field displays the timeout for the PPPoE session, in seconds.
DS / US VC Profile	This shows which VC profile this channel uses for downstream traffic shaping. The VC profile for upstream policing also displays if the channel is configured to use one.
Access Concentrator Name	This field displays the name of the specified remote access concentrator, if any.
Service Name	This field displays the name of the service that uses this PVC on the remote access concentrator.
Select Delete	Select the check box in the **Select** column for an entry, and click **Delete** to remove the entry.
Select All	Click this to select all entries in the table.
Select None	Click this to un-select all entries in the table.

28.3 PPPoA to PPPoE Status Screen

Use this screen to look at the current status of each PPPoA to PPPoE conversion. To open this screen, click **Advanced Application**, **PPPoA to PPPoE**, and then click an index number.

Figure 105 PPPoA to PPPoE Status



The following table describes the labels in this screen.

Table 65 PPPoA to PPPoE Status

LABEL	DESCRIPTION
PPPoA to PPPoE	Click **PPPoA to PPPoE** to open the screen where you can set up PPPoA-to-PPPoE conversions on each port (see Section 28.2 on page 207).
PVC	This field displays the port number, VPI, and VCI of the PVC.
Session Status	
Session State	This field displays whether or not the current session is **Up** or **Down**.
Session ID	This field displays the ID of the current session. It displays **0** if there is no current session.
Session Uptime	This field displays how long the current session has been up.

Table 65 PPPoA to PPPoE Status (continued)

LABEL	DESCRIPTION
AC Name	This field displays the hostname of the remote access concentrator if there are two access concentrators (or BRAS) on the network or if you want to allow PAE translation to the specified access concentrator.
Service Name	This field specifies the name of the service that uses this PVC.
Counter Status	
Tx/Rx	The values in these columns are for packets transmitted (`tx`) or received (`rx`) by the AAM1212.
PPP LCP Config-Request	This field displays the number of config-request PDUs received by the AAM1212 from the CPE (client) device.
PPP LCP Echo-Request	This field displays the number of echo-request PDUs received by the AAM1212 from the CPE (client) device.
PPP LCP Echo-Reply	This field displays the number of echo-reply PDUs received by the AAM1212 from the CPE (client) device.
PPPoE PADI	This field displays the number of padi PDUs sent by the AAM1212 to the BRAS.
PPPoE PADO	This field displays the number of pado PDUs sent by the BRAS to the AAM1212.
PPPoE PADR	This field displays the number of padr PDUs sent by the AAM1212 to the BRAS.
PPPoE PADS	This field displays the number of pads PDUs sent by the BRAS to the AAM1212.
PPPoE PADT	This field displays the number of padt PDUs sent and received by the AAM1212.
PPPoE Service Name Error	This field displays the number of service name errors; for example, the AAM1212's specified service is different than the BRAS's setting.
PPPoE AC System Error	This field displays the number of times the access concentrator experienced an error while performing the Host request; for example, when resources are exhausted in the access concentrator. This value does not include the number of times the AAM1212 checks the AC name field in the BRAS's reply PDU and finds a mismatch, however.
PPPoE Generic Error	This field displays the number of other types of errors that occur in the PPPoE session between the AAM1212 and the BRAS.

29

DSCP

This chapter shows you how to set up DSCP on each port and how to convert DSCP values to IEEE 802.1p values.

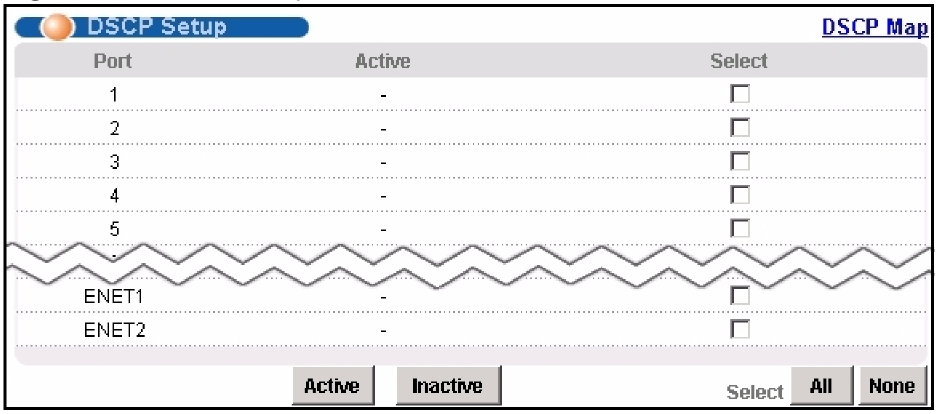
29.1 DSCP Overview

DiffServ Code Point (DSCP) is a field used for packet classification on DiffServ networks. The higher the value, the higher the priority. Lower-priority packets may be dropped if the total traffic exceeds the capacity of the network.

29.2 DSCP Setup Screen

Use this screen to activate or deactivate DSCP on each port. To open this screen, click **Advanced Application**, **DSCP**.

Figure 106 DSCP Setup



The following table describes the labels in this screen.

Table 66 DSCP Setup

LABEL	DESCRIPTION
DSCP Map	Click **DSCP Map** to open the screen where you can set up the mapping between source DSCP priority and IEEE 802.1p priority (see Section 29.3 on page 214).
Port	This field displays each port number.

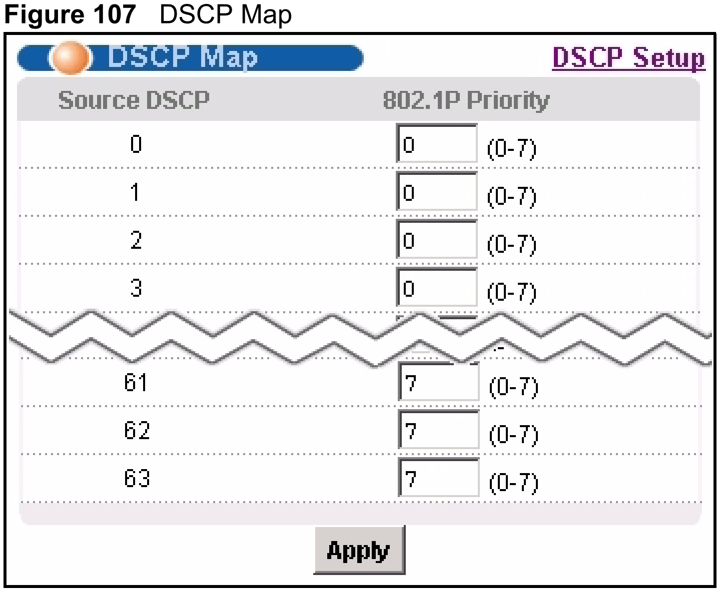
Table 66 DSCP Setup (continued)

LABEL	DESCRIPTION
Active	This field displays whether DSCP is active ("V") or inactive ("-") on this port.
Select	Select this, and click **Active** or **Inactive** to enable or disable the DSCP on this port.
Active	Click this to enable DSCP on the selected ports.
Inactive	Click this to disable DSCP on the selected ports.
All	Click this to select all entries in the table.
None	Click this to un-select all entries in the table.

29.3 DSCP Map Screen

Use this screen to convert DSCP priority to IEEE 802.1p priority. To open this screen, click **Advanced Application**, **DSCP, DSCP Map**.

Figure 107 DSCP Map



The following table describes the labels in this screen.

Table 67 DSCP Map

LABEL	DESCRIPTION
DSCP Map	Click **DSCP Setup** to open the screen where you can activate or deactivate DSCP on each port (see Section 29.2 on page 213).
Source DSCP	This field displays each DSCP value.
802.1P Priority	Enter the IEEE 802.1p priority to which you would like to map this DSCP value.
Apply	Click **Apply** to save your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.

30

TLS PVC

This chapter shows you how to set up Transparent LAN Service (VLAN stacking, Q-in-Q) on each port.

30.1 Transparent LAN Service (TLS) Overview

Transparent LAN Service (also known as VLAN stacking or Q-in-Q) allows a service provider to distinguish multiple customers VLANs, even those with the same (customer-assigned) VLAN ID, within its network.

Use TLS to add an outer VLAN tag to the inner IEEE 802.1Q tagged frames that enter the network. By tagging the tagged frames ("double-tagged" frames), the service provider can manage up to 4,094 VLAN groups with each group containing up to 4,094 customer VLANs. This allows a service provider to provide different services, based on specific VLANs, for many different customers.

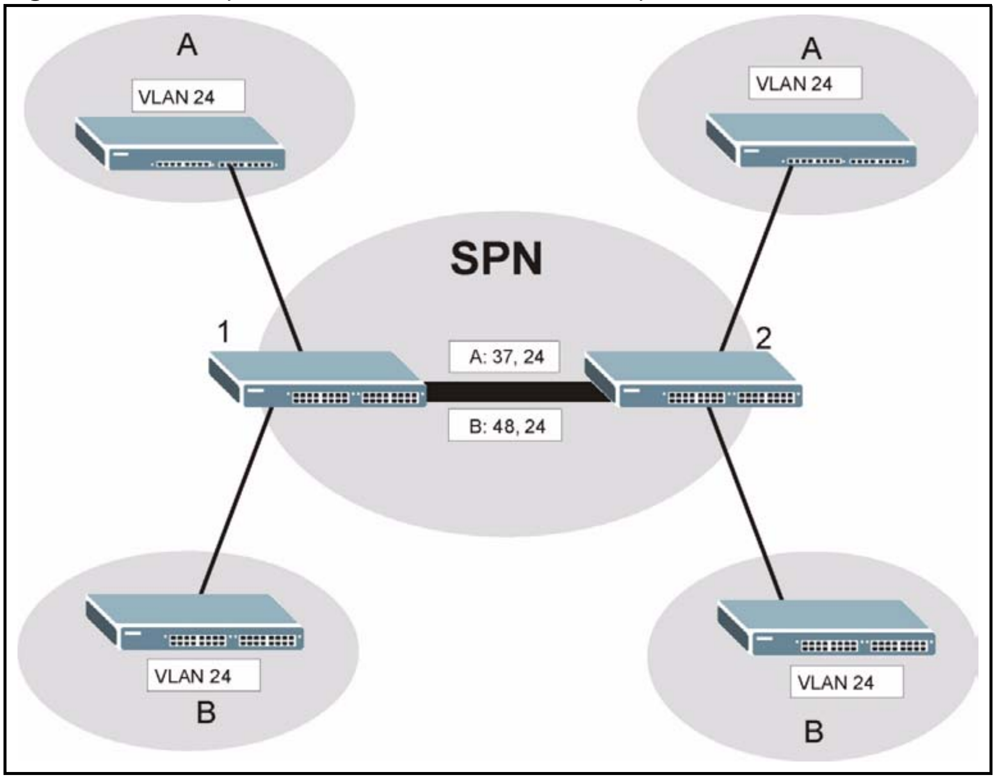
A service provider's customers may require a range of VLANs to handle multiple applications. A service provider's customers can assign their own inner VLAN tags to traffic. The service provider can assign an outer VLAN tag for each customer. Therefore, there is no VLAN tag overlap among customers, so traffic from different customers is kept separate.

Before the AAM1212 sends the frames from the customers, the VLAN ID is added to the frames. When packets intended for specific customers are received on the AAM1212, the outer VLAN tag is removed before the traffic is sent.

30.1.1 TLS Network Example

In the following example figure, both A and B are Service Provider's Network (SPN) customers with VPN tunnels between their head offices and branch offices, respectively. Both have an identical VLAN tag for their VLAN group. The service provider can separate these two VLANs within its network by adding tag 37 to distinguish customer A and tag 48 to distinguish customer B at edge device 1 and then stripping those tags at edge device 2 as the data frames leave the network.

Figure 108 Transparent LAN Service Network Example

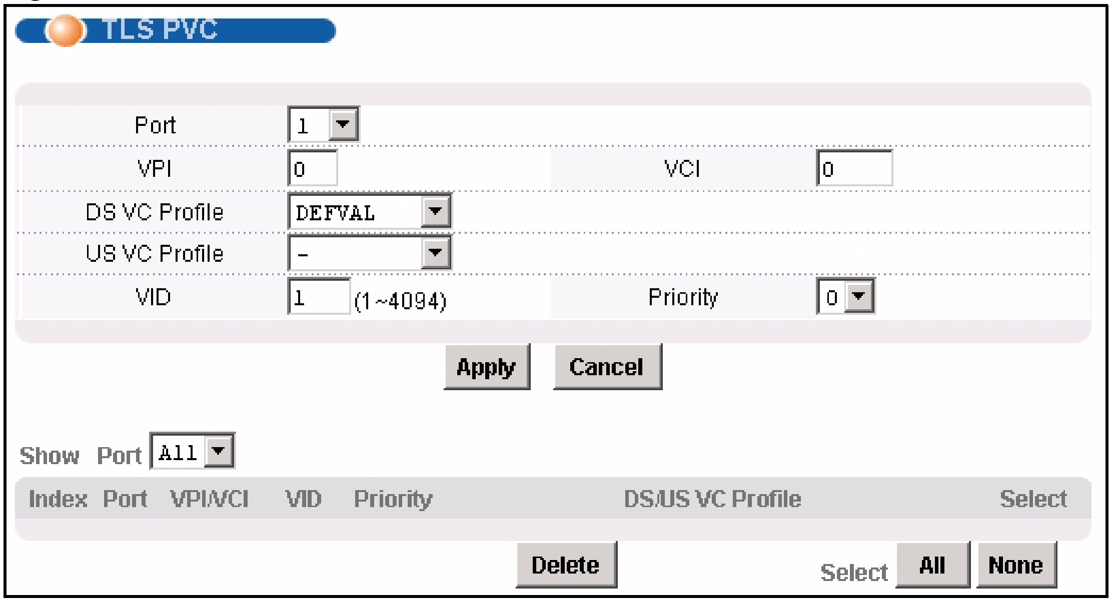


30.2 TLS PVC Screen

Use this screen to set up Transparent LAN Services on each port. This is set up by creating a TLS PVC. See Chapter 30 on page 215 for background information about creating PVCs. To open this screen, click **Advanced Application**, **TLS PVC**.

Note: You can NOT configure PPPoA-to-PPPoE and TLS settings on the same PVC.

Figure 109 TLS PVC



The following table describes the labels in this screen.

Table 68 TLS PVC

LABEL	DESCRIPTION
Port	Use this drop-down list box to select a port for which you wish to set up a TLS PVC. This field is read-only once you click on a port number below.
VPI	Type the Virtual Path Identifier for a channel on this port.
VCI	Type the Virtual Circuit Identifier for a channel on this port.
DS VC Profile	Use the drop-down list box to select a VC profile to use for this channel's downstream traffic shaping.
US VC Profile	Use the drop-down list box to select a VC profile to use for this channel's upstream traffic. The AAM1212 does not perform upstream traffic policing if you do not specify an upstream VC profile. **Note:** Upstream traffic policing should be used in conjunction with the ATM shaping feature on the subscriber's device. If the subscriber's device does not apply the appropriate ATM shaping, all upstream traffic will be discarded due to upstream traffic policing.
VID	Type a VLAN ID to assign to frames received on this channel. **Note:** Make sure the VID is not already used for PPPoA-to-PPPoE conversions.
Priority	Use the drop-down list box to select the priority value (0 to 7) to add to incoming frames without a (IEEE 802.1p) priority tag.
Apply	Click this to add or save channel settings on the selected port. This saves your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.

Table 68 TLS PVC (continued)

LABEL	DESCRIPTION
Cancel	Click **Cancel** to start configuring the screen again.
Show Port	Select which DSL port(s) for which to display TLS PVC settings.
Index	This field displays the number of the PVC. Click a PVC's index number to use the top of the screen to edit the PVC. **Note:** At the time of writing, you cannot edit the VPI and VCI. If you want to change them, add a new PVC with the desired settings. Then you can delete any unwanted PVCs.
Port	This field displays the number of the DSL port on which the PVC is configured.
VPI/VCI	This field displays the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI). The VPI and VCI identify a channel on this port.
VID	This is the VLAN ID assigned to frames received on this channel.
Priority	This is the priority value (0 to 7) added to incoming frames without a (IEEE 802.1p) priority tag.
DS/US VC Profile	This shows which VC profile this channel uses for downstream traffic shaping. The VC profile for upstream policing also displays if the channel is configured to use one.
Select Delete	Select the check box in the **Select** column for an entry, and click **Delete** to remove the entry.
Select All	Click this to select all entries in the table.
Select None	Click this to un-select all entries in the table.

31

ACL

This chapter shows you how to set up ACL profiles on each port.

31.1 Access Control Logic (ACL) Overview

An ACL (Access Control Logic) profile allows the AAM1212 to classify and perform actions on the upstream traffic. Each ACL profile consists of a rule and an action, and you assign ACL profiles to PVCs.

31.1.1 ACL Profile Rules

Each ACL profile uses one of 14 rules to classify upstream traffic. These rules are listed below by rule number.

1. etype <etype> vlan <vid>
2. etype <etype> smac <mac>
3. etype <etype> dmac <mac>
4. vlan <vid> smac <mac>
5. vlan <vid> dmac <mac>
6. smac <mac> dmac <mac>
7. vlan <vid> priority <priority>
8. etype <etype>
9. vlan <vid>
10. smac <mac>
11. dmac <mac>
12. priority <priority>
13. protocol <protocol>
14. {srcip <ip>/<mask>{|dstip <ip>/<mask>{|tos <stos> <etos> {|srcport <sport> <eport> {|dstport <sport> <eport>}}}}}

The input values for these values have the following ranges.

- <vid>: 1~4094
- <priority>: 1~7
- <etype>: 0~65535
- <protocol>: `tcp|udp|ospf|igmp|ip|gre|icmp|<ptype>`
- <ptype>: 0~255
- <mask>: 0~32
- <tos>: 0~255
- <port>: 0~65535

If you apply multiple profiles to a PVC, the AAM1212 checks the profiles by rule number. The lower the rule number, the higher the priority the rule (and profile) has. For example, there are two ACL profiles assigned to a PVC. Profile1 is for VLAN ID 100 (rule number 9) traffic, and Profile2 is for IEEE 802.1p priority 0 traffic (rule number 12). The AAM1212 checks Profile1 first. If the traffic is VLAN ID 100, the AAM1212 follows the action in Profile1 and does not check Profile2. You cannot assign profiles that have the same rule numbers to the same PVC.

31.1.2 ACL Profile Actions

The AAM1212 can perform the following actions after it classifies upstream traffic.

- rate <rate>: change the rate to the specified value (1~65535 kbps)
- rvlan <rvlan>: change the VLAN ID to the specified value (1~4094)
- rpri <rpri>: change the IEEE 802.1p priority to the specified value (0~7)
- deny: do not forward the packet

The AAM1212 can apply more than one action to a packet, unless you select deny.

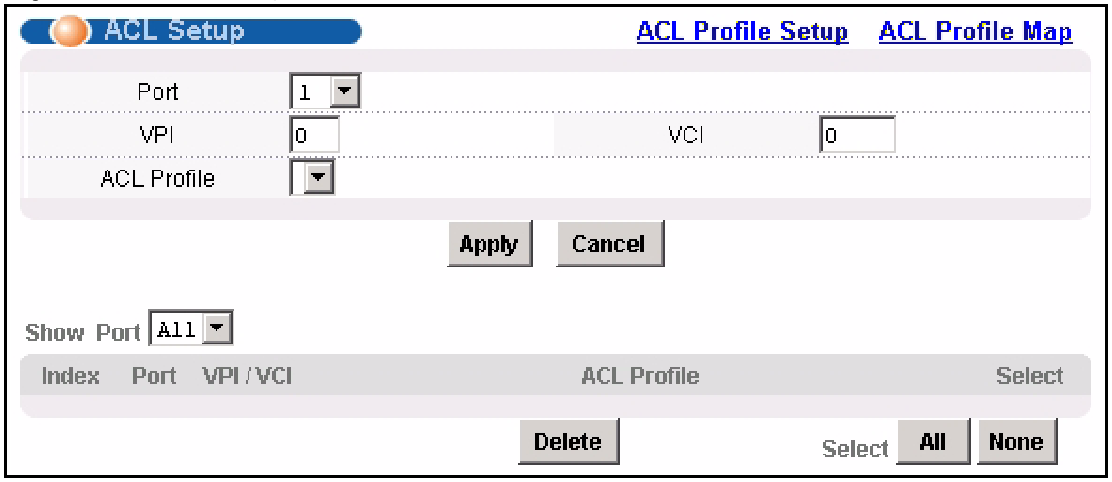
If you select the rvlan action, the AAM1212 replaces the VLAN ID before it compares the VLAN ID of the packet to the VID of the PVC. As a result, it is suggested that you replace VLAN ID on super channels, not normal PVC, since super channels accept any tagged traffic. If you replace the VLAN ID for a normal PVC, the AAM1212 drops the traffic because the new VLAN ID does not match the VID of the PVC. This is illustrated in the following scenario.

There is a normal PVC, and its PVID is 900. You create an ACL rule to replace the VLAN ID with 901. Initially, the traffic for the PVC belongs to VLAN 900. Then, the AAM1212 checks the ACL rule and changes the traffic to VLAN 901. When the AAM1212 finally compares the VLAN ID of the traffic (901) to the VID of the PVC (900), the AAM1212 drops the packets because they do not match.

31.2 ACL Setup Screen

Use this screen to assign ACL profiles to each PVC. To open this screen, click **Advanced Application**, **ACL**.

Figure 110 ACL Setup



The following table describes the labels in this screen.

Table 69 ACL Setup

LABEL	DESCRIPTION
ACL Profile Setup	Click **ACL Profile Setup** to open the screen where you can set up ACL profiles (see Section 31.3 on page 222).
ACL Profile Map	Click **ACL Profile Map** to open the screen where you can look at which ACL profiles are assigned to which PVCs (see Section 31.4 on page 224).
Port	Use this drop-down list box to select a port to which you wish to assign an ACL profile. This field is read-only once you click on a port number below.
VPI	Type the Virtual Path Identifier for a channel on this port.
VCI	Type the Virtual Circuit Identifier for a channel on this port.
ACL Profile	Use the drop-down list box to select the ACL profile you want to assign to this PVC.
Apply	Click this to save your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to start configuring the screen again.
Show Port	Select which DSL port(s) for which to display ACL profile settings.
Index	This field displays the number of the PVC. Click a PVC's index number to use the top of the screen to edit the PVC. **Note:** At the time of writing, you cannot edit the VPI and VCI. If you want to change them, add a new PVC with the desired settings. Then you can delete any unwanted PVCs.
Port	This field displays the number of the DSL port on which the PVC is configured.
VPI/VCI	This field displays the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI). The VPI and VCI identify a channel on this port.
ACL Profile	This field shows the ACL profile assigned to this PVC.
Select Delete	Select the check box in the **Select** column for an entry, and click **Delete** to remove the entry.

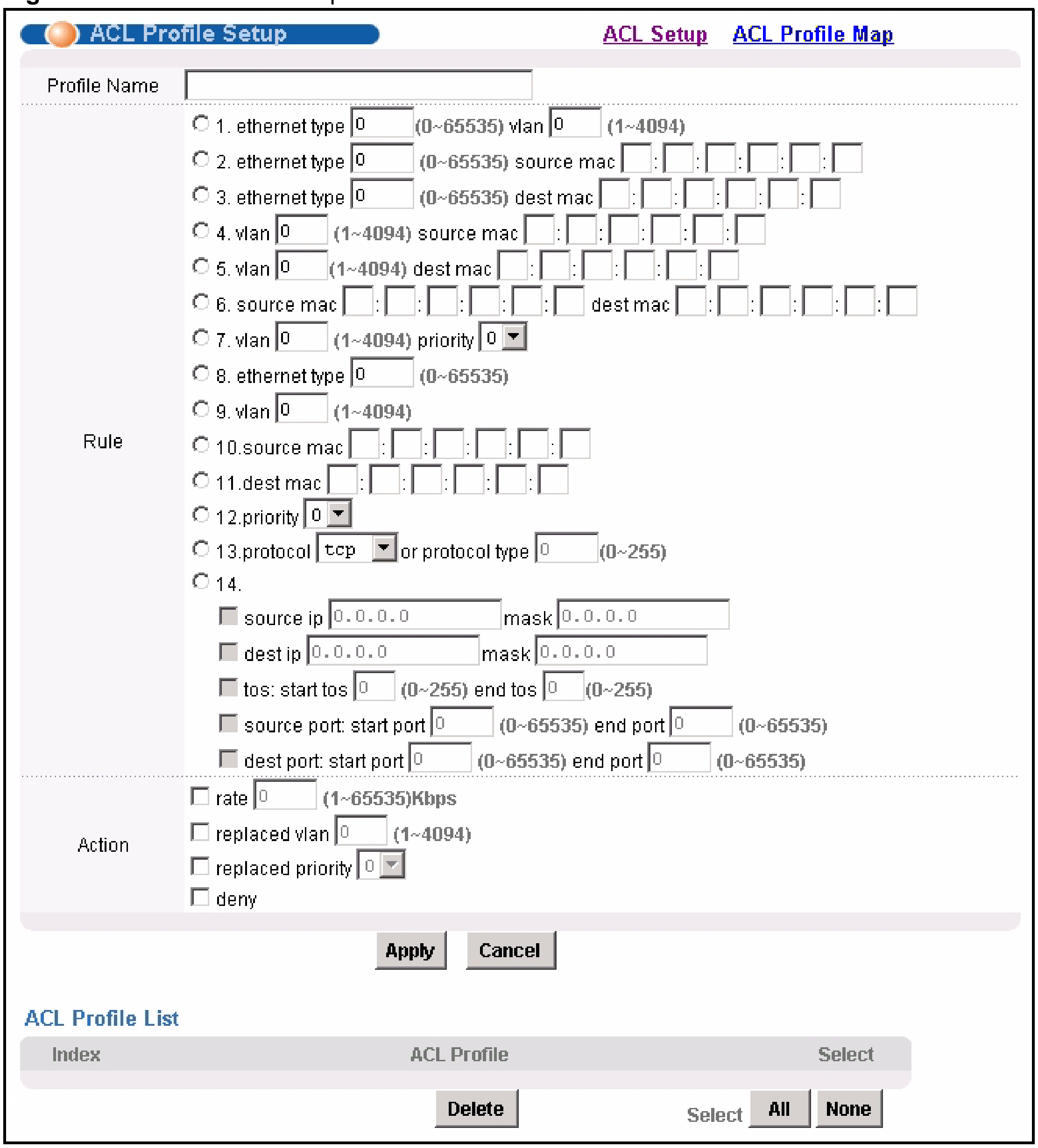
Table 69 ACL Setup (continued)

LABEL	DESCRIPTION
Select All	Click this to select all entries in the table.
Select None	Click this to un-select all entries in the table.

31.3 ACL Profile Setup Screen

Use this screen to set up ACL profiles. To open this screen, click **Advanced Application**, **ACL, ACL Profile Setup**.

Figure 111 ACL Profile Setup



The following table describes the labels in this screen.

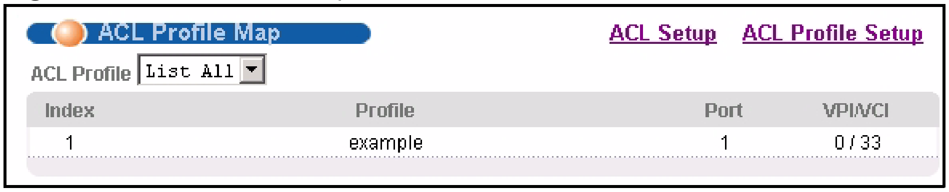
Table 70 ACL Profile Setup

LABEL	DESCRIPTION
ACL Setup	Click **ACL Setup** to open the screen where you can assign ACL profiles to PVCs (see Section 31.2 on page 220).
ACL Profile Map	Click **ACL Profile Map** to open the screen where you can look at which ACL profiles are assigned to which PVCs (see Section 31.4 on page 224).
Profile Name	Enter a descriptive name for the ACL profile. The name can be 1-31 printable ASCII characters long. Spaces are not allowed.
Rule	Select which type of rule to use. **Note:** The lower the number (1-14), the higher the priority the rule has. Provide additional information required for the selected rule. Additional rules consist of one or more of the following criteria.
ethernet type	Enter the 16-bit EtherType value between 0 and 65535.
vlan	Enter a VLAN ID between 1 and 4094.
source mac	Enter the source MAC address.
dest mac	Enter the destination MAC address.
priority	Select the IEEE 802.1p priority.
protocol	Select the IP protocol used.
protocol type	Enter the IP protocol number (between 0 and 255) used.
source ip	Enter the source IP address and subnet mask in dotted decimal notation.
dest ip	Enter the source IP address and subnet mask in dotted decimal notation.
tos	Enter the start and end Type of Service between 0 and 255.
source port	Enter the source port or range of source ports.
dest port	Enter the destination port or range of destination ports.
Action	Select which action(s) the AAM1212 should follow when the criteria are satisfied.
rate	Enter the maximum bandwidth this traffic is allowed to have.
replaced vlan	Enter the VLAN ID that this traffic should use.
replaced priority	Select the IEEE 802.1p priority that this traffic should have.
deny	Select this if you want the AAM1212 to reject this kind of traffic.
ACL Profile List	
Index	This field displays a sequential value. The sequence in this table is not important. Click this to edit the associated ACL profile in the section above.
ACL Profile	This field displays the name of this ACL profile.
Select Delete	Select the check box in the **Select** column for an entry, and click **Delete** to remove the entry.
Select All	Click this to select all entries in the table.
Select None	Click this to un-select all entries in the table.

31.4 ACL Profile Map Screen

Use this screen to look at all the ACL profiles and the PVCs to which each one is assigned. To open this screen, click **Advanced Application**, **ACL, ACL Profile Map**.

Figure 112 ACL Profile Map



The following table describes the labels in this screen.

Table 71 ACL Profile Map

LABEL	DESCRIPTION
ACL Setup	Click **ACL Setup** to open the screen where you can assign ACL profiles to PVCs (see Section 31.2 on page 220).
ACL Profile Setup	Click **ACL Profile Setup** to open the screen where you can set up ACL profiles (see Section 31.3 on page 222).
ACL Profile	Select the ACL profile(s) for which you want to see which PVCs are assigned to it.
Index	This field displays the number of an entry.
Profile	This field shows the ACL profile assigned to this PVC.
Port	This field displays the DSL port number on which the PVC is configured.
VPI/VCI	This field displays the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI). The VPI and VCI identify a channel on this port.

32

Downstream Broadcast

This chapter shows you how to allow or block downstream broadcast traffic.

32.1 Downstream Broadcast

Downstream broadcast allows you to block downstream broadcast packets from being sent to specified VLANs on specified ports.

32.2 Downstream Broadcast Screen

To open this screen, click **Advanced Application**, **Downstream Broadcast**.

Figure 113 Downstream Broadcast

The following table describes the labels in this screen.

Table 72 Downstream Broadcast

LABEL	DESCRIPTION
Port	Use this drop-down list box to select a port for which you wish to configure settings.
VLAN	Specify the number of a VLAN (on this entry's port) to which you do not want to send broadcast traffic. The VLAN must already be configured in the system.
Add	Click **Add** to save your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.

Table 72 Downstream Broadcast (continued)

LABEL	DESCRIPTION
Blocking Table	
Port	Use this drop-down list box to select a port for which you wish to display settings.
Index	This field displays the number of the downstream broadcast blocking entry.
Port	This is the number of a DSL port through which you will block downstream broadcast traffic (on a specific VLAN).
VLAN	This field displays the number of a VLAN to which you do not want to send broadcast traffic (on the entry's port).
Select	Select an entry's **Select** check box and click **Delete** to remove the entry. Clicking **Delete** saves your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Select All	Click **All** to mark all of the check boxes.
Select None	Click **None** to un-mark all of the check boxes.

33

Syslog

This chapter explains how to set the syslog parameters.

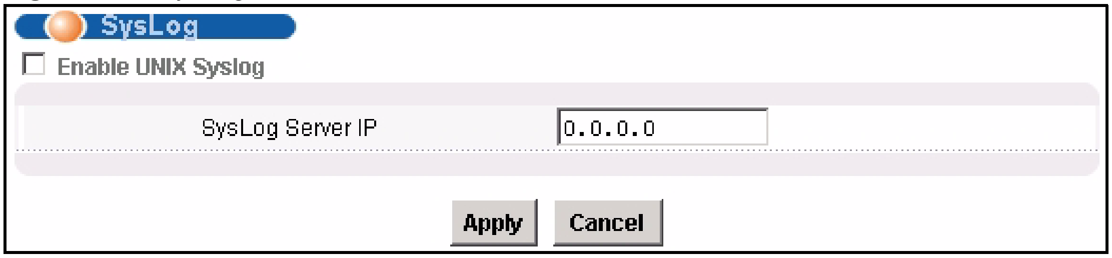
33.1 Syslog

The syslog feature sends logs to an external syslog server.

33.2 SysLog Screen

To open this screen, click **Advanced Application**, **SysLog**.

Figure 114 SysLog



The following table describes the labels in this screen.

Table 73 SysLog

LABEL	DESCRIPTION
Enable Unix Syslog	Select this check box to activate syslog (system logging) and then configure the syslog parameters described in the following fields.
Syslog Server IP	Enter the IP address of the syslog server. (The log facility is specified in **Alarm > Alarm Event Setup**. See Section 40.4 on page 255.)
Apply	Click **Apply** to save your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

34

Access Control

This chapter describes how to configure access control.

34.1 Access Control Screen

Use this screen to configure SNMP and enable/disable remote service access.

To open this screen, click **Advanced Application**, **Access Control**.

Figure 115 Access Control

34.2 Access Control Overview

A console port or Telnet session can coexist with one FTP session, a web configurator session and/or limitless SNMP access control sessions.

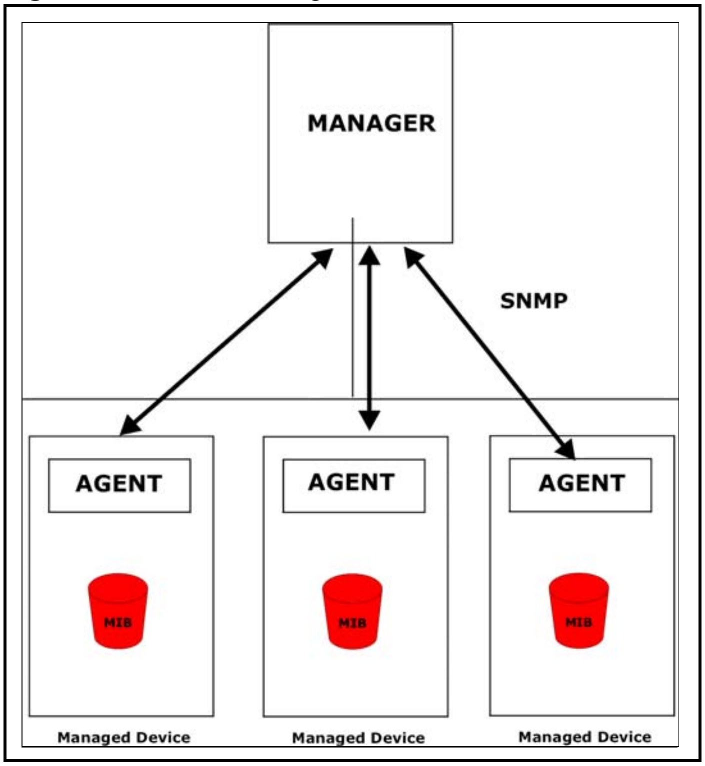
Table 74 Access Control Summary

	CONSOLE PORT	TELNET	FTP	WEB	SNMP
Number of sessions allowed	1	5	1	No limit	No limit

34.3 SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. SNMP is a member of TCP/IP protocol suite. A manager station can manage and monitor the AAM1212 through the network via SNMP version one (SNMPv1) and/or SNMP version 2c. The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

Figure 116 SNMP Management Model



An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed device (the AAM1212). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

Table 75 SNMP Commands

COMMAND	DESCRIPTION
Get	Allows the manager to retrieve an object variable from the agent.
GetNext	Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.

Table 75 SNMP Commands (continued)

COMMAND	DESCRIPTION
Set	Allows the manager to set values for object variables within an agent.
Trap	Used by the agent to inform the manager of some events.

34.3.1 Supported MIBs

MIBs let administrators collect statistics and monitor status and performance. See Chapter 34 on page 229 for the list of MIBs the AAM1212 supports.

34.3.2 SNMP Traps

The AAM1212 can send the following SNMP traps to an SNMP manager when an event occurs. ATUC refers to the downstream channel (for traffic going from the AAM1212 to the subscriber). ATUR refers to the upstream channel (for traffic coming from the subscriber to the AAM1212).

Table 76 SNMPv2 Traps

TRAP NAME	DESCRIPTION
coldStart	This trap is sent when the AAM1212 is turned on.
warmStart	This trap is sent when the AAM1212 restarts.
linkDown	This trap is sent when the Ethernet link is down. Enterprise specific (adsl_atuc_los) traps are sent when an ADSL link is down.
linkUp	This trap is sent when the Ethernet or ADSL link comes up.
authenticationFailure	This trap is sent when the SNMP community check fails.
reboot	This trap is sent when the system is going to reboot. The variable is the reason for the system reboot.
overheat	This trap is sent when the system is overheated. The variable is the current system temperature in Celsius.
overheatOver	This trap is sent when the system is no longer overheated. The variable is the current system temperature in Celsius.
voltageOutOfRange	This trap is sent when the voltage of the system is out of the normal range. The variable is the current voltage of the system in volts.
voltageNormal	This trap is sent when the voltage of the system is back within the normal range. The variable is the current voltage of the system in volts.
thermalSensorFailure	This trap is sent when the thermal sensor fails.
adslAtucLof	This trap is sent when a Loss Of Frame is detected on the ATUC.
adslAturLof	This trap is sent when a Loss Of Frame is detected on the ATUR.
adslAtucLos	This trap is sent when a Loss Of Signal is detected on the ATUC.
adslAturLos	This trap is sent when a Loss Of Signal is detected on the ATUR.
adslAturLpr	This trap is sent when a Loss Of Power is detected on the ATUR.
adslAtucLofClear	This trap is sent when the Loss Of Frame detected on the ATUC is over.

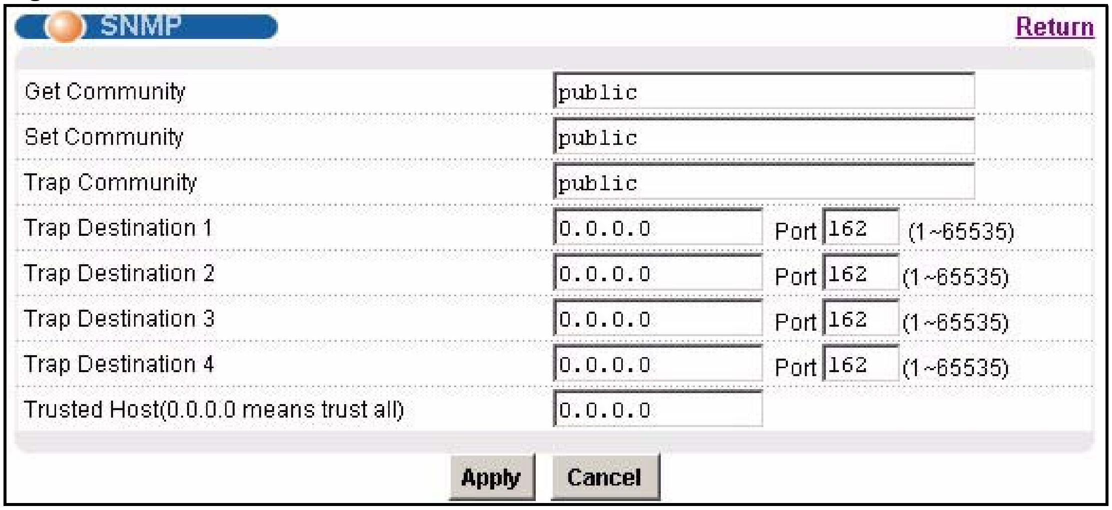
Table 76 SNMPv2 Traps (continued)

TRAP NAME	DESCRIPTION
adslAturLofClear	This trap is sent when the Loss Of Frame detected on the ATUR is over.
adslAtucLosClear	This trap is sent when the Loss Of Signal detected on the ATUC is over.
adslAturLosClear	This trap is sent when the Loss Of Signal detected on the ATUR is over.
adslAturLprClear	This trap is sent when the Loss Of Power detected on the ATUR is over.
adslAtucPerfLofsThreshTrap	The number of times a Loss Of Frame has occurred within 15 minutes for the ATUC has reached the threshold. currValue is the number of times a Loss Of Frame has occurred within the 15-minute interval.
adslAtucPerfLossThreshTrap	The number of times a Loss Of Signal has occurred within 15 minutes for the ATUC has reached the threshold. currValue is the number of times a Loss Of Signal has occurred within the 15 minute interval.
adslAtucPerfLprsThreshTrap	The number of times a Loss Of Power has occurred within 15 minutes for the ATUC has reached the threshold. currValue is the number of times a Loss Of Power has occurred within the 15-minute interval.
adslAtucPerfESsThreshTrap	The number of error seconds within 15 minutes for the ATUC has reached the threshold. currValue is the number of error seconds that have occurred within the 15-minute interval.
adslAtucPerfLolsThreshTrap	The number of times a Loss Of Link has occurred within 15 minutes for the ATUC has reached the threshold. currValue is the number of times a Loss Of Link has occurred within the 15-minute interval.
adslAturPerfLofsThreshTrap	The number of times a Loss Of Frame has occurred within 15 minutes for the ATUR has reached the threshold. currValue is the number of times a Loss Of Frame has occurred within the 15-minute interval.
adslAturPerfLossThreshTrap	The number of times a Loss Of Signal has occurred within 15 minutes for the ATUR has reached the threshold. currValue is the number of times a Loss Of Signal has occurred within the 15-minute interval.
adslAturPerfLprsThreshTrap	The number of times a Loss Of Power has occurred within 15 minutes for the ATUR has reached the threshold. currValue is the number of times a Loss Of Power has occurred within the 15-minute interval.
adslAturPerfESsThreshTrap	The number of error seconds within 15 minutes for the ATUR has reached the threshold. currValue is the number of error seconds that have occurred within the 15-minute interval.
adslAtucSesLThreshTrap	The number of severely errored seconds within 15 minutes for the ATUC has reached the threshold. currValue is the number of severely errored seconds that have occurred within the 15-minute interval.
adslAtucUasLThreshTrap	The number of Unavailable seconds within 15 minutes for the ATUC has reached the threshold. currValue is the number of Unavailable seconds that have occurred within the 15-minute interval.
adslAturSesLThreshTrap	The number of severely errored seconds within 15 minutes for the ATUR has reached the threshold. currValue is the number of severely errored seconds that have occurred within the 15-minute interval.
adslAturUasLThreshTrap	The number of Unavailable seconds within 15 minutes for the ATUR has reached the threshold. currValue is the number of Unavailable seconds that have occurred within the 15-minute interval.

34.4 SNMP Screen

To open this screen, click **Advanced Application**, **Access Control**, **SNMP**.

Figure 117 SNMP



The following table describes the labels in this screen.

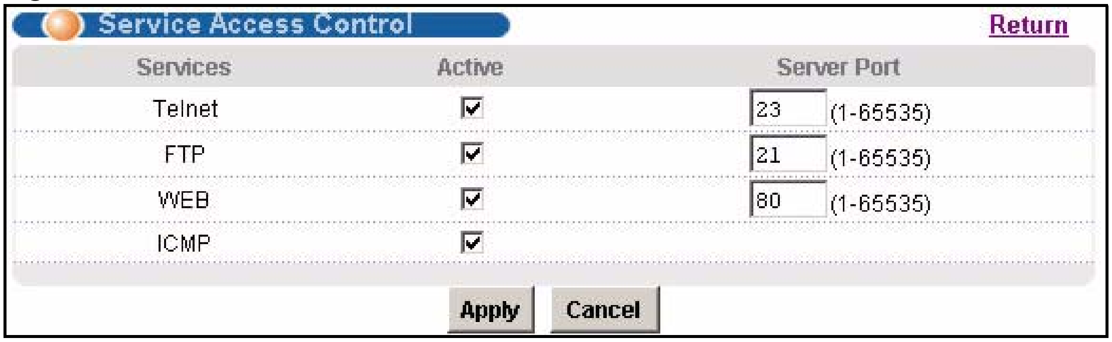
Table 77 SNMP

LABEL	DESCRIPTION
Return	Click **Return** to go back to the previous screen.
Get Community	Enter the get community, which is the password for the incoming Get- and GetNext- requests from the management station.
Set Community	Enter the set community, which is the password for incoming Set- requests from the management station.
Trap Community	Enter the trap community, which is the password sent with each trap to the SNMP manager.
Trap Destination 1~4	Enter the IP address of a station to send your SNMP traps to.
Port	Enter the port number upon which the station listens for SNMP traps.
Trusted Host	A “trusted host” is a computer that is allowed to use SNMP with the AAM1212. **0.0.0.0** allows any computer to use SNMP to access the AAM1212. Specify an IP address to allow only the computer with that IP address to use SNMP to access the AAM1212.
Apply	Click **Apply** to save your changes to the AAM1212’s volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

34.5 Service Access Control Screen

To open this screen, click **Advanced Application**, **Access Control**, **Service Access Control**.

Figure 118 Service Access Control



The following table describes the labels in this screen.

Table 78 Service Access Control

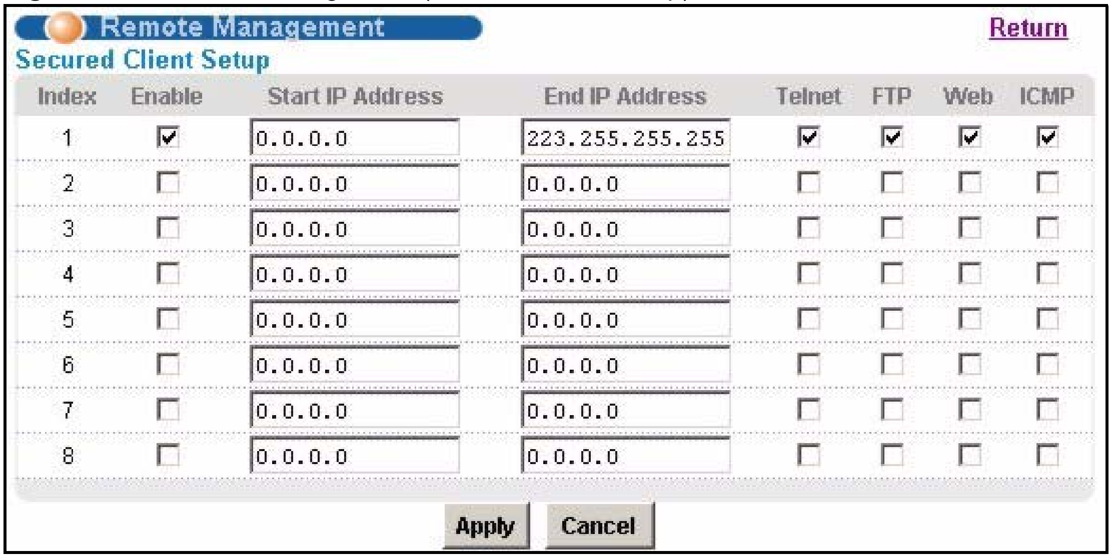
LABEL	DESCRIPTION
Return	Click **Return** to go back to the previous screen.
Services	Services you may use to access the AAM1212 are listed here.
Active	Select the **Active** check boxes for the corresponding services that you want to allow to access the AAM1212.
Server Port	For Telnet, FTP or web services, you may change the default service port by typing the new port number in the **Server Port** field. If you change the default port number then you will have to let people (who wish to use the service) know the new port number for that service.
Apply	Click **Apply** to save your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

34.6 Remote Management Screen

Use this screen to configure the IP address ranges of trusted computers that may manage the AAM1212.

To open this screen, click **Advanced Application**, **Access Control**, **Secured Client**.

Figure 119 Remote Management (Secured Client Setup)



The following table describes the labels in this screen.

Table 79 Remote Management (Secured Client Setup)

LABEL	DESCRIPTION
Return	Click **Return** to go back to the previous screen.
Index	This is the client set index number. A “client set” is a group of one or more “trusted computers” from which an administrator may use a service to manage the AAM1212.
Enable	Select this check box to activate this secured client set. Clear the check box if you wish to temporarily disable the set without deleting it.
Start IP Address End IP Address	Configure the IP address range of trusted computers from which you can manage the AAM1212. The AAM1212 checks if the client IP address of a computer requesting a service or protocol matches the range set here. The AAM1212 immediately disconnects the session if it does not match.
Telnet/FTP/Web/ ICMP	Select services that may be used for managing the AAM1212 from the specified trusted computers.
Apply	Click **Apply** to save your changes to the AAM1212’s volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring this screen afresh.

35

PPPoE Intermediate Agent

This chapter describes how the AAM1212 gives a PPPoE termination server additional information that the server can use to identify and authenticate a PPPoE client.

35.1 PPPoE Intermediate Agent Tag Format

If the PPPoE Intermediate Agent is enabled, the AAM1212 adds a vendor-specific tag to PADI (PPPoE Active Discovery Initialization) and PADR (PPPoE Active Discovery Request) packets from PPPoE clients. This tag is defined in RFC 2516 and has the following format for this feature.

Table 80 PPPoE Intermediate Agent Vendor-specific Tag Format

Tag_Type (0x0105)	Tag_Len	Value	i1	i2

The Tag_Type is 0x0105 for vendor-specific tags, as defined in RFC 2516. The Tag_Len indicates the length of Value, i1 and i2. The Value is the 32-bit number 0x00000DE9, which stands for the "ADSL Forum" IANA entry. i1 and i2 are PPPoE intermediate agent sub-options, which contain additional information about the PPPoE client. The AAM1212 supports two formats for the PPPoE intermediate agent sub-options: private and TR-101.

35.1.0.1 Private Format

There are two types of sub-option: "Agent Circuit ID Sub-option" and "Agent Remote ID Sub-option". They have the following formats.

Table 81 PPPoE Intermediate Agent Vendor-specific Tag Format

SubOpt (0x01)	Length	Slot ID (1 byte)	Port No (1 byte)	VLAN ID (2 bytes)	Extra Information (0~23 bytes)

Table 82 PPPoE Intermediate Agent Remote ID Sub-option Format

SubOpt (0x02)	Length	MAC (6 bytes)

The AAM1212 adds the slot ID of the PPPoE client, the port number of the PPPoE client, the VLAN ID on the PPPoE packet, and any extra information (for example, the device name) into the Agent Circuit ID Sub-option. In addition, the AAM1212 puts the PPPoE client's MAC address into the Agent Remote ID Sub-option. The slot ID is zero, if this value is not applicable. If the AAM1212 adds extra information, it does not append a trailing 0x00 (00h).

35.1.0.2 TR-101 Format

The PPPoE Intermediate Agent sub-option includes the system name or IP address, slot ID, port number, VPI, and VCI on which the TCP/IP configuration request was received.

The following figure shows the format of the TR-101 PPPoE Intermediate Agent sub-option. The 1 in the first field identifies this as an Agent Circuit ID sub-option. The next field specifies the length of the field. The hostname field displays the system name, if it has been configured, the extra information field (A) if the hostname was not configured, or the IP address in dotted decimal notation (w.x.y.z), if neither the system name nor the extra information field was been configured. In either case, the hostname is truncated to 23 characters, and trailing spaces are discarded. The hostname field is followed by a space, the string “atm”, and another space. Then, a 1-byte Slot ID field specifies the ingress slot number, and a 1-byte Port No field specifies the ingress port number. Next, the VPI and VCI denote the virtual circuit that received the DHCP request message from the subscriber. If the VID is turned on, there is a colon and then the VLAN ID (1 ~ 4094). If the VID is turned off, there is neither colon nor VID.

The slot ID, port number, VPI, VCI and MAC are separated from each other by a forward slash (/) colon (:) or period (.). An example is “SYSNAME atm 3/10:0.33:12”.

Table 83 PPPoE Intermediate Agent Sub-option Format: TR-101 (VID on)

1	N	hostname / A / IP	“ atm “	Slot ID	/	Port No.	:	VPI	.	VCI	:	VLAN ID

Table 84 PPPoE Intermediate Agent Sub-option Format: TR-101 (VID off)

1	N	hostname / A / IP	“ atm “	Slot ID	/	Port No.	:	VPI	.	VCI

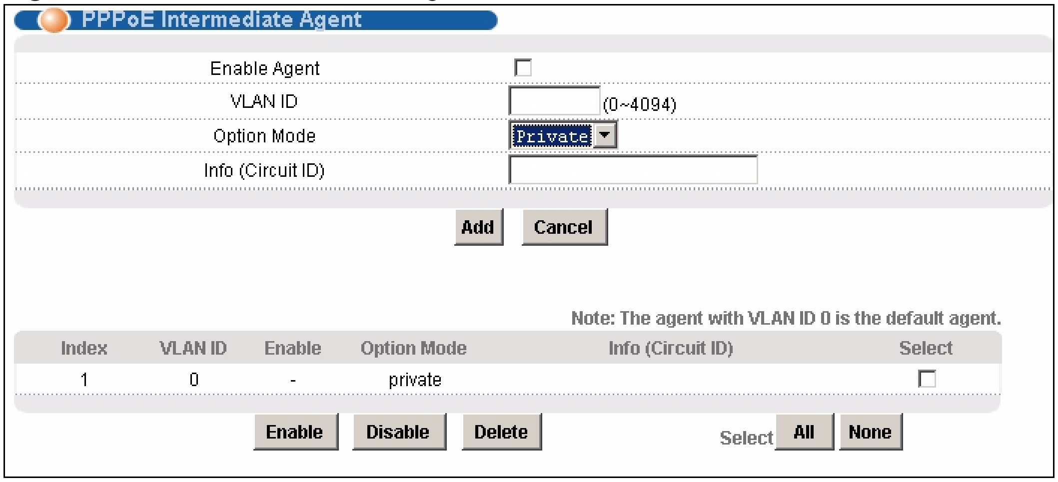
Unlike the private format for PPPoE intermediate agent, the TR-101 format for PPPoE intermediate agent does not include the Remote ID sub-option.

35.2 PPPoE Intermediate Agent Screen

Use this screen to configure the AAM1212 to give a PPPoE termination server additional information that the server can use to identify and authenticate a PPPoE client.

To open this screen, click **Advanced Application** > **PPPoE Intermediate Agent**.

Figure 120 PPPoE Intermediate Agent



The following table describes the labels in this screen.

Table 85 PPPoE Intermediate Agent

LABEL	DESCRIPTION
Enable Agent	Select this if you want the AAM1212 to add a vendor-specific tag to PADI (PPPoE Active Discovery Initialization) and PADR (PPPoE Active Discovery Request) packets from PPPoE clients in the specified VLAN. This tag contains information that a PPPoE termination server can use to identify and authenticate a PPPoE client. This information includes the slot ID, port number, VLAN ID, and MAC address of the PPPoE client, as well as any additional information specified in the **Info** field. Clear this if you do not want the AAM1212 to add a vendor-specific tag to PADI and PADR packets from PPPoE clients in the specified VLAN.
VLAN ID	Enter the source VLAN ID for which the PPPoE intermediate agent settings apply. Enter **0** if you want to configure the default settings for all VLAN.
Option Mode	Select either the **Private** or **TR-101** PPPoE Intermediate Agent sub-option.
Info (Circuit ID)	Enter any extra information the AAM1212 adds to PADI and PADR packets in the specified VLAN. You can enter up to 23 printable English keyboard characters or spaces.
Add	Click **Add** to save the settings. The settings then display in the summary table at the bottom of the screen. Clicking **Add** saves your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring the fields afresh.
Index	This field displays the index number of the entry.
VLAN ID	This field displays the source VLAN ID for which the PPPoE intermediate agent settings apply.
Enable	This field displays whether or not the AAM1212 adds a vendor-specific tag to PADI (PPPoE Active Discovery Initialization) and PADR (PPPoE Active Discovery Request) packets from PPPoE clients in the specified VLAN.
Option Mode	This field displays which method (**Private** or **TR-101**) is used to encode PPPoE line information in PPPoE discover packets.
Info (Circuit ID)	This field displays any extra information the AAM1212 adds to PADI and PADR packets in the specified VLAN, if the PPPoE intermediate agent is turned on.

Table 85 PPPoE Intermediate Agent (continued)

LABEL	DESCRIPTION
Select Enable	Select the check box in the **Select** column for an entry, and click **Enable** to add a vendor-specific tag to PADI and PADR packets for PPPoE clients in the selected VLAN(s).
Select Disable	Select the check box in the **Select** column for an entry, and click **Disable** to not add a vendor-specific tag to PADI and PADR packets for PPPoE clients in the selected VLAN(s).
Select Delete	Select the check box in the **Select** column for an entry, and click **Delete** to delete the PPPoE intermediate agent settings for subscribers in the selected VLAN(s). This also disables this feature for PPPoE clients in the selected VLAN(s).
Select All	Click **All** to mark all of the check boxes.
Select None	Click **None** to un-mark all of the check boxes.

36

Maximum MTU Size

This chapter describes how to configure the Maximum Transmission Unit (MTU) for the Ethernet interfaces. The Ethernet interfaces discard any packets larger than this.

36.1 Maximum MTU Size Screen

Use this screen to configure the Maximum Transmission Unit (MTU) for the Ethernet interfaces. The Ethernet interfaces discard any packets larger than this.

To open this screen, click **Advanced Application, Maximum MTU Size**.

Figure 121 Maximum MTU

The following table describes the labels in this screen.

Table 86 Maximum MTU

LABEL	DESCRIPTION
Maximum MTU Size	Enter the size, in bytes, of the Maximum Transmission Unit (MTU) for the Ethernet interfaces. The Ethernet interfaces discard any packets larger than this size.
Apply Setting	Click **Apply Setting** to save your MTU settings. Clicking **Apply Setting** saves your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.

37

PVC Upstream Limit

This chapter describes how to limit the transmission rate for upstream traffic by PVC.

You can set this limit for regular PVCs, priority PVCs, TLS PVCs, and IP bridge PVCs.

These limits are packet-based, not cell-based. If the limit is exceeded, the packet is discarded the moment it exceeds the limit, regardless of 802.1p priority. The AAM1212 does not check the p-bit of incoming packets from subscribers when it discards the packet.

These limits are completely managed by the AAM1212, regardless of the CPE device’s settings, which makes this approach more flexible and easier for operators to deploy.

37.1 PVC Upstream Limit and Upstream VC Profiles

You can also set limits on the transmission rate for upstream traffic in upstream VC profiles, but this approach has some limitations.

- It is cell-based. If one ATM cell is lost, you lose one complete Ethernet frame from the AAM1212. In contrast, PVC upstream rate limits are packet-based. If the limit is 500 Kbps and users inject data at 600 Kbps, you can still get around 500 Kbps traffic. If you use upstream VC profiles, you might get a much lower data rate.
- The AAM1212 has to work together with the CPE device's ATM output shaping. If the CPE device does not support this or does not do it accurately, it is very easy to violate the upstream VC profile and get poor throughput through the AAM1212.

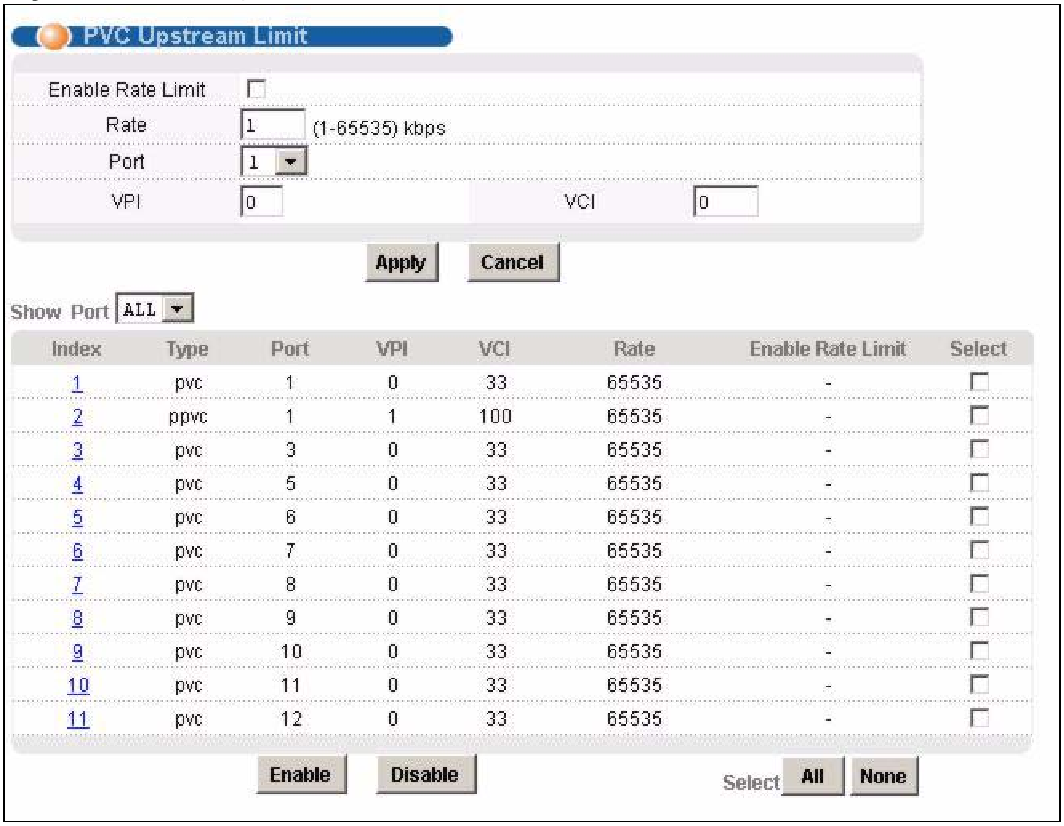
If there are limits on the transmission rate for upstream traffic both in upstream VC profiles and in this feature, the AAM1212 enforces the limit in the upstream VC profile first.

37.2 PVC Upstream Limit Screen

Use this screen to limit the transmission rate for upstream traffic by PVC.

To open this screen, click **Advanced Application, PVC Upstream Limit**.

Figure 122 PVC Upstream Limit



The following table describes the labels in this screen.

Table 87 PVC Upstream Limit

LABEL	DESCRIPTION
Enable Rate Limit	Select this to set a limit on the upstream transmission rate for the specified PVC. Clear this if there is no limit.
Rate	This field has no effect unless **Enable Rate Limit** is selected. Enter the maximum upstream transmission rate, in kbps, for the specified PVC.
Port	Use this drop-down list box to select the port for the PVC for which you wish to configure the maximum upstream transmission rate.
VPI	Type the Virtual Path Identifier for the PVC for which you wish to configure the maximum upstream transmission rate.
VCI	Type the Virtual Circuit Identifier for the PVC for which you wish to configure the maximum upstream transmission rate.
Apply	Click **Apply** to save the settings. The settings then display in the summary table at the bottom of the screen. Clicking **Apply** saves your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to begin configuring the fields afresh.
Show Port	Select a port for which you wish to view information.
Index	This field displays the index number for each PVC. Click it to edit the settings for the maximum upstream transmission rate.
Type	This field displays what type of PVC the specified PVC is.

Table 87 PVC Upstream Limit (continued)

LABEL	DESCRIPTION
Port	This field displays the port number for the specified PVC.
VPI	This field displays the Virtual Path Identifier for the specified PVC.
VCI	This field displays the Virtual Circuit Identifier for the specified PVC.
Rate	This field displays the maximum upstream transmission rate for the specified PVC. This has no effect, however, unless **Enable Rate Limit** is enabled.
Select Enable	Select the check box in the **Select** column for an entry, and click **Enable** to activate the limit on the upstream transmission rate for the select PVC(s).
Select Disable	Select the check box in the **Select** column for an entry, and click **Disable** to deactivate the limit on the upstream transmission rate for the select PVC(s).
Select All	Click **All** to mark all of the check boxes.
Select None	Click **None** to un-mark all of the check boxes.

38

OUI Filter

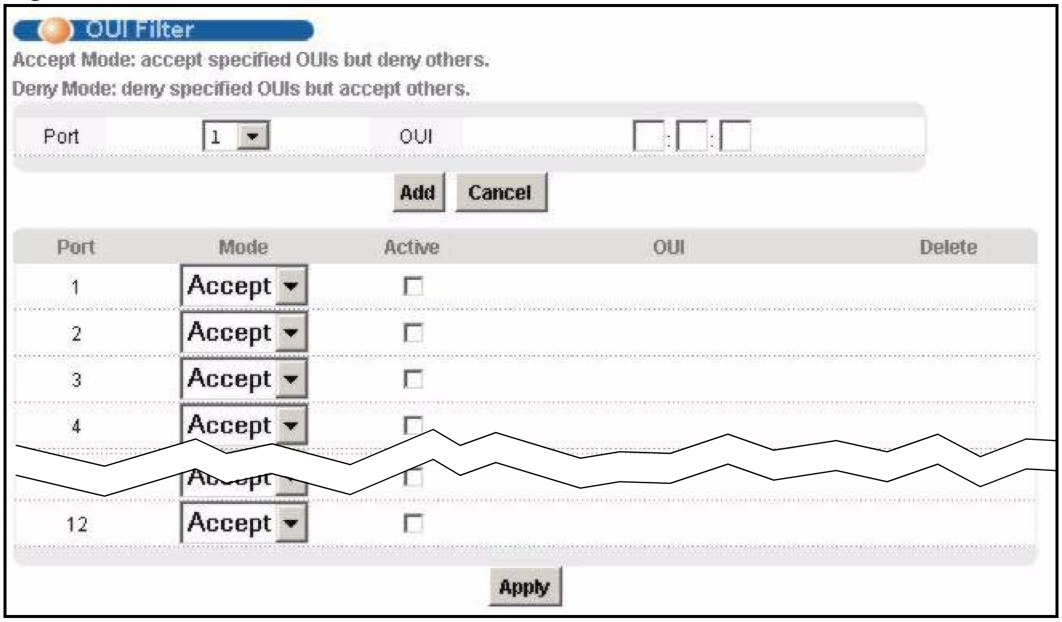
This chapter describes the **OUI Filter** screen.

Configure an OUI (Organizationally Unique Identifier) filter to block or forward packets from devices with the specified OUI in the MAC address.

The OUI field is the first three octets in a MAC address. An OUI uniquely identifies the manufacturer of a network device and allows you to identify from which device brands the switch will accept traffic or send traffic to. The OUI value is assigned by the IANA.

Click **Advanced Application > OUI Filter** to display the following screen.

Figure 123 OUI Filter



The following table describes the labels in this screen.

Table 88 OUI Filter

LABEL	DESCRIPTION
Port	Select a port for which you wish to configure packet type filtering.
OUI	Enter the first three octets of a MAC address in the format xx:xx:xx. For example, 00:AF:FF.
Add	Click this to save the **OUI** to the specified port.
Cancel	Click this to reset the **OUI** field.
Port	This displays the AAM1212's port number.

Table 88 OUI Filter (continued)

LABEL	DESCRIPTION
Mode	Specify the action on matched frames. Select **accept** to allow frames with a matched OUI field in the MAC addresses. The switch blocks frames with other OUIs not specified. Select **deny** to block frames with a matched OUI field in the MAC addresses. The switch allows frames with other OUIs not specified.
Active	Select this to activate this filter. Clear this check box to disable the filter without deleting it.
OUI	This displays the first three octets of a MAC address in the format xx:xx:xx.
Delete	Click this to remove the OUI filter from the port.
Apply	Click **Apply** to save the changes in this screen to the system's volatile memory. The system loses these changes if it is turned off or loses power, so use the **Config Save** on the navigation panel and then the **Save** button to save your changes to the non-volatile memory when you are done configuring.

PART IV
Routing Protocol

Static Routing (251)

39

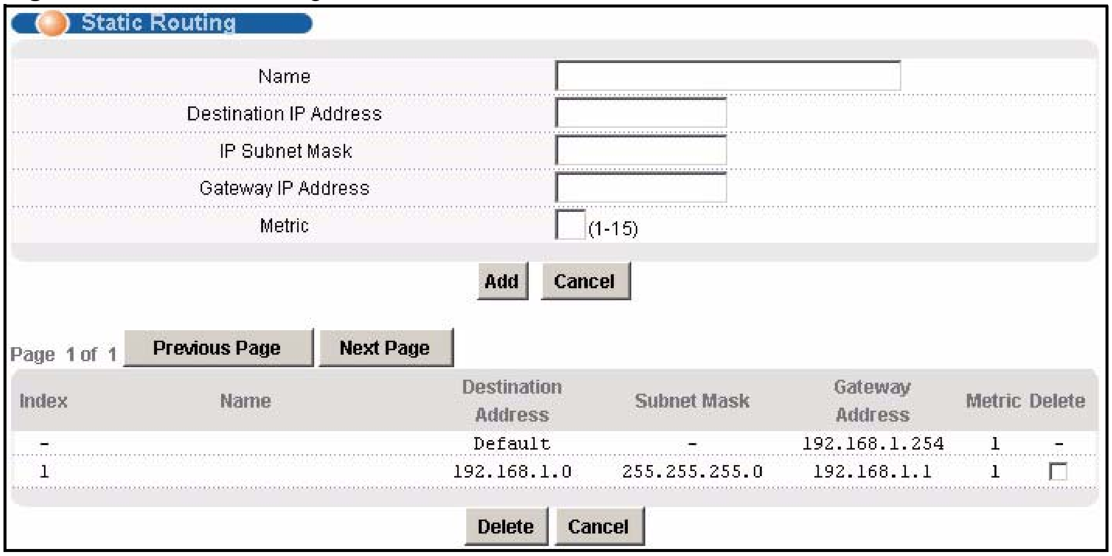
Static Routing

This chapter shows you how to configure the static routing function.

Static routes tell the AAM1212 how to forward the AAM1212's own IP traffic when you configure the TCP/IP parameters manually. This is generally useful for allowing management of the device from a device with an IP address on a different subnet from that of the device's IP address (remote management).

To open this screen, click **Routing Protocol**, **Static Routing**.

Figure 124 Static Routing



The following table describes the labels in this screen.

Table 89 Static Routing

LABEL	DESCRIPTION
	Use this section to create a new static route.
Name	Type a name to identify this static route. Use up to 31 ASCII characters. Spaces and tabs are not allowed.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the subnet mask for this destination.

Table 89 Static Routing (continued)

LABEL	DESCRIPTION
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your device that will forward the packet to the destination. The gateway must be a router on the same segment as your device.
Metric	The metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Add	Click **Add** to save the new rule to the AAM1212’s volatile memory. It then displays in the summary table at the bottom of the screen. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to reset the fields to your previous configuration.
	Use this section to look at a summary of all static routes in the AAM1212.
Previous Page	Click this to display the preceding page of static route entries.
Next Page	Click this to display the following page of static route entries.
Index	This field displays the index number of the route.
Name	This field displays the name of this static route.
Destination Address	This field displays the IP network address of the final destination.
Subnet Mask	This field displays the subnet mask for this destination.
Gateway Address	This field displays the IP address of the gateway. The gateway is an immediate neighbor of your device that will forward the packet to the destination.
Metric	This field displays the cost of transmission for routing purposes.
Delete	Select the rule(s) that you want to remove in the **Delete** column, and then click the **Delete** button.
Cancel	Click **Cancel** to clear the selected check boxes in the **Delete** column.

40 Alarm

This chapter shows you how to display the alarms, sets the severity level of an alarm(s) and where the system is to send the alarm(s) and set port alarm severity level threshold settings.

40.1 Alarm

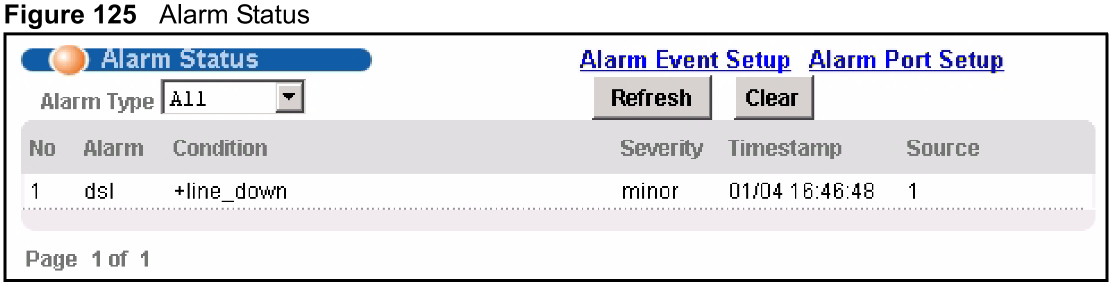
The AAM1212 monitors for equipment, DSL and system alarms and can report them via SNMP or syslog. You can specify the severity level of an alarm(s) and where the system is to send the alarm(s). You can also set the alarm severity threshold for recording alarms on an individual port(s). The system reports an alarm on a port if the alarm has a severity equal to or higher than the port's threshold.

40.2 Alarm Status Screen

This screen displays the alarms that are currently in the system.

To open this screen, click **Alarm**, **Alarm Status**.

Figure 125 Alarm Status



The following table describes the labels in this screen.

Table 90 Alarm Status

LABEL	DESCRIPTION
Alarm Event Setup	Click **Alarm Event Setup** to go to a screen where you can configure the severity level of an alarm(s) and where the system is to send the alarm(s). See Section 40.4 on page 255.
Alarm Port Setup	Click **Alarm Port Setup** to go to a screen where you can configure the alarm severity threshold for recording alarms on an individual port(s). See Section 40.5 on page 258.
Alarm Type	Select which type of alarms to display by **Severity**, or select **All** to look at all the alarms.
Refresh	Click this button to update this screen.

Table 90 Alarm Status (continued)

LABEL	DESCRIPTION
Clear	Click this button to erase the clearable alarm entries.
No	This field displays the index number of the alarm entry in the system.
Alarm	This field displays the alarm category to which the alarm belongs.
Condition	This field displays a text description for the condition under which the alarm applies.
Severity	This field displays the alarm severity level (critical, major, minor or info).
Timestamp	This field displays the month, day, hour, minute and second that the system created the log.
Source	This field displays where the alarm originated. This is either a DSL port number, one of the Ethernet ports (enet 1 or 2), or “eqpt” for the system itself.
Page X of X	This identifies which page of information is displayed and the total number of pages of information.
Previous Page	Click this to display the preceding page of entries.
Next Page	Click this to display the following page of entries.

40.3 Alarm Descriptions

This table describes alarms that the system can send.

ATUC refers to the downstream channel (for traffic going from the AAM1212 to the subscriber). ATUR refers to the upstream channel (for traffic coming from the subscriber to the AAM1212). A “V” in the **CLEARABLE** column indicates that an administrator can remove the alarm.

Table 91 Alarm Descriptions

NO	ALARM	CONDITION	FACILITY	SNMP	SYSLOG	SEVERITY	CLEARABLE
1	dsl	(5000)line_up	local1	V	V	info	-
2	dsl	(5001)line_down	local1	V	V	minor	V
3	dsl	(5002)ad_perf_lol_thresh	local1	V	V	minor	V
4	dsl	(5003)ad_perf_lof_thresh	local1	V	V	minor	V
5	dsl	(5004)ad_perf_los_thresh	local1	V	V	minor	V
6	dsl	(5005)ad_perf_lop_thresh	local1	V	V	minor	V
7	dsl	(5006)ad_perf_es_thresh	local1	V	V	minor	V
8	dsl	(5007)ad_perf_ses_thresh	local1	V	V	minor	V
9	dsl	(5008)ad_perf_uas_thresh	local1	V	V	minor	V
10	dsl	(5009)ad_atuc_loftrap	local1	V	V	minor	-
11	dsl	(5010)ad_atuc_lostrap	local1	V	V	minor	-

Table 91 Alarm Descriptions (continued)

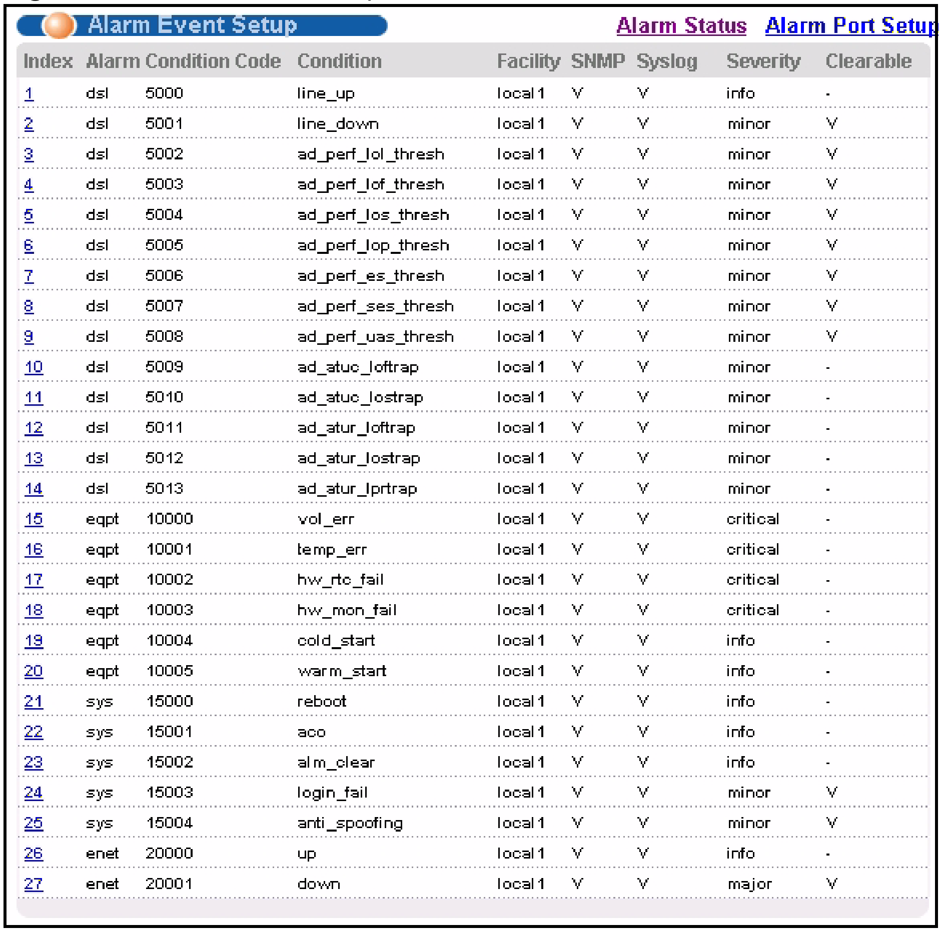
NO	ALARM	CONDITION	FACILITY	SNMP	SYSLOG	SEVERITY	CLEARABLE
12	dsl	(5011)ad_atur_loftrap	local1	V	V	minor	-
13	dsl	(5012)ad_atur_lostrap	local1	V	V	minor	-
14	dsl	(5013)ad_atur_lprtrap	local1	V	V	minor	-
15	eqpt	(10000)vol_err	local1	V	V	critical	-
16	eqpt	(10001)temp_err	local1	V	V	critical	-
17	eqpt	(10002)hw_rtc_fail	local1	V	V	critical	-
18	eqpt	(10003)hw_mon_fail	local1	V	V	critical	-
19	eqpt	(10004)cold_start	local1	V	V	info	-
20	eqpt	(10005)warm_start	local1	V	V	info	-
21	sys	(15000)reboot	local1	V	V	info	-
22	sys	(15001)aco	local1	V	V	info	-
23	sys	(15002)alm_clear	local1	V	V	info	-
24	sys	(15003)login_fail	local1	V	V	minor	V
25	sys	(15004)anti_spoofing	local1	V	V	minor	V
26	enet	(20000)up	local1	V	V	info	-
27	enet	(20001)down	local1	V	V	major	V

40.4 Alarm Event Setup Screen

This screen lists the alarms that the system can generate along with the severity levels of the alarms and where the system is to send them.

To open this screen, click **Alarm**, **Alarm Event Setup**.

Figure 126 Alarm Event Setup



Index	Alarm Condition Code		Condition	Facility	SNMP	Syslog	Severity	Clearable
1	dsl	5000	line_up	local1	V	V	info	-
2	dsl	5001	line_down	local1	V	V	minor	V
3	dsl	5002	ad_perf_lol_thresh	local1	V	V	minor	V
4	dsl	5003	ad_perf_lof_thresh	local1	V	V	minor	V
5	dsl	5004	ad_perf_los_thresh	local1	V	V	minor	V
6	dsl	5005	ad_perf_lop_thresh	local1	V	V	minor	V
7	dsl	5006	ad_perf_es_thresh	local1	V	V	minor	V
8	dsl	5007	ad_perf_ses_thresh	local1	V	V	minor	V
9	dsl	5008	ad_perf_uas_thresh	local1	V	V	minor	V
10	dsl	5009	ad_atuc_loftrap	local1	V	V	minor	-
11	dsl	5010	ad_atuc_lostrap	local1	V	V	minor	-
12	dsl	5011	ad_atur_loftrap	local1	V	V	minor	-
13	dsl	5012	ad_atur_lostrap	local1	V	V	minor	-
14	dsl	5013	ad_atur_lprtrap	local1	V	V	minor	-
15	eqpt	10000	vol_err	local1	V	V	critical	-
16	eqpt	10001	temp_err	local1	V	V	critical	-
17	eqpt	10002	hw_rtc_fail	local1	V	V	critical	-
18	eqpt	10003	hw_mon_fail	local1	V	V	critical	-
19	eqpt	10004	cold_start	local1	V	V	info	-
20	eqpt	10005	warm_start	local1	V	V	info	-
21	sys	15000	reboot	local1	V	V	info	-
22	sys	15001	aco	local1	V	V	info	-
23	sys	15002	alm_clear	local1	V	V	info	-
24	sys	15003	login_fail	local1	V	V	minor	V
25	sys	15004	anti_spoofing	local1	V	V	minor	V
26	enet	20000	up	local1	V	V	info	-
27	enet	20001	down	local1	V	V	major	V

The following table describes the labels in this screen.

Table 92 Alarm Event Setup

LABEL	DESCRIPTION
Alarm Status	Click **Alarm Status** to go to a screen that displays the alarms that are currently in the system (see Section 40.2 on page 253).
Alarm Port Setup	Click **Alarm Port Setup** to go to a screen where you can configure the alarm severity threshold for recording alarms on an individual port(s). See Section 40.5 on page 258.
Index	This field displays the index number of the alarm in the list. Click this to specify the severity level of an alarm(s) and where the system is to send the alarm(s). See Section 40.4.1 on page 257.
Alarm	This field displays the alarm category to which the alarm belongs. **eqpt** represents equipment alarms. **dsl** represents Digital Subscriber Line (DSL) alarms. **enet** represents Ethernet alarms. **sys** represents system alarms.
Condition Code	This field displays the condition code number for the specific alarm message.
Condition	This field displays a text description for the condition under which the alarm applies.
Facility	This field displays the log facility (local1~local7) on the syslog server where the system is to log this alarm. This is for alarms that send alarms to a syslog server.

Table 92 Alarm Event Setup (continued)

LABEL	DESCRIPTION
SNMP	This field displays “V” if the system is to send this alarm to an SNMP server. It displays “-“ if the system does not send this alarm to an SNMP server.
Syslog	This field displays “V” if the system is to send this alarm to a syslog server. It displays “-“ if the system does not send this alarm to a syslog server.
Severity	This field displays the alarm severity level (critical, major, minor or info).
Clearable	This displays “V” if the alarm clear command removes the alarm from the system. It displays “-“if the alarm clear command does not remove the alarm from the system.

40.4.1 Edit Alarm Event Setup Screen

Use this screen to specify the severity level of an alarm(s) and where the system is to send the alarm(s).

To open this screen, click **Alarm**, **Alarm Status**. Then, click an alarm’s index number.

Figure 127 Alarm Event Setup Edit

The following table describes the labels in this screen.

Table 93 Alarm Event Setup Edit

LABEL	DESCRIPTION
Alarm	This field displays the alarm category to which the alarm belongs. **eqpt** represents equipment alarms. **dsl** represents Digital Subscriber Line (DSL) alarms. **enet** represents Ethernet alarms. **sys** represents system alarms.
Condition Code	This field displays the condition code number for the specific alarm message.
Condition	This field displays a text description for the condition under which the alarm applies.
Facility	The log facility (local1~local7) has the device log the syslog messages to a particular file in the syslog server. Select a log facility (local1~local7) from the drop-down list box if this entry is for sending alarms to a syslog server. See your syslog program’s documentation for details.
SNMP	Select this check box to have the system send this alarm to an SNMP server.
Syslog	Select this check box to have the system send this alarm to a syslog server.
Severity	Select an alarm severity level (critical, major, minor or info) for this alarm. Critical alarms are the most severe, major alarms are the second most severe, minor alarms are the third most severe and info alarms are the least severe.
Clearable	Select this check box to allow administrators to use the management interface to remove an alarm report generated by this alarm event entry. Select this check box to keep an alarm report generated by this alarm event in the system until the conditions that caused the alarm report are no longer present.

Table 93 Alarm Event Setup Edit (continued)

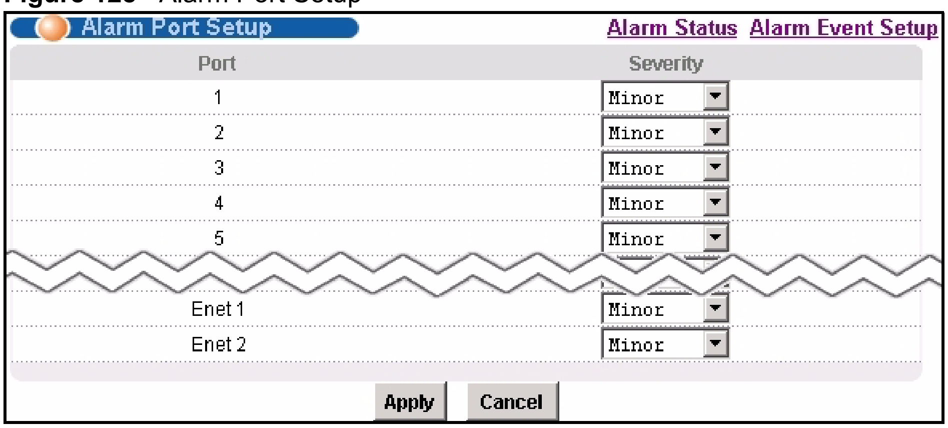
LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Close	Click **Close** to exit the screen without saving your changes.

40.5 Alarm Port Setup Screen

Use this screen to set the alarm severity threshold for recording alarms on an individual port(s). The system reports an alarm on a port if the alarm has a severity equal to or higher than the port's threshold.

To open this screen, click **Alarm**, **Alarm Port Setup**.

Figure 128 Alarm Port Setup



The following table describes the labels in this screen.

Table 94 Alarm Port Setup

LABEL	DESCRIPTION
Alarm Status	Click **Alarm Status** to go to a screen that displays the alarms that are currently in the system (see Section 40.2 on page 253).
Alarm Event Setup	Click **Alarm Event Setup** to go to a screen where you can configure the severity level of an alarm(s) and where the system is to send the alarm(s). See Section 40.4 on page 255.
Port	This column lists the device's individual DSL and Ethernet interfaces.
Severity	Select an alarm severity level (critical, major, minor or info) as the threshold for recording alarms on this port. Critical alarms are the most severe, major alarms are the second most severe, minor alarms are the third most severe and info alarms are the least severe.
Apply	Click **Apply** to save your changes to the AAM1212's volatile memory. The AAM1212 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to start configuring the screen again.

PART V
Maintenance

Maintenance (261)
Diagnostic (265)
MAC Table (269)
ARP Table (271)

41 Maintenance

This chapter explains how to use the maintenance screens.

41.1 Maintenance Screen

To open this screen, click **Management**, **Maintenance**.

Figure 129 Maintenance

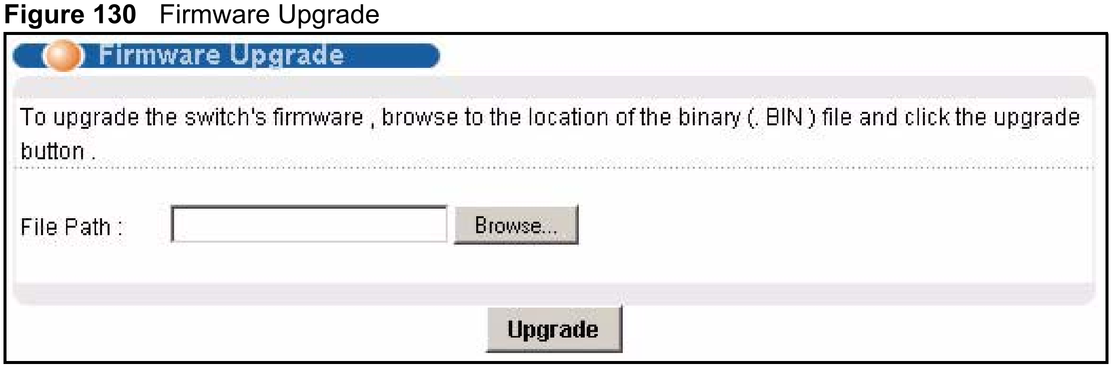
41.2 Firmware Upgrade Screen

Use this screen to upgrade your device firmware. See the **System Info** screen to verify your current firmware version number. Make sure you have downloaded (and unzipped) the correct model firmware and version to your computer before uploading to the device.

Note: Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

To open this screen, click **Management**, **Maintenance**, **Click here** (Firmware Upgrade).

Figure 130 Firmware Upgrade



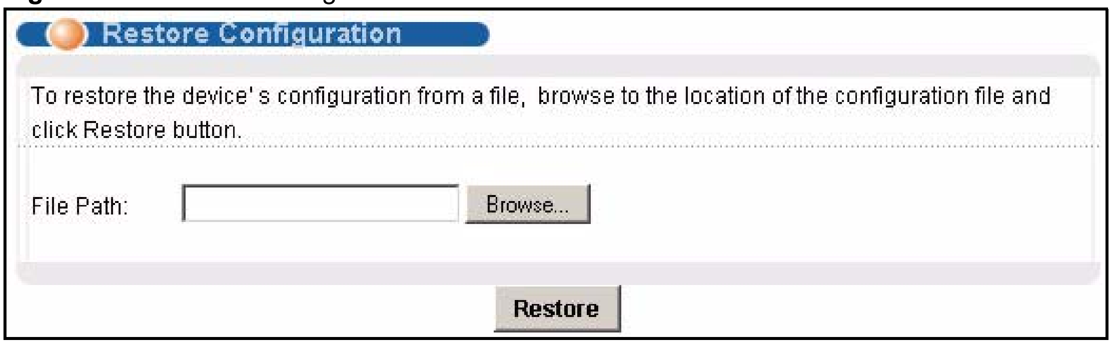
Type the path and file name of the firmware file you wish to upload to the device in the **File Path** text box or click **Browse** to locate it. After you have specified the file, click **Upgrade**.

41.3 Restore Configuration Screen

Use this screen to load a configuration file from your computer to the device.

To open this screen, click **Management**, **Maintenance**, **Click here** (Restore Text Configuration).

Figure 131 Restore Configuration



Type the path and file name of the configuration file you wish to restore in the **File Path** text box or click **Browse** to display a **Choose File** screen from which you can locate it. After you have specified the file, click **Restore**. "conf-0" is the name of the configuration file on the device, so your backup configuration file is automatically renamed when you restore using this screen.

Note: Warning! If you load an invalid configuration file, it may corrupt the settings, and you might have to use the console to reconfigure the system.

41.4 Backing Up a Configuration File

Backing up your device configurations allows you to create various “snap shots” of your device from which you may restore at a later date.

Click **Management**, **Maintenance**, and do the following to save your device’s configuration to your computer.

1 Right-click the **Click here** (Backup Text Configuration) link and click **Save Target As**.

Or:

Click the **Click here** (Backup Text Configuration) link and then click **File**, **Save As**.

2 In the **Save As** screen, choose a location to save the file on your computer from the **Save in** drop-down list box and type a descriptive name for it in the **File name** list box. Click **Save** to save the configuration file to your computer.

Note: See the CLI chapters to edit the configuration text file.

Note: You can change the ".dat" file to a ".txt" file and still upload it back to the AAM1212.

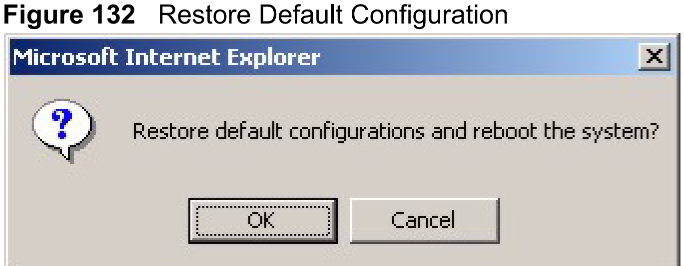
41.5 Load Factory Defaults

Use this function to clear all device configuration information you configured and return to the factory defaults.

Note: Warning! Restoring the default configuration deletes all the current settings. It is recommended to back up the configuration file before restoring the default configuration.

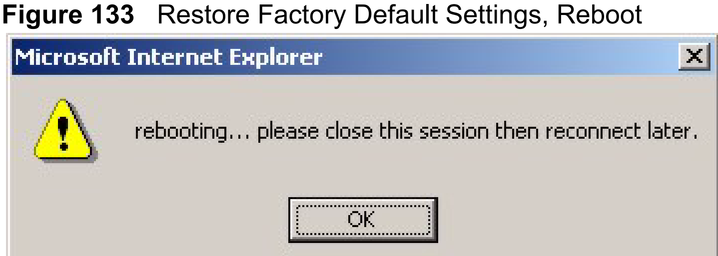
To do this, click **Management**, **Maintenance**, **Click here** (Restore Default Configuration).

Figure 132 Restore Default Configuration



Click **OK** to begin resetting all device configurations to the factory defaults and then wait for the device to restart. This takes up to two minutes. If you want to access the web configurator again, you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1).

Figure 133 Restore Factory Default Settings, Reboot



41.6 Reboot System

Use this function to restart the device without physically turning the power off.

To open this screen, click **Management**, **Maintenance**, **Click here** (Reboot System).

Figure 134 Reboot System

Click **OK**. You then see the screen as shown in Figure 133 on page 263. Click **OK** again and wait for the device to restart. This takes up to two minutes. This does not affect the device's configuration.

41.7 Command Line FTP

See Chapter 41 on page 261 for how to upload or download files to or from the device using FTP commands.

42

Diagnostic

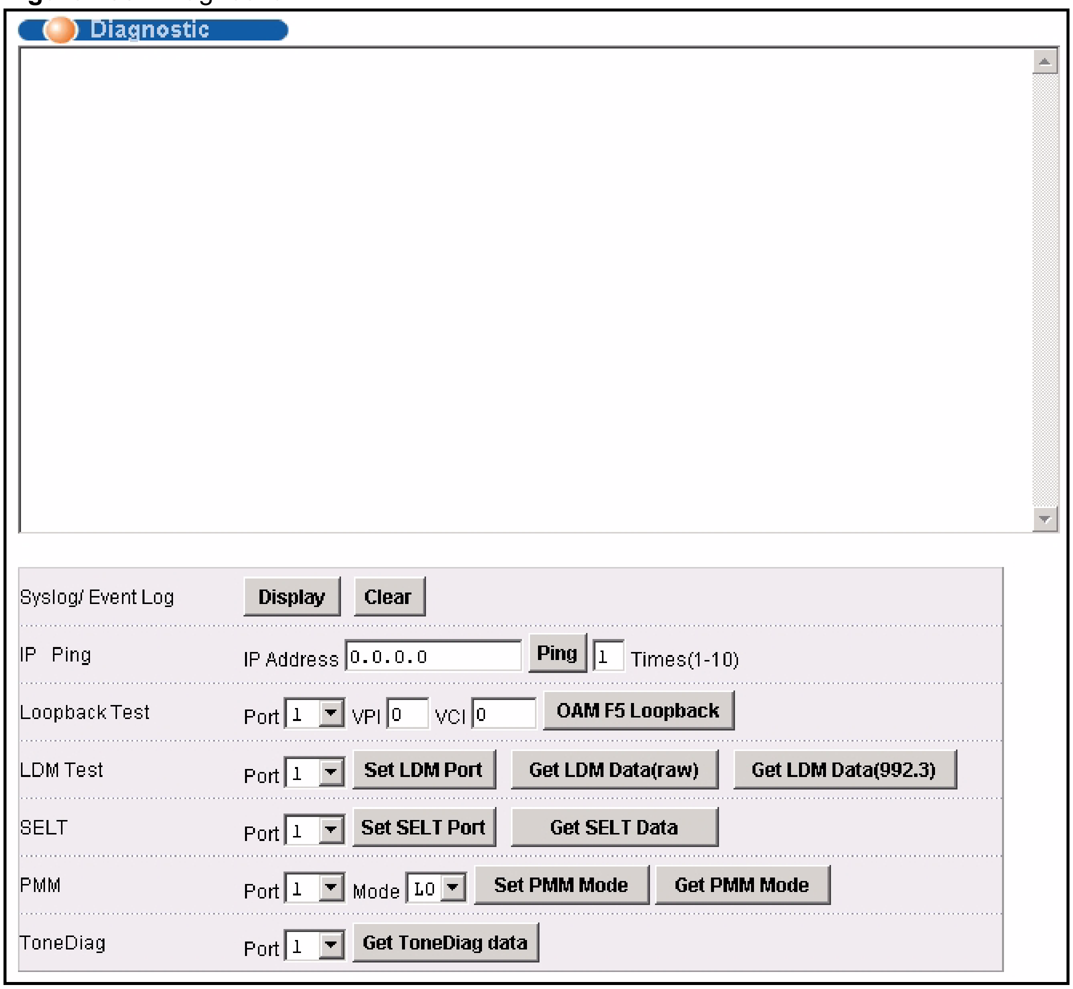
This chapter explains the Diagnostic screens.

42.1 Diagnostic Screen

Use this screen to check system logs, ping IP addresses or perform loopback tests.

To open this screen, click **Management, Diagnostic**.

Figure 135 Diagnostic



The following table describes the labels in this screen.

Table 95 Diagnostic

LABEL	DESCRIPTION
Syslog/ Event Log	Click **Display** to display a log of events in the multi-line text box. Click **Clear** to empty the text box and reset the log.
IP Ping	Type the IP address of a device that you want to ping in order to test a connection. In the field to the right specify the number of times that you want to ping the IP address. Click **Ping** to have the device ping the IP address (in the field to the left).
Loopback Test	Select a port number from the **Port** drop-down list box and enter a VPI/VCI to specify a PVC. Click **OAM F5 Loopback** to perform an OAMF5 loopback test on the specified DSL port. An Operational, Administration and Maintenance Function 5 test is used to test the connection between two DSL devices. First, the DSL devices establish a virtual circuit. Then the local device sends an ATM F5 cell to be returned by the remote DSL device (both DSL devices must support ATM F5 in order to use this test). The results ("Passed" or "Failed") display in the multi-line text box.
LDM Test	Select a port number from the **Port** drop-down list box and click **Set LDM Port** to have the AAM1212 perform line diagnostics on the specified port. The ADSL port must be set to ADSL2 or ADSL2+ ADSL operational mode and have a connection. It takes about one minute for the line diagnostics to finish. The screen displays a message confirming upon which ADSL port line diagnostics will be performed. Click **Get LDM Data** to display the line diagnostics results after using the **Set LDM Port** button on an ADSL port. Use the line diagnostics results to analyze problems with the physical ADSL line. Click **Get LDM Data(raw)** to display the unformatted line diagnostics results. Click **Get LDM Data(992.3)** to display the line diagnostics results in the format defined in the ITU-T G.992.3 standard. **Note:** Wait at least one minute after using Set LDM Port before using Get LDM Data.
SELT	Select a port number from the **Port** drop-down list box and click **Set SELT Port** to perform a Single End Loop Test (SELT) on the specified port. This test checks the distance to the subscriber's location. **Note:** The port must have an open loop. There cannot be a DSL device, phone, fax machine or other device connected to the subscriber's end of the telephone line. The SELT takes at least fifteen seconds. To check the status of the SELT or to look at the results when the SELT is complete, select a port number from the **Port** drop-down list box and click **Get SELT Data**. The results tell you what gauge of telephone wire is connected to the port and the approximate length of the line.

Table 95 Diagnostic (continued)

LABEL	DESCRIPTION
PMM	Select a port number from the **Port** drop-down list box and a power management mode from the **Mode** drop-down list box and click **Set PMM Mode** to have the specified port use the specified power management mode. Select **L0** to turn off power management on the port. Select **L2** to scale back the power usage to just support the transmission rate that the subscriber is using. Select **L2** to have the ADSL connection use power saving mode and reduce the rate when there is no traffic. The rate comes back up when there is traffic. The ADSL port must be set to ADSL2 or ADSL2+ ADSL operational mode. Click **Get PMM Mode** to display which power mode the ADSL port is currently set to use.
ToneDiag	Select a port number from the **Port** drop-down list box. The ADSL port must be set to ADSL2 or ADSL2+ ADSL operational mode and have a connection. Click **Get ToneDiag data** to display the ADSL port's tone diagnostics. The tone diagnostic information displays in the format defined in the ITU-T G.992.3 standard. Use the information to analyze problems with the physical ADSL line. **Note:** ToneDiag is faster than the LDM test but displays less information.

43

MAC Table

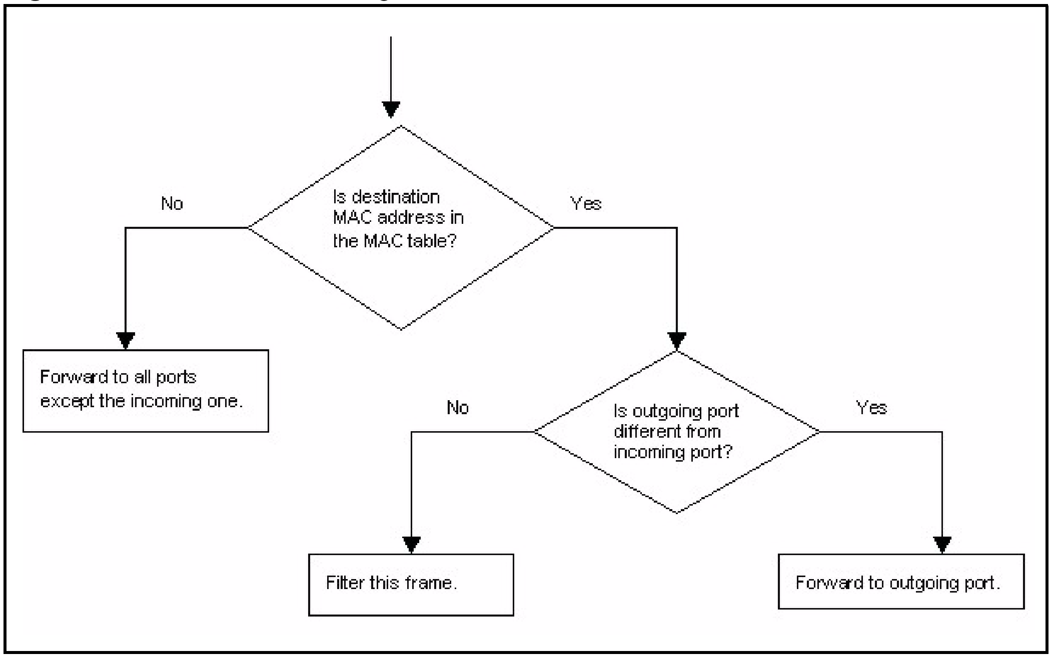
This chapter introduces the MAC Table.

43.1 Introduction to MAC Table

The MAC table lists device MAC addresses that are dynamically learned by the AAM1212. The table shows the following for each MAC address: the port upon which Ethernet frames were received from the device, to which VLAN groups the device belongs (if any) and to which channel it is connected (for devices connected to DSL ports).

The device uses the MAC table to determine how to forward frames. See the following figure.

Figure 136 MAC Table Filtering Flowchart



1 The device examines a received frame and learns the port on which this source MAC address came.

2 The device checks to see if the frame's destination MAC address matches a source MAC address already learned in the MAC table.

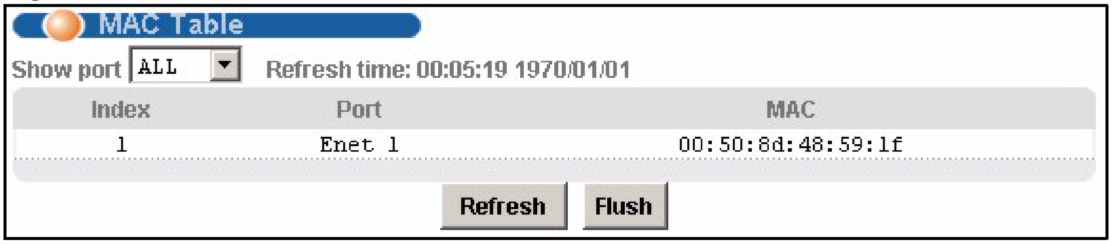
- If the device has already learned the port for this MAC address, then it forwards the frame to that port.

- If the device has not already learned the port for this MAC address, then the frame is flooded to all ports. Too much port flooding leads to network congestion.
- If the device has already learned the port for this MAC address, but the destination port is the same as the port it came in on, then it filters the frame.

43.2 MAC Table Screen

To open this screen, click **Management, MAC Table**.

Figure 137 MAC Table



The following table describes the labels in this screen.

Table 96 MAC Table

LABEL	DESCRIPTION
Show port	Select a port for which to display learned MAC addresses (or display all of them).
Page X of X	This identifies which page of information is displayed and the total number of pages of information.
Previous/Next	Click one of these buttons to show the previous/next screen if all of the information cannot be seen in one screen.
Index	This is the number of the MAC table entry.
Port	This is the port to which the MAC address is associated.
MAC	This is the MAC address of the device from which this incoming frame came.
Refresh	Click **Refresh** to update the list of dynamically learned MAC addresses.
Flush	Click **Flush** to remove all of the dynamically learned MAC address entries from the MAC table.

44

ARP Table

This chapter describes the ARP Table.

44.1 Introduction to ARP Table

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network.

An IP (version 4) address is 32 bits long. In an Ethernet LAN, MAC addresses are 48 bits long. The ARP Table maintains an association between each MAC address and its corresponding IP address.

44.1.1 How ARP Works

When an incoming packet destined for a host device on a local area network arrives at the device, the device's ARP program looks in the ARP Table and, if it finds the address, sends it to the device.

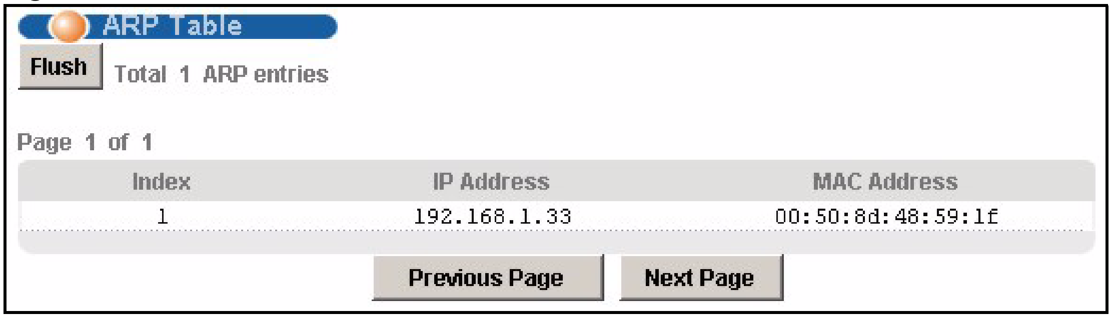
If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The device fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the device puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP Table for future reference and then sends the packet to the MAC address that replied.

44.2 ARP Table Screen

The ARP table can hold up to 500 entries.

To open this screen, click **Management, ARP Table**.

Figure 138 ARP Table



The following table describes the labels in this screen.

Table 97 ARP Table

LABEL	DESCRIPTION
Flush	Click **Flush** to remove all of the entries from the ARP table.
Total X ARP Entries	This displays the number of entries in the ARP table.
Page X of X	This identifies which page of information is displayed and the total number of pages of information.
Index	This is the ARP table entry number.
IP Address	This is the learned IP address of a device connected to a port.
MAC Address	This is the MAC address of the device with the listed IP address.
Previous Page Next Page	Click one of these buttons to show the preceding or following screen if the information cannot be displayed in one screen.

PART VI
CLI Commands

Commands (275)
Command Examples (311)
Alarm Commands (321)
DHCP Commands (329)
IEEE 802.1Q Tagged VLAN Commands (339)
MAC Commands (347)
IGMP Commands (353)
Packet Filter Commands (369)
IP Commands (373)
G.Bond Commands (379)
Firmware and Configuration File Maintenance (381)
SNMP (387)
ADSL Commands (391)
Virtual Channel Management (427)
ACL Commands (453)

45

Commands

This chapter introduces the command line interface and lists the available commands.

45.1 Command Line Interface Overview

Note: See the previous chapters for background information on features configurable by the web configurator. The web configurator is the preferred configuration tool.

You can use text command lines for software configuration. The rules of the commands are listed next.

1 The command keywords are in `courier new font`.

2 Commands can be abbreviated to the smallest unique string that differentiates the command. For example, the "`system date`" command could be abbreviated to "`sy d`".

3 The optional fields in a command are enclosed in square brackets []. For instance, `config [save]` means that the `save` field is optional.

4 "Command" refers to a command used in the command line interface (CI command).

5 The | symbol means "or".

Note: Using commands not documented in the User's Guide can damage the unit and possibly render it unusable.

45.2 Command Privilege Levels

There is a high, middle or low privilege level for each command.

High privilege commands are only available to administrators with high privilege access. High privilege commands include things like creating administrator accounts, restarting the system and resetting the factory defaults. Administrators with high privilege access can use all commands including the lower privilege commands.

Administrators with middle privilege access can use middle or low privilege commands.

Administrators with the low privilege level are restricted to using only low privilege commands. Low privilege commands are read only.

45.3 Saving Your Configuration

Use the following command to save your configuration when you are done with a configuration session.

```
ras> config save
```

Note: Do not turn off your AAM1212 while saving your configuration.

This command saves all system configurations to nonvolatile memory. You must use this command to save any configuration changes that you make, otherwise the AAM1212 returns to its default settings when it is restarted. Save your changes after each configuration session.

Nonvolatile memory refers to the AAM1212's storage that remains even if the AAM1212's power is turned off. Run-time (memory) is lost when the AAM1212's power is turned off.

45.4 ADSL Command Input Values

The following table describes the values required in ADSL commands. Other values are discussed with the corresponding commands.

Table 98 ADSL Command Input Values

LABEL	DESCRIPTION
`ip`	An IP address in dotted decimal notation. For example, 192.168.1.3.
`netmask`	The subnet mask in dotted decimal notation, for example, 255.255.255.0.
`portlist`	You can specify a single ADSL port `<1>`, all ADSL ports `<*>` or a list of ADSL ports `<1,3,5>`. You can also include a range of ports `<1,5,6~10>`.
`profile`	A descriptive name for the profile that will define the settings of this port.
`vlanlist`	You can specify a single VLAN <1>, all VLANs <*> or a list of VLANs <1,3,5>. You can also include a range of VLANs <1,5,6~10>.
`vpi`, `vci`	The Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) identify a channel on this port. Possible values for the VPI are 0~255. Possible values for the VCI are 32~65535 if the VPI is 0. If the VPI is not 0, possible values for the VCI are 1~65535.

45.5 Commands

The following table lists commands that you can use with the AAM1212.

The **P** column on the right indicates the administrator privilege level needed to use the command (**H** for high, **M** for middle or **L** for low) and the equivalent in the web configurator (**H** for high or **L** for low).

Table 99 Commands

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
adsl				
	alarmprofile delete	<profile>	This command allows you to delete an individual ADSL alarm profile by its name. You cannot delete the DEFVAL alarm profile.	H/H
	alarmprofile map	<portlist> <profile>	Sets the AAM1212 to use an (already-configured) alarm profile with the specified ADSL ports.	H/H
	alarmprofile set	<profile> [<atuc lofs> <atur lofs> <atuc loss> <atur loss> <atuc olls> <atuc lprs> <atur lprs> <atuc ess> <atur ess> <atuc fast rateup> <atur fast rateup> <atuc interleave rateup> <atur interleave rateup> <atuc fast ratedown> <atur fast ratedown> <atuc interleave ratedown> <atur interleave ratedown> <init fail enable> <atuc fail fast> <atuc ses> <atur ses> <atuc uas> <atur uas>]	This command configures settings and thresholds that define when the AAM1212 is to send an alarm trap and generate a syslog entry. Configure alarm profiles first and then use the alarmprofile map command to set the AAM1212 to use them with specific ADSL ports. See Section 57.3.2 on page 422 for details on the parameters of this command.	H/H
	alarmprofile show	[profile]	Displays the settings of the specified alarm profile (or all of them if you do not specify one).	L/L
	alarmprofile showmap	[port number]	Displays alarm profile to ADSL port mapping.	L/L
	alarmprofile showport	<port number>	Displays which alarm profile parameters are mapped to an ADSL port.	L/~
	annexl disable	<portlist>	(AAM1212-51) Turns off the Annex L feature on the specified port(s).	H/H
	annexl enable	<portlist>	(AAM1212-51) Turns on the Annex L feature on the specified port(s).	H/H
	annexl show	<portlist>	(AAM1212-51) Displays the Annex L feature setting for the specified port(s).	M/L
	annexm disable	<portlist>	(AAM1212-51) Turns off the Annex M feature on the specified port(s).	H/H

Table 99 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	annexm enable	<portlist>	(AAM1212-51) Turns on the Annex M feature on the specified port(s).	H/H
	annexm show	<portlist>	(AAM1212-51) Displays the Annex M feature setting for the specified port(s).	M/L
	disable	<portlist>	Turns off the specified ADSL ports.	M/H
	dsbcast disable	<port number> <vlanlist>	Disables downstream broadcast on the specified xDSL port.	H/H
	dsbcast enable	<port number> <vlanlist>	Enables downstream broadcast on the specified xDSL port	H/H
	dsbcast show	<portlist>	Show downstream broadcast on the specified xDSL port.	M/L
	dscarrier0	<port number> [<m1> <m2> <m3> <m4> <m5> <m6> <m7>]	Displays or sets masks for downstream carrier tones from 33 to 255. Masking a carrier tone disables the use of that tone on the specified ADSL port. The most significant bit defines the lowest tone number in a mask. m1:tones 32~63 m2:tones 64~95 m3:tones 96~127 m4:tones 128~159 m5:tones 160~191 m6:tones 192~223 m7:tones 224~255	H/H
	dscarrier1	<port number> [<m0> <m1> <m2> <m3> <m4> <m5> <m6> <m7>]	Displays or sets masks for downstream carrier tones from 256 to 511 on the specified ADSL2+ port(s). Use this command to have the system not use an ADSL line's tones that are known to have a high noise level. m0: tones 256~287 m1:tones 288~319 m2:tones 320~351 m3:tones 352~383 m4:tones 384~415 m5:tones 416~447 m6:tones 448~479 m7:tones 480~511	H/H
	dsnompsd	<port number> [<max_nominal_psd>]	Displays or sets the maximum downstream nominal PSD (Power Spectral Density) values. This is for testing purposes. [<max_nominal_psd>]: Downstream PSD (-400 ~ 40 in 0.1dBm/Hz).	H/H

Table 99 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	enable	<portlist>	Turns on the specified ADSL ports.	M/H
	gbond delete	<bond_name>	Removes G.bond settings from the DSL lines specified in the G.bond group. <bond_name>: The name of a DSL line group with G.bond configured on them.	H/H
	gbond set	<bond_name> <portlist>	Configures a G.bond group or modifies the membership of a G.bond group. <portlist>: A list of pairs of consecutive ports, for example, (1, 2), (3, 4) and so on up to (47, 48).	H/H
	gbond show		Shows G.bond settings for all ports.	L/L
	inp	<portlist> [<usINP> [,<dsINP>]]	Sets the upstream (us) and downstream (ds) impulse noise protection minimum setting on the specified ADSL port(s). Sudden spikes in the line's noise level (impulse noise) can cause errors and result in lost packets. Set the impulse noise protection minimum to have a buffer to protect the ADSL physical layer connection against impulse noise. This buffering causes a delay that reduces transfer speeds. It is recommended that you use a non-zero setting for real time traffic that has no error correction (like videoconferencing). <usINP>: Sets the minimum upstream (us) impulse noise protection setting. Use 0~3 to define a number of DMT symbols. 0 = 0 DMT symbols, 1 = 0.5 DMT symbols, 2 = 1 DMT symbols, 3 = 2 DMT symbols. <dsINP>: Sets the minimum downstream (ds) impulse noise protection setting. Use 0~3 to define a number of DMT symbols. 0 = 0 DMT symbols, 1 = 0.5 DMT symbols, 2 = 1 DMT symbols, 3 = 2 DMT symbols.	H/H

Table 99 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	`linediag getld`	`<port number>`	Displays the line diagnostics results after using the line diagnostics set command on an ADSL port. Use the line diagnostics results to analyze problems with the physical ADSL line. Note: Wait at least one minute after using the line diagnostic set command before using this command.	L/L
	`linediag getld992_3`	`<port number>`	Displays the line diagnostics results in the format defined in the ITU-T G.992.3 standard after using the line diagnostics set command on an ADSL port. Use the line diagnostics results to analyze problems with the physical ADSL line. Note: Wait at least one minute after using the line diagnostic set command before using this command.	L/L
	`linediag getselt`	`<port number>`	Displays the status and the results of the SELT test on the specified port. The report tells you what gauge of telephone wire is connected to the port and the approximate length of the line measured both in meters and thousands of feet.	L/L
	`linediag setld`	`<port number>`	Performs line diagnostics on the specified port. The ADSL port must be set to ADSL2 or ADSL2+ ADSL operational mode and have a connection. It takes about one minute for the line diagnostics to finish.	H/H

Table 99 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	`linediag setselt`	`<port number>`	Performs a single end line test on the specified port. This test checks the distance to the subscriber's location. Note: The port must have an open loop. There cannot be a DSL device, phone, fax machine or other device connected to the subscriber's end of the telephone line.	H/H
	`linediag toneDiag`	`<port number>`	Displays the tone diagnostics for a port in the format defined in the ITU-T G.992.3 standard. You do not need to use the line diagnostics set command first. Use the tone diagnostics to analyze problems with the physical ADSL line.	L/L
	`loopback`	`<portlist> <f5> <vpi> <vci>`	Performs an OAMF5 loopback test on the specified ADSL port(s). `<f5>`: Use f5 to perform an OAMF5 loopback test on the specified DSL port. An Operational, Administration and Maintenance Function 5 test is used to test the connection between two DSL devices. First, the DSL devices establish a virtual circuit. Then the local device sends an ATM F5 cell to be returned by the remote DSL device (both DSL devices must support ATM F5 in order to use this test).	H/H
	`name`	`<portlist> <name>`	Sets the name of an ADSL port(s). `<name>`: A descriptive name for the port. You can use up to 31 printable ASCII characters (including spaces and hyphens).	M/L
	`paepvc counter`	`<portlist> [<vpi> <vci>]`	This command displays statistics about PAE PVC activity.	L/L
	`paepvc delete`	`<portlist> <vpi> <vci>`	Deletes PPPoAoE settings for a PVC (Permanent Virtual Circuit)	M/H
	`paepvc session`	`<portlist> [<vpi> <vci>]`	This command displays the status of PAE PVC sessions on the specified port(s) or PVCs.	L/L

Table 99 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	paepvc set	<portlist> <vpi> <vci> <DS vcprofile[,US vcprofile]> <pvid> <priority> [acname <string32>] [srvcname <string32>] [hellotime <time>]	Creates a PAE PVC to allow communication between the ATM (CPE) and Ethernet network (BRAS) segments. The PVC is mapped to a PPPoE session that connects to the specified BRAS (Broadband Remote Access Server). acname*:* Specifies the hostname of a remote access concentrator if there are two access concentrators (or BRAS) on the network or that you want to allow PAE translation to the specified access concentrator. srvcname*:* Specifies the name of the service that uses this PVC. This must be a service name that you configure on the remote access concentrator. hellotime: Specifies the timeout, (0~600 seconds) for the PPPoE session. Enter 0 if there is no timeout.	M/H
	paepvc show	<portlist> [detail]	Displays detailed PPPoAoE PVC settings on the specified port.	L/L
	pmm disable	<portlist>	Turns off power management on the specified port(s).	H/H
	pmm enable	<portlist> <L2|L3>	Turns on power management on the specified port(s). Enables Power ManageMent (PMM) to reduce the amount of power used overall and reduce the instances of the connection going down. PMM increases or decreases the transmission power based on line conditions. PMM also reduces the number of service interruptions. L2: Low Power. Sets the power management feature to scale back line usage to the minimum level sufficient to maintain an active connection when there is low level of traffic. L3: Idle. Sets the power management feature to reduce the power consumption when there is no traffic. Ports may be disabled or go into monitor mode in this state.The power level comes back up when there is traffic.	H/H

Table 99 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	pmm param	<portlist> [<l0time> <l2time> <l2atpr> <l2atprt>][<max_l2 rate> <min_l2rate> <l0tol2_rate>]	Displays or sets PMM parameters for the specified ADSL port(s). See Section 57.1.16 on page 402 for more information on the parameters of this command.	H/H
	pmm set	<portlist> <L0|L2>	Sets the power management mode. L0: Turns off power management on a port. L2: Low Power. Sets the power management feature to scale back line usage to the minimum level sufficient to maintain an active connection when there is low level of traffic.	H/H
	pmm show	<portlist>	Displays the PMM settings for the specified port(s).	M/L
	ppvc delete	<portlist> <vpi> <vci>	Removes a Priority PVC from a port.	H/H
	ppvc member delete	<portlist> <vpi> <vci> <member vpi> <member vci>	Removes a PPVC. Removing a PPVC also deletes all of the member PVCs.	H/H
	ppvc member set	<portlist> <vpi> <vci> <member vpi> <member vci> <DS vcprofile[,US vcprofile]> <level>	Adds a member PVC to a PPVC. You must create the PPVC before you use this command to add a member. Note: Only the member PVCs need to be created on the subscriber's device.	H/H
	ppvc member show	[portlist] [<vpi> <vci>]	Displays PPVC member settings.	M/L
	ppvc set	<portlist> <vpi> <vci> <encap> <pvid> <priority>	Creates a Priority PVC (PPVC). This allows you to give different priorities to PVCs that are members of the same VLAN.	H/H
	ppvc show	[portlist] [<vpi> <vci>]	Displays priority PVC settings.	M/L
	profile delete	<profile>	Removes an ADSL profile.	H/H
	profile map	<portlist> <profile> <glite|gdmt|t1413|auto|adsl2|adsl2+>	AAM1212-51: Assigns a specific profile to a port(s) and sets the port's ADSL mode.	H/H
	profile map	<portlist> <profile> <gdmt|etsi|auto|adsl2|adsl2+>	AAM1212-53: Assigns a specific profile to a port(s) and sets the port's ADSL mode.	H/H

Table 99 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	profile set	<profile> <fast|interleave [=<up delay>,<down delay>]> <up max rate> <down max rate> [<up target margin> <up min margin> <up max margin> <up min rate> <down target margin> <down min margin> <down max margin> <down min rate> <up down-shift margin> <up up-shift margin> <down down-shift margin> <down up-shift margin>]	The profile is a table that contains information on ADSL line configuration. Each entry in this table reflects a parameter defined by a manager, which can be used to configure the ADSL line. Note that the default value will be used for any of the above fields that are omitted. The upstream rate must be less than or equal to the downstream rate. Even though you can specify arbitrary numbers in the profile set command, the actual rate is always a multiple of 32 Kbps. If you enter a rate that is not a multiple of 32 Kbps, the actual rate will be the next lower multiple of 32 Kbps. For instance, if you specify 60 Kbps for a port, the actual rate for that port will not exceed 32 Kbps, and if you specify 66 Kbps, the actual rate will not be over 64 Kbps. The ADSL up/down shift noise margins define the threshold that triggers rate adaptation. For example: The target SNR is 6, and the up/down shift noise margins are 9/3. If the signal becomes better and the SNR is higher than 9, rate adaptation is triggered and the line rate becomes higher. If the signal becomes bad and the SNR is lower than 3, rate adaptation is triggered and the line rate becomes lower.	H/H
	profile show	[profile]	Displays the specified ADSL profile or all ADSL profiles if you do not specify one.	L/L
	pvc delete	<portlist> <vpi> <vci>	Removes a PVC from a port.	H/H

Table 99 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	pvc set	<portlist> <vpi> <vci> <super |vid = 1..4094 <priority>> <DS vcprofile[,US vcprofile]>	Allows the configuration of a PVC (permanent virtual circuit) for one or a range of ADSL ports. super: Enable the super channel option to allow a channel to forward frames belonging to multiple VLAN groups (that are not assigned to other channels). The AAM1212 forwards frames belonging to VLAN groups that are not assigned to specific channels to the super channel. The super channel functions in the same way as the channel in a single channel environment. One port can have only one super channel.	H/H
	pvc show	[portlist] [<vpi> <vci>]	Displays the Permanent Virtual Circuit (PVC) parameters of the specified ADSL port(s) or all of the ADSL ports if you do not specify any.	M/L
	queuemap set	<priority> <queue>	IEEE 802.1p defines up to 8 separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Frames without an explicit priority tag are given the default priority of the ingress port. Use this command to configure the priority level-to-physical queue mapping. <queue>: The device has 4 physical queues that you can map to the 8 priority levels for outgoing Ethernet traffic. The device has 8 physical queues that you can map to the 8 priority levels for outgoing DSL traffic. Traffic assigned to higher index queues gets through the device faster while traffic in lower index queues is dropped if the network is congested.	H/H
	queuemap show		Displays the ADSL priority level to 802.1p bit queue mapping.	M/L
	reset	<portlist>	Resets an xDSL port.	H/H
	rpvc arp agingtime set	<sec, 10..10000|0:disabled>	Configures how long the device stores the IP addresses of CPE devices using 2684 routed mode in the Address Resolution Protocol table. sec: The number of seconds (10~10000) the device is to keep the Address Resolution Protocol table's entries of IP addresses of 2684 routed mode gateways. Use 0 to disable the aging time.	M/L

Table 99 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	rpvc arp agingtime show		Displays RPVC ARP proxy aging time.	H/H
	rpvc arp flush		Flushes RPVC ARP proxy table.	H/H
	rpvc arp show		Shows the RPVC ARP proxy table.	M/L
	rpvc delete	<portlist> <vpi> <vci>	Deletes RPVC on a port.	H/H
	rpvc gateway delete	<gateway ip>	Removes the gateway IP address that the device was set to use for 2684 routed mode traffic.	H/H
	rpvc gateway set	<gateway ip> <vlan id> [<priority>]	Adds a gateway IP address to use for 2684 routed mode traffic.	H/H
	rpvc gateway show		Displays the gateway IP addresses that are configured for use with 2684 routed mode traffic.	M/L
	rpvc route delete	<port number> <vpi> <vci> <ip>/<netmask>	Deletes RPVC routing subnet on a port.	H/H
	rpvc route set	<port number> <vpi> <vci> <ip>/<netmask>	Sets RPVC routing subnet on a port.	H/H
	rpvc route show	<portlist>	Displays RPVC routing subnet on a port.	M/L
	rpvc set	<portlist> <vpi> <vci> <DS vcprofile[,US vcprofile]> <ip>/<netmask> <gateway ip>	This command adds a PVC to handle 2684 routed mode traffic. Make sure that the routed PVC's subnet does not include the AAM1212's IP address. Note: You must use the rpvc gateway set command to configure the gateway's settings before you use the rpvc set command.	H/H
	rpvc show	<portlist>	Displays RPVC on a port.	M/L
	show	[portlist]	Shows the activation status, ADSL mode, maximum upstream and downstream rate settings, profile and name of each ADSL port.	L/L
	sra disable	<portlist>	Turns off SRA ADSL2+ on the specified port(s).	H/H
	sra enable	<portlist>	Turns on Seamless Rate Adaptation (SRA) ADSL2+ on the specified port(s).	H/H
	sra show	<portlist>	Displays the SRA ADSL2+ setting for the specified port(s).	M/L

Table 99 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	`tel`	`<portlist> <tel>`	Records an ADSL port(s) subscriber's telephone number. `<tel>`: An ADSL subscriber's telephone number. You can use up to 15 ASCII characters (including spaces and hyphens).	M/L
	`tlspvc delete`	`<portlist> <vpi> <vci>`	Clears Transparent LAN Services (TLS) settings for the PVC.	M/H
	`tlspvc set`	`<portlist> <vpi> <vci> <DS vcprofile[,US vcprofile]> <pvid> <priority>`	Uses TLS to add an outer VLAN tag to the inner IEEE 802.1Q tagged frames that enter the network. By tagging the tagged frames ("double-tagged" frames) the service provider can manage up to 4094 VLANs groups with each group containing up to 4094 customer VLANs. This allows a service provider to provide different services, based on specific VLANs, for many different customers. Sets untagged traffic with a tag including the specified VLAN ID and priority. If traffic is already tagged, this command adds a tag with the specified VLAN ID and the original priority setting for the traffic, not the priority setting specified in the command.	M/H
	`tlspvc show`	`portlist [detail]`	Displays detailed TLS PVC settings	L/L

Table 99 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	uscarrier	<port number> [<m0> <m1>]	Displays or sets masks for upstream carrier tones from 0 to 63. Masking a carrier tone disables the use of that tone on the specified ADSL port. Use this command to have the system not use an ADSL line's tones that are known to have a high noise level. The most significant bit defines the lowest tone number in a mask. The hexadecimal digit is converted to binary and a '1' masks (disables) the corresponding tone. Disabling a carrier tone turns it off so the system does not send data on it. The most significant bit defines the first tone sequentially. For example, in <m0>, 0x00000001 means tone 31. For example, you could use 0xffff0000 for <m0> to disable upstream carrier tones 0~15 and leave tones 16 ~ 31 enabled. m0: tones 0~31 m1: tones 32~63	H/H
	uslimit disable	<portlist> <vpi> <vci>	Turns off the limit on the transmission rate for upstream traffic for the specified PVC.	H/H
	uslimit enable	<portlist> <vpi> <vci>	Turns on the limit on the transmission rate for upstream traffic for the specified PVC.	H/H
	uslimit set	<portlist> <vpi> <vci> <rate>	Sets the limit on the transmission rate for upstream traffic for the specified PVC. (A PVC could be PVC, PPVC, IPBPVC or TLSPVC). Enable the upstream limit before using this command. <rate>: The limit on the transmission rate (1~65535 kbps) for upstream traffic.	H/H
	uslimit show		Displays the limit(s) on the transmission rate for upstream traffic for the specified port(s) or PVC(s).	L/L
	usnompsd	<port number> [<max nominal psd>]	Displays or sets the upstream maximum nominal transmit PSD (Power Spectral Density). [<max nominal psd>]: -400 ~ 40 (unit of measure is 0.1dBm/Hz)	H/H
	vcprofile delete	<vcprofile>	Removes a virtual channel profile.	H/H

Table 99 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	vcprofile set	<vcprofile> <vc|llc> <ubr|cbr> <pcr> <cdvt>	Creates a virtual channel profile. vc|llc: The type of encapsulation. VC Mux is a type of encapsulation where, by prior agreement, each protocol is assigned to a specific virtual circuit, for example, VC1 carries IP and VC2 carries IPX. LLC is a type of encapsulation where one VC carries multiple protocols with each packet header containing protocol identifying information. ubr|cbr: Specify either a unspecified bit rate (UBR) or constant bit rate (CBR). <pcr>: The Peak Cell Rate (150~300 000) is the maximum rate (measured in cells per second) at which the sender can send cells. <cdvt>: Cell Delay Variation Tolerance (CDVT) is the accepted tolerance of the difference between a cell's transfer delay and the expected transfer delay (measured in number of cells). Possible values are 0~255 or * (means 0).	H/H

Table 99 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	vcprofile set	<vcprofile> <vc|llc> <vbr(rt-vbr)|nrt-vbr> <pcr> <cdvt> <scr> <bt>	Creates a virtual channel profile. After you create a virtual channel profile, you can assign it to any of the ADSL ports on any of the ADSL AAM1212 in the AAM1212. vbr(rt-vbr)|nrt-vbr: The Real-Time Variable Bit Rate (RT-VBR) or Non Real-Time (NRT-VBR) Variable Bit Rate ATM traffic class. <pcr>: Peak Cell Rate (PCR) is the maximum rate (150 to 300000 cells per second) at which the sender can send cells. <cdvt>: Cell Delay Variation Tolerance (CDVT) is the accepted tolerance of the difference between a cell's transfer delay and the expected transfer delay measured in number of cells. Enter from 0 to 255 or * (means 0). <scr>: The Sustained Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted (measured in cells per second). SCR applies to the VBR traffic class. <bt>: Burst Tolerance (BT) is the maximum number of cells that the port is guaranteed to handle without any discards (number of cells). BT applies to the VBR traffic class.	H/H
	vcprofile show	[vcprofile]	Displays the settings of the specified virtual channel profile (or all of them if you do not specify one).	L/L
alarm				
	clear		Erases historic alarm entries.	M/L
	cutoff		This command cancels an alarm. This stops the sending of the alarm signal current. This is useful in stopping an alarm if you have the alarm output connector pins connected to a visible or audible alarm. The alarm entry remains in the system.	M/~
	history clear	<alarm>|all <condition>|all	Removes historic alarm entries by alarm category and alarm condition or by severity.	M/~
	history clear	<severity>		M/~

Table 99 Commands (continued)

<table>
<tr><th>CLASS</th><th>COMMAND</th><th>PARAMETERS</th><th>DESCRIPTION</th><th>P</th></tr>
<tr><td></td><td>history show</td><td>[<severity>|all]
[<alarm>|all]
[<condition>|all]
[<sdate>|all]
[<edate>|all]
[for|rev] [detail]</td><td>This command displays historic alarms by severity, alarm category, alarm condition and/or dates.
<severity>: Specify an alarm severity level (critical, major, minor, info or all). Critical alarms are the most severe, major alarms are the second most severe, minor alarms are the third most severe and info alarms are the least severe.
<alarm>: Specify a category of alarms.
eqpt represents equipment alarms.
dsl represents Digital Subscriber Line (DSL) alarms.
enet represents Ethernet alarms.
sys represents system alarms.
all specifies every alarm category.
condition: This is the text description for the condition under which the alarm applies. Use the alarm tablelist to find alarm conditions.
sdate: The start date, in yyyy/mm/dd format.
edate: The end date, in yyyy/mm/dd format.
for|rev: The displaying order. Use for to display in chronological order starting from the oldest alarm. Use rev to display in reverse chronological order starting from the most recent alarm.
detail: Display in-depth alarm information.</td><td>L/~</td></tr>
<tr><td></td><td>port set</td><td><all|enet1|enet2|port> <severity></td><td>This command sets the alarm severity threshold for recording alarms on an individual port(s). The system reports an alarm on a port if the alarm has a severity equal to or higher than the port's threshold.
all|enet1|enet2|port: Ports on the AAM1212.</td><td>M/L</td></tr>
<tr><td></td><td>port show</td><td>[<severity>|all]</td><td>This command displays port alarm severity level thresholds. The system reports an alarm on a port if the alarm has a severity equal to or higher than the port's threshold.</td><td>L/L</td></tr>
</table>

Table 99 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	show	[<severity>|all] [<alarm>|all] [<condition>|all] [<sdate>|all] [<edate>|all] [for|rev] [detail]	Displays current alarm settings.	L/L
	tablelist	[<alarm>|all] [<severity>|all] [<fac>|all] [<target>[,<target>]] [<condition>|all]	This command lists alarm settings. <fac>: The log facility (local1~local7) that has the device log the syslog messages to different files in the syslog server. See your syslog program's documentation for details. <target>: snmp|syslog|all The type of alarm messages that the device is to send (SNMP, syslog or all).	L/L

Table 99 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	xedit	<alarm>|all <cond>|<condcode> <severity> <fac> <target>[,<target>] [clearable]	Sets the severity level of an alarm(s) and where the system is to send the alarm(s). Use the alarm tablelist command to display alarm setting details. <cond>: all|condition This is the text description for the condition under which the alarm applies. Use the alarm tablelist to find alarm conditions. <condcode>: The condition code is the number of a specific alarm message. Use the alarm tablelist to find alarm condition codes. <severity>: Specify an alarm severity level (critical, major, minor or info) for this alarm. Critical alarms are the most severe, major alarms are the second most severe, minor alarms are the third most severe and info alarms are the least severe. <fac>: The log facility (local1~local7) has the device log the syslog messages to a particular file in the syslog server. Set this if this entry is for sending alarms to a syslog server. See your syslog program's documentation for details. <target>: snmp|syslog|all The type of alarm messages that the device is to send (SNMP, syslog or all). You can specify more than one, separated by commas. clearable|unclearable This sets whether or not the alarm clear command removes the alarm from the system.	M/L
config				
	restore		Reloads the factory default configuration.	H/H
	save		Saves the current configuration.	H/H
	show	<sys|sw|adsl|ip|stat|all> [nopause]	Displays the device's configuration.	M/L
exit			Ends the console or telnet session.	L/L
ip				
	arp flush		Clears the device's IP Address Resolution Protocol (ARP) table.	H/H

Table 99 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	arp show		Displays the AAM1212's IP Address Resolution Protocol (ARP) table. This is the list of IP addresses and matching MAC addresses that the AAM1212 has resolved.	M/L
	gateway	<gateway ip>	Changes the default gateway (next hop). This tells the AAM1212 where to send packets that have a destination IP address that is not on the same subnet as the AAM1212's IP address.	H/H
	ping	<ip> [count]	Checks for network functionality by sending an echo request to another IP host and waiting for the reply.	M/L
	route delete	<dst ip>[/netmask]	Removes a routing table entry.	H/H
	route flush		Clears the routing table.	H/~
	route set	<dst ip>[/netmask] <gateway ip> [metric] <name>	Defines a new, static IP forwarding route or edits an existing one.	H/H
	route set default	<gateway ip> <metric>	Sets the device's default route.	H/H
	route show		Displays the routing table.	M/L
	set	<ip>[/netmask]	Sets the management IP address and subnet mask.	H/H
	show	[inband|outband]	Displays the management IP address settings.	M/L
statistics				
	adsl 15mperf	<portlist> [count <0..96>]	Displays line performance statistics for the current and previous 15-minute periods. count <0~96>: Specify for which 15-minute interval (0~96) you want to display performance statistics. 0 is the current 15 minutes.	M/L
	adsl 1dayperf	<portlist>	Displays line performance statistics for the current and previous 24 hours.	M/L
	adsl gbond		Displays gbond settings and upstream and downstream transmission speeds on a gbond bundle.	M/L

Table 99 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	adsl linedata	<portlist>	Shows the line bit allocation of an ADSL port. Discrete Multi-Tone (DMT) modulation divides up a line's bandwidth into tones. This command displays the number of bits transmitted for each tone. This can be used to determine the quality of the connection, whether a given sub-carrier loop has sufficient margins to support ADSL transmission rates, and possibly to determine whether certain specific types of interference or line attenuation exist. See the ITU-T G.992.1 recommendation for more information on DMT. The better (or shorter) the line, the higher the number of bits transmitted for a DMT tone. The maximum number of bits that can be transmitted per DMT tone is 15. "upstream carrier load" displays the number of bits transmitted per DMT tone for the upstream channel (from the subscriber's DSL modem or router to the AAM1212). "downstream carrier load" displays the number of bits received per DMT tone for the downstream channel (from the AAM1212 to the subscriber's DSL modem or router). The bit allocation contents are only valid when the link is up.	M/L
	adsl lineinfo	<portlist>	Displays the information on line(s) connected to specified ADSL ports.	M/L
	adsl lineperf	<portlist>	Displays the performance statistics of the specified ADSL port.	M/L
	adsl linerate	<portlist>	Displays the line rate.	M/L
	adsl show	[portlist]	Displays ADSL port connection status.	M/L
	dhcp counter	[<portlist> [clear]]	Displays DHCP statistics for a port.	L/L
	dhcp snoop	<portlist>	Displays DHCP snooping related statistics	L/L
	dot1x	[portlist]	Displays detailed IEEE 802.1x authentication- related statistics.	M/L
	enet		Displays Ethernet port settings and statistics.	M/L

Table 99 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	igmpsnoop group	[<vid> [<mcast_ip>]]	Displays the information about IGMP groups learned on the system, specified VLAN, or specified multicast address on the specified VLAN(s). <vid>: The VLAN ID [1 – 4094]. [<mcast_ip>]: The multicast IP address.	L/L
	igmpsnoop info	[clear]	Displays protocol packets counters & number of learned groups.	L/L
	igmpsnoop port group	<portlist>	Displays joined groups in this port.	M/L
	igmpsnoop port info	[<portlist> [clear]]	Displays received protocol packets counters, number of joined groups.	L/L
	ip		Displays the management port's status and performance data.	M/~
	mac		Displays the current MAC address forwarding table.	M/L
	monitor		Displays the hardware monitor status.	M/L
	port	<portlist> [<vpi> <vci>] [clear]	Displays and/or erases port statistics.	M/L
	rmon	stats|history enet1|enet2	Displays uplink/subtending link RMON information.	M/L
	rstp		Enables RSTP (Rapid Tree Spanning Protocol).	M/L
	vlan	[vlanlist]	Displays detailed VLAN related statistics.	M/L
switch				
	acl delete	<portlist> <vpi> <vci> <profile>	Removes an acl profile from PVC. <profile>: up to 32 characters up to 8 profiles if only one PVC has profiles.	M/H
	acl profile delete	<name>	Deletes an acl profile.	M/H
	acl profile set	<name> <rule> <action>	Configures an ACL rule to classify the upstream traffic and perform action(s) on the classified traffic. See Section 59.1.1 on page 453 for information on configuring an ACL profile rule.	M/H
	acl profile show	[<name>]	Displays an acl profile.	L/L
	acl profile showmap	<name>	Displays acl profile reference.	L/L
	acl set	<portlist> <vpi> <vci> <profile>	Applies an acl profile to a PVC. Max. 8 profiles per port.	M/H
	acl show	[portlist] [<vpi> <vci>]	Shows an acl profile setting for a PVC.	L/L

Table 99 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	dhcprelay disable		Turns off DHCP relay.	H/H
	dhcprelay enable		Turns on DHCP relay.	H/H
	dhcprelay opt82sub2 disable		Turns off option 82 sub-option 2.	M/H
	dhcprelay opt82sub2 enable		Turns on option 82 sub-option 2.	M/H
	dhcprelay opt82sub2 set	<vid>|all <relay info>	Adds the specified information for sub-option 2.	M/H
	dhcprelay option82 disable		Turns off the DHCP relay agent information (Option 82) feature.	M/H
	dhcprelay option82 enable		Turns on the DHCP relay agent information (Option 82) feature.	M/H
	dhcprelay option82 set	<vid>|all <relay info>	Adds the specified information for the relay agent.	M/H
	dhcprelay optionmode	<<vid>|all> <private|tr101>	Selects the method (Private or TR-101) by which DHCP relay information is sent on the specified VLAN(s).	H/H
	dhcprelay relaymode	<vid>|all <mode>	Sets which DHCP relay mode the system uses for the specified VLAN. <mode>: The relay process mode. Options are auto or both. auto: Sends the requests to the active DHCP server first. If the active DHCP server does not respond, the switch sends the DHCP request to the backup DHCP server. both: Sends the requests to both the active and backup DHCP servers.	M/H
	dhcprelay server active	<vid> <active-server>	Activates the DHCP server for the specified VLAN. <active-server>: The IP address for the DHCP server.	M/H
	dhcprelay server delete	<vid> [<primary-server>]	Removes the DHCP server setting for the specified VLAN.	M/H

Table 99 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	dhcprelay server set	<vid> <primary-server> [<secondary-server>]	Specifies the DHCP server(s) that serve the specified VLAN. The primary server is required; the secondary server is optional. The AAM1212 routes DHCP requests to the specified DHCP server(s) according to the relaymode. Use VLAN ID 0 to set up the default DHCP server(s) for all non-listed VLAN. <vid>: The ID of the VLAN to which to apply the setting. <primary-server>: The IP address of one DHCP server. <secondary-server>: The IP address of a second DHCP server. Maximum 32 entries can be configured. Default: (empty list)	M/H
	dhcprelay show		Displays the DHCP relay settings for each VLAN. These settings include whether or not this feature is activated for each VLAN, the relay mode, the current list of DHCP servers, the status of the DHCP relay agent info option 82 feature and the information configured for it.	L/L
	dhcpsnoop disable	<portlist>	Disables IP spoofing for a port.	M/H
	dhcpsnoop enable	<portlist>	Enables IP spoofing for a port.	M/H
	dhcpsnoop flush	<portlist>	Flushes the DHCP snooping table for a port.	M/H
	dhcpsnoop pool delete	<port> <ip>	Removes the static IP address from the DHCP snooping table.	M/H
	dhcpsnoop pool set	<port> <ip>	Adds a static IP address to the DHCP snooping table. You can add up to 3 static IP addresses per port.	M/H
	dhcpsnoop show	<portlist>	Displays the DHCP snooping results for a port.	L/L
	dot1x auth	<profile|radius>	Sets the authentication method for a profile or radius server.	H/H
	dot1x disable		Turns off IEEE 802.1x authentication.	H/H
	dot1x enable		Turns on IEEE 802.1x authentication.	H/H

Table 99 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	dot1x port control	<portlist> <auto|auth|unauth>	Sets the IEEE 802.1x port authentication option for specific subscriber ports. auto: authentication required auth: forced authentication unauth: forced no authentication	H/H
	dot1x port disable	<portlist>	Turns off IEEE 802.1x authentication on a port.	H/H
	dot1x port enable	<portlist>	Turns on IEEE 802.1x authentication on a port.	H/H
	dot1x port period	<portlist> <period>	Sets the IEEE 802.1x re-authentication period (60~65535) for specific subscriber ports.	H/H
	dot1x port reauth	<portlist> <on|off>	Enables/disables the IEEE 802.1x re-authentication option for specific subscriber ports.	H/H
	dot1x profile delete	<name>	Removes account for profile mode.	H/H
	dot1x profile set	<name> <password>	Sets account and password for profile mode.	H/H
	dot1x profile show		Displays accounts for profile mode.	M/L
	dot1x radius ip	<ip>	Sets the IP address of the external RADIUS server	H/H
	dot1x radius port	<port>	Sets the external RADIUS server port number of the specified RADIUS server.	H/H
	dot1x radius secret	<secret>	Sets the authentication and encryption key of the specified RADIUS server. <secret>: The authentication encryption key (<=31 characters).	H/H
	dot1x radius show		Displays radius server settings.	M/L
	dot1x show	[portlist]	Displays IEEE 802.1x settings.	M/L
	dscp disable	<portlist>	Stops the DSCP (Differentiated Services Code Point) service on the specified slot and port. DSCP is a field in the header of IP packets for packet classification purposes. QoS (Quality-of-Service) uses DSCP to provide different level of services and priorities.	M/H
	dscp enable	<portlist	Enables DSCP service on the specified slot and port.	M/H

Table 99 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	dscp map set	<srccp> <mappri>	Sets the DSCP code to 802.1p mapping table. <srccp>: source code point, 0~63 <mappri>: mapping priority, 0~7	M/H
	dscp map show	[portlist]	Displays the DSCP code to 802.1p mapping table.	L/L
	dscp show	[portlist]	Displays per port DSCP settings.	L/L
	enet disable	<portlist>	Turns off the specified Ethernet port(s).	H/H
	enet enable	<portlist>	Turns on the specified Ethernet port(s).	H/H
	enet length set	<portlist> auto|<length>	Displays the ENET cable length setting. <length>: 0~15, in units of 10 m.	H/~
	enet length show		Sets the ENET cable length manually when cable length is not accurately detected.	M/~
	enet maxmtu set	<size>	Sets the maximum transmission unit size. <size>: 1526~1600 bytes, default 1526 bytes.	H/H
	enet maxmtu show		Shows the maximum transmission unit size.	M/L
	enet name	<portlist> <name>	Sets the Ethernet port(s) name.	H/H
	enet reset	<portlist>	Reset the ENET interface	H/H
	enet show		Displays the Ethernet port settings.	M/L
	enet speed	<portlist> <10copper|100copper|auto>	Sets the Ethernet port(s) connection speed.	H/H
	garptimer join	<join msec>	Sets system's GARP join time. Sets the GARP timer's join timer. <join msec>: (100~32766 milliseconds).	H/H
	garptimer leave	<leave msec>	Sets the GARP timer's leave timer. <leave msec>: 201~65534 milliseconds.	H/H
	garptimer leaveall	<leaveall msec>	Sets the GARP timer's Leave All Timer. <leaveall msec>: 202~65535 milliseconds	H/H
	garptimer show		Displays the system's GARP settings.	M/L
	igmpfilter profile delete	<name>	Removes an IGMP filter profile.	H/H

Table 99 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	igmpfilter profile set	<name> <index> <startip> <endip>	Configures an IGMP filter profile.	H/H
	igmpfilter profile show	[name]	Displays an IGMP filter profile's settings.	M/L
	igmpfilter set	<portlist> <name>	Sets an ADSL port(s) to use an IGMP filter profile.	H/H
	igmpfilter show	[portlist]	Displays which IGMP filter profile an ADSL port(s) is using.	M/L
	igmpsnoop bandwidth default	<bandwidth>	Sets default bandwidth for multicast IP channels.	M/H
	igmpsnoop bandwidth delete	<index>	Deletes an entry of bandwidth budget setting specified in <index> field.	M/H
	igmpsnoop bandwidth port disable	<portlist>	Disables bandwidth budget control for a port.	M/H
	igmpsnoop bandwidth port enable	<portlist>	Enables bandwidth budget control for a port.	L/H
	igmpsnoop bandwidth port set	<portlist> <bandwidth>	Sets the bandwidth threshold for a port. <bandwidth>: 1~100,000, in units of kbps.	M/H
	igmpsnoop bandwidth port show	<portlist>	Shows the bandwidth control setting for a port.	L/L
	igmpsnoop bandwidth set	<index> <start-mcast-ip> <end-mcast-ip> <bandwidth>	Sets bandwidth budget for a range of multicast IP channels specified in <index> field. <index>: 1~96 <start-mcast-ip>: Start multicast IP address <end-mcast-ip>: End multicast IP address	M/H
	igmpsnoop bandwidth show		Shows bandwidth budget for a range of multicast IP channels.	L/L
	igmpsnoop disable		Turns off IGMP snooping.	H/H
	igmpsnoop enable	<proxy|snooping>	Sets IGMP snooping mode. Turns on IGMP proxy or snooping. Use proxy to have the device use IGMP proxy. Use snooping to have the device passively learn multicast groups.	H/H
	igmpsnoop igmpcount disable	<portlist>	Disables IGMP count limiting to subscriber port.	H/H
	igmpsnoop igmpcount enable	<portlist>	Enables IGMP count limiting to subscriber port.	H/H
	igmpsnoop igmpcount set	<portlist> <count>	Sets IGMP count limiting number to subscriber port.	H/H

Table 99 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	igmpsnoop igmpcount show	[portlist]	Displays IGMP count limiting setting status on the specified slot.	M/L
	igmpsnoop mvlan delete	<vlanlist>	Removes a MVLAN entry.	H/H
	igmpsnoop mvlan disable	<vid>	Turns off a MVLAN entry.	H/H
	igmpsnoop mvlan enable	<vid>	Turns on a MVLAN entry.	H/H
	igmpsnoop mvlan group delete	<vid> <index>	Delete a multicast to VLAN translation entry.	H/H
	igmpsnoop mvlan group set	<vid> <index> <start_mcast_ip> <end_mcast_ip>	Create a multicast to VLAN translation entry. <index>: 1~16 Note: The IP address range in an entry should not overlap those of other entries.	H/H
	igmpsnoop mvlan group show	<vlanlist>	Shows a multicast to VLAN translation entry.	M/L
	igmpsnoop mvlan name	<vid> <name>	Sets the name of the multicast VLAN.	H/H
	igmpsnoop mvlan set	<vid> <portlist>:<F<T|U>|X> [<portlist>:<F<T|U>|X> ...] [name]	Creates a multicast VLAN and sets the allowed/blocked port member(s). This command is similar to the command to create a regular VLAN. F<T|U>: Stands for a fixed registrar administration control flag and registers a <portlist> to the static VLAN table with <*vid*>. For a fixed port, you also have to specify <T|U>, the tag control flag. T: has the device add an IEEE 802.1Q tag to frames going out through this port(s). U: has the device send frames out through this port(s) without an IEEE 802.1Q tag. X: This is the registrar administration control flag. It stands for forbidden and blocks a <portlist> from joining the static VLAN table with <*vid*>. [name]: A name to identify the SVLAN entry.	H/H
	igmpsnoop mvlan show	<vlanlist>	Displays multicast VLAN settings.	M/L

Table 99 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	igmpsnoop qryvid delete	<vid>	Removes a VLAN ID in the IGMP proxy query VLAN table. Use these qryvid commands only when IGMP proxy is enabled. (You can use the multicast igmp qryvid enable proxy command to turn IGMP proxy on.)	H/H
	igmpsnoop qryvid set	<vid>	Adds a static VLAN ID in the IGMP proxy query VLAN table.	H/H
	igmpsnoop qryvid show		Displays the VLAN IDs in the IGMP proxy query VLAN table.	M/L
	igmpsnoop show		Displays the IGMP snooping setting.	M/L
	isolation daisychain		Sets the switch mode to daisychain mode.	H/H
	isolation disable		Turns the subscriber isolation feature off.	H/H
	isolation enable		Turns the subscriber isolation feature on.	H/H
	isolation show		Displays the subscriber isolation feature's current setting.	M/L
	isolation standalone		Sets the switch mode to standalone mode.	H/H
	isolation vlan delete	<vid>	Turns off per-VLAN isolation for the specified VLAN.	H/H
	isolation vlan set	<vid>	Turns on per-VLAN isolation for the specified VLAN.	H/H
	mac agingtime set	<sec, 10..10000|0:disabled>	Sets the MAC aging out time period.	H/H
	mac agingtime show		Displays the MAC aging out time period.	M/L
	mac antispoofing disable		Turns off MAC anti-spoofing.	H/H
	mac antispoofing enable		Turns on MAC anti-spoofing.	H/H
	mac antispoofing show		Show the MAC anti-spoofing status	M/L
	mac count disable	<portlist>	Turns off the MAC address count filter for an ADSL port(s).	H/H
	mac count enable	<portlist>	Turns on the MAC address count filter for an ADSL port(s).	H/H
	mac count set	<portlist> <count>	Sets the MAC address count filter for an ADSL port(s).	H/H
	mac count show	[portlist]	Displays the system's current MAC address count settings.	M/L

Table 99 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	`mac filter delete`	`<port> <mac> [<mac> <mac> ...]`	Removes a MAC filter MAC entry on an ADSL port(s).	H/H
	`mac filter disable`	`[portlist]`	Turns off the MAC filter.	H/H
	`mac filter enable`	`[portlist]`	Turns on the MAC filter.	H/H
	`mac filter mode`	`<port> <accept|deny>`	Sets the MAC filter to accept or deny.	H/H
	`mac filter set`	`<port> <mac> [<mac> <mac> ...]`	Adds a MAC filter MAC entry on an ADSL port(s).	H/H
	`mac filter show`	`[portlist]`	Displays MAC filter settings.	M/L
	`mac flush`		Clears learned MAC addresses from the forwarding table.	H/H
	`ouifilter delete`	`<port> <oui> [<oui> <oui> ...]`	Removes the OUI filter on the specified port. The OUI (Organization Unit Identifier) filter allows or drops packets with MAC addresses from specific vendors. `<oui>`: The first three octets of the MAC address.	H/H
	`ouifilter disable`	`<portlist>`	Deactivates OUI filtering on the specified port(s).	H/H
	`ouifilter enable`	`<portlist>`	Enables OUI filtering on the specified port(s).	H/H
	`ouifilter mode`	`<port> <accept|deny>`	Set OUI filter operating mode. `accept`: Accept packets from specified OUIs, and deny packets from other OUIs. `deny`: Deny packets from specified OUIs, and accept packets from other OUIs.	H/H
	`ouifilter set`	`<port> <oui> [<oui> <oui> ...]`	Creates a OUI filter. `oui`: The first three octets of the MAC address.	H/H
	`ouifilter show`		Displays OUI filter settings.	M/L
	`pktfilter pppoeonly`	`<portlist>`	Accepts only PPPoE packets and rejects all other packet types on this port. (Point-to-Point Protocol over Ethernet) relies on PPP and Ethernet. PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as a single DSL line, wireless device or cable modem	H/H

Table 99 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	pktfilter set	<portlist> <filter>	Sets the packet type filter for the specified subscriber ports. Packet type filter allows or drops specified packet types on the specified subscriber ports. <filter>: Filter options include [pppoe] [ip] [arp] [netbios] [dhcp] [eapol] [igmp] [none]. Setting the filter to none will allow all types of packet to pass.	H/H
	pktfilter show	[portlist]	Displays packet filter settings.	M/L
	poeagent clearinfo	<<vid>|all>	Resets the PPPoE line description.	H/H
	poeagent delete	<<vid>|all>	Removes PPPoE Agent Information settings for the specified VLAN.	H/H
	poeagent disable	<<vid>|all>	Sets the AAM1212 to not add line information to PPPoE discover packets.	H/H
	poeagent enable	<<vid>|all>	Sets the AAM1212 to add a vendor-specific tag to PADI (PPPoE Active Discovery Initiation) and PADR (PPPoE Active Discovery Request) packets from PPPoE clients. This tag gives a PPPoE termination server additional information (such as the port number, VLAN ID, and MAC address) that the server can to identify and authenticate a PPPoE client.	H/H
	poeagent info	<<vid>|all> <info>	Specifies the PPPoE line information the switch is to add to PPPoE discover packets from the specified VLAN. <info>: Enter a description up to 24 alphanumerical characters.	H/H
	poeagent optionmode	<<vid>|all> <private|tr101>	Selects the method (Private or TR-101) in which PPPoE line information is encoded in PPPoE discover packets on the specified VLAN, and whether the VLAN ID is transmitted within the packet or not.	H/H
	poeagent set	<vid>	Creates a PPPoE agent information entry for the VLAN. After you have created an entry for a VLAN, you can configure the line information settings	H/H
	poeagent show		Displays PPPoE line information settings.	M/L
	queuemap set	<priority> <queue level>	Sets a queue's priority.	H/H

Table 99 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	queuemap show		Displays the queues' priorities	M/L
	rstp disable		Turn system's RSTP off.	H/H
	rstp enable		Turn system's RSTP (Rapid Tree Spanning Protocol) on.	H/H
	rstp fwdelay	<fwdelay sec>	Set system RSTP's forward delay time.	H/H
	rstp hellotime	<hellotime sec>	Set system RSTP's hello time.	H/H
	rstp maxage	<maxage sec>	Set system RSTP's max age.	H/H
	rstp port disable	<portlist>	Set enet port to disable RSTP.	H/H
	rstp port enable	<portlist>	Set enet port to enable RSTP.	H/H
	rstp port pathcost	<portlist> <pathcost>	Set enet port's RSTP pathcost.	H/H
	rstp port priority	<portlist> <priority>	Set enet port's RSTP priority.	H/H
	rstp port show		Display enet port RSTP status.	M/L
	rstp priority	<priority>	Set system RSTP's priority.	H/H
	rstp show		Display the system's RSTP settings.	M/L
	smcast delete	<mac>	Removes a static multicast filter entry by deleting the associated MAC address.	H/H
	smcast set	<adsl_port> <mac> <join|leave>	Use join/leave to add/ remove multicast MAC addresses on specified ADSL ports, a range of ADSL ports or all ADSL ports.	H/H
	smcast show		Display all MAC addresses joined to ADSL ports.	M/L
	vlan cpu set	<vid>	Sets the VLAN ID of the Management VLAN.	H/~
	vlan cpu show		Displays the VLAN ID of the Management VLAN.	M/~
	vlan delete	<vlanlist>	Removes a VLAN entry.	H/H
	vlan disable	<vid>	Turns off a VLAN entry.	H/H
	vlan enable	<vid>	Turns on a VLAN entry.	H/H
	vlan frametype	<portlist> <all|tag>	Sets the specified DSL port to accept tagged, untagged or Ethernet frames (or both). Note: enet1, enet2 are fixed at 'all'.	H/H
	vlan gvrp	<portlist> <enable|disable>	Set the port(s) to enable or disable GVRP.	H/H
	vlan name	<vid> <name>	Sets the name of a VLAN.	H/H
	vlan portshow	[portlist]	Displays the port(s) VLAN settings.	M/L

Table 99 Commands (continued)

<table>
<tr><th>CLASS</th><th>COMMAND</th><th>PARAMETERS</th><th>DESCRIPTION</th><th>P</th></tr>
<tr><td></td><td>vlan priority</td><td><portlist> <priority></td><td>Sets a port’s default IEEE 802.1p priority.</td><td>H/H</td></tr>
<tr><td></td><td>vlan pvid</td><td><portlist> <pvid></td><td>Sets the PVID (Port VLAN ID) assigned to untagged frames or priority frames (0 VID) received on this port(s).</td><td>H/H</td></tr>
<tr><td></td><td>vlan set</td><td><vid> <portlist>:<F<T|U>|X|N> [<portlist>:<F<T|U>|X|N> ...] [name]</td><td>Adds or modifies an entry in the static VLAN table.
<vid>: The VLAN ID [1 – 4094].
F<T|U>: The <F> stands for a fixed registrar administration control flag and registers a <portlist> to the static VLAN table with <vid>. For a fixed port, you also have to specify <T|U>, the tag control flag.
T: has the device add an IEEE 802.1Q tag to frames going out through this port(s).
U: has the device send frames out through this port(s) without an IEEE 802.1Q tag.
X: This is the registrar administration control flag. X stands for forbidden and blocks a <portlist> from joining the static VLAN table with <vid>.
N: stands for normal and confirms registration of the <portlist> to the static VLAN table with <vid>. This is used in GVRP applications.
[name]: A name to identify the SVLAN entry.</td><td>H/H</td></tr>
<tr><td></td><td>vlan show</td><td><vlanlist></td><td>Displays VLAN settings.</td><td>M/L</td></tr>
<tr><td>sys</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td>client disable</td><td><index></td><td>Turns off a secure client.</td><td>H/H</td></tr>
<tr><td></td><td>client enable</td><td><index></td><td>Turns on a secure client.</td><td>H/H</td></tr>
<tr><td></td><td>client set</td><td><index> <start ip> <end ip> [[telnet] [ftp] [web] [icmp] [snmp]]</td><td>Sets a secured client set: a range of IP addresses from which you can manage the device and the protocols that can be used.</td><td>H/H</td></tr>
<tr><td></td><td>client show</td><td></td><td>Displays the device’s secured client settings.</td><td>M/L</td></tr>
<tr><td></td><td>date set</td><td><yyyy> <mm> <dd></td><td>Sets the system’s date.</td><td>H/H</td></tr>
<tr><td></td><td>date show</td><td></td><td>Displays the system’s current date.</td><td>L/L</td></tr>
<tr><td></td><td>info contact</td><td><contact></td><td>Sets contact person information.</td><td>M/L</td></tr>
<tr><td></td><td>info hostname</td><td><hostname></td><td>Sets the system name.</td><td>M/L</td></tr>
<tr><td></td><td>info location</td><td><location></td><td>Sets location information.</td><td>M/L</td></tr>
</table>

Table 99 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	info show		Displays general system information.	L/L
	log clear		Clears the device's logs.	H/H
	log show		Displays the device's logs.	M/L
	monitor disable		Turns the hardware monitor off.	H/H
	monitor enable		Turns the hardware monitor on.	H/H
	monitor show		Displays the hardware monitor's statistics.	L/L
	monitor tlimit	<idx> <high> <low>	Sets the maximum (<high>) or minimum (<low>) temperature at the specified temperature sensor. You can specify a temperature with up to three digits after a decimal point (-50.025 for example). Temperature sensor locations: <idx>: 1: DSL 2: CPU 3: HW monitor	H/H
	monitor vlimit	<idx> <high> <low>	Sets the maximum (<high>) or minimum (<low>) voltage at the specified voltage sensor. You can specify a voltage with up to three digits after a decimal point (0.941 for example). Normal voltage at each sensor: <idx>: 1: 1.2v 2: 1.8v 3: 3.3v 4: 24v	H/H
	reboot	[show|sec|cancel]	Sets the reboot timer or displays the timer and remaining time for reboot. If a reboot has been scheduled, use this command to prevent a reboot.	H/H
	server disable	<telnet|ftp|web|icmp>	Turns off a service.	H/H
	server enable	<telnet|ftp|web|icmp>	Turns on a service.	H/H
	server port	<telnet|ftp|web|icmp> <port>	Sets a port for a service.	H/H
	server show		Displays the device's service status and port numbers.	M/L
	snmp getcommunity	<community>	Sets the password for the incoming Get- and GetNext-requests from the management station.	H/H

Table 99 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	snmp setcommunity	<community>	Sets the password for the incoming Set- requests from the management station.	H/H
	snmp show		Displays SNMP settings.	M/L
	snmp trapcommunity	<community>	Sets the password sent with each trap to the SNMP manager.	H/H
	snmp trapdst del	<index>	Deletes the SNMP trap server.	H/H
	snmp trapdst set	<index> <ip> [<port>]	Specifies the IP address (and port number) of a trap server to which the AAM1212 sends SNMP traps. If you leave the trap destination set to 0.0.0.0 (default), the AAM1212 will not send any SNMP traps. <index>: The number of the trap server (1~4). [<port>]: The port number upon which the trap server listens for SNMP traps. The AAM1212 uses the default of 162 if you do not specify a trap port.	H/H
	snmp trusthost	<ip>	Specifies the IP address a trusted host. If you enter a specific IP address, the AAM1212 will only respond to SNMP messages from this address. You can use the sys client set command to specify additional IP addresses, if necessary. If you specify 0.0.0.0, the AAM1212 responds to all SNMP messages it receives, regardless of the settings for the sys client set command.	H/H
	stdio set	<minute|0>	Sets the console timeout period in minutes. 0:no timeout	H/H
	stdio show		Displays the console timeout period.	L/L
	syslog disable		Turns off the syslog logging.	H/H
	syslog enable		Turns on the syslog logging.	H/H
	syslog server	<ip>	Sets the IP address of the syslog server.	H/H
	syslog show		Displays the syslog settings.	M/L
	time set	<hh> [<mm> [ss]]	Sets the system's time.	H/H
	time show		Displays the system's current time.	L/L
	timeserver set	<daytime> <ip> [nosync]	Sets the time service protocol, time server's IP address and the device's time zone.	H/H
	timeserver set	<none>	Sets the system to not use a time server.	H/H

Table 99 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	timeserver set	<time|ntp> <ip> <utc[<+|->0100~1200]> [nosync]	Sets the time service protocol, time server's IP address and the device's time zone.	H/H
	timeserver show		Displays the system's time server.	M/L
	timeserver sync		Retrieves the date and time from the time server.	H/H
	user auth	<local|radius|landr>	Sets the authentication method.	H/H
	user delete	<name>	Removes the specified user name of multi-login.	H/H
	user disable	<name>	Turns off the specified user name of multi-login.	H/H
	user enable	<name>	Turns on the specified user name of multi-login.	H/H
	user online		Displays online user details.	M/~
	user server	<ip> <port> <secret> [high|middle|low|deny]	Sets the remote authentication server IP address and secret.	H/H
	user set	<username> <password> <high|middle|low>	Creates or edits the password and privilege level of the specified user name.	H/H
	user show		Displays the authentication mode, RADIUS server settings and user info.	M/L
	wdog set	<msec|0:disable>	Sets the watchdog count. 0 turns the watchdog off.	H/~
	wdog show		Displays the current watchdog firmware protection feature status and timer.	H/~

46

Command Examples

This chapter gives some examples of commands.

46.1 Command Examples Overview

These are commands that you may use frequently in configuring and maintaining your AAM1212. See Chapter 49 on page 339 for commands that deal with the IEEE 802.1Q Tagged VLAN.

46.2 Sys Commands

These are the commonly used commands that belong to the sys (system) group of commands.

46.2.1 Log Show Command

Syntax:

```
ras> sys log show
```

This command displays the system error log. An example is shown next.

Figure 139 Log Show Command Example

```
ras> sys log show
   1 Wed Aug 11 20:37:11 2004 telnetd   INFO  Session Begin!
   2 Wed Aug 11 20:37:05 2004 telnetd   INFO  Session Begin!
   3 Wed Aug 11 20:36:56 2004 telnetd   INFO  Session Begin!
```

46.3 Log Format

The common format of the system logs is: `<item no> <time> <process> <type> <log message>`.

Table 100 Log Format

LABEL	DESCRIPTION
`<item no>`	This is the index number of the log entry.
`<time>`	This is the time and date when the log was created.
`<process>`	This is the process that created the log.
`<type>`	This identifies what kind of log it is. "INFO" identifies an information log. "WARN" identifies a warning log.
`<log message>`	This is the log's detailed information (see Table 101 on page 312)

46.3.1 Log Messages

The following table lists and describes the system log messages.

Table 101 Log Messages

LOG MESSAGE	TYPE	DESCRIPTION
`ADSL <port> Link Up(SN=<seq no>): <ds rate>/<us rate>!` or `ADSL Link Info: NM:<ds NM>/<us NM>!`	INFO	An ADSL port established a connection. `<port>` - port number `<seq no>` - sequence number of the connection `<ds rate>` - downstream rate `<us rate>` - upstream rate `<us NM>` - upstream noise margin `<ds NM>` - downstream noise margin
`ADSL <port> Link Down(SN=<seq no>)!`	WARN	An ADSL port lost its connection. `<port>` - port number `<seq no>` - sequence number of the connection
`ADSL <port> Link Loss of Power Dying-Gasp Event!`	WARN	The subscriber device connected to an ADSL port experienced a loss of power (Dying-Gasp). `<port>` - port number
`Change time server to none.`	INFO	The time server setting was changed to none.
`Change time server to TIME. IP:<ip> Timezone: <time zone>.`	INFO	The time server protocol setting was changed to TIME. The time server's IP address and time zone are displayed.
`Change time server to DAYTIME. IP: <ip>`	INFO	The time server protocol setting was changed to DAYTIME. The time server's IP address and time zone are displayed.
`Change time server to NTP. IP: <ip> Timezone: <time zone>`	INFO	The time server protocol setting was changed to NTP. The time server's IP address and time zone are displayed.

Table 101 Log Messages (continued)

LOG MESSAGE	TYPE	DESCRIPTION
`Ether <port> Link Down(SN=N)!`	WARN	An Ethernet link is down. `<port>` - 1 is ENET1, 2 is ENET2 SN - an internal sequencer number
`Ether N Link Up(SN=N): <speed>!`	INFO	An Ethernet link is up. `<port>` - 1 is ENET1, 2 is ENET2 SN - an internal sequencer number `<speed>` - Ethernet connection speed, for example 1000M or 100M
`Incorrect Password!`	WARN	Someone attempted to use the wrong password to start a console, telnet or FTP session (see the <process> field for the type of session).
`Session Begin!`	INFO	A console, telnet or FTP session has begun (see the <process> field for the type of session).
`Session End!`	INFO	A console telnet or FTP session has terminated (see the <process> field for the type of session).
`Sync with timeserver <ip> failed!`	WARN	The device was not able to synchronize the time with the time server at the listed IP address.
`Sync with timeserver <ip> successful!`	INFO	The device synchronized the time with the time server at the listed IP address.
`Received File <file>!`	INFO	A file was uploaded to the AAM1212 by FTP. `<file>` - received file's name
`Received Firmware Checksum Error!`	WARN	A checksum error was detected during an attempted FTP firmware upload.
`Received Firmware Invalid!`	WARN	Someone attempted to upload a firmware file with a wrong identity via FTP.
`Received Firmware Size too large!`	WARN	The file size was too large with an attempted FTP firmware upload.
`THERMO LOW  VOLTAGE: dev: <id> limit: <threshold> value: <voltage>!`	WARN	The device's voltage went above the accepted operating range. `<id>` 1=1.2 V, 2=1.8 V, 3=3.3 V, 4=18 V `<threshold>` - voltage limit `<voltage>` - voltage of the DC power when logged
`THERMO LOW TEMPERATURE: dev:<id> threshold:<threshold>(degree C) value:<temp>(degree C)!`	WARN	The temperature was too low at one of the temperature sensors. `<id>` - 0: sensor near the ADSL chipset 1: sensor near the CPU 2: thermal sensor chip `<threshold>` - temperature limit `<temp>` - temperature when the entry was logged
`THERMO OVER TEMPERATURE: dev:<id> threshold:<threshold>(degree C) value:<temp>(degree C)!`	WARN	The temperature was too high at one of the temperature sensors. `<id>` - 0: sensor near the ADSL chipset 1: sensor near the CPU 2: thermal sensor chip `<threshold>` - temperature limit `<temp>` - temperature when the entry was logged

Table 101 Log Messages (continued)

LOG MESSAGE	TYPE	DESCRIPTION
THERMO OVER TEMPERATURE released: dev:<id> threshold:<threshold>(degree C) value:<temp>(degree C)!	INFO	The temperature at one of the temperature sensors has come back to normal. <id> - 0: sensor near the ADSL chipset 1: sensor near the CPU 2: thermal sensor chip <threshold> - temperature limit <temp> - temperature when the entry was logged
THERMO OVER VOLTAGE: dev: <id> limit: <threshold> value: <voltage>!	WARN	The voltage at one of the voltage sensors went above the accepted operating range. <id> 1=1.2v, 2=1.8v, 3=3.3v, 4=24v <threshold> - voltage limit <voltage> - voltage of the DC power when logged
THERMO OVER VOLTAGE released: nominal:<nominal>(mV) value:<voltage> (mV)!	INFO	The device's voltage is back inside the accepted operating range. <nominal> - nominal voltage of the DC power <voltage> - voltage of the DC power when logged

46.3.2 Log Clear Command

Syntax:

```
ras> sys log clear
```

This command clears the system error log.

Note: If you clear a log (using the log clear command), you cannot view it again.

46.3.3 Info Show Command

Syntax:

```
ras> sys info show
```

This command shows general system settings, the BIN (firmware) version, system uptime and bootbase version.

An example is shown next.

Figure 140 Info Show Example

```
ras> sys info show
        Hostname:
        Location:
         Contact:
           Model: AAM1212-51
   ZyNOS version: V3.52(ABA.0) | 07/07/2006
        F/W size: 2747672
     MAC address: 00:13:49:DE:00:AD
  System up time:   0(days) :   22:31:49
Bootbase version: V1.03(AAM1212-51) | 02/18/2005
  F/W build date: Jul  7 2006 10:00:31
DSP code version:  6.04.0003
Hardware version:
   Serial number:
```

46.4 Isolation Commands

Turn on port isolation to block communications between subscriber ports. When you enable port isolation, you do not need to configure the VLAN to isolate subscribers.

46.4.1 Isolation Show Command

Syntax:

```
ras> switch isolation show
```

This command displays the current setting of the subscriber isolation feature.

An example is shown next.

Figure 141 Isolation Show Example

```
ras> switch isolation show
system isolation: enabled
```

46.4.2 Isolation Enable Command

Syntax:

```
ras> switch isolation enable
```

This command turns on the subscriber isolation feature.

46.4.3 Isolation Disable Command

Syntax:

```
ras> switch isolation disable
```

This command turns off the subscriber isolation feature.

46.5 switch ouifilter Commands

Use the following OUI (Organizationally Unique Identifier) filter commands to filter out packets from devices with the specified OUI in the MAC address field.

The OUI field is the first three octets in a MAC address. An OUI uniquely identifies the manufacturer of a network device and allows you to identify from which device brands the switch will accept traffic or send traffic to. The OUI value is assigned by the IANA.

46.5.1 switch ouifilter disable Command

Syntax:

`switch ouifilter disable <port>`

This command deactivates MAC OUI filtering on the specified port(s).

46.5.2 switch ouifilter enable Command

Syntax:

`switch ouifilter enable <port>`

This command activates MAC OUI filtering on the specified port(s).

46.5.3 switch ouifilter mode Command

Syntax:

`switch ouifilter mode <port> accept|deny`

where

`accept|deny`	`accept`: Allows frames from MAC addresses with the OUI(s) that you specify and blocks frames with MAC addresses of other OUIs. `deny`: Blocks frames from MAC addresses with the OUI(s) that you specify and allows frames from other MAC addresses.

This command activates MAC OUI filtering on the specified port(s). Use the `switch ouifilter set` command to set the OUI value(s).

The following example sets the system to drop packets with the specified OUI value on port 1.

```
ras> switch ouifilter mode 1 deny
```

46.5.4 switch ouifilter set Command

Syntax:

`switch ouifilter set <port> <mac-oui>`

where

mac-oui	The first three octets of a MAC address in the format xx:xx:xx. For example, 00:0F:FE.

This command specifies a MAC OUI whose packets you want to filter. Use the `switch ouifilter mode` command to set the action on the matched packets.

The following example sets the system to filter packets with an OUI value of 00-0F-FE on port 1.

```
ras> switch ouifilter set 1 00:0f:fe
```

46.5.5 switch ouifilter show Command

Syntax:

`switch ouifilter show <port>`

This command displays the OUI filtering status (V for enabled, - for disabled) and the OUI value(s) of the MAC address on a DSL port(s) or on all of the DSL ports if no port is specified. The following example displays the OUI filter setting of port 1.

```
ras> switch ouifilter show 1
     status:V, enable oui filter function.
     status:-, disable oui filter function.
port  mode  status oui
---- ------ ------ -----------------
   1 accept   -    -
```

46.6 Statistics Monitor Command

Syntax:

```
ras> statistics monitor
```

This command shows the current hardware status (voltage and temperature).

An example is shown next.

Figure 142 Statistics Monitor Command Example

```
ras> statistics monitor
Hardware monitor status: enabled
      nominal limit(hi) limit(lo)   current      min      max      avg status
      ------- --------- --------- --------- -------- -------- -------- -----
---
v1(v)   1.200     1.344     1.056     1.152    1.139    1.152    1.148 Normal
v2(v)   1.800     1.944     1.656     1.820    1.820    1.820    1.820 Normal
v3(v)   3.300     3.564     3.036     3.200    3.200    3.200    3.200 Normal
v4(v)  18.000    19.440    16.560    18.175   18.175   18.175   18.175 Normal

      limit(hi) limit(lo)   current       min       max       avg status
      --------- --------- --------- --------- --------- --------- --------
t1(c)    97.000   -55.000    43.000    40.000    52.000    43.000 Normal
t2(c)    97.000   -55.000    46.000    41.000    59.000    46.000 Normal
t3(c)    97.000   -55.000    47.000    42.000    58.000    47.000 Normal
```

46.7 Statistics Port Command

Syntax:

```
ras> statistics port <portlist> [<vpi> <vci>] [clear]
```

where

`<portlist>`	=	You can specify a single port <1>, all ports <*> or a list of ports <1,3,enet1>. You can also include a range of ports <1,5,6~10,enet1,enet2>.
`<vpi> <vci>`	=	The VPI and VCI of an individual PVC.
`[clear]`	=	Use `clear` to have the AAM1212 set the specified port(s) or PVC's counters back to zero.

This command displays and/or erases port statistics.

The following example displays port statistics for DSL port 1.

Figure 143 Statistics Port Command Example

```
ras> statistics port 1
[adsl port 1]
tx packets        : 20
rx packets        : 0
tx uni-packets    : 1
rx uni-packets    : 0
tx nonuni-packets : 19
rx nonuni-packets : 0
tx discard packets: 0
rx discard packets: 0
errors            : 0
tx rate  (bytes/s): 0
rx rate  (bytes/s): 128
tx bytes          : 5904
rx bytes          : 0
```

where

`tx uni-packets`	=	This field shows the number of unicast packets transmitted on this port.
`rx uni-packets`	=	This field shows the number of unicast packets received on this port.
`tx nonuni-packets`	=	This field shows the number of non-unicast (broadcast and multicast) packets transmitted on this port.
`rx nonuni-packets`	=	This field shows the number of non-unicast (broadcast and multicast) packets received on this port.

See Chapter 6 on page 73 for details on the other port statistics fields.

47

Alarm Commands

This chapter describes the alarm management commands.

47.1 Alarm Commands

Use these commands to view, customize and clear alarms. You can also set the device to report alarms to an SNMP or syslog server that you specify.

47.2 General Alarm Command Parameters

The following table describes commonly used alarm command parameter notation.

Table 102 General Alarm Command Parameters

NOTATION	DESCRIPTION
`<alarm>`	Specify a category of alarms. eqpt represents equipment alarms. dsl represents Digital Subscriber Line (DSL) alarms. enet represents Ethernet alarms. sys represents system alarms. all specifies every alarm category.
`<severity>`	Specify an alarm severity level (critical, major, minor, info or all). Critical alarms are the most severe, major alarms are the second most severe, minor alarms are the third most severe and info alarms are the least severe.
`<condition>`	This is the text description for the condition under which the alarm applies. Use the alarm tablelist to find alarm conditions.

47.3 Alarm Show Command

Syntax:

```
ras> alarm show [<severity>|all] [<alarm>|all] [<condition>|all] [detail]
```

where

`[detail]` = Display in-depth alarm information.

This command displays the current alarms by severity, alarm category or alarm condition.

The following example displays the current critical level alarms for all alarm categories and conditions.

The source is where the alarm originated. This is either a DSL port number, one of the Ethernet ports (enet 1 or 2), or "eqpt" for the system itself.

Figure 144 Alarm Show Command Example

```
ras> alarm tablelist
 no alarm         condition          facility snmp syslog severity clearable
--- -----  -------------------------   -------- ---- ------ -------- -------
  1   dsl  ( 5000)line_up              local1    V      V    info       -
  2   dsl  ( 5001)line_down            local1    V      V    minor      V
  3   dsl  ( 5002)ad_perf_lol_thresh   local1    V      V    minor      V
  4   dsl  ( 5003)ad_perf_lof_thresh   local1    V      V    minor      V
  5   dsl  ( 5004)ad_perf_los_thresh   local1    V      V    minor      V
  6   dsl  ( 5005)ad_perf_lop_thresh   local1    V      V    minor      V
  7   dsl  ( 5006)ad_perf_es_thresh    local1    V      V    minor      V
  8   dsl  ( 5007)ad_perf_ses_thresh   local1    V      V    minor      V
  9   dsl  ( 5008)ad_perf_uas_thresh   local1    V      V    minor      V
 10   dsl  ( 5009)ad_atuc_loftrap      local1    V      V    minor      -
 11   dsl  ( 5010)ad_atuc_lostrap      local1    V      V    minor      -
 12   dsl  ( 5011)ad_atur_loftrap      local1    V      V    minor      -
 13   dsl  ( 5012)ad_atur_lostrap      local1    V      V    minor      -
 14   dsl  ( 5013)ad_atur_lprtrap      local1    V      V    minor      -
 15  eqpt  (10000)vol_err              local1    V      V    critical   -
 16  eqpt  (10001)temp_err             local1    V      V    critical   -
 17  eqpt  (10002)hw_rtc_fail          local1    V      V    critical   -
 18  eqpt  (10003)hw_mon_fail          local1    V      V    critical   -
 19  eqpt  (10004)cold_start           local1    V      V    info       -

    Press any key to continue, 'e' to exit, 'n' for nopause
```

47.4 Alarm Port Show Command

Syntax:

```
ras> alarm port show [<severity>|all]
```

This command displays port alarm severity level thresholds. The system reports an alarm on a port if the alarm has a severity equal to or higher than the port's threshold.

The following example displays the port alarm thresholds for all ports. “ifindex” identifies the interface.

Figure 145 Alarm Port Show Command Example

```
ras> alarm port show
 no      ifindex       severity
-----   ----------    -----------
01       01           minor
02       02           minor
03       03           minor
04       04           minor
05       05           minor
=================================== SNIP ==================================

    Press any key to continue, 'e' to exit, 'n' for nopause
```

47.5 Alarm Port Set Command

Syntax:

```
ras> alarm port set <all|enet1|enet2|port> <severity>
```

where

`<all|enet1|enet2|port>`	=	Ports on the AAM1212.

This command sets the alarm severity threshold for recording alarms on an individual port(s). The system reports an alarm on a port if the alarm has a severity equal to or higher than the port’s threshold.

The following example has the AAM1212 only record critical alarms on DSL port 7.

Figure 146 Alarm Port Set Command Example

```
ras> alarm port set 7 critical
```

47.6 Alarm Tablelist Command

Syntax:

```
  ras> alarm tablelist [<alarm>|all] [<severity>|all]
[<fac>|all][<target>[,<target>]] [<condition>|all]
```

where

`<fac>`	=	The log facility (`local1~local7`) that has the device log the syslog messages to different files in the syslog server. See your syslog program's documentation for details.
`<target>`	=	`snmp|syslog|all` The type of alarm messages that the device is to send (SNMP, syslog or all).

This command lists alarm settings.

The following example displays the supported minor level alarms for all alarm categories, facilities, types of alarm messages and conditions.

Figure 147 Alarm Tablelist Command Example

```
ras> alarm table
 no alarm         condition          facility snmp syslog severity clearable
--- -----  -------------------------   -------- ---- ------ -------- -------
  1   dsl  ( 5000)line_up              local1    V     V    info       -
  2   dsl  ( 5001)line_down            local1    V     V    minor      V
  3   dsl  ( 5002)ad_perf_lol_thresh   local1    V     V    minor      V
  4   dsl  ( 5003)ad_perf_lof_thresh   local1    V     V    minor      V
  5   dsl  ( 5004)ad_perf_los_thresh   local1    V     V    minor      V
  6   dsl  ( 5005)ad_perf_lop_thresh   local1    V     V    minor      V
  7   dsl  ( 5006)ad_perf_es_thresh    local1    V     V    minor      V
  8   dsl  ( 5007)ad_perf_ses_thresh   local1    V     V    minor      V
  9   dsl  ( 5008)ad_perf_uas_thresh   local1    V     V    minor      V
 10   dsl  ( 5009)ad_atuc_loftrap      local1    V     V    minor      -
 11   dsl  ( 5010)ad_atuc_lostrap      local1    V     V    minor      -
 12   dsl  ( 5011)ad_atur_loftrap      local1    V     V    minor      -
 13   dsl  ( 5012)ad_atur_lostrap      local1    V     V    minor      -
 14   dsl  ( 5013)ad_atur_lprtrap      local1    V     V    minor      -
 15  eqpt  (10000)vol_err              local1    V     V    critical   -
 16  eqpt  (10001)temp_err             local1    V     V    critical   -
 17  eqpt  (10002)hw_rtc_fail          local1    V     V    critical   -
 18  eqpt  (10003)hw_mon_fail          local1    V     V    critical   -
 19  eqpt  (10004)cold_start           local1    V     V    info       -
==================================== SNIP =================================
```

47.7 Log Format

The following table describes the columns in the list.

Table 103 Log Format

LABEL	DESCRIPTION
`no`	This is the index number of the alarm entry in this list display.
`alarm`	This is the category of alarms. eqpt represents equipment alarms. dsl represents Digital Subscriber Line (DSL) alarms. enet represents Ethernet alarms. sys represents system alarms.

Table 103 Log Format (continued)

LABEL	DESCRIPTION
condition	There is a condition code number for the specific alarm message and a text description for the condition under which the alarm applies.
facility	This is the log facility (local1~local7) on the syslog server where the system is to log this alarm. This is for alarms that send alarms to a syslog server.
snmp	This displays “V” if the system is to send this alarm to an SNMP server. It displays “-“ if the system does not send this alarm to an SNMP server.
syslog	This displays “V” if the system is to send this alarm to a syslog server. It displays “-“ if the system does not send this alarm to a syslog server.
severity	This is the alarm severity level (critical, major, minor or info).
clearable	This displays “V” if the alarm clear command removes the alarm from the system. It displays “-“if the alarm clear command does not remove the alarm from the system.

47.8 Alarm History Show Command

Syntax:

```
  ras> alarm history show [<severity>|all] [<alarm>|all] [<condition>|all]
[<sdate>|all] [<edate>|all] [for|rev] [detail]]
```

where

`<sdate>`	=	The start date, in `yyyy/mm/dd` format.
`<edate>`	=	The end date, in `yyyy/mm/dd` format.
`[for|rev]`	=	The displaying order. Use `for` to display in chronological order starting from the oldest alarm. Use `rev` to display in reverse chronological order starting from the most recent alarm.
`[detail]`	=	Display in-depth alarm information.

This command displays historic alarms by severity, alarm category, alarm condition and/or dates.

The following example displays the historic critical level alarms for all alarm categories, and all conditions.

Figure 148 Alarm History Show Command Example

```
ras> alarm history show major all all all all rev detail
    no alarm   condition            severity timestamp      source
------ ------  -------------------- -------- -------------- -------
     1 enet   -down                 major    01/01 00:00:12 enet 1
               * NTENET1:GbE interface is down
     2 enet   +down                 major    01/01 00:00:10 enet 1
               * NTENET1:GbE interface is down
```

47.9 Alarm History Clear Command

Syntax:

```
ras> alarm history clear [<alarm>|all <condition>|all] <severity>
```

This command removes historic alarm entries by alarm category, alarm condition or severity.

The following example removes the historic minor level alarms for all alarm categories, and all conditions.

Figure 149 Alarm History Clear Command Example

```
ras> alarm history clear minor
```

47.10 Alarm XEdit Command

Syntax:

```
ras> alarm xedit <alarm>|all <cond>|<condcode> <severity> <fac>
<target>[,<target>] [clearable]
```

where

`<cond>`	=	`all|condition` This is the text description for the condition under which the alarm applies. Use the `alarm tablelist` to find alarm conditions.
`<condcode >`	=	The condition code is the number of a specific alarm message. Use the `alarm tablelist` to find alarm condition codes.
`<severity>`	=	Specify an alarm severity level (critical, major, minor or info) for this alarm. Critical alarms are the most severe, major alarms are the second most severe, minor alarms are the third most severe and info alarms are the least severe.
`<fac>`	=	The log facility (`local1~local7`) has the device log the syslog messages to a particular file in the syslog server. Set this if this entry is for sending alarms to a syslog server. See your syslog program's documentation for details.
`<target>`	=	`snmp|syslog|all` The type of alarm messages that the device is to send (SNMP, syslog or all). You can specify more than one separated by commas.
`[clearable]`	=	`clearable|unclearable` This sets whether or not the alarm clear command removes the alarm from the system.

This command sets the severity level of an alarm(s) and where the system is to send the alarm(s).

Note: Use the `alarm tablelist` command to display alarm setting details.

The following example creates an alarm report entry that sets all system alarms to the major severity level and sends them to an SNMP server at the local 3 log facility.

Figure 150 Alarm Xedit Command Example

```
ras> alarm xedit sys all major local3 syslog
```

47.11 Alarm Cutoff Command

Syntax:

```
ras> alarm cutoff
```

This command cancels an alarm. This stops the sending of the alarm signal current. This is useful in stopping an alarm if you have the alarm output connector pins connected to a visible or audible alarm. The alarm entry remains in the system.

47.12 Alarm Clear Command

Syntax:

```
ras> alarm clear
```

This command erases the clearable alarm entries.

48

DHCP Commands

This chapter describes how to use the DHCP Relay and DHCP Snoop commands.

48.1 DHCP Relay Commands

Use these commands to configure the DHCP relay feature. See Chapter 25 on page 191 for background information on DHCP relay.

48.1.1 Show Command

Syntax:

```
ras> switch dhcprelay show
```

This command displays whether or not the DHCP relay feature is activated, which relay mode the AAM1212 is using, the current list of DHCP servers by VLAN, the status of the DHCP relay agent info option 82 feature and the information configured for it.

Figure 151 Show Command Example

```
ras> switch dhcprelay show
DHCP relay status: disable
DHCP relay mode:   auto
Server list:
index  vid  primary-server     secondary-server
----- ----- ------------------ ------------------
    1     1 (*)212.212.212.212 213.213.213.213
    2     2 (*)214.214.214.214 215.215.215.251

option82 sub-opt1 info (Circuit ID)
----------------- ------------------------------
        -

option82 sub-opt2 info (Remote ID)
----------------- ------------------------------
        -
```

48.1.2 Enable Command

Syntax:

```
ras> switch dhcprelay enable
```

This command turns on the DHCP relay feature.

48.1.3 Disable Command

Syntax:

```
ras> switch dhcprelay disable
```

This command turns off the DHCP relay feature.

48.1.4 Server Set Command

Syntax:

```
ras> switch dhcprelay server set <vid> <primary-server> [<secondary-server>]
```

where

`<vid>`	=	The ID of the VLAN served by the specified DHCP server(s).
`<primary-server>`	=	The IP address of one DHCP server.
`<secondary-server>`	=	The IP address of a second DHCP server.

This command specifies the DHCP server(s) that serve the specified VLAN. The primary server is required; the secondary server is optional. The AAM1212 routes DHCP requests to the specified DHCP server(s) according to the `relaymode`. See Section 48.1.7 on page 331.

Use VLAN ID 0 to set up the default DHCP server(s) for all non-listed VLAN.

48.1.5 Server Delete Command

Syntax:

```
ras> switch dhcprelay server delete <vid> [<primary-server>]
```

where

`<vid>`	=	The ID of the VLAN served by the specified DHCP server(s).

`<primary-server>`	=	The IP address of one DHCP server.

This command deletes all information about DHCP servers for the specified VLAN. Afterwards, the specified VLAN can uses the default DHCP server(s) set up for VLAN ID 0, if any.

48.1.6 Server Active Command

Syntax:

```
ras> switch dhcprelay server active <vid> <active-server>
```

where

`<vid>`	=	The ID of the VLAN served by the specified DHCP server(s).
`<active-server>`	=	**1**: The primary DHCP server is active. **2**: The secondary DHCP server is active.

This command has no effect if the **relaymode** is **both**. If the **relaymode** is **auto**, this command specifies to which DHCP server (the primary one or the secondary one) the AAM1212 should relay DHCP requests for the selected VLAN.

48.1.7 Relaymode Command

Syntax:

```
ras> switch dhcprelay relaymode <mode>
```

where

`<mode>`	=	relay process mode; it controls to which DHCP server(s) the AAM1212 relays DHCP requests. **auto** - the AAM1212 relays DHCP requests to the active server for each VLAN **both** - the AAM1212 relays DHCP requests to the primary and secondary server for each VLAN, regardless of which one is active

This command controls how the AAM1212 routes DHCP requests. The AAM1212 can route DHCP requests to the active DHCP server for the VLAN, or it can route DHCP requests to all DHCP servers set up for the VLAN.

48.2 DHCP Relay Option 82 (Agent Information) Sub-option 1 (Circuit ID)

Use the following commands to configure the DHCP relay Option 82 (agent information) feature, sub-option 1. This feature applies regardless of whether or not the DHCP relay is on.

48.2.1 Option 82 Sub-option 1 Enable Command

Syntax:

```
ras> switch dhcprelay option82 enable
```

This command turns on the DHCP relay agent information (Option 82 Sub-option 1) feature.

48.2.2 Option 82 Sub-option 1 Disable Command

Syntax:

```
ras> switch dhcprelay option82 disable
```

This command turns off the DHCP relay agent information (Option 82, Sub-option 1) feature.

48.2.3 Option 82 Sub-option 1 Set Command

Syntax:

```
ras> switch dhcprelay option82 set [<relay info>]
```

where

`[<relay info>]`	=	Up to 23 ASCII characters of additional information for the AAM1212 to add to the DHCP requests that it relays to a DHCP server. Examples of information you could add would be the name of the AAM1212 or the ISP.

This command adds the specified information for the relay agent.

48.3 DHCP Relay Option 82 (Agent Information) Sub-option 2 (Remote ID)

Use the following commands to configure the DHCP relay Option 82 (agent information) feature, sub-option 2. This feature applies regardless of whether or not the DHCP relay is on.

48.3.1 Option 82 Sub-option 2 Enable Command

Syntax:

```
ras> switch dhcprelay opt82sub2 enable
```

This command turns on the DHCP relay agent information (Option 82, Sub-option 2) feature.

48.3.2 Option 82 Sub-option 2 Disable Command

Syntax:

```
ras> switch dhcprelay opt82sub2 disable
```

This command turns off the DHCP relay agent information (Option 82, Sub-option 2) feature.

48.3.3 Option 82 Sub-option 2 Set Command

Syntax:

```
ras> switch dhcprelay opt82sub2 set [<relay info>]
```

where

[<relay info>]	=	Up to 23 ASCII characters of additional information for the AAM1212 to add to the DHCP requests that it relays to a DHCP server. Examples of information you could add would be the name of the AAM1212 or the ISP.

This command adds the specified information for the relay agent.

48.4 DHCP Snoop Commands

Use these commands to configure or show DHCP snooping settings on the subscriber ports. The system gets the client MAC-IP address information (in the reply from a DHCP server) and stores it in the DHCP snooping table. The system only forwards packets from the clients whose MAC-IP address is in the DHCP snooping table. Packets from unknown IP address(es) are not forwarded (dropped). This feature prevents clients from assigning their own static IP addresses.

48.4.1 DHCP Snoop Enable Command

Syntax:

```
ras> switch dhcpsnoop enable <portlist>
```

where

`<portlist>`	=	You can specify a single port <1>, all ports <*> or a list of ports <1,3,enet1>. You can also include a range of ports <1,5,6~10,enet1,enet2>.

This command activates the DHCP snooping feature on the specified port(s). The following example enables DHCP snooping on port 1.

Figure 152 DHCP Snoop Enable Command Example

```
ras> switch dhcpsnoop enable 1
```

48.4.2 DHCP Snoop Disable Command

Syntax:

```
ras> switch dhcpsnoop disable <portlist>
```

where

`<portlist>`	=	You can specify a single port <1>, all ports <*> or a list of ports <1,3,enet1>. You can also include a range of ports <1,5,6~10,enet1,enet2>.

This command disables the DHCP snooping feature on the specified port(s).

48.4.3 DHCP Snoop Flush Command

Syntax:

```
ras> switch dhcpsnoop flush <portlist>
```

where

`<portlist>`	=	You can specify a single port <1>, all ports <*> or a list of ports <1,3,enet1>. You can also include a range of ports <1,5,6~10,enet1,enet2>.

This command clears the DHCP snooping binding table on the specified port(s). The system also automatically clears the binding table when you disable DHCP snooping.

48.4.4 DHCP Snoop Show Command

Syntax:

```
ras> switch dhcpsnoop show <portlist>
```

where

`<portlist>`	=	You can specify a single port <1>, all ports <*> or a list of ports <1,3,enet1>. You can also include a range of ports <1,5,6~10,enet1,enet2>.

Use this command to display the current DHCP snooping settings of the specified port(s). The following example displays the settings of ports 1-5.

Figure 153 DHCP Snoop Show Command Example

```
ras> switch dhcpsnoop show 1~5
 port  enable
----- --------
    1  V
    2  -
    3  -
    4  -
    5  -
```

48.4.5 DHCP Counter Statistics Command

Syntax:

```
ras> statistics dhcp counter [<portlist> [clear]]
```

where

`<portlist>`	=	You can specify a single port <1>, all ports <*> or a list of ports <1,3,enet1>. You can also include a range of ports <1,5,6~10,enet1,enet2>.

Use this command to display a summary of DHCP packets on the specified port(s). The following example displays the settings of port 1.

Figure 154 DHCP Counter Statistics Command Example

```
ras> statistics dhcp counter 1
 port discover  offer    request    ack    overflow
----- -------- -------- -------- -------- --------
   1         0        0        0        0        0
```

Each field is described in the following table.

port	=	The selected DSL port number(s).
discover	=	The number of DHCP Discover packets on this port.
offer	=	The number of DHCP Offer packets on this port.
request	=	The number of DHCP Request packets on this port.
ack	=	The number of DHCP Ack packets on this port.
overflow	=	The DHCP server can assign up to 32 IP addresses at one time to each port. This field displays the number of requests from DHCP clients above this limit.

48.4.6 DHCP Snoop Statistics Command

Syntax:

```
ras> statistics dhcp snoop <portlist>
```

where

<portlist>	=	You can specify a single port <1>, all ports <*> or a list of ports <1,3,enet1>. You can also include a range of ports <1,5,6~10,enet1,enet2>.

Use this command to look at the DHCP snooping table on the specified port(s). The following example displays the settings of port 1.

Figure 155 DHCP Snoop Statistics Command Example

```
ras> statistics dhcp snoop 1
port overflow       mac               ip
---- -------- ----------------- ---------------
```

Each field is described in the following table.

port	=	The selected DSL port number(s).

`overflow`	=	The DHCP server can assign up to 32 IP addresses at one time to each port. This field displays the number of requests from DHCP clients above this limit.
`mac`	=	The MAC address of a client on this port to which the DHCP server assigned an IP address.
`ip`	=	The IP address assigned to a client on this port.

49

IEEE 802.1Q Tagged VLAN Commands

This chapter describes the IEEE 802.1Q Tagged VLAN commands.

49.1 Introduction to VLANs

See Chapter 16 on page 149 for more background information on VLANs.

49.2 IEEE 802.1Q Tagging Types

There are two kinds of tagging:

- Explicit Tagging

A VLAN identifier is added to the frame header that identifies the source VLAN.

- Implicit Tagging

The MAC (Media Access Control) number, the port or other information is used to identify the source of a VLAN frame.

The IEEE 802.1Q Tagged VLAN uses both explicit and implicit tagging.

It is important for the AAM1212 to determine what devices are VLAN-aware and VLAN-unaware so that it can decide whether to forward a tagged frame (to a VLAN-aware device) or first strip the tag from a frame and then forward it (to a VLAN-unaware device).

49.3 Filtering Databases

A filtering database stores and organizes VLAN registration information useful for switching frames to and from the AAM1212. A filtering database consists of static entries (Static VLAN or SVLAN table).

49.3.1 Static Entries (SVLAN Table)

Static entry registration information is added, modified and removed by administrators only.

49.4 IEEE VLAN1Q Tagged VLAN Configuration Commands

These switch commands allow you to configure and monitor the IEEE 802.1Q Tagged VLAN.

49.4.1 VLAN Port Show Command

Syntax:

```
ras> switch vlan portshow [portlist]
```

where

[portlist]	=	You can specify a single port <1>, all ports <*> or a list of ports <1,3,enet1>. You can also include a range of ports <1,5,6~10,enet1,enet2>.

This command displays the port's IEEE 802.1Q VLAN tag settings.

The following example shows the settings for DSL port 1.

Figure 156 VLAN Port Show Command Example

```
ras> switch vlan portshow 3
 port pvid priority frametype
----- ---- -------- ---------
    3    1        0       all
```

49.4.2 VLAN PVID Command

Syntax:

```
ras> switch vlan pvid <portlist> <pvid>
```

where

<portlist>	=	You can specify a single port <1>, all ports <*> or a list of ports <1,3,enet1>. You can also include a range of ports <1,5,6~10,enet1,enet2>.
<pvid>	=	The VLAN ID. Valid parameter range = [1 – 4094].

This command sets a default VLAN ID for all untagged packets that come in through the specified port.

The following example sets the default VID of port 1 to 200.

Figure 157 VLAN PVID Command Example

```
ras> switch vlan pvid 1 200
```

49.4.3 VLAN Priority Command

Syntax:

```
ras> switch vlan priority <portlist> <priority>
```

where

`<portlist>`	=	You can specify a single port: <1>, all ports: <*>, a list of ports: <1,3,enet1>, you can also include a range of ports: <1,5,6~10,enet1,enet2>.
`<priority>`	=	This is the priority value (0 to 7) to use for incoming frames with an IEEE 802.1Q VLAN tag.

This command sets the priority of incoming frames with an IEEE 802.1Q VLAN tag.

The following example sets a priority of three for frames (with an IEEE 802.1Q VLAN tag) that come in on DSL port 2.

Figure 158 VLAN CPU Set Command Example

```
ras> switch vlan priority 2 3
```

49.4.4 VLAN Set Command

Syntax:

```
ras> switch vlan set <vid> <portlist>:<F<T|U>|X|N> [<portlist>:<F<T|U>|X>
...][name]
```

where

`<vid>`	=	The VLAN ID [1 – 4094].
`<portlist>`	=	You can specify a single port: <1>, all ports: <*>, a list of ports: <1,3,enet1>, you can also include a range of ports: <1,5,6~10,enet1,enet2>.

`<F<T|U>|`	=	The <F> stands for a fixed registrar administration control flag and registers a <port #> to the static VLAN table with <vid>. For a fixed port, you also have to specify <T|U>, the tag control flag. <T> has the device add an IEEE 802.1Q tag to frames going out through this port(s). <U> has the device send frames out through this port(s) without an IEEE 802.1Q tag.
`|X|N>`	=	This is the registrar administration control flag. <X> stands for forbidden and blocks a <port #> from joining the static VLAN table with <vid>. <N> stands for normal and confirms registration of the <port #> to the static VLAN table with <vid>. This is used in GVRP applications.
`[name]`	=	A name to identify the SVLAN entry.

This command adds or modifies an entry in the static VLAN table. Use the `switch vlan show` command to display your configuration. An example of a configuration is shown next.

49.4.4.1 Modify a Static VLAN Table Example

The following is an example of how to modify a static VLAN table.

Figure 159 Modifying the Static VLAN Example

```
ras> switch vlan set 2000 1:FU
ras> switch vlan set 2001 2:FU
```

49.4.4.2 Forwarding Process Example

Tagged Frames

1 First the AAM1212 checks the VLAN ID (VID) of tagged frames or assigns temporary VIDs to untagged frames (see Section 49.4.2 on page 340).
2 The AAM1212 checks the frame's source MAC address against the MAC filter.
3 The AAM1212 then checks the VID in a frame's tag against the SVLAN table.
4 The AAM1212 notes what the SVLAN table says (that is, the SVLAN tells the AAM1212 whether or not to forward a frame and if the forwarded frames should have a tag).
5 Frames might be dropped if they are sent to a CPE (customer premises equipment) DSL device that does not accept tagged frames.

Untagged Frames

1 An untagged frame comes in from the LAN.
2 The AAM1212 checks the frame's source MAC address against the MAC filter.
3 The AAM1212 checks the PVID table and assigns a VID and IEEE 802.1Q priority.
4 The AAM1212 ignores the port from which the frame came, because the AAM1212 does not send a frame to the port from which it came. The AAM1212 also does not forward frames to "forbidden" ports.
5 If after looking at the SVLAN, the AAM1212 does not have any ports to which it will send the frame, it drops the frame.

49.4.5 VLAN Frame Type Command

Syntax:

```
ras> switch vlan frametype <portlist> <all|tag>
```

where

<portlist>	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3 >. You can also include a range of DSL ports <1,5,6~10>.
<all|tag>	=	Use `tag` to have the specified port(s) accept only incoming Ethernet frames that have a VLAN tag. Use `all` to have the specified port(s) accept both tagged and untagged incoming Ethernet frames.

This command sets the specified DSL ports to accept VLAN tagged Ethernet frames, or both tagged and untagged Ethernet frames.

Note: The AAM1212 accepts both tagged and untagged incoming frames on the Ethernet ports.

The following example sets the AAM1212 to accept only VLAN tagged Ethernet frames on DSL port 3.

Figure 160 VLAN Frame Type Command Example

```
ras> switch vlan frametype 3 tag
```

49.4.6 VLAN CPU Show Command

Syntax:

```
ras> switch vlan cpu show
```

This command displays the management VLAN (CPU). You can only use ports that are members of this management VLAN in order to manage the AAM1212.

The following example sets VLAN ID 2 to be the CPU (management) VLAN.

Figure 161 VLAN CPU Set Command Example

```
ras> switch vlan cpu set 2
```

49.4.7 VLAN CPU Set Command

Syntax:

```
ras> switch vlan cpu set <vid>
```

where

`<vid>`	=	The VLAN ID. Valid parameter range = [1 – 4094].

This command sets the management VLAN (CPU). You can only use ports that are members of this management VLAN in order to manage the AAM1212.

The following example sets VLAN ID 2 to be the CPU (management) VLAN.

Figure 162 VLAN CPU Set Command Example

```
ras> switch vlan cpu set 2
```

49.4.8 Configuring Management VLAN Example

Note: After the following example configuration, you must connect to the first Ethernet port through a VLAN aware device that is using the proper VLAN ID in order to perform management.

By default, the AAM1212's DSL ports are members of the management VLAN (VID 1). The following procedure shows you how to configure a tagged VLAN that limits management access to just one Ethernet port.

Note: Use the console port to configure the AAM1212 if you misconfigure the management VLAN and lock yourself out.

1 Use the `switch vlan set` command to configure a VLAN ID (VID 3 in this example) for managing the AAM1212 (the "management" or "CPU" VLAN).

Figure 163 CPU VLAN Configuration and Activation Example

```
ras> switch vlan set 3 enet1:FT
```

2 Use the `switch vlan1q vlan cpu` command to set VID 3 as the management VLAN.

Figure 164 Deleting Default VLAN Example

```
ras> switch vlan cpu set 3
```

49.4.9 VLAN Delete Command

Syntax:

```
ras> switch vlan delete <vlanlist>
```

where

`<vlanlist>`	=	You can specify a single VID: <1>, all VIDs: <*>, a list of VIDs: <1,3>, you can also include a range of VIDs: <1,5,6~10>.

This command deletes the specified VLAN ID entry from the static VLAN table. The following example deletes entry 2 in the static VLAN table.

Figure 165 VLAN Delete Command Example

```
ras> switch vlan delete 2
```

49.5 VLAN Enable

Syntax:

```
ras> switch vlan enable <vid>
```

This command enables the specified VLAN ID in the SVLAN (Static VLAN) table.

49.6 VLAN Disable

Syntax:

```
ras> switch vlan disable <vid>
```

This command disables the specified VLAN ID in the SVLAN (Static VLAN) table.

49.6.1 VLAN Show Command

Syntax:

```
ras> switch vlan show <vlanlist>
```

where

`<vlanlist>`	=	You can specify a single VID: <1>, all VIDs: <*>, a list of VIDs: <1,3>, you can also include a range of VIDs: <1,5,6~10>.

This command shows information about the specified port's VLAN settings.

The following example shows the settings for all VIDs.

Figure 166 VLAN Show Command Example

```
ras> switch vlan show *
 vid name                           F:fixed X:forbidden N:normal U:untag T:tag
---- ------------------------------- -------------------------------------
   1 DEFAULT
     enabled                           123456789012 12
                                       FFFFFFFFFFFF FF
                                       UUUUUUUUUUUU UU
```

50

MAC Commands

This chapter describes how to configure the AAM1212's MAC commands.

50.1 MAC Commands Overview

Use the MAC commands to configure MAC filtering or limit the MAC count.

50.2 MAC Filter Commands

Use the MAC filter to control from which MAC (Media Access Control) addresses frames can (or cannot) come in through a port.

50.2.1 MAC Filter Show Command

Syntax:

```
ras> switch mac filter show [portlist]
```

where

`[portlist]`	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.

This command displays the MAC filtering status (V for enabled, - for disabled) and the fixed source MAC addresses on the specified DSL port(s) or on all DSL ports if no port is specified.

The following example displays the MAC filtering mode, status and the fixed source MAC addresses on DSL port 5.

Figure 167 MAC Filter Show Command Example

```
ras> sw mac filter show 5
     status:V, enable mac filter function.
     status:-, disable mac filter function.
port  mode  status mac
---- ------ ------ -----------------
   5 accept   -    00:a0:c5:12:34:56
```

50.2.2 MAC Filter Enable Command

Syntax:

```
ras> switch mac filter enable [portlist]
```

where

[portlist]	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.

This command turns on the MAC filtering feature on the specified DSL port(s) or on all DSL ports if no port is specified.

The following example turns on the MAC filtering feature on DSL port 5.

Figure 168 MAC Filter Enable Command Example

```
ras> switch mac filter enable 5
```

50.2.3 MAC Filter Disable Command

Syntax:

```
ras> switch mac filter disable [portlist]
```

where

[portlist]	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.

This command turns off the MAC filtering feature on the specified DSL port(s) or on all DSL ports if no port is specified.

The following example turns off the MAC filtering feature on DSL port 5.

Figure 169 MAC Filter Disable Command Example

```
ras> switch mac filter disable 5
```

50.2.4 MAC Filter Mode Command

Syntax:

```
ras> switch mac filter mode <port> <accept|deny>
```

where

`<accept|deny>`	=	accept = Only allow frames from MAC addresses that you specify and block frames from other MAC addresses. deny = Block frames from MAC addresses that you specify and allow frames from other MAC addresses.

This command sets whether the AAM1212 allows or blocks access for the MAC addresses you specify.

The following example sets DSL port 5 to allow frames from the MAC addresses specified for DSL port 5.

Figure 170 MAC Filter Mode Command Example

```
ras> switch mac filter mode 5 accept
```

50.2.5 MAC Filter Set Command

Syntax:

```
ras> switch mac filter set <port> <mac> [<mac> <mac> ...]
```

where

`<port>`	=	The number of a DSL port.
`<mac>`	=	The source MAC address in "00:a0:c5:12:34:56" format.

This command adds an allowed source MAC address on the specified DSL port.

The following example adds source MAC address 00:a0:c5:12:34:56 for DSL port 5.

Figure 171 MAC Filter Set Command Example

```
ras> switch mac filter set 5 00:a0:c5:12:34:56
```

50.2.6 MAC Filter Delete Command

Syntax:

```
ras> switch mac filter delete <port> <mac> [<mac> <mac> ...]
```

where

`<port>`	=	The number of a DSL port.

`<mac>`	=	The source MAC address in "00:a0:c5:12:34:56" format.

This command removes a configured source MAC address from the DSL port that you specify.

The following example removes the source MAC address of 00:a0:c5:12:34:56 from the MAC filter for DSL port 5.

Figure 172 MAC Filter Delete Command Example

```
ras> switch mac filter delete 5 00:a0:c5:12:34:56
```

50.3 MAC Count Commands

Use MAC count commands to limit how many MAC addresses may be dynamically learned. MAC count commands are listed next. When the MAC filter accept mode is enabled (see Section 50.2 on page 347), the AAM1212 ignores the MAC count setting and accepts all of the MAC addresses listed for the port in the MAC filter settings.

50.3.1 MAC Count Show Command

Syntax:

```
ras> switch mac count show [portlist]
```

where

`[portlist]`	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.

This command displays the MAC count settings on the specified DSL port(s) or on all DSL ports if no port is specified.

The following example displays the MAC count settings for DSL port 4.

Figure 173 MAC Count Show Command Example

```
ras> switch mac count show 4
port status count
---- ------ -----
   4   V      128
```

50.3.2 MAC Count Enable Command

Syntax:

```
ras> switch mac count enable <portlist>
```

where

`<portlist>`	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.

This command enables the MAC count filter on the specified DSL port(s). When the MAC filter accept mode is enabled (see Section 50.2 on page 347), the AAM1212 ignores the MAC count setting and accepts all of the MAC addresses listed for the port in the MAC filter settings.

The following example turns on the MAC count filter on DSL port 4.

Figure 174 MAC Count Enable Command Example

```
ras> switch mac count enable 4
```

50.3.3 MAC Count Disable Command

Syntax:

```
ras> switch mac count disable <portlist>
```

where

`<portlist>`	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.

This command disables the MAC filtering feature on the specified DSL port(s).

The following example turns off the MAC count filter on DSL port 4.

Figure 175 MAC Count Disable Command Example

```
ras> switch mac count disable 4
```

50.3.4 MAC Count Set Command

Syntax:

```
ras> switch mac count set <portlist> <count>
```

where

`<portlist>`	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.
`<count>`	=	Set the limit for how many MAC addresses that a port may dynamically learn. For example, if you are configuring port 2 and you set this field to "5", then only five devices with dynamically learned MAC addresses may access port 2 at any one time. A sixth device would have to wait until one of the five learned MAC addresses ages out. The valid range is from "1" to "128".

This command sets the limit for how many MAC addresses may be dynamically learned on the specified DSL port(s).

The following example sets the MAC count filter to allow up to 50 MAC addresses to be dynamically learned on DSL port 7.

Figure 176 MAC Count Set Command Example

```
ras> switch mac count set 7 50
```

51

IGMP Commands

This chapter describes the IGMP snooping and filtering commands.

51.1 Multicast Overview

See Chapter 18 on page 167 for background information on this feature.

51.2 IGMP Snoop Commands

Use the IGMP snoop commands to enable or disable IGMP proxy or IGMP snooping.

51.2.1 IGMP Snoop Show Command

Syntax:

```
ras> switch igmpsnoop show
```

This command displays the IGMP mode (proxy, snooping or disabled).

The following is an example.

Figure 177 IGMP Snoop Show Command Example

```
ras> switch igmpsnoop show
IGMP Snooping/Proxy is Disable
```

51.2.2 IGMP Snoop Enable Command

Syntax:

```
ras> switch igmpsnoop enable <proxy|snooping>
```

This command turns on IGMP proxy or snooping. Use proxy to have the device use IGMP proxy. Use IGMP snooping to have the device passively learn multicast groups.

The following example sets the device to use IGMP proxy.

Figure 178 IGMP Snoop Enable Command Example

```
ras> switch igmpsnoop enable proxy
```

51.2.3 IGMP Snoop Disable Command

Syntax:

```
ras> switch igmpsnoop disable
```

This command turns off IGMP proxy or snooping.

The following example sets the device to not use IGMP proxy or snooping.

Figure 179 IGMP Snoop Disable Command Example

```
ras> switch igmpsnoop disable
```

51.3 IGMP Filter Commands

Use the IGMP filter commands to define IGMP filter profiles and assign them to DSL ports.

IGMP filter profiles allow you to control access to IGMP multicast groups. You can have a service available to a specific IGMP multicast group. You can configure an IGMP filter profile for an IGMP multicast group that has access to a service (like a SIP server for example). Then you can assign the IGMP filter profile to DSL ports that are allowed to use the service.

51.3.1 IGMP Filter Show Command

Syntax:

```
ras> switch igmpfilter show [portlist]
```

where

`[portlist]`	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.

This command displays which IGMP filter profile a DSL port(s) is using.

The following example displays which IGMP filter profile DSL port 5 is using.

Figure 180 IGMP Filter Show Command Example

```
ras> switch igmpfilter show 5
port                           profile
--------------------------------------
   9                             DEFVAL
```

51.3.2 IGMP Filter Set Command

Syntax:

```
ras> switch igmpfilter set [<port>|*] <name>
```

where

`[<port>|*]`	=	You can specify a single DSL port <1> or all DSL ports <*>.
`<name>`	=	The name of an IGMP filter profile.

This command sets a DSL port(s) to use an IGMP filter profile.

The following example sets DSL port 5 to use the voice IGMP filter profile.

Figure 181 IGMP Filter Set Command Example

```
ras> switch igmpfilter set 5 voice
```

51.3.3 IGMP Filter Profile Set Command

Syntax:

```
ras> switch igmpfilter profile set <name> <index> <startip> <endip>
```

where

`<name>`	=	Specify a name to identify the IGMP filter profile (you cannot change the name of the DEFVAL profile). You can use up to 31 ASCII characters; spaces are not allowed.
`<index>`	=	The number (1~16) to identify a multicast IP address range.
`<startip>`	=	Type the starting multicast IP address for a range of multicast IP addresses that you want to belong to the IGMP filter profile.

`<endip>`	=	Type the ending multicast IP address for a range of IP addresses that you want to belong to the IGMP filter profile. If you want to add a single multicast IP address, enter it in both the **Start IP** and **End IP** fields.

This command configures an IGMP filter profile.

The following example configures an IGMP filter profile named voice with a range of multicast IP addresses (index 1) from 224.1.1.10 to 224.1.1.44.

Figure 182 IGMP Filter Profile Set Command Example

```
ras> switch igmpfilter profile set test1 1 224.1.1.10 224.1.1.44
```

51.3.4 IGMP Filter Profile Delete Command

Syntax:

```
ras> switch igmpfilter profile delete <name>
```

where

`<name>`	=	The name of an IGMP filter profile.

This command removes an IGMP filter profile.

The following example removes the voice IGMP filter profile.

Figure 183 IGMP Filter Profile Delete Command Example

```
ras> switch igmpfilter profile delete voice
```

51.3.5 IGMP Filter Profile Show Command

Syntax:

```
ras> switch igmpfilter profile show [<name>|*]
```

where

`[<name>|*]`	=	The name of an IGMP filter profile or all of the IGMP filter profiles <*>.

This command displays an IGMP filter profile’s settings.

The following example displays the voice IGMP filter profile's settings.

Figure 184 IGMP Filter Show Command Example

```
ras> switch igmpfilter profile show voice
                          profile  index          startip            endip
----------------------------------------------------------------------------
                            voice      1       224.1.1.10       224.1.1.44
                            voice      2          0.0.0.0          0.0.0.0
                            voice      3          0.0.0.0          0.0.0.0
                            voice      4          0.0.0.0          0.0.0.0
                            voice      5          0.0.0.0          0.0.0.0
                            voice      6          0.0.0.0          0.0.0.0
                            voice      7          0.0.0.0          0.0.0.0
                            voice      8          0.0.0.0          0.0.0.0
                            voice      9          0.0.0.0          0.0.0.0
                            voice     10          0.0.0.0          0.0.0.0
                            voice     11          0.0.0.0          0.0.0.0
                            voice     12          0.0.0.0          0.0.0.0
                            voice     13          0.0.0.0          0.0.0.0
                            voice     14          0.0.0.0          0.0.0.0
                            voice     15          0.0.0.0          0.0.0.0
                            voice     16          0.0.0.0          0.0.0.0
```

51.4 IGMP Bandwidth Commands

Use the IGMP bandwidth commands to set up bandwidth budgets for specific multicast channels.

51.4.1 IGMP Bandwidth Default Command

Syntax:

```
ras> switch igmpsnoop bandwidth default <bandwidth>
```

where

`<bandwidth>`	=	Allowed bandwidth between 1 and 1000 000 kbps (kilo bits per second).

This command sets the default bandwidth for multicast channels for which you have not configured bandwidth requirements yet. Multicast bandwidth settings on channels (using the `switch igmpsnoop bandwidth set` command) have higher priority over this default setting.

51.4.2 IGMP Bandwidth Set Command

Syntax:

```
ras> switch igmpsnoop bandwidth set <index> <start-mcast-ip> <end-mcast-ip>
<bandwidth>
```

where

<index>	=	1..96; a unique number for this setting.
<start-mcast-ip>	=	224.0.0.0..239.255.255.255; the beginning of the multicast range.
<end-mcast-ip>	=	224.0.0.0..239.255.255.255; the end of the multicast range. It must be greater than <start-mcast-ip>.
<bandwidth>	=	1..100000, in units of kbps

This command configures bandwidth allocation for the multicast channel(s). For multicast channel(s) for which you have not configured bandwidth settings, the default multicast bandwidth setting applies (see the `switch igmpsnoop bandwidth default` command).

51.4.3 IGMP Bandwidth Delete Command

Syntax:

```
ras> switch igmpsnoop bandwidth delete <index>
```

where

<index>	=	1..96; a unique number for this setting.

This command removes the specified multicast bandwidth configuration profile.

51.5 IGMP Bandwidth Port Commands

Use the IGMP bandwidth port commands to set up bandwidth budgets for multicast traffic on specific ports.

51.5.1 IGMP Bandwidth Port Disable Command

Syntax:

```
ras> switch igmpsnoop bandwidth port disable <portlist>
```

where

`<portlist>`	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.

This command deactivates multicast bandwidth settings of the specified port.

51.5.2 IGMP Bandwidth Port Enable Command

Syntax:

```
ras> switch igmpsnoop bandwidth port enable <portlist>
```

where

`<portlist>`	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.

This command activates multicast bandwidth setting on the specified port.

51.5.3 IGMP Bandwidth Port Set Command

Syntax:

```
ras> switch igmpsnoop bandwidth port set <portlist> <bandwidth>
```

where

`<portlist>`	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.
`<bandwidth>`	=	1..100000, in units of kbps

This command sets the bandwidth allowed for multicast traffic on the specified port(s). It does not automatically enable it, however.

51.5.4 IGMP Bandwidth Port Show Command

Syntax:

```
ras> switch igmpsnoop bandwidth port show <portlist>
```

where

`<portlist>`	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.

This command displays the multicast bandwidth setting on the specified port(s) and whether or not this setting is active. The following example displays the bandwidth budget for port 1.

Figure 185 IGMP Bandwidth Port Show Command Example

```
ras> switch igmpsnoop bandwidth port show 1
 port  enable   bandwidth
------ ------ -----------
    1     -        4096
```

51.6 IGMP Count Limit Commands

Use these commands to limit the number of IGMP groups a subscriber on a port can join. This allows you to control the distribution of multicast services (such as content information distribution) based on service plans and types of subscription.

IGMP count is useful for ensuring the service quality of high bandwidth services like video or Internet Protocol television (IPTV). IGMP count can limit how many channels (IGMP groups) the subscriber connected to a DSL port can use at a time. If each channel requires 4~5 Mbps of download bandwidth, and the subscriber's connection supports 11 Mbps, you can use IGMP count to limit the subscriber to using just 2 channels at a time. This also effectively limits the subscriber to using only two IPTVs with the DSL connection.

51.6.1 IGMP Count Disable Command

Syntax:

```
ras> switch igmpsnoop igmpcount disable <portlist>
```

where

`<portlist>`	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.

This command turns off the IGMP count limit for the specified DSL port(s).

The following command turns off the IGMP count limit for port 4.

Figure 186 IGMP Count Disable Command Example

```
ras> switch igmpsnoop igmpcount disable 4
```

51.6.2 IGMP Count Enable Command

Syntax:

```
ras> switch igmpsnoop igmpcount enable <portlist>
```

where

`<portlist>`	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.

This command turns on the IGMP count limit for the specified DSL port(s).

The following command turns on the IGMP count limit for port 4.

Figure 187 IGMP Count Enable Command Example

```
ras> switch igmpsnoop igmpcount enable 4
```

51.6.3 IGMP Count Set Command

Syntax:

```
ras> switch igmpsnoop igmpcount set <portlist> <count>
```

where

`<portlist>`	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.
`<count>`	=	0..16; the maximum number of IGMP groups subscribers on the specified port(s) can join.

This command sets the IGMP count limit for the specified DSL port(s).

The following command sets a IGMP count limit of 2 for port 4.

Figure 188 IGMP Count Set Command Example

```
ras> switch igmpsnoop igmpcount set 4 2
```

51.6.4 IGMP Count Show Command

Syntax:

```
ras> switch igmpsnoop igmpcount show [portlist]
```

where

`[portlist]`	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.

This command displays the IGMP count limit setting status for the specified DSL port(s). The following example displays the IGMP count limit settings for ports 1-5.

Figure 189 IGMP Count Show Command Example

```
ras> switch igmpsnoop igmpcount show 1~5
port enable count
---- ------ -----
   1   -        5
   2   -        5
   3   -        5
   4   -        5
   5   -        5
```

51.7 IGMP Snoop Statistics Commands

Use the IGMP Snoop Statistics commands to display current IGMP settings and statistics.

51.7.1 IGMP Snoop Info Statistics Command

Syntax:

```
ras> statistics igmpsnoop info [clear]
```

This command displays the current IGMP settings and the number of IGMP-related packets received. The following figure shows an example.

Figure 190 IGMP Snoop Info Statistics Command Example

```
ras> statistics igmpsnoop info
IGMP Snooping/Proxy is Disable
number of query    = 0
number of report   = 0
number of leave    = 0
number of groups   = 0
```

51.7.2 IGMP Group Statistics Command

Syntax:

```
ras> statistics igmpsnoop group [<vid> [<mcast_ip>]]
```

where

<vid>	=	The VLAN ID [1 – 4094].
<mcast_ip>	=	The multicast IP address.

This command displays the information about IGMP groups learned on the system, specified VLAN, or specified multicast address on the specified VLAN(s).

Figure 191 IGMP Group Statistics Command Example

```
ras> statistics igmpsnoop group
[group info]
group            vid port
--------------- ---- ------------------------------------------------ --
```

51.7.3 IGMP Port Info Statistics Command

Syntax:

```
ras> statistics igmpsnoop port info [portlist]
```

where

[portlist]	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.

This command displays the number of IGMP-related packets received on the specified port(s). The following figure shows the number of IGMP packets for port 1.

Figure 192 IGMP Port Info Statistics Command Example

```
ras> statistics igmpsnoop port info 1
port  group_cnt query_cnt  join_cnt leave_cnt
----- --------- --------- --------- ---------
    1         0         0         0         0
```

51.7.4 IGMP Port Group Statistics Command

Syntax:

```
  ras> statistics igmpsnoop port group <portlist>
```

where

<portlist>	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.

This command displays the IGMP groups a port joins. The following figure shows an example for port 1.

Figure 193 IGMP Port Group Statistics Command Example

```
ras> statistics igmpsnoop port group 1
port   vid mcast_ip        source ip
----- ---- --------------- ---------------
```

51.8 Multicast VLAN Commands

Use these commands to configure VLAN multicast settings and set multicast port members.

Multicast VLAN allows one single multicast VLAN to be shared among different subscriber VLANs on the network. This improves bandwidth utilization by reducing multicast traffic in the subscriber VLANs and simplifies multicast group management.

51.8.1 Multicast VLAN Set Command

Syntax:

```
  ras> switch igmpsnoop mvlan set <vid> <portlist>:<F<T|U>|X>
[<portlist>:<F<T|U>|X> ...] [name]
```

where

`<vid>`	=	The VLAN ID [1 – 4094].
`<portlist>`	=	You can specify a single port: <1>, all ports: <*>, a list of ports: <1,3,enet1>, you can also include a range of ports: <1,5,6~10,enet1,enet2>.
`<F<T|U>|`	=	The <F> stands for a fixed registrar administration control flag and registers a <port #> to the static VLAN table with <vid>. For a fixed port, you also have to specify <T|U>, the tag control flag. <T> has the device add an IEEE 802.1Q tag to frames going out through this port(s). <U> has the device send frames out through this port(s) without an IEEE 802.1Q tag.
`|X>`	=	This is the registrar administration control flag. <X> stands for forbidden and blocks a <port #> from joining the static VLAN table with <vid>.
`[name]`	=	A name to identify the SVLAN entry.

This command creates a multicast VLAN and sets the allowed/blocked port member(s).

This command is similar to the command to create a regular VLAN. See Section 49.4.4 on page 341 for examples and more information.

51.8.2 Multicast VLAN Delete Command

Syntax:

```
ras> switch igmpsnoop mvlan delete <vlanlist>
```

where

`<vlanlist>`	=	You can specify a single VLAN: <1>, all VLAN: <*>, a list of VLAN: <1,3>, you can also include a range of VLAN: <1,5,6~10>.

This command removes the specified multicast VLAN configuration(s).

51.8.3 Multicast VLAN Disable Command

Syntax:

```
ras> switch igmpsnoop mvlan disable <vid>
```

where

`<vid>` = The multicast VLAN ID [1 – 4094].

This command deactivates the specified multicast VLAN. The following example disables multicast VLAN 12.

Figure 194 Multicast VLAN Disable Command Example

```
ras> switch igmpsnoop mvlan disable 12
```

51.8.4 Multicast VLAN Enable Command

Syntax:

```
ras> switch igmpsnoop mvlan enable <vid>
```

where

`<vid>` = The multicast VLAN ID [1 – 4094].

This command activates the specified multicast VLAN.

51.8.5 Multicast VLAN Show Command

Syntax:

```
ras> switch igmpsnoop mvlan show <vlanlist>
```

where

`<vlanlist>` = You can specify a single VLAN: <1>, all VLAN: <*>, a list of VLAN: <1,3>, you can also include a range of VLAN: <1,5,6~10>.

This command displays the current multicast VLAN settings. In the state column, “-” indicates the multicast VLAN is not active while “V” indicates the multicast VLAN is active.

Figure 195 Multicast VLAN Show Command Example

```
ras> switch igmpsnoop mvlan show 1
 vid name             F:fixed X:forbidden    U:untag T:tag
---- ---------------- ----------------------------------------
```

51.8.6 Multicast VLAN Group Set Command

Syntax:

```
ras> switch igmpsnoop mvlan group set <vid> <index> <start-mcast-ip> <end-mcast-ip>
```

where

`<vid>`	=	The multicast VLAN ID [1 – 4094].
`<index>`	=	1..16; a unique number for this setting.
`<start-mcast-ip>`	=	Start of the multicast IP address range.
`<end-mcast-ip>`	=	End of the multicast IP address range.

This command creates a multicast VLAN group. The following example creates a multicast VLAN with VID 10 and group index 1. The multicast address range is 224.224.224.1 ~ 224.224.224.10.

Figure 196 Multicast VLAN Group Set Command Example

```
ras> switch igmpsnoop mvlan group set 10 1 224.224.224.1
224.224.224.10
```

51.8.7 Multicast VLAN Group Delete Command

Syntax:

```
ras> switch igmpsnoop mvlan group delete <vid> <index>
```

where

`<vid>`	=	The multicast VLAN ID [1 – 4094].
`<index>`	=	1..16; a unique number for this setting.

This command removes the specified multicast VLAN group setting.

51.8.8 Multicast VLAN Group Show Command

Syntax:

```
ras> switch igmpsnoop mvlan group show [<vid>]
```

where

`<vid>`	=	The multicast VLAN ID [1 – 4094].

This command displays a multicast to VLAN translation entry.

52

Packet Filter Commands

This chapter describes the packet filter commands.

52.1 Packet Filter Commands

Use the following packet filter commands to filter out specific types of packets on specific ports.

52.1.1 Packet Filter Show Command

Syntax:

```
ras> switch pktfilter show [portlist]
```

where

`[portlist]`	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.

This command displays the packet type filter settings on the specified DSL port(s) or on all DSL ports if no port is specified.

The following example displays the packet type filter settings for DSL ports 1 and 2. "V" displays for the packet types that the AAM1212 is to accept on the port. "-" displays for packet types that the AAM1212 is to reject on the port (packet types that are not listed are accepted). When you use PPPoE only,"#" appears for all of the packet types. With PPPoE only, the AAM1212 rejects all packet types except for PPPoE (packet types that are not listed are also rejected).

Figure 197 Packet Filter Show Command Example

```
ras> switch pktfilter show 1~2
V: pass through, -: filter out, #:Don't care
E: Enable, D: Disable
port pppoe ip arp netbios dhcp eapol igmp  | PPPoE-Only
---- ----- -- --- ------- ---- ----- ----  | ----------
   1    V   V   V      V     V     V    V    |     D
   2    V   V   V      V     V     V    V    |     D
```

52.1.2 Packet Filter Set Command

Syntax:

```
ras> switch pktfilter set <portlist> [filter]
```

where

`<portlist>`	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.
`[filter]`	=	[pppoe] Reject PPPoE packets. (Point-to-Point Protocol over Ethernet) relies on PPP and Ethernet. PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as a single DSL line, wireless device or cable modem. [ip] Reject IP packets. Internet Protocol. The underlying protocol for routing packets on the Internet and other TCP/IP-based networks. [arp] Reject ARP packets. Address Resolution Protocol is a protocol for mapping an Internet Protocol address (IP address) to a physical computer address that is recognized in the local network. [netbios] Reject NetBIOS packets. (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. [dhcp] Reject DHCP packets. Dynamic Host Configuration Protocol automatically assigns IP addresses to clients when they log on. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses, for a period of time, which means that past addresses are "recycled" and made available for future reassignment to other systems. [eapol] Reject EAPol packets. EAP (Extensible Authentication Protocol, RFC 2486) over LAN. EAP is used with IEEE 802.1x to allow additional authentication methods (besides RADIUS) to be deployed with no changes to the access point or the wireless clients. [igmp] Reject IGMP packets. Internet Group Multicast Protocol is used when sending packets to a specific group of hosts. [none] Accept all packets.

This command sets the packet type filter for the specified DSL port(s).

The following example sets DSL port 5 to reject ARP, PPPoE and IGMP packets.

Figure 198 Packet Filter Set Command Example

```
ras> switch pktfilter set 5 arp pppoe igmp
```

52.1.3 Packet Filter PPPoE Only Command

Syntax:

```
ras> switch pktfilter pppoeonly <portlist>
```

This command sets the AAM1212 to allow only PPPoE traffic on the specified DSL port(s). The system will drop any non-PPPoE packets.

The following example sets DSL port 1 to accept only PPPoE packets.

Figure 199 Packet Filter PPPoE Only Command Example

```
ras> switch pktfilter pppoeonly 1
```

53

IP Commands

This chapter shows you how to use the (standard shell) IP commands to configure the IP (Internet Protocol) parameters.

53.1 IP Commands Introduction

Use the AAM1212's management IP addresses to manage it through the network.

53.2 IP Settings and Default Gateway

Use the following command sequence to set the AAM1212's IP settings for the Ethernet 1 and 2, and DSL ports, VID and default gateway. With the Ethernet 1 and 2, and DSL ports, you must connect to the AAM1212 through a port that is a member of the management (CPU) VLAN in order to perform in-band management.

Figure 200 IP Settings and Default Gateway Address Commands

```
ras> ip set <new ip address> [</netmask>]
ras> ip gateway <ip>
ras> config save
```

where

`<new ip address>`	=	The IP address you want to configure for the AAM1212.
`</netmask>`	=	The bit number of the subnet mask of the IP address you want to configure for AAM1212's uplink, downlink and AAM1212 DSL ports. To find the bit number, convert the subnet mask to binary and add all of the 1's together. Take "255.255.255.0" for example. 255 converts to eight 1's in binary. There are three 255's, so add three eights together and you get the bit number (24).
`<ip>`	=	The default gateway IP address you want to configure for the AAM1212.

The first command changes the IP settings for the AAM1212's uplink, downlink and AAM1212 DSL ports. If you don't enter the subnet mask, the system automatically computes the subnet mask.

The second command changes the default gateway (next hop). This tells the AAM1212 where to send packets that have a destination IP address that is not on the same subnet as the AAM1212's IP address.

The third command saves the new configuration to the nonvolatile memory.

For example, use the following command sequence sets the AAM1212 to have 192.168.1.3 as the IP address, 255.255.255.0 for the subnet mask and 192.168.1.233 for the default gateway.

Figure 201 IP Settings and Default Gateway Address Command Example

```
ras> ip set 192.168.1.3/24
ras> ip gateway 192.168.1.233
ras> config save
```

The AAM1212 leaves the factory with a default management IP address of 192.168.1.1 and a subnet mask of 255.255.255.0, (ff:ff:ff:00 in hexadecimal notation), and the default gateway set at 192.168.1.254. Make sure that you configure the IP parameters correctly before you connect a AAM1212 to the network, otherwise, you may interrupt services already running.

53.3 General IP Commands

The following is a list of general IP commands that help with the management of the IP parameters.

53.3.1 Show

Syntax:

```
ras> ip show [inband|outband]
```

Use the command to display the current management IP settings.

53.3.2 Ping Command

Syntax:

```
ras> ip ping <ip> [count]
```

This is an IP facility to check for network functionality by sending an echo request to another IP host and waiting for the reply.

53.3.3 Route Set Command

Syntax:

```
ras> ip route set <dst ip>[/netmask] <gateway ip> [metric] <name>
ras> ip route set default            <gateway ip> <metric>
```

where

`<dst ip>`	=	The destination IP address of packets that this static route is to route.
`[/netmask]`	=	The destination subnet mask of packets that this static route is to route.
`<gateway ip>`	=	The IP address of the gateway that you want to send the packets through.
`[metric]`	=	The metric (hop count) of this static route.
`<name>`	=	A name to identify this static route. Up to 31 ASCII characters. Spaces and tabs are not allowed.
`default`	=	Use this to configure the AAM1212's default route.

This command defines a new, static IP forwarding route or edits an existing one.

53.3.4 Route Delete Command

Syntax:

```
ras> ip route delete <dst ip>[/netmask]
```

where

`<dst ip>`	=	The destination IP address of packets to which this static route applies.
`[/netmask]`	=	The destination subnet mask of packets to which this static route applies.

This command removes a static, IP forwarding route.

53.3.5 Route Show Command

Syntax:

```
ras> ip route show
```

This command displays the AAM1212's routing table.

An example is shown next.

Figure 202 Route Show Command Example

```
ras> ip route show
index dest            gateway         metric name
----- --------------- --------------- ------ --------------------------------
1     192.168.1.0/24  192.168.1.1          1
2     default         192.168.1.254        1
```

53.3.6 ARP Show Command

Syntax:

```
ras> ip arp show
```

This command displays the AAM1212's IP Address Resolution Protocol table. This is the list of IP addresses and matching MAC addresses that the AAM1212 has resolved.

An example is shown next.

Figure 203 ARP Show Command Example

```
ras> ip arp show
ip              mac address
---------------  -----------------
172.23.14.254  00:0c:db:30:ac:00
172.23.15.254  00:0c:db:30:ac:00
```

53.3.7 ARP Flush Command

Syntax:

```
ras> ip arp flush
```

This command clears the AAM1212's IP Address Resolution Protocol table.

53.4 Statistics IP Command

Syntax:

```
ras> statistics ip
```

This command shows the statistics for the CPU IP traffic.

An example is shown next.

Figure 204 Statistics IP Command Example

```
ras> statistics ip
[Ethernet]
inet     : 172.23.14.253      netmask: 0.0.0.0
broadcast: 172.23.255.255     mtu: 1500
in octet   :   10728504  in unicast :       738  in multicast    :     232488
in discard :          0  in error   :         0  in unknown proto:          0
out octet  :      41361  out unicast:       861  out multicast   :          0
out discard:          0  out error  :         0
```

54

G.Bond Commands

This chapter shows how to set up port bonding settings on your device.

54.1 G.bond Commands

G.bond (also known as port bonding) allows subscribers to connect to an ISP using data streams spread over multiple DSL lines. The total available bandwidth for the subscriber then becomes the sum of the bandwidth available for each of the subscriber's line connections. As well as extra bandwidth, additional DSL lines also provide backup support.

54.1.1 adsl gbond set Command

Syntax:

```
adsl gbond set <bond_name> <portlist>
where
```

<bond_name>	=	A descriptive name for the gbond group of DSL lines.
<portlist>	=	The ports that connect the DSL lines on which gbond is configured.

This command sets up a gbond group on the specified group of ports. The following is an example.

```
ras> adsl gbond set group2 3,4
```

54.1.2 adsl gbond show Command

Syntax:

```
adsl gbond show [<bond_name>]
where
```

<bond_name>	=	A descriptive name for the gbond group of DSL lines.

This command displays gbond settings on the specified group of ports. The following is an example.

```
ras> adsl gbond show
name                            port list
------------------------------- ---------
group1                                1,2
group2                                3,4
group3                                5,6
```

54.1.3 port gbond delete Command

Syntax:

```
adsl gbond delete <bond_name>
where
```

<bond_name> = A descriptive name for the gbond group of DSL lines.

This command deletes the specified gbond group. The following is an example.

```
ras> adsl gbond delete group3
ras> adsl gbond show
name                            port list
------------------------------- ---------
group1                                1,2
group2                                3,4
```

55

Firmware and Configuration File Maintenance

This chapter tells you how to upload a new firmware and/or configuration file for the AAM1212.

55.1 Firmware and Configuration File Maintenance Overview

The AAM1212's built-in FTP server allows you to use any FTP client (for example, ftp.exe in Windows) to upgrade AAM1212 firmware or configuration files. The firmware or configuration file upgrade is done during operation (run-time).

Note: Do not turn off the power to the AAM1212 during the file transfer process, as it may permanently damage your AAM1212.

Note: The AAM1212 automatically restarts when the upgrade process is complete.

55.2 Filename Conventions

The configuration file (called config-0) contains the factory default settings in the menus such as password, IP address, VLANs and so on. The configuration file arrives with a "rom" filename extension.

The OS (Operating System) firmware (sometimes referred to as the "ras" file) has a "bin" filename extension. With many FTP and clients, the filenames are similar to those shown next.

Figure 205 FTP Put Configuration File Example

```
ftp> put firmware.bin ras
```

This is a sample from a FTP session to transfer the computer file `firmware.bin` to the AAM1212.

Figure 206 FTP Get Configuration File Example

```
ftp> get config-0 config.txt
```

This is a sample from a FTP session to transfer the AAM1212's current configuration file (including the configuration files of all the AAM1212) to the computer file `config.txt`.

If your FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the AAM1212 only recognizes "config-0" and "ras". Be sure you keep unaltered copies of the files for later use.

The following table is a summary. Please note that the internal filename refers to the filename on the AAM1212 and the external filename refers to the filename not on the AAM1212, that is, on your computer, local network or FTP site and so the name (but not the extension) may vary. After uploading new firmware, use the sys version command on the AAM1212 to confirm that you have uploaded the correct firmware version.

Table 104 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	`config-0`	`*.dat`	This is the configuration filename for the AAM1212.
Firmware	`ras`	`*.bin`	This is the Operating System firmware on the AAM1212.

55.3 Editable Configuration File

The configuration file can be downloaded as a plain-text (ASCII) file. Edits to the configuration can be made to this file before it is uploaded again to the AAM1212.

Note: You can change the ".dat" file to a ".txt" file and still upload it back to the AAM1212.

Note: Do not upload any invalid files to the AAM1212's configuration file, as it may permanently damage your AAM1212.

55.3.1 Editable Configuration File Backup

Configure your system, and then use FTP to backup the plain-text configuration file onto your computer. Do the following to backup the configuration file:

Use an FTP client to connect to the AAM1212.

Figure 207 Example: Use an FTP Client to Connect to the AAM1212

```
C:\> ftp <AAM1212 IP address>
Type your user name and press [ENTER].
User (172.23.15.86:(none)): admin
```

Enter the management password (`1234` by default).

Figure 208 Example: Enter the Management Password

```
Password: 1234
230 Logged in
```

Use `get` to transfer the configuration file to the computer. The configuration file on the system (that you want to backup to the computer) is named `config-0`.

Figure 209 Example: Get the Configuration File config-0

```
ftp> get config-0
```

Quit FTP.

Figure 210 Example: Close FTP Client

```
ftp> quit
```

55.3.2 Edit Configuration File

Open the `config-0` file via Notepad (see the following example) and edit to a desired configuration.

Note: Ensure that any changes you make to the commands in the configuration file correspond to the commands documented in this User's Guide. The wrong configuration file or an incorrectly configured configuration file can render the device inoperable.

Figure 211 Configuration File Example

```
#### sysinfo
sys info hostname ""
sys info location ""
sys info contact ""
#### snmp
sys snmp getcommunity public
sys snmp setcommunity public
sys snmp trapcommunity public
sys snmp trustedhost 0.0.0.0
sys snmp trapdst set 1 0.0.0.0 162
sys snmp trapdst set 2 0.0.0.0 162
sys snmp trapdst set 3 0.0.0.0 162
sys snmp trapdst set 4 0.0.0.0 162
#### server
sys server enable telnet
sys server enable ftp
sys server enable web
sys server enable icmp
sys server port telnet 23
sys server port ftp 21
--------------- Snip ------------------------------------------------------
-------------
```

Note: The `sys user set admin` command is encrypted and you cannot edit it in a text editor. Attempting to edit it and upload it to the AAM1212 will lock you out after the system restarts. If this happens you will have to use the console port to restore the default configuration file, and all of your configuration changes will be lost.

55.3.3 Editable Configuration File Upload

You can upload the configuration file by following the steps below.

Use an FTP client to connect to the AAM1212.

Figure 212 Example: Use an FTP Client to Connect to the AAM1212

```
C:\> ftp <AAM1212 IP address>
Type your user name and press [ENTER].
User (172.23.15.86:(none)): admin
```

Enter the management password (`1234` by default).

Figure 213 Example: Enter the Management Password

```
Password: 1234
230 Logged in
```

Use `put` to transfer the configuration file from the computer. The configuration file on the system is named `config-0`.

Figure 214 Example: Upload the Configuration File config-0

```
ftp> put xxx.dat config-0
```

Quit FTP.

Figure 215 Example: Close FTP Client

```
ftp> quit
```

Wait for the update to finish. The system restarts automatically.

55.4 Firmware File Upgrade

Use the following procedure to upload firmware to the AAM1212.

Use an FTP client to connect to the AAM1212.

Figure 216 Example: Use an FTP Client to Connect to the AAM1212

```
C:\> ftp <AAM1212 IP address>
Type your user name and press [ENTER].
User (172.23.15.86:(none)): admin
```

Enter the management password (`1234` by default).

Figure 217 Example: Enter the Management Password

```
Password: 1234
230 Logged in
```

Transfer the firmware file to the AAM1212. The firmware file on your computer (that you want to put onto the AAM1212 is named `firmware.bin`. The internal firmware file on the AAM1212 is named `ras`.

Figure 218 Example: Transfer the Firmware File

```
ftp> put firmware.bin ras
```

Quit FTP.

Figure 219 Example: Close FTP Client

```
ftp> quit
```

Wait for the update to finish. The AAM1212 restarts automatically.

56

SNMP

This chapter covers Simple Network Management Protocol (SNMP) with the AAM1212.

56.1 SNMP Commands

Use these commands to configure SNMP settings. See Chapter 34 on page 229 for more information about SNMP.

56.1.1 Get Community Command

Syntax:

```
ras> sys snmp getcommunity <community>
```

where

`<community>`	=	The password for the incoming `Get-` and `GetNext-` requests from the management station.

Enter this command with the community to set the password.

56.1.2 Set Community Command

Syntax:

```
ras> sys snmp setcommunity <community>
```

where

`<community>`	=	The password for the incoming `Set-` requests from the management station.

Enter this command with the community to set the password.

56.1.3 Trusted Host Set Command

Syntax:

```
ras> sys snmp trusthost <ip>
```

where

`<ip>`	=	The IP address of a trusted host.

Use this command to add the host IP address to the list of trusted hosts. If you enter a trusted host, your AAM1212 will only respond to SNMP messages from this address. If you leave the trusted host set to 0.0.0.0 (default), the AAM1212 will respond to all SNMP messages it receives, regardless of source.

56.1.4 Trap Community Command

Syntax:

```
ras> sys snmp trapcommunity <community>
```

where

`<community>`	=	The password sent with each trap to the SNMP manager.

Enter this command with the community to set the password.

56.1.5 Trap Destination Set Command

Syntax:

```
ras> sys snmp trapdst set <index> <ip> [<port>]
```

where

`<index>`	=	The number of the trap server (1~4).
`<ip>`	=	The IP address of the trap server.
`[<port>]`	=	The port number upon which the trap server listens for SNMP traps. The AAM1212 uses the default of 162 if you do not specify a trap port.

Use this command specify the IP address (and port number) of a trap server to which the AAM1212 sends SNMP traps. If you leave the trap destination set to 0.0.0.0 (default), the AAM1212 will not send any SNMP traps.

56.1.6 Show SNMP Settings Command

Syntax:

```
ras> sys snmp show
```

This command displays the current SNMP get community, set community, trap community, trusted hosts and trap destination settings.

57

ADSL Commands

This chapter describes some of the commands that allow you to configure and monitor the DSL ports.

57.1 DSL Port Commands

Use these commands to configure the DSL ports. See Chapter 13 on page 107 for background information on DSL and ADSL.

57.1.1 DSL Port Show Command

Syntax:

```
ras> adsl show [portlist]
```

where

[portlist]	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.

This command shows the activation status, operational mode, maximum upstream and downstream rate settings, profile and name of each DSL port.

The following example displays information on DSL port 5.

Figure 220 DSL Port Show Command Example

```
ras> adsl show 5
port enable mode     up/downstream profile          name
---- ------ -------- ------------- ---------------- ----------------
   5    -     auto        512/  2048 DEFVAL           -
```

57.1.2 DSL Port Enable Command

Syntax:

```
ras> adsl enable <portlist>
```

where

`<portlist>`	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.

This command forcibly enables the specified DSL port(s).

57.1.3 DSL Port Disable Command

Syntax:

```
ras> adsl disable <portlist>
```

where

`<portlist>`	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.

This command forcibly disables the specified DSL port(s).

Note: The factory default of all ports is enabled.

57.1.4 DSL Port Profile Show Command

Syntax:

```
ras> adsl profile show [profile]
```

where

`<profile>`	=	A profile name.

This command displays the specified DSL profile or all DSL profiles if you do not specify one.

The following example displays the DSL DEFVAL profile.

Figure 221 DSL Profile Show Command Example

```
ras> adsl profile show DEFVAL
01. DEFVAL    latency mode: interleave
                    up stream down stream
                    --------- -----------
max rate    (kbps):       512        2048
min rate    (kbps):        32          32
latency delay (ms):         4           4
max margin    (db):        31          31
min margin    (db):         0           0
target margin (db):         6           6
up shift margin(db):       9           9
down shift margin(db):       3           3
```

57.1.5 DSL Port Profile Set Command

Syntax:

```
ras> adsl profile set <profile> <fast|interleave[=<up delay>,<down delay>]>
  <up max rate> <down max rate>
  [<up target margin> <up min margin> <up max margin> <up min rate>
  <down target margin> <down min margin> <down max margin> <down min rate>
  <up down-shift margin> <up up-shift margin>
  <down down-shift margin> <down up-shift margin>]
```

where

`<profile>`	=	The descriptive name for the profile.
`<fast|interleave[=<up delay>,<down delay>]>`	=	The latency mode. With interleave, you must also define the upstream and downstream delay (1-255 ms). It is recommended that you configure the same delay for both upstream and downstream.
`<up max rate>`	=	The maximum DSL upstream transmission rate (64-4096 Kbps).
`<down max rate>`	=	The maximum DSL downstream transmission rate (64-32000 Kbps).
`<up target margin>`	=	The target DSL upstream signal/noise margin (0-31db).
`<up min margin>`	=	The minimum acceptable DSL upstream signal/noise margin (0-31db).
`<up max margin>`	=	The maximum acceptable DSL upstream signal/noise margin (0-31db).
`<up min rate>`	=	The minimum DSL upstream transmission rate (32-4096 Kbps).
`<down target margin>`	=	The target DSL downstream signal/noise margin (0-31db).

`<down min margin>`	=	The minimum acceptable DSL downstream signal/noise margin (0-31db).
`<down max margin>`	=	The maximum acceptable DSL downstream signal/noise margin (0-31db).
`<down min rate>`	=	The minimum DSL downstream transmission rate (32-32000 Kbps).
`<up down shift margin>`	=	The upstream down shift noise margin (0~31 in dB).
`<up up shift margin>`	=	The upstream up shift noise margin (0~31 in dB).
`<down down shift margin>`	=	The downstream down shift noise margin (0~31 in dB).
`<down up shift margin>]`	=	The downstream up shift noise margin (0~31 in dB).

The profile is a table that contains information on DSL line configuration. Each entry in this table reflects a parameter defined by a manager, which can be used to configure the DSL line.

Note that the default value will be used for any of the above fields that are omitted.

The upstream rate must be less than or equal to the downstream rate.

Even though you can specify arbitrary numbers in the profile set command, the actual rate is always a multiple of 32 Kbps. If you enter a rate that is not a multiple of 32 Kbps, the actual rate will be the next lower multiple of 32Kbps. For instance, if you specify 60 Kbps for a port, the actual rate for that port will not exceed 32 Kbps, and if you specify 66 Kbps, the actual rate will not be over 64Kbps.

The DSL up/down shift noise margins define the threshold that triggers rate adaptation. For example:

The target SNR is 6, and the up/down shift noise margins are 9/3.

If the signal becomes better and the SNR is higher than 9, rate adaptation is triggered and the line rate becomes higher

If the signal becomes bad and the SNR is lower than 3, rate adaptation is triggered and the line rate becomes lower.

The following example creates a premium profile (named gold) for providing subscribers with very high connection speeds and no interleave delay. It also sets the upstream target signal/noise margin to 5 db, the upstream minimum acceptable signal/noise margin to 0 db, the upstream maximum acceptable signal/noise margin to 30 db, the upstream minimum DSL transmission rate to 128 Kbps, the downstream target signal/noise margin to 5 db, the downstream minimum acceptable signal/noise margin to 0 db, the downstream maximum acceptable signal/noise margin to 30 db and the downstream minimum DSL transmission rate to 256Kbps.

The upstream down shift noise margin is 0 dB. The upstream up shift noise margin is 6 dB. The downstream down shift noise margin is 0 dB. The downstream up shift noise margin is 6 dB.

Figure 222 DSL Port Profile Set Command Example 1

```
ras> adsl profile set gold fast 1200 24000 5 0 30 128 5 0 30 256 0 6 0 6
```

This next example creates a similar premium profile (named `goldi`), except it sets an interleave delay of 16 ms for both upstream and downstream traffic.

Figure 223 DSL Port Profile Set Command Example 2

```
ras> adsl profile set goldi interleave=16,16 1200 24000 5 0 30 128 5 0 30 256
0 6 0 6
```

After you create a DSL profile, you can assign it to any of the DSL ports on the AAM1212.

57.1.6 DSL Port Profile Delete Command

Syntax:

```
ras> adsl profile delete <profile>
```

where

`<profile>` = A profile name.

This command allows you to delete an individual DSL profile by its name. You cannot delete a profile that is assigned to any of the DSL ports in the AAM1212. Assign a different profile to any DSL ports that are using the profile that you want to delete, and then you can delete the profile.

The following example deletes the gold DSL profile.

Figure 224 DSL Port Profile Delete Command Example

```
ras> adsl profile delete gold
```

57.1.7 DSL Port Profile Map Command

Syntax: (AAM1212-51)

```
  ras> adsl profile map <portlist> <profile>
-> <glite|gdmt|t1413|auto|adsl2|adsl2+>
```

Syntax: (AAM1212-53)

```
ras> adsl profile map <portlist> <profile>
-> <gdmt|etsi|auto|adsl2|adsl2+>
```

where

`<portlist>`	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.
`<profile>`	=	The profile that will define the settings of this port.
`<glite|gdmt|etsi|t1413|auto|adsl2|adsl2+>`	=	The ADSL operational mode. The AAM1212-51 and the AAM1212-53 have different choices.

This command assigns a specific profile to an individual port and sets the port's operational mode (or standard). The profile defines the maximum and minimum upstream/downstream rates, the target upstream/downstream signal noise margins, and the maximum and minimum upstream/downstream acceptable noise margins of all the DSL ports to which you assign the profile.

When set to auto, the port follows whatever mode is set on the other end of the line.

Note: When the mode is set to `auto`, the connection rates are governed by the negotiated operational mode regardless of the rates configured in the profile. For example, if the profile is set to use a rate of 18000 Kbps, that speed is only supported if the negotiated operational mode is ADSL 2+. Any other operational mode will limit the rate to what is supported by the specific standard.

When the mode is set to `auto` in the AAM1212-51, the `t1413` mode has been removed from the `auto` mode selection list. When a profile is assigned to a line in `auto` mode, the line will not go to showtime if the modem is configured in `t1413` mode only or if it is an old modem that only supports `t1413`. You have to explicitly configure the line in `t1413` mode to make the modem initialize.

The following example sets DSL port 1 to have the gold profile in G.dmt mode.

Figure 225 DSL Port Profile Delete Command Example

```
ras> adsl profile map 1 gold gdmt
```

57.1.8 DSL Port Name Command

Syntax:

```
ras> adsl name <portlist> <name>
```

where

`<portlist>`	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.
`<name>`	=	A descriptive name for the port. You can use up to 31 printable ASCII characters (including spaces and hyphens).

This command sets the name of a DSL port(s).

The following example sets DSL port 5 to have the name super.

Figure 226 DSL Port Name Command Example

```
ras> adsl name 5 super
```

57.1.9 DSL Port Tel Command

Syntax:

```
ras> adsl tel <portlist> <tel>
```

where

`<portlist>`	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.
`<tel>`	=	a DSL subscriber’s telephone number. You can use up to 15 ASCII characters (including spaces and hyphens).

This command records the telephone number of a DSL subscriber telephone number.

The following example records the telephone number 12345678 for DSL port 5.

Figure 227 DSL Port Tel Command Example

```
ras> adsl tel 5 12345678
```

57.1.10 DSL Port Loopback Command

Syntax:

```
ras> adsl loopback <portlist> < f5> <vpi> <vci>
```

where

`<portlist>`	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.
`< f5>`	=	Use f5 to perform an OAMF5 loopback test on the specified DSL port. An Operational, Administration and Maintenance Function 5 test is used to test the connection between two DSL devices. First, the DSL devices establish a virtual circuit. Then the local device sends an ATM F5 cell to be returned by the remote DSL device (both DSL devices must support ATM F5 in order to use this test).
`<vpi> <vci>`	=	When you perform an OAMF5 loopback test, specify a VPI/VCI.

This command has the AAM1212 perform an OAMF5 loopback test on the specified DSL port(s).

The following example has the AAM1212 perform an OAMF5 loopback test on DSL port 1's PVC at VPI 0 and VCI 33.

Figure 228 DSL Port Loopback Command Example

```
ras> adsl loopback 1 f5 0 33
port[1] OAM F5 loopback test: failed
```

57.1.11 DSL Port Upstream PSD Command

Syntax:

```
ras> adsl usnompsd <portNo> [<max nominal psd>]
```

where

`<max nominal psd>`	=	-400 ~ 40 (unit of measure is 0.1dBm/Hz)

This command displays or sets the upstream maximum nominal transmit PSD (Power Spectral Density).

The following example sets the upstream maximum nominal transmit PSD for port 7 to -10 dBm/Hz.

Figure 229 DSL Port Upstream PSD Command Example

```
ras> adsl usnompsd 7 -100
```

57.1.12 DSL Port Downstream PSD Command

Syntax:

```
ras> adsl dsnompsd <portNo> [<max nominal psd>]
```

where

`<max nominal psd>`	=	-400 ~ 40 (unit of measure is 0.1dBm/Hz)

This command displays or sets the downstream maximum nominal transmit PSD (Power Spectral Density).

The following example sets the downstream maximum nominal transmit PSD for port 7 to -10 dBm/Hz.

Figure 230 DSL Port Downstream PSD Command Example

```
ras> adsl dsnompsd 7 -100
```

57.1.13 DSL Port Upstream Carrier Command

Syntax:

```
ras> adsl uscarrier <portNo> [<m0> <m1>]
```

where

`<m0>,<m1>`	=	The upstream subcarriers to be masked (disabled). Each <mx> can use up to 8 hexadecimal digits (00000000~ffffffff). Each <mx> represents 32 carrier tones (each hexadecimal digit represents 4 tones). `<m0>` = tones 0~31 `<m1>` = tones 32~63 The hexadecimal digit is converted to binary and a '1' disables the corresponding tone. Disabling a carrier tone turns it off so the system does not send data on it.

The hexadecimal digit is converted to binary and a '1' masks (disables) the corresponding tone. Disabling a carrier tone turns it off so the system does not send data on it.

This command displays or sets masks for upstream carrier tones from 0 to 63. Masking a carrier tone disables the use of that tone on the specified DSL port. Use this command to have the system not use a DSL line's tones that are known to have a high noise level. The most significant bit defines the lowest tone number in a mask.

The most significant bit defines the first tone sequentially. For example, in <m0>, 0x00000001 means tone 31. For example, you could use 0xffff0000 for <m0> to disable upstream carrier tones 0~15 and leave tones 16 ~ 31 enabled.

The following example disables upstream carrier tones 0~15 for DSL port 5.

Figure 231 DSL Port Upstream Carrier Command Example

```
ras> adsl uscarrier 5 ffff0000 00000000
```

The following example displays the results.

Figure 232 DSL Port Upstream Carrier Command Display Example

```
ras> adsl uscarrier 5

          us carrier
port      m0       m1
----  |--------|--------|
   5   FFFF0000 00000000
Tone:
m0:0-31, m1:32-63
```

57.1.14 DSL Port Downstream Carrier0 Command

Syntax:

```
ras> adsl dscarrier0 <port number> [<m1> <m2> <m3> <m4> <m5> <m6> <m7>]
```

where

`<m1> - <m7>`	=	The downstream carrier tones to be masked (disabled). Each <mx> can use up to 8 hexadecimal digits (0~ffffffff). Each <mx> represents 32 carrier tones (each hexadecimal digit represents 4 tones).
`<m1>`	=	tones 32~63
`<m2>`	=	tones 64~95
`<m3>`	=	tones 96~127
`<m4>`	=	tones 128~159
`<m5>`	=	tones 160~191
`<m6>`	=	tones 192~223
`<m7>`	=	tones 224~255

The hexadecimal digit is converted to binary and a '1' masks (disables) the corresponding tone. Disabling a carrier tone turns it off so the system does not send data on it.

This command displays or sets masks for downstream carrier tones from 33 to 255. Masking a carrier tone disables the use of that tone on the specified DSL port. The most significant bit defines the lowest tone number in a mask.

The following example disables downstream carrier tone 71 for DSL port 5.

Figure 233 DSL Port Downstream Carrier0 Command Example 1

```
ras> adsl dscarrier0 5 0 01000000 0 0 0 0 0
```

The following example displays the results.

Figure 234 DSL Port Downstream Carrier0 Command Display Example

```
ras> adsl dscarrier0 5
                                 ds carrier
port      m1       m2       m3       m4       m5       m6       m7
----  |--------|--------|--------|--------|--------|--------|--------|
   5   00000000 01000000 00000000 00000000 00000000 00000000 00000000
Tone:
m1:32-63, m2:64-95, m3:96-127, m4:128-159
m5:160-191, m6:192-223, m7:224-255
```

This example disables downstream carrier tones 70 and 71 for DSL port 5.

Figure 235 DSL Port Downstream Carrier0 Command Example 2

```
ras> adsl dscarrier0 5 0 03000000 0 0 0 0 0
```

57.1.15 DSL Port Downstream Carrier1 Command

Syntax:

```
ras> adsl dscarrier1 <port number> [<m0> <m1> <m2> <m3> <m4> <m5> <m6> <m7>]
```

where

`<m0> - <m7>`	=	The downstream carrier tones to be masked (disabled). Each `<mx>` can use up to 8 hexadecimal digits (0~ffffffff). Each `<mx>` represents 32 carrier tones (each hexadecimal digit represents 4 tones).
`<m0>`	=	tones 256~287
`<m1>`	=	tones 288~319
`<m2>`	=	tones 320~351
`<m3>`	=	tones 352~383

<m4>	=	tones 384~415
<m5>	=	tones 416~447
<m6>	=	tones 448~479
<m7>	=	tones 480~511

The hexadecimal digit is converted to binary and a '1' masks (disables) the corresponding tone. Disabling a carrier tone turns it off so the system does not send data on it.

This command displays or sets masks for downstream carrier tones from 256 to 511 on the specified ADSL2+ port(s). Use this command to have the system not use a DSL line's tones that are known to have a high noise level.

The following example disables downstream carrier tone 307 for ADSL2+ port 5.

Figure 236 DSL Port Downstream Carrier1 Command Example 1

```
ras> adsl dscarrier1 5 0 00001000 0 0 0 0 0 0
```

The following example disables downstream carrier tones 304 to 307 for ADSL2+ port 5.

Figure 237 DSL Port Downstream Carrier1 Command Example 2

```
ras> adsl dscarrier1 5 0 0000f000 0 0 0 0 0 0
```

The following example displays the results.

Figure 238 DSL Port Downstream Carrier1 Command Display Example

```
ras> adsl dscarrier1 5
                                 ds carrier
port      m0       m1       m2       m3       m4       m5       m6       m7
----  |--------|--------|--------|--------|--------|--------|--------|-----
---|
   5   00000000 000F0000 00000000 00000000 00000000 00000000 00000000
00000000
Tone:
m0:256-287, m1:288-319, m2:320-351, m3:352-383
m4:384-415, m5:416-447, m6:448-479, m7:480-511
```

57.1.16 PMM Parameters Command

Syntax:

```
ras> adsl pmm param <portlist> [<l0time> <l2time> <l2atpr> <l2atprt>]
  [<max_l2rate> <min_l2rate> <l0tol2_rate>]
```

where

`<portlist>`	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.
`<l0time>`	=	Set the minimum time in seconds (10~65535) that the DSL line must stay in L0 power mode before changing to the L2 power mode.
`<l2time>`	=	Set minimum time in seconds (10~65535) that the DSL line must stay in the L2 power mode before reducing the power again in the L2 power mode.
`<l2atpr>`	=	Set the maximum Aggregate Transmit Power Reduction (ATPR) in decibels (dB) that is permitted in a L2 power reduction. The system can gradually decrease the DSL line transmission power while it is in the L2 power mode. This is the largest individual power reduction allowed in the L2 power mode. The range is 0~15(dB).
`<l2atprt>`	=	Set the maximum Aggregate Transmit Power Reduction Total (ATPRT) in decibels (dB) that is permitted in the L2 power mode. This is the total transmit power decrease that is allowed to occur in the L2 power mode. The range is 0~15(dB).
`<max_l2rate>`	=	Set the maximum transfer rate (in Kilobits per second) that is permitted while the port is in the L2 power mode. The supported range is 32~4096 Kbps in 4 Kbps increments. If you enter a number that is not a multiple of 4, the system uses the next lower multiple of 4. If you enter 39 for example, the system will use 36.
`<min_l2rate>`	=	Set the minimum transfer rate (in Kilobits per second) that is permitted while the port is in the L2 power mode. The supported range is 32~4096 Kbps in 4 Kbps increments. If you enter a number that is not a multiple of 4, the system uses the next lower multiple of 4. If you enter 39 for example, the system will use 36.
`<l0tol2_rate>`	=	Set the down stream transfer rate (in Kilobits per second) that serves as the threshold for whether the port is to use the L0 or the L2 power mode. The system changes from L0 mode to L2 mode when the downstream transfer rate stays below this threshold for **L0 Time**. The system changes back from L2 mode to L0 mode when the downstream transfer rate goes above this threshold. This rate must be less than or equal to one half of the **Min L2 Rate** and at least 16 Kbps.

Use this command to display or set Power ManageMent (PMM) parameters for the specified DSL port(s).

The following example sets DSL port 5 to use the following PMM settings.

- Stay in the L0 power mode for 180 seconds before a change to the L2 power mode is permitted.
- Once in L2 power mode, wait for 90 seconds before further reducing the transmission power.
- Each L2 power mode power reduction can only be 2 dB or less.
- The total power reduction allowed in the L2 power mode is 40 dB.

Figure 239 PMM Parameters Command Example

```
ras> adsl pmm param 5 180 90 2 40
```

57.1.17 Impulse Noise Protection Command

Syntax:

```
ras> adsl inp <portlist> [<usINP> [,<dsINP>]]
```

where

`<usINP>`	=	Sets the minimum upstream (us) impulse noise protection setting. Use 0~3 to define a number of DMT symbols. 0 = 0 DMT symbols, 1 = 0.5 DMT symbols, 2 = 1 DMT symbols, 3 = 2 DMT symbols.
`<dsINP>`	=	Sets the minimum downstream (ds) impulse noise protection setting. Use 0~3 to define a number of DMT symbols. 0 = 0 DMT symbols, 1 = 0.5 DMT symbols, 2 = 1 DMT symbols, 3 = 2 DMT symbols.

This command sets the upstream (us) and downstream (ds) impulse noise protection minimum setting on the specified DSL port(s). Sudden spikes in the line’s noise level (impulse noise) can cause errors and result in lost packets. Set the impulse noise protection minimum to have a buffer to protect the DSL physical layer connection against impulse noise. This buffering causes a delay that reduces transfer speeds. It is recommended that you use a non-zero setting for real time traffic that has no error correction (like videoconferencing).

The following example sets the impulse noise protection minimum to 1 DMT symbols for upstream and 0.5 DMT symbols for downstream for DSL port 5.

Figure 240 Impulse Noise Protection Command Example

```
ras> adsl inp 5 2 1
```

57.1.18 Annex L Enable Command

This command is available for the AAM1212-51.

Syntax:

```
ras> adsl annexl enable <portlist>
```

This command turns on the Annex L reach extended feature on the specified ADSL2 port(s). Annex L can be used with Annex A (ADSL over POTS), not Annex B (ADSL over ISDN).

The following example turns on the Annex L feature for port 5.

Figure 241 Annex L Enable Command Example

```
ras> adsl annexl enable 5
```

57.1.19 Annex L Disable Command

This command is available for the AAM1212-51.

Syntax:

```
ras> adsl annexl disable <portlist>
```

This command turns off the Annex L reach extended feature on the specified ADSL2 port(s).

The following example turns off the Annex L feature for port 5.

Figure 242 Annex L Disable Command Example

```
ras> adsl annexl disable 5
```

57.1.20 Annex M Enable Command

This command is available for the AAM1212-51.

Syntax:

```
ras> adsl annexm enable <portlist>
```

This command turns on the Annex M double upstream feature on the specified ADSL2/2+ port(s). This has the upstream connection use tones 6 to 63.

The following example turns on the Annex M feature for port 5.

Figure 243 Annex M Enable Command Example

```
ras> adsl annexm enable 5
```

57.1.21 Annex M Disable Command

This command is available for the AAM1212-51.

Syntax:

```
ras> adsl annexm disable <portlist>
```

This command turns off the Annex M double upstream feature on the specified ADSL2/2+ port(s).

The following example turns off the Annex M feature for port 5.

Figure 244 Annex M Disable Command Example

```
ras> adsl annexm disable 5
```

57.1.22 Annex I Enable Command

This command is available for the AAM1212-51.

Syntax:

```
ras> adsl annexi enable <portlist>
```

This command turns on the Annex I all digital mode feature on the specified ADSL2/2+ port(s). With Annex I, the DSL connection uses the full spectrum of the physical line and the user can not use POTS or ISDN service.

The following example turns on the Annex I feature for port 5.

Figure 245 Annex I Enable Command Example

```
ras> adsl annexi enable 5
```

57.1.23 Annex I Disable Command

This command is available for the AAM1212-51.

Syntax:

```
ras> adsl annexi disable <portlist>
```

This command turns off the Annex I all digital mode feature on the specified ADSL2/2+ port(s).

The following example turns off the Annex I feature for port 5.

Figure 246 Annex I Disable Command Example

```
ras> adsl annexi disable 5
```

57.2 DSL Port Statistics Commands

Use these commands to display DSL port statistics.

57.2.1 DSL Port Show Command

Syntax:

```
ras> statistics adsl show [portlist]
```

where

`[portlist]`	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.

This command displays DSL port connection statistics including the status (V for enabled, - for disabled), operational mode, upstream and downstream maximum rates, up time and the number of errored seconds.

The following example displays connection statistics for DSL port 1.

Figure 247 DSL Port Show Command Example

```
ras> statistics adsl show 1
port status mode     up/downstream        up time error second(15M/24H)
---- ------ -------- ------------- -------------- ---------------------
   1   V    adsl2       512/  9089 00000:00:04:59       15/15
```

57.2.2 Linedata Command

Syntax:

```
ras> statistics adsl linedata <portlist>
```

where

`<portlist>`	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.

This command shows the line bit allocation of a DSL port.

Discrete Multi-Tone (DMT) modulation divides up a line's bandwidth into tones. This command displays the number of bits transmitted for each tone. This can be used to determine the quality of the connection, whether a given sub-carrier loop has sufficient margins to support DSL transmission rates, and possibly to determine whether certain specific types of interference or line attenuation exist. See the ITU-T G.992.1 recommendation for more information on DMT.

The better (or shorter) the line, the higher the number of bits transmitted for a DMT tone. The maximum number of bits that can be transmitted per DMT tone is 15.

"upstream carrier load" displays the number of bits transmitted per DMT tone for the upstream channel (from the subscriber's DSL modem or router to the AAM1212).

"downstream carrier load" displays the number of bits received per DMT tone for the downstream channel (from the AAM1212 to the subscriber's DSL modem or router).

The bit allocation contents are only valid when the link is up.

In the following example, the upstream channel is carried on tones 7 to 39 and the downstream channel is carried on tones 53 to 259 (space is left between the channels to avoid interference).

Figure 248 Linedata Command Example

```
ras> statistics adsl linedata 1
[port 1]
up stream carrier load: number of bits per symbol(tone):
tone    0-  19: 00 00 00 00 00 00 02 03 04 05 - 06 07 07 07 07 07 07 07 08 08
tone   20-  39: 08 08 07 08 08 07 07 06 06 05 - 04 03

down stream carrier load: number of bits per symbol(tone):
tone    0-  19: 00 00 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 00 00
tone   20-  39: 00 00 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 00 00
tone   40-  59: 00 00 00 00 00 00 00 00 00 00 - 00 00 00 01 01 01 01 01 01 02
tone   60-  79: 02 02 02 02 00 02 02 02 02 02 - 02 02 02 02 02 02 02 02 02 02
tone   80-  99: 02 02 02 02 02 02 02 02 02 02 - 02 02 02 02 02 02 02 02 02 02
tone  100- 119: 02 02 02 02 02 02 02 02 02 02 - 02 02 02 02 02 02 02 02 02 02
tone  120- 139: 02 02 02 02 02 02 02 02 02 02 - 02 02 02 02 02 02 02 02 02 02
tone  140- 159: 02 02 02 02 02 02 02 02 02 02 - 02 02 02 02 02 02 02 02 02 02
tone  160- 179: 02 02 02 02 02 02 02 02 02 02 - 02 02 02 02 02 02 02 02 02 02
tone  180- 199: 02 02 02 02 02 02 02 02 02 02 - 02 02 02 02 02 02 02 02 02 02
tone  200- 219: 02 02 02 02 02 02 02 02 02 02 - 02 02 02 02 02 02 02 02 02 02
tone  220- 239: 02 02 02 02 02 02 02 02 02 02 - 02 02 02 02 02 02 02 02 02 02
tone  240- 259: 02 02 02 02 02 02 02 02 02 02 - 02 02 02 02 02 02
```

57.2.3 Lineinfo Command

Syntax:

```
ras> statistics adsl lineinfo <portlist>
```

where

<portlist>	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.

This command shows the line operating values of a DSL port.

An example is shown next.

Figure 249 Lineinfo Command Example

```
ras> statistics adsl lineinfo 8
[port 8]
operating modes:
- service type in operation: adsl2+
- TRELLIS operation mode   : on
connection detail:
- down/up stream interleaved delay (ms):  3/ 2
- total transceiver DS output power  (dbm): -2.5
- total transceiver US output power  (dbm): 11.5

atuc information:
- vendor id:      30304235303035300000000000000000
- version number: 66323330323030300000000000000000
- serial number :
30323030306530336539303030370000000000000000000000000000000000
00
atur information:
- vendor id:      b5004244434d00000000000000000000
- version number: 41327042303139610000000000000000
- serial number :
0000000000000000000000000000000000000000000000000000000000000000
```

The service type in operation is the ADSL standard that the port is using: G.dmt (AAM1212-51), G.dmt Annex B (AAM1212-53), ETSI (AAM1212-53), G.lite (AAM1212-51), ANSI T1.413 issue 2 (AAM1212-51), ADSL2, or ADSL2+.

Trellis coding helps to reduce the noise in DSL transmissions. Trellis may reduce throughput but it makes the connection more stable.[3]

3. At the time of writing, the AAM1212 always uses Trellis coding.

The numbers of milliseconds of interleave delay for downstream and upstream transmissions are listed. The total output power of the transceiver varies with the length and line quality. The farther away the subscriber's DSL modem or router is or the more interference there is on the line, the higher the power will be. "DS" refers to the power output of the AAM1212 "US" refers to the power output of the subscriber's DSL modem or router.

Information obtained prior to training to steady state transition will not be valid or will be old information.

The `atuc information` fields show data acquired from the ATUC (ADSL Termination Unit – Central), in this case AAM1212, during negotiation/provisioning message interchanges.

The `atur information` fields show data acquired from the ATUR (ADSL Termination Unit – Remote), in this case the subscriber's DSL modem or router, during negotiation/provisioning message interchanges. This information can help in identifying the subscriber's DSL modem or router.

The vendor ID, vendor version number and product serial number are obtained from vendor ID fields (see ITU-T G.994.1) or R-MSGS1 (see T1.413).

57.2.4 Lineperf Command

Syntax:

```
ras> statistics adsl lineperf <portlist>
```

where

`<portlist>`	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.

This command shows the line performance counters of a DSL port.

An example is shown next.

Figure 250 Lineperf Command Example

```
ras> statistics adsl lineperf 1
[port 1] Perf since boot up
nfebe-I/nfebe-ni   :         46/         0 (Far End CRC)
ncrc-I/ncrc-ni     :          5/         0 (Near End CRC)
nfecc-I/nfecc-ni   :          0/         0 (Far End Corrected FEC)
nfec-I/nfec-ni     :         28/         0 (Near End Corrected FEC)
init-atuc/init-atur:         23/         -
es-atuc /es-atur   :         27/        92
ses-atuc /ses-atur :         26/        60
uas-atuc /uas-atur :       1515/      1515
lpr-atuc /lpr-atur :          -/         2
```

These counters display line performance data that has been accumulated since the system started. In the list above the definitions of near end/far end will always be relative to the ATU-C (ADSL Termination Unit-Central Office). Downstream (ds) refers to data from the ATU-C and upstream (us) refers to data from the ATU-R. “I” stands for interleaved and “ni” stands for non-interleaved (fast mode).

A block is a set of consecutive bits associated with the path; each bit belongs to one and only one block. Consecutive bits may not be contiguous in time.

Table 105 Line Performance Counters

LABEL	DESCRIPTION
nfebe	The Number of Far End Block Errors (Cyclic Redundancy Check).
ncrc	Near end Cyclic Redundancy Check errors.
nfecc	The Far End blocks repaired by Forward Error Correction.
nfec	The Near End blocks repaired by Forward Error Correction.
init	The number of link ups and link downs.
es	The Number of Errored Seconds. This is how many seconds contained at least one errored block or at least one defect.
ses	The Number of Severely Errored Seconds. This is how many seconds contained 30% or more errored blocks. This is a subset of n-es.
uas	The Number of Unavailable Seconds.
lpr	The Number of Loss of Power Seconds (on the ATUR) that have occurred.

57.2.5 15 Minute Performance Command

Syntax:

```
ras> statistics adsl 15mperf <portlist> [count <0..96>]
```

where

`<portlist>`	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.
`[count <0..96>]`	=	Specify for which 15-minute interval (0~96) you want to display performance statistics. 0 is the current 15 minutes.

This command displays line performance statistics for the current and previous 15-minute periods.

An example is shown next.

Figure 251 15 Minute Performance Command Example

```
ras> statistics adsl 15mperf 1 1
Port 1 Current 15 Min elapsed time:12 sec (Link Down)
   Current 15 Min PM:      ATUC      ATUR
                lofs:         0         0
                loss:         0         0
                lols:         0         -
                lprs:         -         0
                  es:         0         0
                init:         0         -
                 ses:         0         0
                 uas:         0         0
  History 15 Min PM-1:      ATUC      ATUR
                lofs:         0         0
                loss:         0         0
                lols:         0         -
                lprs:         -         0
                  es:         0         0
                init:         0         -
                 ses:         0         0
                 uas:         0         0
```

The following table explains these counters.

Table 106 15 Minute Performance Counters

LABEL	DESCRIPTION
atuc	Upstream. These statistics are for the connection (or traffic) coming from the subscriber's device to the AAM1212.
atur	Downstream. These statistics are for the connection (or traffic) going from the AAM1212 to the subscriber's device.
lofs	The number of Loss Of Frame seconds that have occurred within the 15-minute period.
loss	The number of Loss Of Signal seconds that have occurred within the 15-minute period.
lols	The number of Loss Of Link seconds that have occurred within the 15-minute period.
lprs	The number of Loss of Power seconds (on the ATUR) that have occurred within the 15-minute period.
eS	The number of Errored Seconds that have occurred within the 15-minute period.
init	The number of link ups and link downs that have occurred within the 15-minute period.
ses	The number of Severely Errored Seconds that have occurred within the 15-minute period.
uas	The number of UnAvailable Seconds that have occurred within the 15-minute period.

These counters are also used in the alarm profiles (see Section 57.2.9 on page 416).

57.2.6 1 Day Performance Command

Syntax:

```
ras> statistics adsl 1dayperf <portlist>
```

where

`<portlist>`	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.

This command displays line performance statistics for the current and previous 24 hours.

An example is shown next.

Figure 252 1Day Performance Command Example

```
ras> statistics adsl 1dayperf 1
 Port 1 current 1 day elapsed time:81985 sec (Link Down)
 Current 1 Day Perf        ATUC       ATUR
                lofs          0          0
                loss          0          0
                lols          0          -
                lprs          -          0
                  es          0          0
                init          0          -
                 ses          0          0
                 uas          0          0

 Port 1 previous 1 day elapsed time:0 sec
 Previous 1 Day Perf       ATUC       ATUR
                lofs          0          0
                loss          0          0
                lols          0          -
                lprs          -          0
                  es          0          0
                init          0          -
                 ses          0          0
                 uas          0          0
```

See Table 106 on page 412 for details about these counters.

57.2.7 Line Diagnostics Set Command

Syntax:

```
ras> adsl linediag setld <port number>
```

This command has the AAM1212 perform line diagnostics on the specified port. The DSL port must be set to ADSL2 or ADSL2+ operational mode and have a connection. It takes about one minute for the line diagnostics to finish.

The following example performs line diagnostics on DSL port 1. The screen displays a message confirming upon which DSL port line diagnostics will be performed.

Figure 253 Line Diagnostics Set Command Example

```
ras> adsl linediag setld 1
Line- 1 set to Line Diagnostic Mode
```

57.2.8 Line Diagnostics Get Command

Syntax:

```
ras> adsl linediag getld <port number>
```

Use this command to display the line diagnostics results after using the line diagnostics set command on a DSL port. Use the line diagnostics results to analyze problems with the physical DSL line.

Note: Wait at least one minute after using the line diagnostic set command before using this command.

The following example displays the line diagnostics results for DSL port 1.

Figure 254 Line Diagnostics Get Command Example

```
ras> adsl linediag getld 1
Line_Diagnostics_Parameter,_channel: 0

number_of_subcarries: 256       32
hlinScale: 19625        32767
latn: 54        0
satn: 52        8
snrm: 60        60
attndr: 12140000        1120000
farEndActatp: 75        125
i       li.rl   li.im   log     QLN     SNR
0       32768   32768   1023    255     255
1       32768   32768   1023    255     255
2       32768   32768   1023    255     255
3       32768   32768   1023    255     255
4       32768   32768   1023    255     255
5       32768   32768   1023    255     255
6       11604   4752    83      191     132
7       17794   5598    48      190     139
8       22385   5567    30      184     147
9       24903   5163    21      163     152
10      26768   5013    15      185     159
11      29179   5494    8       175     165
12      31605   6574    1       172     168
13      32766   8020    1023    186     170
14      32159   9597    1023    183     173
15      30990   11350   1023    182     173
16      30432   13730   1023    186     172
17      30259   16694   1023    182     170
18      29137   19570   1023    171     170
19      26499   21554   1023    186     172
20      23288   22973   0       173     174
```

The following table lists the line diagnostics test parameters that display, see the ITU-T's G.992.3 for more information.

Table 107 Line Diagnostics Get Command

LABEL	DESCRIPTION
number_of_ subcarries	Discrete Multi-Tone (DMT) modulation divides up a line's bandwidth into sub-carriers (sub-channels) of 4.3125 kHz each. The first number is the total number of DMT sub-carriers the DSL connection is using. The second number indicates how many upstream DMT sub-carriers the DSL connection is using.
hlinScale:	The channel characteristics function is represented in linear format by a scale factor and a complex number. These are the maximum upstream and downstream scale factors used in producing the channel characteristics function.
latn:	This is the upstream and downstream Line Attenuation (in .1 dB).
satn:	This is the upstream and downstream Signal Attenuation (in .1 dB).

Table 107 Line Diagnostics Get Command (continued)

LABEL	DESCRIPTION
`snrm:`	This is the upstream and downstream Signal-to-Noise Ratio Margin (in .1 dB). A DMT sub-carrier's SNR is the ratio between the received signal power and the received noise power. The signal-to-noise ratio margin is the maximum that the received noise power could increase with the AAM1212 still being able to meet its transmission targets.
`attndr:`	This is the upstream and downstream Attainable Net Data Rate (in bit/s).
`farEndActatp:`	This is the upstream and downstream Far End Actual Aggregate Transmit Power (in .1 dBm)
`i`	This is the index number of the DMT sub-carrier.
`li.rl`	The channel characteristics function is represented in linear format by a scale factor and a complex number. This is the real part of the complex number used in producing the channel characteristics function for this sub-carrier.
`li.im`	The channel characteristics function is represented in linear format by a scale factor and a complex number. This is the imaginary part of the complex number used in producing the channel characteristics function for this sub-carrier
`log`	This is a format for providing channel characteristics. It provides magnitude values in a logarithmic scale. This can be used in analyzing the physical condition of the DSL line.
`QLN`	The Quiet Line Noise for a DMT sub-carrier is the rms (root mean square) level of the noise present on the line, when no DSL signals are present. It is measured in dBm/Hz. The QLN can be used in analyzing crosstalk.
`SNR`	This is the upstream and downstream Signal-to-Noise Ratio (in .1 dB). A DMT sub-carrier's SNR is the ratio between the received signal power and the received noise power. The SNR can be used in analyzing time dependent changes in crosstalk levels and line attenuation (such as those caused by temperature variations and moisture).

57.2.9 Line Diagnostics Get 992.3 Command

Syntax:

```
ras> adsl linediag getld992_3 <port number>
```

Use this command to display the line diagnostics results in the format defined in the ITU-T G.992.3 standard after using the line diagnostics set command on a DSL port. Use the line diagnostics results to analyze problems with the physical DSL line.

Note: Wait at least one minute after using the line diagnostic set command before using this command.

The following example displays the line diagnostics results for DSL port 1.

Figure 255 Line Diagnostics Get 992.3 Command Example

```
ras> adsl linediag getld992_3 1
port: 1

number_of_subcarries:       256        32
hlinScale:                17024     32767
latn:                       2.0       0.2
satn:                       2.0       0.0
snrm:                      -0.0       6.0
attndr:                10398468   1152000
farEndActatp:              20.4      12.4
  i     li.rl     li.im   log(dB)  QLN(dBm)   SNR(dB)
  0       N/A       N/A       N/A       N/A       N/A
  1       N/A       N/A       N/A       N/A       N/A
  2       N/A       N/A       N/A       N/A       N/A
  3       N/A       N/A       N/A       N/A       N/A
  4       N/A       N/A       N/A       N/A       N/A
  5       N/A       N/A       N/A       N/A       N/A
  6   0.31557   0.00796      -9.9    -120.5       8.5
  7   0.43477  -0.31599      -5.3    -120.0      42.0
  8   0.28313  -0.67576      -2.6    -119.5      44.5
  9  -0.01016  -0.86645      -1.1    -119.0      46.5
 10  -0.28423  -0.89969      -0.4    -118.5      51.5
 11  -0.48750  -0.85403      -0.1    -118.0      52.0
 12  -0.63495  -0.79630       0.2    -118.0      54.5
 13  -0.75373  -0.75644       0.6    -117.5      56.5
 14  -0.84457  -0.72510       1.0    -117.0      56.5
 15  -0.89389  -0.68549       1.1    -116.5      56.5
 16  -0.90713  -0.64631       1.0    -114.5      56.5
 17  -0.91955  -0.63196       1.0    -116.0      57.0
 18  -0.95053  -0.64860       1.3    -116.0      57.0
 19  -0.97781  -0.67563       1.6    -115.5      57.0
 20  -0.97161  -0.69211       1.6    -115.5      57.5
```

The following table lists the line diagnostics test parameters that display, see the ITU-T's G.992.3 for more information.

Table 108 Line Diagnostics Get 992.3 Command

LABEL	DESCRIPTION
number_of_ subcarries	Discrete Multi-Tone (DMT) modulation divides up a line's bandwidth into sub-carriers (sub-channels) of 4.3125 KHz each. The first number is the total number of DMT sub-carriers the DSL connection is using. The second number indicates how many upstream DMT sub-carriers the DSL connection is using.
hlinScale:	The channel characteristics function is represented in linear format by a scale factor and a complex number. These are the maximum upstream and downstream scale factors used in producing the channel characteristics function.
latn:	This is the upstream and downstream Line Attenuation (in dB).
satn:	This is the upstream and downstream Signal Attenuation (in dB).

Table 108 Line Diagnostics Get 992.3 Command (continued)

LABEL	DESCRIPTION
`snrm:`	This is the upstream and downstream Signal-to-Noise Ratio Margin (in dB). A DMT sub-carrier's SNR is the ratio between the received signal power and the received noise power. The signal-to-noise ratio margin is the maximum that the received noise power could increase with the AAM1212 still being able to meet its transmission targets.
`attndr:`	This is the upstream and downstream Attainable Net Data Rate (in bit/s).
`farEndActatp:`	This is the upstream and downstream Far End Actual Aggregate Transmit Power (in dBm)
`i`	This is the index number of the DMT sub-carrier.
`li.rl`	The channel characteristics function is represented in linear format by a scale factor and a complex number. This is the real part of the complex number used in producing the channel characteristics function for this sub-carrier.
`li.im`	The channel characteristics function is represented in linear format by a scale factor and a complex number. This is the imaginary part of the complex number used in producing the channel characteristics function for this sub-carrier
`log`	This is a format for providing channel characteristics. It provides magnitude values in a logarithmic scale. It is measured in dB. This can be used in analyzing the physical condition of the DSL line.
`QLN`	The Quiet Line Noise for a DMT sub-carrier is the rms (root mean square) level of the noise present on the line, when no DSL signals are present. It is measured in dBm. The QLN can be used in analyzing crosstalk.
`SNR`	This is the upstream and downstream Signal-to-Noise Ratio (in dB). A DMT sub-carrier's SNR is the ratio between the received signal power and the received noise power. The SNR can be used in analyzing time dependent changes in crosstalk levels and line attenuation (such as those caused by temperature variations and moisture).

57.2.10 SELT Diagnostic Set Command

Syntax:

```
ras> adsl linediag setselt <port number>
```

This command has the AAM1212 perform a single end line test on the specified port. This test checks the distance to the subscriber's location.

Note: The port must have an open loop. There cannot be a DSL device, phone, fax machine or other device connected to the subscriber's end of the telephone line.

The test takes at least 15 seconds. You can run the SELT Diagnostic Get Command to check the status of the test and to look at the results.

The following example starts a SELT test on DSL port 1.

Figure 256 SELT Diagnostic Set Command Example

```
ras> adsl linediag setselt 1
```

57.2.11 SELT Diagnostic Get Command

Syntax:

```
ras> adsl linediag getselt <port number>
```

Use this command to display the status and the results of the SELT test on the specified port. The report tells you what gauge of telephone wire is connected to the port and the approximate length of the line measured both in meters and thousands of feet.

The following example displays the status and results SELT diagnostic results for DSL port 1.

Figure 257 Line Diagnostics Get Command Example

```
ras> adsl linediag getselt 1
port     inprogress       cableType loopEstimateLength
---- -------------------- --------- ------------------
   1           INPROGRESS     24AWG    0 m(0.00 kFt)
ras> adsl linediag getselt 1
port     inprogress       cableType loopEstimateLength
---- -------------------- --------- ------------------
   1                 DONE     24AWG    0 m(0.00 kFt)
```

57.2.12 Tone Diagnostics 992.3 Command

Syntax:

```
ras> adsl linediag toneDiag <port number>
```

Use this command to display the tone diagnostics for a port in the format defined in the ITU-T G.992.3 standard. You do not need to use the line diagnostics set command first. Use the tone diagnostics to analyze problems with the physical DSL line.

The following example displays the tone diagnostics results for DSL port 8.

Figure 258 Tone Diagnostics Command Example

```
ras> ad lined toneD 1
port: 1

number_of_subcarries:       512        32
latn:                      24.1       2.7
satn:                      24.1      61.3
snrm:                      30.2      25.0
attndr:                28008000   1248000
farEndActatp:             -31.0      11.9
  i   log(dB)  QLN(dBm)   SNR(dB)
  0       N/A       N/A       N/A
  1       N/A       N/A       N/A
  2       N/A       N/A       N/A
  3       N/A       N/A       N/A
  4       N/A       N/A       N/A
  5       N/A       N/A       N/A
  6     -21.1    -125.5      17.5
  7     -15.3    -124.0      26.0
  8      -9.9    -123.0      31.0
  9      -5.7    -120.5      38.0
----------------------Snip------------------------

509       6.0    -124.0      29.0
510       6.0    -124.0      29.0
511       6.0    -123.0      26.5
```

The following table lists the tone diagnostic parameters. See the ITU-T's G.992.3 for more information.

Table 109 ToneDiag Command

LABEL	DESCRIPTION
number_of_ subcarries	Discrete Multi-Tone (DMT) modulation divides up a line's bandwidth into sub-carriers (sub-channels) of 4.3125 KHz each. This number indicates how many upstream and downstream DMT sub-carriers the DSL connection is using.
hlinScale:	The channel characteristics function is represented in linear format by a scale factor and a complex number. This is the maximum upstream and downstream scale factor used in producing the channel characteristics function.
latn:	This is the upstream and downstream Line Attenuation (in dB).
satn:	This is the upstream and downstream Signal Attenuation (in dB).
snrm:	This is the upstream and downstream Signal-to-Noise Ratio Margin (in dB). A DMT sub-carrier's SNR is the ratio between the received signal power and the received noise power. The signal-to-noise ratio margin is the maximum that the received noise power could increase with the AAM1212 still being able to meet its transmission targets.
attndr:	This is the upstream and downstream Attainable Net Data Rate (in bit/s).
farEndActatp:	This is the upstream and downstream Far End Actual Aggregate Transmit Power (in dBm)

Table 109 ToneDiag Command (continued)

LABEL	DESCRIPTION
`i`	This is the index number of the DMT sub-carrier.
`log(dB)`	This is a format for providing channel characteristics. It provides magnitude values in a logarithmic scale. This can be used in analyzing the physical condition of the DSL line.
`QLN(dBm)`	The Quiet Line Noise for a DMT sub-carrier is the rms (root mean square) level of the noise present on the line, when no DSL signals are present. It is measured in dBm/Hz. The QLN can be used in analyzing crosstalk.
`SNR(dB)`	This is the upstream and downstream Signal-to-Noise Ratio (in dB). A DMT sub-carrier's SNR is the ratio between the received signal power and the received noise power. The SNR can be used in analyzing time dependent changes in crosstalk levels and line attenuation (such as those caused by temperature variations and moisture).

57.3 Alarm Profile Commands

Configure alarm profiles to set alarm settings and thresholds for the DSL ports.

57.3.1 Alarm Profile Show Command

Syntax:

```
ras> adsl alarmprofile show [profile]
```

where

`[profile]` = The name of an alarm profile.

Displays the settings of the specified alarm profile (or all of them if you do not specify one).

The following example displays the default alarm profile (DEFVAL).

Figure 259 Alarm Profile Show Command Example

```
ras> adsl alarmprofile show DEFVAL
01. DEFVAL
                                             ATU-C      ATU-R
                                        ---------- ----------
Thresh15MinLofs               (sec):          0          0
Thresh15MinLoss               (sec):          0          0
Thresh15MinLols               (sec):          0        ---
Thresh15MinLprs                    :          0          0
Thresh15MinESs                (sec):          0          0
ThreshFastRateUp              (bps):          0          0
ThreshInterleaveRateUp        (bps):          0          0
ThreshFastRateDown            (bps):          0          0
ThreshInterleaveRateDown      (bps):          0          0
InitFailureTrap(1-enable, 2-disable):          2        ---
Thresh15MinFailedFastRetrain       :          0        ---
Thresh15MinSes                (sec):          0          0
Thresh15MinUas                (sec):          0          0
```

57.3.2 Alarm Profile Set Command

Syntax:

```
  ras> adsl alarmprofile set <profile> [<atuc lofs> <atur lofs> <atuc loss>
<atur loss> <atuc lols> <atuc lprs> <atur lprs> <atuc ess> <atur ess> <atuc
fast rateup> <atur fast rateup> <atuc interleave rateup> <atur interleave
rateup> <atuc fast ratedown> <atur fast ratedown> <atuc interleave ratedown>
<atur interleave ratedown> <init fail enable> <atuc fail fast> <atuc ses>
<atur ses> <atuc uas> <atur uas>]
```

where

<profile>	=	A name for the alarm profile (up to 31 ASCII characters).
atuc	=	Upstream. These parameters are for the connection (or traffic) coming from the subscriber’s device to the AAM1212.
atur	=	Downstream. These parameters are for the connection (or traffic) going from the AAM1212 to the subscriber’s device.
<atuc lofs> <atur lofs>	=	The number of Loss Of Frame seconds that are permitted to occur within 15 minutes.
<atuc loss> <atur loss>	=	The number of Loss Of Signal seconds that are permitted to occur within 15 minutes.
<atuc lols>	=	The number of Loss Of Link seconds that are permitted to occur within 15 minutes.
<atuc lprs> <atur lprs>	=	The number of Loss of Power seconds that are permitted to occur (on the ATUR) within 15 minutes.

`<atuc ess> <atur ess>`	=	The number of Errored Seconds that are permitted to occur within 15 minutes.
`<atuc fast rateup> <atur fast rateup>`	=	A rate in kilobits per second (kbps). If a fast mode connection’s upstream transmission rate increases by more than this number, then a trap is sent.
`<atuc interleave rateup> <atur interleave rateup>`	=	A rate in kilobits per second (kbps). If an interleave mode connection’s upstream transmission rate increases by more than this number, then a trap is sent.
`<atuc fast ratedown> <atur fast ratedown>`	=	A rate in kilobits per second (kbps). If a fast mode connection’s downstream transmission rate decreases by more than this number, then a trap is sent.
`<atuc interleave ratedown> <atur interleave ratedown>`	=	A rate in kilobits per second (kbps). If an interleave mode connection’s upstream transmission rate decreases by more than this number, then a trap is sent.
`<init fail enable>`	=	“1” sets the profile to trigger an alarm for an initialization failures trap. “2” sets the profile to not trigger an alarm for an initialization failures trap.
`<atuc fail fast>`	=	The number of failed fast retrains that are permitted to occur within 15 minutes.
`<atuc ses> <atur ses>`	=	The number of Severely Errored Seconds that are permitted to occur within 15 minutes.
`<atuc uas> <atur uas>`	=	The number of UnAvailable Seconds that are permitted to occur within 15 minutes.

This command configures settings and thresholds that define when the AAM1212 is to send an alarm trap and generate a syslog entry.

Configure alarm profiles first and then use the `alarmprofile map` command to set the AAM1212 to use them with specific DSL ports.

The following example sets an alarm profile named `SESalarm` that has the AAM1212 send an alarm trap and generate a syslog whenever the upstream connection’s number of severely errored seconds exceeds three within a 15 minute period.

Figure 260 Alarm Profile Set Command Example

```
ras> adsl alarmprofile set SESalarm 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 2 0 3
0 0 0
```

57.3.3 Alarm Profile Delete Command

Syntax:

```
ras> adsl alarmprofile delete <profile>
```

where

`<profile>`	=	The name of an alarm profile.

This command allows you to delete an individual alarm profile by its name. You cannot delete the DEFVAL alarm profile.

The following example deletes the `SESalarm` alarm profile.

Figure 261 Alarm Profile Delete Command Example

```
ras> adsl alarm profile delete SESalarm
```

57.3.4 Alarm Profile Map Command

Syntax:

```
ras> adsl alarmprofile map <portlist> <profile>
```

where

`<portlist>`	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.
`<profile>`	=	The name of an alarm profile.

Sets the AAM1212 to use an (already-configured) alarm profile with the specified DSL ports.

The following example sets the AAM1212 to use the `SESalarm` alarm profile with DSL port 5.

Figure 262 Alarm Profile Map Command Example

```
ras> adsl alarmprofile map SESalarm 5
```

57.3.5 Alarm Profile Showmap Command

Syntax:

```
ras> adsl alarmprofile showmap [profile]
```

where

`[profile]` = The name of an alarm profile.

Displays which alarm profiles the AAM1212 is set to use for specific (or all) DSL ports.

The following example displays which alarm profile the AAM1212 is set to use for DSL port 5.

Figure 263 Alarm Profile Showmap Command Example

```
ras> adsl alarmprofile showmap 5
ADSL alarm profile mapping:
Port  5: Alarm Profile = DEFVAL
```

58

Virtual Channel Management

This chapter shows you how to use commands to configure virtual channels.

58.1 Virtual Channel Management Overview

See Chapter 13 on page 115 for background information on virtual channels and ATM QoS.

58.2 Virtual Channel Profile Commands

Use the following commands to configure virtual channel profiles.

58.2.1 Show Virtual Channel Profile Command

Syntax:

```
ras> adsl vcprofile show [vcprofile]
```

where

[vcprofile]	=	The name of the virtual channel profile (up to 31 ASCII characters).

Displays the settings of the specified virtual channel profile (or all of them if you do not specify one).

58.2.2 Set Virtual Channel Profile Command

Syntax:

```
ras> adsl vcprofile set <vcprofile> <vc|llc> <ubr|cbr> <pcr> <cdvt>
ras> adsl vcprofile set <vcprofile> <vc|llc> <vbr(rt-vbr)|nrt-vbr> <pcr>
<cdvt> <scr> <bt>
```

where

<vcprofile>	=	The name of the virtual channel profile (up to 31 ASCII characters). You cannot change the DEFVAL or DEFVAL_VC profiles.
<vc|llc>	=	The type of encapsulation (vc or llc).

<ubr|cbr>	=	The ubr (unspecified bit rate) or cbr (constant bit rate) or ATM traffic class.
<pcr>	=	Peak Cell Rate (150 to 300000), the maximum rate (cells per second) at which the sender can send cells.
[cdvt]	=	Cell Delay Variation Tolerance is the accepted tolerance of the difference between a cell's transfer delay and the expected transfer delay (number of cells). 0 to 255 cells or * (means 0).
<vbr(rt-vbr)|nrt-vbr>	=	The real-time (vbr) or non real-time (nrt-vbr) Variable Bit Rate ATM traffic class.
<scr>	=	The Sustained Cell Rate sets the average cell rate (long-term) that can be transmitted (cells per second). SCR applies with the vbr traffic class.
<bt>	=	Burst Tolerance this is the maximum number of cells that the port is guaranteed to handle without any discards (number of cells). BT applies with the vbr traffic class.

This command creates a virtual channel profile. After you create a virtual channel profile, you can assign it to any of the DSL ports on the AAM1212.

The following example creates a virtual channel profile named gold that uses LLC encapsulation. It uses constant bit rate and has the maximum rate (peak cell rate) set to 300,000 cells per second. The acceptable tolerance of the difference between a cell's transfer delay and the expected transfer delay (CDVT) is set to 5 cells.

Figure 264 Set Virtual Channel Profile Command Example 1

```
ras> adsl vcprofile set gold llc cbr 300000 5
```

The following example creates a virtual channel profile named silver that uses VC encapsulation. It uses real-time variable bit rate and has the maximum rate (peak cell rate) set to 250,000 cells per second. The acceptable tolerance of the difference between a cell's transfer delay and the expected transfer delay (CDVT) is set to 5 cells. The average cell rate that can be transmitted (SCR) is set to 100,000 cells per second. The maximum number of cells that the port is guaranteed to handle without any discards (BT) is set to 200.

Figure 265 Set Virtual Channel Profile Command Example 2

```
ras> adsl vcprofile set silver vc vbr 250000 5 100000 200
```

The following example creates a virtual channel profile named economy that uses LLC encapsulation. It uses unspecified bit rate and has the maximum rate (peak cell rate) set to 50,000 cells per second. The acceptable tolerance of the difference between a cell's transfer delay and the expected transfer delay (CDVT) is set to 100 cells.

Figure 266 Set Virtual Channel Profile Command Example 3

```
ras> adsl vcprofile set gold llc cbr 50000 100
```

58.2.3 Delete Virtual Channel Profile Command

Syntax:

```
ras> adsl vcprofile delete <vcprofile>
```

where

`<vcprofile>`	=	The name of the virtual channel profile (up to 31 ASCII characters). You cannot delete the DEFVAL or DEFVAL_VC profiles.

You cannot delete a virtual channel profile that is assigned to any of the DSL ports. Assign a different profile to any DSL ports that are using the profile that you want to delete, and then you can delete the profile.

The following example deletes the silver virtual channel profile.

Figure 267 Delete Virtual Channel Profile Command Example

```
ras> adsl vcprofile delete silver
```

58.3 PVC Channels

Channels (also called Permanent Virtual Circuits or PVCs) let you set priorities for different services or subscribers. You can define up to eight channels on each DSL port and use them for different services or levels of service. You set the PVID that is assigned to untagged frames received on each channel. You also set an IEEE 802.1p priority for each of the PVIDs. In this way you can assign different priorities to different channels (and consequently the services that get carried on them or the subscribers that use them). Use the following commands to define channels.

58.3.1 PVC Show Command

Syntax:

```
ras> adsl pvc show [portlist] [<vpi> <vci>]
```

where

`<portlist>`	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.
`[<vpi> <vci>]`	=	The VPI and VCI of an individual PVC.

This command allows you to display the PVC parameters of the specified DSL port(s) or all of the DSL ports if you do not specify any.

58.3.2 PVC Set Command

Syntax:

```
  ras> adsl pvc set <portlist> <vpi> <vci> <super |vid = 1..4094 <priority>>
<DS vcprofile[,US vcprofile]>
```

where

`<portlist>`	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.
`<vpi>`	=	The VPI setting can be 0 to 255.
`<vci>`	=	The VCI setting can be 32 to 65535 if the vpi is 0 or 1 to 65535 if the vpi is not 0.
`<super |vid`	=	Enable the super channel option to allow a channel forward frames belonging to multiple VLAN groups (that are not assigned to other channels). The AAM1212 forwards frames belonging to VLAN groups that are not assigned to specific channels to the super channel. The super channel functions in the same way as the channel in a single channel environment. One port can have only one super channel. The default VID (1 to 4094). Each PVC must have a unique VID since the AAM1212 forwards traffic back to the subscribers based on the VLAN ID. You must assign a default VID (1 to 4094) and IEEE 802.1p default priority (0 to 7) to normal channels. Each PVC must have a unique VID (since the AAM1212 forwards traffic back to the subscribers based on the VLAN ID).

`<priority>`	=	This is the priority value (0 to 7) to add to incoming frames without a (IEEE 802.1p) priority tag.
`DS vcprofile`	=	Assign a VC profile to use for this channel's downstream traffic shaping.
`[,US vcprofile]>`	=	Assign a VC profile to use for policing this channel's upstream traffic. The AAM1212 does not perform upstream traffic policing if you do not specify an upstream VC profile.

This command allows the configuration of a PVC (permanent virtual circuit) for one or a range of DSL ports.

The following example sets a PVC on DSL port 1 with VPI 1, VCI 34, default VID 100 priority 3. It sets the "platinum" profile for downstream traffic shaping and a VC profile named "plus" for upstream traffic policing.

Figure 268 PVC Set Command Example

```
ras> adsl pvc set 1 1 34 100 3 platinum,plus
```

58.3.3 PVC Delete Command

Syntax:

```
ras> adsl pvc delete <portlist> <vpi> <vci>
```

where

`<portlist>`	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.
`[<vpi> <vci>]`	=	The VPI and VCI of an individual PVC.

This command deletes the specified PVC channel.

58.4 Priority-based PVCs

A PPVC (Priority-based PVC) allows you to give different priorities to PVCs that are members of the same VLAN.

The AAM1212 uses eight priority queues (also called levels) for the member PVCs. The system maps frames with certain IEEE 802.1p priorities to a PVC with a particular priority queue. See Chapter 61 on page 471 for the factory default mapping.

Use these commands to configure PPVCs and add and remove member PVCs.

58.4.1 PPVC Set Command

Syntax:

```
ras> adsl ppvc set <portlist> <vpi> <vci> <encap> <pvid> <priority>
```

where

<portlist>	=	You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.
<vpi>	=	The VPI setting can be 0 to 255.
<vci>	=	The VCI setting can be 32 to 65535 if the vpi is 0 or 1 to 65535 if the vpi is not 0. This PVC channel is for internal use. The operator does not need to create this PVC on the subscriber's device (the CPE).
<encap>	=	The type of encapsulation: llc, vcmux
<pvid>	=	Type a PVID (Port VLAN ID) to assign to untagged frames received on this PPVC.
<priority>	=	This is the priority value (0 to 7) to add to incoming frames without a (IEEE 802.1p) priority tag.

This command creates a PPVC.

The following example creates a PPVC with VPI 8 and VCI 35 for port 5. The PPVC uses llc encapsulation and default VID 25. Any frames received without an IEEE 802.1p priority tag will be assigned a priority of 3. The AAM1212 uses this PVC channel internally. This PVC is not needed on the subscriber's device.

Figure 269 PPVC Set Command Example

```
ras> adsl ppvc set 5 8 35 llc 25 3
```

58.4.2 PPVC Member Set Command

Syntax:

```
  ras> adsl ppvc member set <portlist> <vpi> <vci> <member vpi> <member vci>
<DS vcprofile[,US vcprofile]> <level>
```

where

`<portlist>`	=	The port(s) of the PPVC. You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.
`<vpi>`	=	The VPI of the PPVC.
`<vci>`	=	The VCI of the PPVC. This PVC channel is for internal use. The subscriber does not need to create this PVC.
`<member vpi>`	=	The VPI of the individual PVC that you are adding to the PPVC. The VPI setting can be 0 to 255.
`<member vci>`	=	The VCI of the individual PVC that you are adding to the PPVC. The VCI setting can be 32 to 65535 with a VPI of 0 or 1 to 65535 if the VPI is not 0. The subscriber's device must create this PVC.
`DS vcprofile`	=	Assign a VC profile to use for this channel's downstream traffic shaping.
`[,US vcprofile]>`	=	Assign a VC profile to use for policing this channel's upstream traffic. The AAM1212 does not perform upstream traffic policing if you do not specify an upstream VC profile.
`<level>`	=	The priority queue (0~7) to use for this PVCs traffic. 7 is the highest priority.

This command adds a member PVC to a PPVC. You must create the PPVC before you use this command to add a member.

Note: Only the member PVCs need to be created on the subscriber's device.

The following example adds a PVC to a PPVC with VPI 8 and VCI 35 for port 5. The PVC uses VPI 8 and VCI 36. It sets the DEFVAL profile for downstream traffic shaping and for upstream traffic policing. It uses priority queue 2.

Figure 270 PPVC Member Set Command Example

```
ras> adsl ppvc member set 5 8 35 8 36 DEFVAL,DEFVAL 2
```

58.5 PPVC Member Delete Command

Syntax:

```
  ras> adsl ppvc member delete <portlist> <vpi> <vci> <member vpi> <member
vci>
```

where

`<portlist>`	=	The port(s) of the PPVC. You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.
`<vpi>`	=	The VPI of the PPVC.
`<vci>`	=	The VCI of the PPVC.
`<member vpi>`	=	The VPI of the individual PVC that you are removing from the PPVC.
`<member vci>`	=	The VCI of the individual PVC that you are removing from the PPVC.

This command removes a PVC from a PPVC.

The following example removes a PVC that uses VPI 8 and VCI 36 from a PPVC with VPI 8 and VCI 35 for port 5.

Figure 271 PPVC Member Delete Command Example

```
ras> adsl ppvc member delete 5 8 35 8 36
```

58.6 PPVC Member Show Command

Syntax:

```
ras> adsl ppvc member show [<portlist> [<vpi> <vci>]]
```

where

`<portlist>`	=	The port(s) of the PPVC. You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.
`<vpi>`	=	The VPI of the PPVC.
`<vci>`	=	The VCI of the PPVC.
`<member vpi>`	=	The VPI of the individual PVC that you are displaying.
`<member vci>`	=	The VCI of the individual PVC that you are displaying.

This command displays the PVCs that are members of a PPVC.

The following example displays the PVCs that are members of a PPVC for port 5.

Figure 272 PPVC Member Show Command Example

```
ras> adsl ppvc member show 5
port vpi   vci mvpi  mvci  level DS/US vcprofile
---- --- ----- ---- ----- ------ --------------------
   5   8    35    8    36      2 DEFVAL/DEFVAL
```

58.6.1 PPVC Show Command

Syntax:

```
ras> adsl ppvc show [<portlist> [<vpi> <vci>]]
```

where

`<portlist>`	=	The port(s) of the PPVC. You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.
`<vpi>`	=	The VPI of the PPVC.
`<vci>`	=	The VCI of the PPVC.

This command displays the runtime configured PPVCs.

The following example displays the PPVCs configured on DSL port 5.

Figure 273 PPVC Show Command Example

```
ras> adsl ppvc show 5
port  vpi    vci  encap pvid pri
================================
  5     8     35   llc    25  6
```

58.6.2 PPVC Delete Command

Syntax:

```
ras> adsl ppvc delete <portlist> <vpi> <vci>
```

where

`<portlist>`	=	The port(s) of the PPVC. You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.
`<vpi>`	=	The VPI of the PPVC.
`<vci>`	=	The VCI of the PPVC.

This command removes a PPVC. Removing a PPVC also deletes all of the member PVCs.

The following example removes a PPVC with VPI 8 and VCI 35 for port 5.

Figure 274 PPVC Delete Command Example

```
ras> adsl ppvc delete 5 8 35
```

58.7 2684 Routed Mode Commands

Use the 2684 routed mode to have the AAM1212 add MAC address headers to 2684 routed mode traffic from a PVC that connects to a subscriber device that uses 2684 routed mode. You can also specify the gateway to which the AAM1212 sends the traffic and the VLAN ID tag to add. See RFC-2684 for details on routed mode traffic carried over AAL type 5 over ATM.

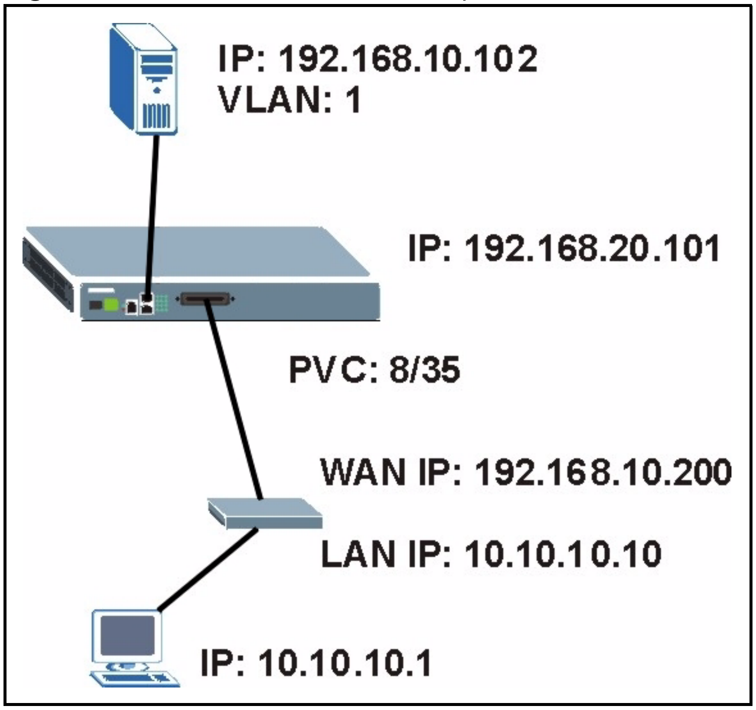
Use the commands in the following order to set up a 2684 routed mode PVC.

1 Use the `adsl rpvc gateway` commands to configure gateway settings.
2 Use the `adsl rpvc set` command to configure RPVCs (2684 routed mode PVCs) for 2684 routed mode traffic.
3 Use the `adsl rpvc route set` command to configure domains for 2684 routed mode traffic. The domain is the range of IP addresses behind the subscriber’s device (the CPE or Customer Premises Equipment). This includes the CPE device’s LAN IP addresses and the IP addresses of the LAN computers.
4 Use the `adsl rpvc arp` commands to view the Address Resolution Protocol table of IP addresses of CPE devices using 2684 routed mode and configure how long the device is to store them.
5 For upstream traffic: Since the subscriber's device will not send out a MAC address, after the AAM1212 reassembles the Ethernet packets from the AAL5 ATM cells, the AAM1212 will append the routed mode gateway's MAC address and the AAM1212's MAC address as the destination/source MAC address.
6 For downstream traffic: When the AAM1212 sees the destination IP address is specified in the RPVC (or RPVC domain), the AAM1212 will strip out the MAC header and send them to the corresponding RPVC.

58.7.1 2684 Routed Mode Example

The following figure shows an example RFC 2684 (formerly RFC 1483) routed mode set up. The gateway server uses IP address 192.168.10.102 and is in VLAN 1. The AAM1212 uses IP address 192.168.20.101. The subscriber's device (the CPE) is connected to DSL port 1 on the AAM1212 and the 2684 routed mode traffic is to use the PVC identified by VPI 8 and VCI 35. The CPE device's WAN IP address is 192.168.10.200. The routed domain is the LAN IP addresses behind the CPE device. The CPE device's LAN IP address is 10.10.10.10 and the LAN computer's IP address is 10.10.10.1. This includes the CPE device's LAN IP addresses and the IP addresses of the LAN computers.

Figure 275 2684 Routed Mode Example



Note the following.

- The CPE device's WAN IP (192.168.10.200 in this example) must be in the same subnet as the gateway's IP address (192.168.10.102 in this example).
- The AAM1212's management IP address can be any IP address, it doesn't have any relationship to the WAN IP address or routed gateway IP address.
- The AAM1212's management IP address should not be in the same subnet as the one defined by the WAN IP address and netmask of the subscriber's device. It is suggested that you set the netmask of the subscriber's WAN IP address to 32 to avoid this problem.
- The AAM1212's management IP address should not be in the same subnet range of any RPVC and RPVC domain. It will make the AAM1212 confused if the AAM1212 receives a packet with this IP as destination IP.
- The AAM1212's management IP address also should not be in the same subnet as the one defined by the LAN IP address and netmask of the subscriber's device. Make sure you assign the IP addresses properly.

- In general deployment, the computer must set the CPE device’s LAN IP address (10.10.10.10 in this example) as its default gateway.
- The subnet range of any RPVC and RPVC domain must be unique.

Use the following command sequence to configure the AAM1212 for this example set up.

Figure 276 2684 Routed Mode Commands Example

```
ras> adsl rpvc gateway set 192.168.10.102 1
ras> adsl rpvc set 1 8 35 DEFVAL 192.168.10.200/32 192.168.10.102
ras> adsl rpvc route set 1 8 35 10.10.10.1/24
```

58.7.2 RPVC Gateway Set Command

Syntax:

```
ras> adsl rpvc gateway set <gateway ip> <vlan id> [<priority>]
```

where

`<gateway ip>`	=	The IP address of the gateway to which you want to send the traffic that the system receives from this PVC. Enter the IP address in dotted decimal notation.
`<vlan id>`	=	The VLAN Identifier to add to Ethernet frames that the system routes to this gateway.
`[<priority>]`	=	Set the IEEE 802.1p priority (0~7) to add to the traffic that you send to this gateway.

This command adds a gateway IP address to use for 2684 routed mode traffic.

The following example has the device use a VLAN ID of 1 and IEEE 802.1p priority of 3 when sending 2684 routed mode traffic to a gateway at IP address 192.168.10.102.

Figure 277 RPVC Gateway Set Command Example

```
ras> adsl rpvc gateway set 192.168.10.102 1 3
```

58.7.3 RPVC Gateway Show Command

Syntax:

```
ras> adsl rpvc gateway show
```

`This command displays` the gateway IP addresses that are configured for use with 2684 routed mode traffic.

The following is an example.

Figure 278 RPVC Gateway Show Command Example

```
ras> adsl rpvc gateway show
gateway ip      vid
--------------- ----
192.168.10.102  1
```

58.7.4 RPVC Gateway Delete Command

Syntax:

```
ras> adsl rpvc gateway delete <gateway ip>
```

where

`<gateway ip>`	=	The IP address of the gateway to which you no longer want the device to send the traffic that the system receives from this PVC. Enter the IP address in dotted decimal notation.

This command removes a gateway IP address that the device was set to use for 2684 routed mode traffic.

The following example has the device remove a 2684 routed mode traffic gateway entry for IP address 192.168.10.102.

Figure 279 RPVC Gateway Delete Command Example

```
ras> adsl rpvc gateway delete 192.168.10.102
```

58.7.5 RPVC Set Command

Syntax:

```
  ras> adsl rpvc set <portlist> <vpi> <vci> <DS vcprofile[,US vcprofile]>
<ip>/<netmask> <gateway ip>
```

where

`<portlist>`	=	The port(s) of the RPVC. You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.
`<vpi>`	=	The VPI of the RPVC.
`<vci>`	=	The VCI of the RPVC.

`DS vcprofile`	=	Assign a VC profile to use for this channel's downstream traffic shaping.
`[,US vcprofile]>`	=	Assign a VC profile to use for policing this channel's upstream traffic. The AAM1212 does not perform upstream traffic policing if you do not specify an upstream VC profile.
`<ip>`	=	The subscriber's CPE WAN IP address in dotted decimal notation.
`/<netmask>`	=	The bit number of the subnet mask of the subscriber's IP address. To find the bit number, convert the subnet mask to binary and add all of the 1's together. Take "255.255.255.0" for example. 255 converts to eight 1's in binary. There are three 255's, so add three eights together and you get the bit number (24). Make sure that the routed PVC's subnet does not include the AAM1212's IP address.
`<gateway ip>`	=	The IP address of the gateway to which you want to send the traffic that the system receives from this PVC. Enter the IP address in dotted decimal notation.

This command adds a PVC to handle 2684 routed mode traffic.

Note: You must use the `rpvc gateway set` command to configure the gateway's settings before you use the `rpvc set` command.

The following example adds a PVC for 2684 routed mode traffic. It is for DSL port 1, VPI 8, VCI 35. It sets the DEFVAL profile for downstream traffic shaping and for upstream traffic policing. The CPE device's WAN IP address is 192.168.10.200 with a netmask of 32 and the gateway's IP address is 192.168.10.102.

Figure 280 RPVC Set Command Example

```
ras> adsl rpvc set 1 8 35 DEFVAL,DEFVAL 192.168.10.200/32 192.168.10.102
```

58.7.6 RPVC Show Command

Syntax:

```
ras> adsl rpvc show <portlist>
```

where

<portlist>	=	The port(s) for which you want to display the RPVCs. You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.

This command lists the PVCs for handling 2684 routed mode traffic (RPVCs).

The following example displays the RPVCs for DSL port 1.

Figure 281 RPVC Show Command Example

```
ras> adsl rpvc show 1
port vpi  vci ip/netmask         gateway ip      DS/US vcprofile
---- --- ---- ------------------ --------------- ---------------------------
   1   8    35 192.168.10.200/32  192.168.10.102  DEFVAL/DEFVAL
```

58.7.7 RPVC Delete Command

Syntax:

```
ras> adsl rpvc delete <portlist> <vpi> <vci>
```

where

<portlist>	=	The port(s) of the RPVC. You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.
<vpi>	=	The VPI of the RPVC.
<vci>	=	The VCI of the RPVC.

This command removes a PVC for 2684 routed mode traffic.

The following example removes a PVC for 2684 routed mode traffic. It is for DSL port 1, VPI 8, VCI 35.

Figure 282 RPVC Delete Command Example

```
ras> adsl rpvc delete 1 8 35
```

58.7.8 RPVC Route Set Command

Syntax:

```
ras> adsl rpvc route set <port number> <vpi> <vci> <ip>/<netmask>
```

where

`<port number>`	=	The port of the RPVC. Specify a single DSL port <1>.
`<vpi>`	=	The VPI of the RPVC.
`<vci>`	=	The VCI of the RPVC.
`<ip>`	=	The subscriber's CPE LAN IP address in dotted decimal notation.
`/<netmask>`	=	The bit number of the subnet mask of the subscriber's IP address. To find the bit number, convert the subnet mask to binary and add all of the 1's together. Take "255.255.255.0" for example. 255 converts to eight 1's in binary. There are three 255's, so add three eights together and you get the bit number (24).

This command adds a domain for 2684 routed mode traffic. The domain includes the subscriber's LAN IP addresses.

Note: You must use the `rpvc gateway set` and the `rpvc set` commands before you use the `rpvc route set` command.

The following example adds a domain for a CPE device is connected to DSL port 1 on the AAM1212 and the 2684 routed mode traffic is to use the PVC identified by VPI 8 and VCI 35. The CPE device's LAN IP address is 10.10.10.10 and uses a subnet mask of 255.255.255.0. This includes the CPE device's LAN IP addresses and the IP addresses of the LAN computers.

Figure 283 RPVC Route Set Command Example

```
ras> adsl rpvc route set 1 8 35 10.10.10.1/24
```

58.7.9 RPVC Route Show Command

Syntax:

```
ras> adsl rpvc route show <portlist>
```

where

`<portlist>`	=	The port(s) of the RPVC. You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.

This command lists the domains for 2684 routed mode traffic.

The following example displays the domains for 2684 routed mode traffic for devices connected to DSL ports 1 and 2.

Figure 284 RPVC Route Show Command Example

```
ras> adsl rpvc route show 1,2
port vpi vci ip/netmask
---- --- --- ------------------
   1   8  35 10.10.10.0/24
   2   8  35 10.10.11.0/24
```

58.7.10 RPVC Route Delete Command

Syntax:

```
ras> adsl rpvc route delete <port number> <vpi> <vci> <ip>/<netmask>
```

where

`<port number>`	=	The port of the RPVC. Specify a single DSL port <1>.
`<vpi>`	=	The VPI of the RPVC.
`<vci>`	=	The VCI of the RPVC.
`<ip>`	=	The subscriber’s CPE LAN IP address in dotted decimal notation.
`/<netmask>`	=	The bit number of the subnet mask of the subscriber’s IP address. To find the bit number, convert the subnet mask to binary and add all of the 1’s together. Take “255.255.255.0” for example. 255 converts to eight 1’s in binary. There are three 255’s, so add three eights together and you get the bit number (24).

This command removes a domain for 2684 routed mode traffic. The domain includes the subscriber’s LAN IP addresses.

The following example removes a domain for a CPE device is connected to DSL port 1 on the AAM1212 and the 2684 routed mode traffic is to use the PVC identified by VPI 8 and VCI 35. The CPE device's LAN IP address is 10.10.10.10 and uses a subnet mask of 255.255.255.0. This includes the CPE device's LAN IP addresses and the IP addresses of the LAN computers.

Figure 285 RPVC Route Delete Command Example

```
ras> adsl rpvc route delete 1 8 35 10.10.10.1/24
```

58.7.11 RPVC ARP Agingtime Set Command

Syntax:

```
ras> adsl rpvc arp agingtime set <sec>
```

where

<sec>	=	The number of seconds (10~10000) the device is to keep the Address Resolution Protocol table's entries of IP addresses of 2684 routed mode gateways. Use 0 to disable the aging time.

This command configures how long the device stores the IP addresses of CPE devices using 2684 routed mode in the Address Resolution Protocol table.

The following example sets the device to store the IP addresses 2684 routed mode gateways in the Address Resolution Protocol table for 500 seconds.

Figure 286 RPVC ARP Agingtime Command Example

```
ras> adsl rpvc arp agingtime set 500
```

58.7.12 RPVC ARP Agingtime Show Command

Syntax:

```
ras> adsl rpvc arp agingtime show
```

This command displays how long the device stores the IP addresses of 2684 routed mode gateways in the Address Resolution Protocol table.

The following is an example.

Figure 287 RPVC ARP Agingtime Show Command Example

```
ras> adsl rpvc arp agingtime show
rpvc aging time (sec): 500
```

58.7.13 RPVC ARP Show Command

Syntax:

```
ras> adsl rpvc arp show
```

`This command` displays how long the device stores the IP addresses of 2684 routed mode gateways in the Address Resolution Protocol table.

The following is an example.

Figure 288 RPVC ARP Agingtime Show Command Example

```
ras> adsl rpvc arp show
gateway ip       vid  mac
---------------  ---- -----------------
192.168.10.102      1 00:0d:9d:d9:43:3b
```

58.7.14 RPVC ARP Flush Command

Syntax:

```
ras> adsl rpvc arp flush
```

`This command` clears the IP addresses of 2684 routed mode gateways from the Address Resolution Protocol table.

58.8 PPPoA to PPPoE (PAE) Commands

You can use these commands to create PVCs for PAE translation.

58.8.1 PAE PVC Delete Command

Syntax:

```
ras> adsl paepvc delete <portlist> <vpi> <vci>
```

where

`<portlist>`	=	The port number of the PAE PVC. You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.
`<vpi>`	=	The VPI of the PAE PVC.
`<vci>`	=	The VCI of the PAE PVC.

This command removes a PAE PVC.

58.8.2 PAE PVC Set Command

Syntax:

```
  ras> adsl paepvc set <portlist> <vpi> <vci> <DS vcprofile[,US vcprofile]>
<pvid> <priority> [acname <acname>] [srvcname <srvcname>] [hellotime
<hellotime>]
```

where

`<portlist>`	=	The port number of the PAE PVC. You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.
`<vpi>`	=	The VPI of the PAE PVC.
`<vci>`	=	The VCI of the PAE PVC.
`<DS vcprofile`	=	Assign a VC profile to use for this channel's downstream traffic shaping.
`[,US vcprofile]>`	=	Assign a VC profile to use for policing this channel's upstream traffic. The AAM1212 does not perform upstream traffic policing if you do not specify an upstream VC profile.
`<pvid>`	=	1 – 4094; the VLAN Identifier to add to Ethernet frames that the system routes using this PVC.
`<priority>`	=	Set the IEEE 802.1p priority (0~7) to add to the traffic that uses this PVC.
`<acname>`	=	This field is optional. Specify the hostname of a remote access concentrator if there are two access concentrators (or BRAS) on the network or that you want to allow PAE translation to the specified access concentrator.
`<srvcname>`	=	This field is optional. Specify the name of the service that uses this PVC. This must be a service name that you configure on the remote access concentrator.
`<hellotime>`	=	0 - 600; specify the timeout, in seconds, for the PPPoE session. Enter 0 if there is no timeout.

This command creates a PPPoA-to-PPPoE PVC to allow communication between the ATM (CPE) and Ethernet network (BRAS) segments. The PVC is mapped to a PPPoE session that connects to the specified BRAS.

The following example creates a PPPoA-to-PPPoE PVC (`1/33`) for port `1`. The VLAN ID is 1, and the IEEE 802.1p priority is 0. This configuration is for the `video` service on the `vom` access concentrator. The switch waits 10 seconds before terminating the PPPoE session.

Figure 289 PAE PVC Set Command Example

```
ras> adsl paepvc set 1 1 33 DEFVAL 1 0 acname vom srvcname video hellotime 10
```

58.8.3 PAE PVC Show Command

Syntax:

```
ras> adsl paepvc show <portlist> [<vpi> <vci>]
```

where

`<portlist>`	=	The port number of the PAE PVC. You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.
`<vpi>`	=	The VPI of the PAE PVC.
`<vci>`	=	The VCI of the PAE PVC.

This command displays the PPPoA-to-PPPoE PVC settings for the specified port(s) or PVCs.

The following example displays the settings for port 1.

Figure 290 PAE PVC Show Command Example

```
ras> adsl paepvc show 1
port vpi   vci pvid pri htime US/DS vcprofile/acname/srvcname
---- --- ----- ---- --- ----- ----------------------------------
   1   1    33    1   0    10 dsprofile: DEFVAL
                              usprofile:
                              acname   : vom
                              srvcname : video
```

58.8.4 PAE PVC Session Command

Syntax:

```
ras> adsl paepvc session <portlist> [<vpi> <vci>]
```

where

`<portlist>`	=	The port number of the PAE PVC. You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.
`<vpi>`	=	The VPI of the PAE PVC.
`<vci>`	=	The VCI of the PAE PVC.

This command displays the status of PPPoA-to-PPPoE PVC sessions on the specified port(s) or PVCs.

The following example displays the settings for port 1.

Figure 291 PAE PVC Session Command Example

```
ras> adsl paepvc session 1
pvc 1-1/33
session state : down
session id    : 0
session uptime: 0 secs
acname        :
srvcname      :
```

58.8.5 PAE PVC Counter Command

Syntax:

```
ras> adsl paepvc counter <portlist> [<vpi> <vci>]
```

where

`<portlist>`	=	The port number of the PAE PVC. You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.
`<vpi>`	=	The VPI of the PAE PVC.
`<vci>`	=	The VCI of the PAE PVC.

This command displays statistics about PPPoA-to-PPPoE PVC activity.

The following example displays the statistics for port 1.

Figure 292 PAE PVC Counter Command Example

```
ras> adsl paepvc counter 1
pvc 1-1/33
                                 tx                rx
                          ---------------- ----------------
 ppp lcp config-request :                -                0
 ppp lcp echo-request   :                -                0
 ppp lcp echo-reply     :                -                0
 pppoe padi             :                0                -
 pppoe pado             :                -                0
 pppoe padr             :                0                -
 pppoe pads             :                -                0
 pppoe padt             :                0                0
 pppoe srvcname error   :                -                0
 pppoe ac system error  :                -                0
 pppoe generic error    :                0                0
```

Each value is described below.

`tx/rx`	=	The values in these columns are for packets transmitted (`tx`) or received (`rx`) by the AAM1212.
`ppp lcp config-request`	=	The number of config-request PDUs received by the AAM1212 from the CPE (client) device.
`ppp lcp echo-request`	=	The number of echo-request PDUs received by the AAM1212 from the CPE (client) device.
`ppp lcp echo-reply`	=	The number of echo-reply PDUs received by the AAM1212 from the CPE (client) device.
`pppoe padi`	=	The number of padi PDUs sent by the AAM1212 to the BRAS.
`pppoe pado`	=	The number of pado PDUs sent by the BRAS to the AAM1212.
`pppoe padr`	=	The number of padr PDUs sent by the AAM1212 to the BRAS.
`pppoe pads`	=	The number of pads PDUs sent by the BRAS to the AAM1212.
`pppoe padt`	=	The number of padt PDUs sent and received by the AAM1212.
`pppoe srvcname error`	=	The number of service name errors; for example, the AAM1212's specified service is different than the BRAS's setting.
`pppoe ac system error`	=	The number of times the access concentrator experienced an error while performing the Host request; for example, when resources are exhausted in the access concentrator. This value does not include the number of times the AAM1212 checks the AC name field in the BRAS's reply PDU and finds a mismatch, however.
`pppoe generic error`	=	The number of other types of errors that occur in the PPPoE session between the AAM1212 and the BRAS.

58.9 Transparent LAN Service (TLS) Commands

Note: You can NOT configure PPPoA-to-PPPoE and TLS settings on the same PVC.

58.9.1 TLS PVC Delete Command

Syntax:

```
ras> adsl tlspvc delete <portlist> <vpi> <vci>
```

where

`<portlist>`	=	The port number of the TLS PVC. You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.

<vpi>	=	The VPI of the TLS PVC.
<vci>	=	The VCI of the TLS PVC.

This command clears TLS settings for the PVC.

58.9.2 TLS PVC Set Command

Syntax:

```
  ras> adsl tlspvc set <portlist> <vpi> <vci> <DS vcprofile[,US vcprofile]>
<pvid> <priority>
```

where

<portlist>	=	The port number of the TLS PVC. You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.
<vpi>	=	The VPI of the TLS PVC.
<vci>	=	The VCI of the TLS PVC.
<DS vcprofile	=	Assign a VC profile to use for this channel's downstream traffic shaping.
[,US vcprofile]>	=	Assign a VC profile to use for policing this channel's upstream traffic. The AAM1212 does not perform upstream traffic policing if you do not specify an upstream VC profile.
<pvid>	=	1 – 4094; the (second) VLAN Identifier to add to Ethernet frames that the system routes using this PVC.
<priority>	=	Set the IEEE 802.1p priority (0~7) to add to the traffic that uses this PVC.

This command sets the second VLAN tag to add to the packets from the PVC.

The following example adds VLAN tag `100` to traffic using the `DEFVAL` ATM profile on PVC (`1/33`) on port `2`.

Figure 293 TLS PVC Set Command Example

```
ras> adsl tlspvc set 2 1 33 DEFVAL 100 0
```

58.9.3 TLS PVC Show Command

Syntax:

```
  ras> adsl tlspvc show <portlist> [<vpi> <vci>]
```

where

`<portlist>`	=	The port number of the TLS PVC. You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.
`<vpi>`	=	The VPI of the TLS PVC.
`<vci>`	=	The VCI of the TLS PVC.

This command displays the TLS settings for the specified port(s) or PVC(s). The following example shows the TLS settings on port 2.

TLS PVC Show Command Example

```
ras> adsl tlspvc show 2
port vpi   vci  pvid pri DS/US vcprofile
---- --- ----- ----- --- ----------------------------------
   2   1    33   100   0 DEFVAL
```

59

ACL Commands

An ACL (Access Control Logic) profile allows the system to classify and perform actions on the upstream traffic. Use the ACL Profile commands to set up ACL profiles and the ACL Assignment commands to apply them to PVCs.

59.1 ACL Profile Commands

Use these commands to set up ACL profiles.

59.1.1 ACL Profile Set Command

Syntax:

```
ras> switch acl profile set <name> <rule> <action>
```

where

`<name>`	=	The name of the ACL profile.
`<rule>`	=	The rule that classifies traffic flows. See below.
`<action>`	=	One or more actions to perform on the classified packets. You can select one or more of the following actions.

- `rate <rate>` = Sets the transmission rate (1~65535 in kbps) for the matched traffic.
- `rvlan <rvlan>` = Replaces the VLAN ID with this VLAN ID (1~4094).
- `rpri <rpri>` = Replaces the priority with this priority (0 ~7) of the matched packets.
- `deny` = Drops the packets.

This command configures an ACL rule to classify the upstream traffic and perform action(s) on the classified traffic.

The following lists the set of criteria you can configure for rules in ACL profiles. The rules are listed in sequence from highest priority to lowest priority. The criteria within a rule are position-independent.

- `etype <etype> vlan <vid>`
- `etype <etype> smac <mac>`
- `etype <etype> dmac <mac>`

- vlan < vid > smac <mac>
- vlan < vid > dmac <mac>
- smac < mac > dmac <mac>
- vlan < vid > priority <priority>
- etype <etype>
- vlan <vid>
- smac <mac>
- dmac <mac>
- priority <priority>
- protocol <protocol>
- srcip <ip>/<mask> [dstip <ip>/<mask> [tos <tos> [srcport <sport> <eport> [dstport <sport> <eport>]]]]

where

- etype <etype> = Ethernet type (0~65535).
- vlan <vid> = VLAN ID (1~4094).
- smac <mac> = Source MAC address.
- dmac <mac> = Destination MAC address.
- priority <priority> = Priority (0 ~ 7)
- protocol <protocol> = Protocol type: tcp, udp, ospf, igmp, ip, gre, icmp or user specified IP protocol number <0 ~ 255>.
- srcip <ip>/<mask> = Source IP address and subnet mask (0~32).
- dstip <ip>/<mask> = Destination IP address and subnet mask (0~32).
- tos <stos> <etos> = Sets the ToS (Type of Service) range between 0 and 255.
- srcport <sport> <eport> = Source port range (0~65535).
- dstport <sport> <eport> = Destination port range (0~65535).

The following guidelines apply to classifiers.

- You can apply one classifier for a protocol on a port's PVC.
- You cannot create a classifier that contains matching criteria for layer 2 and layer 3 fields. For example switch acl profile set test protocol tcp vlan 15 deny is not allowed as protocol type and VLAN do not belong to the same network layer.
- Each type of criteria can only be used once in a classifier. For example, profile acl set test protocol tcp protocol udp deny is not allowed. For this example, you need to create a separate classifier for each protocol and apply them to the same PVC(s).

The following example creates an ACL rule example named test for traffic from VLAN 10 with a priority level of 2. This rule limits the rate on the classified traffic to 1000 kbps and changes the priority level to 7.

Figure 294 ACL Profile Set Command Example

```
ras> switch acl profile set test vlan 10 priority 2 rate 1000 rpri 7
```

59.1.2 ACL Profile Delete Command

Syntax:

```
ras> switch acl profile delete <name>
```

where

`<name>`	=	The name of the ACL profile.

This command removes the specified ACL profile.

Note: You cannot remove the ACL profile(s) that is currently in use.

59.1.3 ACL Profile Show Map Command

Syntax:

```
ras> switch acl profile showmap <name>
```

where

`<name>`	=	The name of the ACL profile.

This command displays the DSL port(s) to which the specified ACL profile is applied.

The following example displays the port mapping table for the `example` ACL profile.

Figure 295 ACL Profile Show Map Command Example

```
ras> switch acl profile showmap test
profile: test
port type   vpi   vci
---- ------ --- -----
```

59.1.4 ACL Profile Show Command

Syntax:

```
ras> switch acl profile show [<name>]
```

where

`<name>`	=	The name of the ACL profile.

This command lists the names of every ACL profile or displays the detailed settings of the specified ACL profile.

Figure 296 ACL Profile Show Command Example

```
ras> switch acl profile show test
profile test:
rule:
  vlan   :10
  priority:2

action:
  rpri    :7
  rate    :1000
```

59.2 ACL Assignment Commands

Use these commands to apply ACL profiles to PVCs.

59.2.1 ACL Assignment Set Command

Syntax:

```
ras> switch acl set <portlist> <vpi> <vci> <profile>
```

where

`<portlist>`	=	The port number of the PVC. You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.
`<vpi>`	=	The VPI of the PVC.
`<vci>`	=	The VCI of the PVC.
`<profile>`	=	The name of the ACL profile.

This command allows you to apply an ACL profile to the specified port(s). You can apply up to eight profiles to a subscriber port.

The following example applies the ACL profile “test” to a PVC.

Figure 297 ACL Assignment Set Command Example

```
ras> switch acl set 1 0 33 test
```

59.2.2 ACL Assignment Delete Command

Syntax:

```
ras> switch acl delete <portlist> <vpi> <vci> <profile>
```

where

<portlist>	=	The port number of the PVC. You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.
<vpi>	=	The VPI of the PVC.
<vci>	=	The VCI of the PVC.
<profile>	=	The name of the ACL profile.

This command allows you to remove an ACL profile from the specified PVC.

59.2.3 ACL Assignment Show Command

Syntax:

```
ras> switch acl show [<portlist>] [<vpi> <vci>]
```

where

<portlist>	=	The port number of the PVC. You can specify a single DSL port <1>, all DSL ports <*> or a list of DSL ports <1,3,5>. You can also include a range of ports <1,5,6~10>.
<vpi>	=	The VPI of the PVC.
<vci>	=	The VCI of the PVC.

This command displays the current ACL profiles applied to the specified PVC(s). The following figure shows an example.

Figure 298 ACL Assignment Show Command Example

```
ras> switch acl show
port vpi   vci type profile
---- --- ----- ---- --------------------------------
   1   0    33 PVC  test
```

PART VII
Troubleshooting and Product Specifications

Troubleshooting (461)
Product Specifications (471)

60

Troubleshooting

This chapter covers potential problems and possible remedies. After each problem description, some steps are provided to help you to diagnose and solve the problem.

60.1 The SYS LED Does Not Turn On

The SYS LED does not turn on.

Table 110 SYS LED Troubleshooting

STEP	CORRECTIVE ACTION
1	Make sure the AAM1212 is securely connected to the IES-1000.
2	Make sure the IES-1000 is properly connected to the power supply and the power supply is operating normally. Make sure you are using the correct power source. (See the IES-1000 User's Guide.)
3	The LED itself or the unit may be faulty; contact your vendor.

60.2 The ALM LED Is On

The **ALM** (alarm) LED lights when the AAM1212 is overheated or the voltage readings are outside the tolerance levels.

Table 111 ALM LED Troubleshooting

STEP	CORRECTIVE ACTION
1	Use the statistics monitor command to verify the cause of the alarm. See step 2 if the unit is overheated and step 3 if the voltages are out of the allowed ranges.
2	Ensure that the AAM1212 is installed in a well-ventilated area. Keep the bottom, top and all sides clear of obstructions and away from the exhaust of other equipment.
3	If the voltage levels are outside the allowed range, take a screen shot of the statistics monitor command display and contact your vendor.

60.3 LAN Port LEDs Do Not Turn On

A LAN port's LEDs do not turn on.

Table 112 10/100 LED Troubleshooting

STEPS	CORRECTIVE ACTION
1	Check the **Speed Mode** settings in the **ENET Port Setup** screen. Make sure that the LAN port's connection speed is set to match that of the port on the peer Ethernet device.
2	Check the Ethernet cable and connections between the LAN port and the peer Ethernet device.
3	Make sure that the peer Ethernet device is functioning properly. If the Ethernet cable and peer Ethernet device are both OK and the LEDs still stay off, there may be a problem with the port. Contact the distributor.

60.4 LAN Port Data Transmission

The LAN port's LED is on, but data cannot be transmitted.

Table 113 Troubleshooting Data Transmission

STEPS	CORRECTIVE ACTION
1	Make sure that the LAN port has the appropriate mode setting.
2	Make sure that the AAM1212's IP settings are properly configured.
3	Check the VLAN configuration.
4	Ping the AAM1212 from a computer behind the peer Ethernet device.
5	If you cannot ping, check the Ethernet cable and connections between the Ethernet port and the Ethernet switch or router.
6	Check the switch mode. In daisychain mode, if you have a loop topology and enable RSTP, it is possible for RSTP to disable Ethernet port 1 (the uplink port). **Note:** It is not recommended to use daisychain mode in a loop topology.

60.5 DSL Data Transmission

The DSL link is up, but data cannot be transmitted.

Table 114 DSL Data Transmission Troubleshooting

STEPS	CORRECTIVE ACTION
1	Check the switch mode and port isolation settings. Check to see that the VPI/VCI and multiplexing mode (LLC/VC) settings in the subscriber's DSL modem or router match those of the DSL port. If the subscriber is having problems with a video or other high-bandwidth services, make sure the AAM1212's DSL port's data rates are set high enough.
2	Check the VLAN configuration.
3	Ping the AAM1212 from the computer behind the DSL modem or router.
4	If you cannot ping, connect a DSL modem to a DSL port (that is known to work). If the DSL modem or router works with a different DSL port, there may be a problem with the original port. Contact the distributor.
5	If using a different port does not work, try a different DSL modem or router with the original port.

60.6 There Is No Voice on a DSL Connection

The AAM1212 has internal splitters and CO side Telco-50 connectors that allow the telephone wiring used for DSL connections to also simultaneously carry normal voice conversations.

Table 115 DSL Voice Troubleshooting

STEP	CORRECTIVE ACTION
1	Make sure the subscriber has a splitter properly installed.
2	Check the DSL line pin assignments shown in Chapter 61 on page 471.
3	Check the telephone wire connections between the subscriber and the MDF(s).
4	Check the telephone wire and connections between the MDF(s) and **USER** port(s).
5	Check the telephone wire and connections between the MDF(s) and the **CO** connector(s). Check the connection from the MDF(s) to the telephone company or the PBX.
6	Check the telephone wire mapping on the MDF(s).
7	Make sure the in-house wiring works and is connected properly.
8	Repeat the steps above using a different DSL port.

60.7 Testing Wiring

Use the following tests if there is no voice.

Systematically test wiring using a functioning telephone to determine if there is a wiring problem. If the connection is good, the telephone will return a dial tone. Letters in the figure shown next indicate the systematic tests to be done. Suppose you're using installation scenario "B" as shown in the chapter on MDF connections. The logic for other scenarios should be similar.

Use steps A-D if there is no voice but you can transmit data. Use all of the steps if there is no voice and you cannot transmit data.

Table 116 Wiring Tests

TEST	DESCRIPTION
A.	Test A determines if there is a wiring problem between the TELCO (telephone company) and MDF 1.
B.	Test B determines if there is a wiring problem between MDF 1 and MDF 2.
C.	Test C determines if there is a wiring problem between MDF 2 and your device.
D.	Test D determines if there is a problem with your device's internal splitter.
E.	Test E determines if there is a wiring problem between your device and MDF 3.
F.	Test F determines if there is a building-wiring problem between the subscriber's wall jack and MDF 3.

Figure 299 Testing In-house Wiring

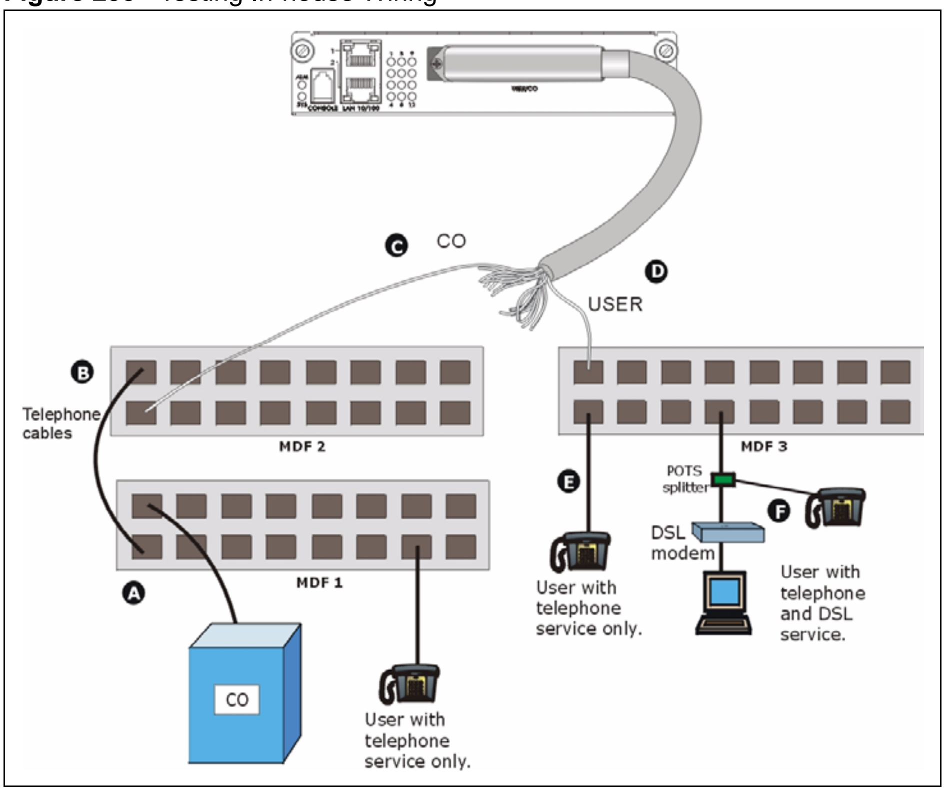


Table 117 Testing In-house Wiring

STEP	TEST
A	Connect a standard telephone to MDF 1. If there is no dial tone, then a problem with the wire or wire connections between MDF 1 and the TELCO exists. Contact your telephone company for troubleshooting.
B	Connect a telephone to the upper port of MDF 2. If there is no dial tone, then the problem is between MDF 1 and MDF 2. Check the telephone wire and connections between MDFs 1 and 2.
C	Disconnect the telephone wire from **CO**. Connect a telephone to the telephone wire. If there is no dial tone, then the problem is between your device and MDF 2. Check the telephone wire's pin assignments (see Chapter 61 on page 471 for the proper pin assignments). Replace the telephone wire if the pin assignments are OK and there is still no dial tone.
D	Reconnect the telephone wire to **CO**. Disconnect the telephone wire from **USER**. Connect a telephone to **USER** (see Chapter 61 on page 471 for the proper pin assignments). If there is no dial tone, your device's internal splitter may be faulty, contact your vendor.
E	Reconnect the telephone wire to **USER**. Connect a telephone to a lower port of MDF 3. If there is no dial tone, then the problem is between your device and MDF 3. Check the pin assignments of the telephone wire's connector that connects to **USER**. Replace the telephone wire connecting your device to MDF 3. If there is no dial tone, then MDF 3 may be faulty. Contact the telephone company if that is the case.
F	Disconnect the DSL modem from the wall jack and connect the telephone to the wall jack. If there is no dial tone, then there is a problem with the building wiring between the DSL subscriber's home and the MDF. Contact your telephone company for troubleshooting.

60.8 Local Server

The computer behind a DSL modem or router cannot access a local server connected to the AAM1212.

Table 118 Troubleshooting a Local Server

STEPS	CORRECTIVE ACTION
1	See Section 60.5 on page 463 to make sure that the subscriber is able to transmit to the AAM1212.
2	Make sure the computer behind the DSL device has the correct gateway IP address configured.
3	Check the VLAN configuration (see Chapter 16 on page 149).
4	Check the cable and connections between the AAM1212 and the local server.
5	Try to access another local server. If data can be transmitted to a different local server, the local server that could not be accessed may have a problem.

60.9 Data Rate

The SYNC-rate is not the same as the configured rate.

Table 119 Troubleshooting the SYNC-rate

STEPS	CORRECTIVE ACTION
1	Connect the DSL modem or router directly to the DSL port using a different telephone wire.
2	If the rates match, the quality of the telephone wiring that connects the subscriber to the DSL port may be limiting the speed to a certain rate. If they do not match when a good wire is used, contact the distributor.

60.10 Configured Settings

The configured settings do not take effect.

Table 120 Troubleshooting the AAM1212's Configured Settings

CORRECTIVE ACTION
Use the "config save" command after you finish configuring to save the AAM1212's settings.

60.11 Password

If you forget your password, you will need to use the console port to reload the factory-default configuration file (see Section 60.15 on page 467).

60.12 System Lockout

Any of the following could also lock you and others out from using in-band management (managing through the data ports).

1. Deleting the management VLAN (default is VLAN 1).
2. Incorrectly configuring the CPU VLAN.
3. Incorrectly configuring the access control settings.
4. Disabling all ports.

Note: Be careful not to lock yourself and others out of the system.

If you lock yourself (and others) out of the system, you can try using the console port to reconfigure the system. See Section 60.15 on page 467.

60.13 SNMP

The SNMP manager server cannot get information from the AAM1212.

Table 121 Troubleshooting the SNMP Server

STEPS	CORRECTIVE ACTION
1	Ping the AAM1212 from the SNMP server. If you cannot, check the cable, connections and IP configuration.
2	Check to see that the community (or trusted host) in the AAM1212 matches the SNMP server's community.
3	Make sure that your computer's IP address matches a configured trusted host IP address (if configured).
4	Incorrectly configuring the access control settings may lock you out from using in-band management. Try using the console port to reconfigure the system.

60.14 Telnet

I cannot telnet into the AAM1212.

Table 122 Troubleshooting Telnet

STEPS	CORRECTIVE ACTION
1	Make sure that the number of current telnet sessions does not exceed the maximum allowed number. You cannot have more than five telnet sessions at one time.
2	Make sure that your computer's IP address matches a configured secured client IP address (if configured). The AAM1212 immediately disconnects the telnet session if secured host IP addresses are configured and your computer's IP address does not match one of them.
3	Make sure that you have not disabled the Telnet service or changed the server port number that the AAM1212 uses for Telnet.
4	Ping the AAM1212 from your computer. If you are able to ping the AAM1212 but are still unable to telnet, contact the distributor. If you cannot ping the AAM1212, check the cable, connections and IP configuration.
5	Incorrectly configuring the access control settings may lock you out from using in-band management. Try using the console port to reconfigure the system.

60.15 Resetting the Defaults

If you lock yourself (and others) from the AAM1212, you will need to reload the factory-default configuration file. Uploading the factory-default configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all previous configurations and the speed of the console port will be reset to the default of 9600 bps with 8 data bit, no parity, one stop bit and flow control set to none. The user name will be reset to “admin” and the password will be reset to “1234” and the IP address to 192.168.1.1.

60.15.1 Resetting the Defaults Via Command

If you know the password, you can reload the factory-default configuration file via Command Line Interface (CLI) command. Use the following procedure.

1 Connect to the console port using a computer with terminal emulation software. See Section 3.1.3 on page 48 for details.

2 Enter your password.

3 Type `config restore`.

4 Type `y` at the question “Do you want to restore default ROM file(y/n)?”

5 The AAM1212 restarts.

Figure 300 Resetting the Switch Via Command

```
ras> config restore

System will reboot automatically after restoring default configuration.
Do you want to proceed(y/n)? >
restoring configuration...
saving configuration to flash...
```

The AAM1212 is now reinitialized with a default configuration file including the default user name of “admin” and the default password of “1234”.

60.15.2 Uploading the Default Configuration File

If you forget your password or cannot access the AAM1212, you will need to reload the factory-default configuration file. Uploading the factory-default configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all previous configurations and the speed of the console port will be reset to the default of 9600 bps with 8 data bit, no parity, one stop bit and flow control set to none. The password will also be reset to “1234” and the IP address to 192.168.1.1.

Note: Uploading the factory default configuration file erases the AAM1212’s entire configuration.

Obtain the default configuration file, unzip it and save it in a folder. Use a console cable to connect a computer with terminal emulation software to the AAM1212’s console port. Turn the AAM1212 off and then on to begin a session. When you turn on the AAM1212 again you will see the initial screen. When you see the message `Press any key to enter Debug Mode within 3 seconds` press any key to enter debug mode.

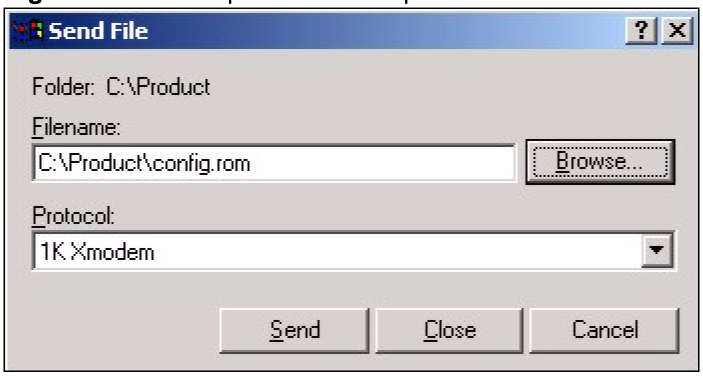
To upload the configuration file, do the following:

1 Type `atlc` after the `Enter Debug` Mode message.

2 Wait for the `Starting XMODEM upload` message before activating XMODEM upload on your terminal.

3 This is an example Xmodem configuration upload using HyperTerminal. Click **Transfer**, then **Send File** to display the following screen.

Figure 301 Example Xmodem Upload



Type the configuration file's location, or click **Browse** to search for it. Choose the **1K Xmodem** protocol. Then click **Send**.

4 After a successful configuration file upload, type `atgo` to restart the AAM1212.

The AAM1212 is now reinitialized with a default configuration file including the default password of “1234”.

60.16 Recovering the Firmware

Usually you should use FTP or the web configurator to upload the AAM1212’s firmware. If the AAM1212 will not start up, the firmware may be lost or corrupted. Use the following procedure to upload firmware to the AAM1212 only when you are unable to upload firmware through FTP.

Note: This procedure is for emergency situations only.

1 Obtain the firmware file, unzip it and save it in a folder on your computer.

2 Connect your computer to the console port and use terminal emulation software configured to the following parameters:

- VT100 terminal emulation
- 9600 bps
- No parity, 8 data bits, 1 stop bit
- No flow control

3 Turn off the AAM1212 and turn it back on to restart it and begin a session.

4 When you see the message `Press any key to enter Debug Mode within 3 seconds`, press a key to enter debug mode.

5 Type `atba5` after the `Enter Debug Mode` message (this changes the console port speed to 115200 bps).

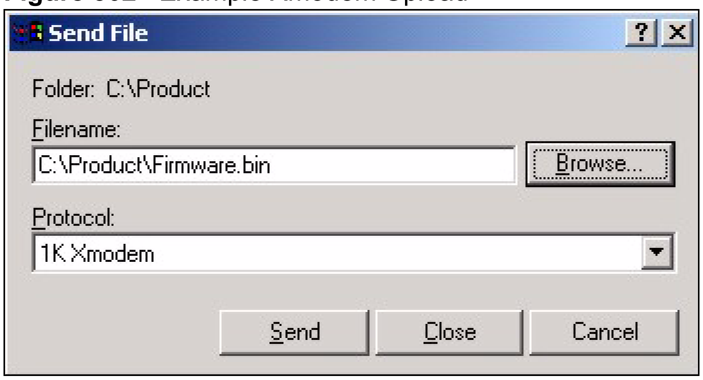
6 Change the configuration of your terminal emulation software to use 115200 bps and reconnect to the AAM1212.

7 Type `atur` after the `Enter Debug Mode` message.

8 Wait for the `Starting XMODEM upload` message before activating XMODEM upload on your terminal.

9 This is an example Xmodem configuration upload using HyperTerminal. Click **Transfer**, then **Send File** to display the following screen.

Figure 302 Example Xmodem Upload



10 Type the firmware file's location, or click **Browse** to search for it. Choose the **1K Xmodem** protocol. Then click **Send**.

11 After a successful firmware upload, type `atgo` to restart the AAM1212. The console port speed automatically changes back to 9600 bps when the AAM1212 restarts.

61

Product Specifications

This chapter provides the specifications for the AAM1212.

Table 123 Device Specifications

FEATURE	DESCRIPTION
Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
User Name	admin
Default Password	1234
Dimensions	166.8 mm (W) x 296 mm (D) x 44.45 mm (H)
Weight	1.234 kg
Power Specification	15V DC 25Watts
Interface	• One Telco-50 connector: 12 ADSL2+ Ports (Pin 1~12 and 26~37 for CO, Pin 14~25 and 39~50 for USER) • One mini RJ11 console port for local management • Two 10/100BASE-T Ethernet ports for uplink
MAC Address Table	Up to 9.5K entries
ARP Table	Up to 500 entries
Operation Temperature	0º C ~ 50º C
Storage Temperature	-40º C ~ 85º C
Operation Humidity	10% ~ 95% RH (non-condensing)
Storage Humidity	5% ~ 95% RH (non-condensing)
Certifications	Safety UL1950 CSA C22.2 No. 950 EN60950-1, EN41003 EMC FCC Part 15 Class A EN55022 Class A
System Management	• Embedded Web Configurator (HTTP) • CLI (Command Line Interpreter) • Remote Management via Telnet or Web • SNMP manageable • Firmware Upgrade (web configurator, FTP)

Table 123 Device Specifications (continued)

FEATURE	DESCRIPTION
Other Features	• MAC filtering • MAC count limiting • Access Control List • Hardware-based multicasting • IEEE 802.1Q VLAN Tagging • GVRP • IEEE 802.1p CoS with priority queuing • IEEE 802.1w RSTP • IGMP v1 & v 2 snooping • DHCP relay option82 • IEEE 802.1x Port-based Authentication • SNMP v1 & v2c
MIBs	• MIB-II, IF-MIB, Q-MIB, P-MIB • ADSL line MIB • ZyXEL proprietary MIBs

Per ADSL port limitations:

- Number of MAC filter: 10
- Number of PVC: 8
- Number of PPVC: 2
- Number of PPVC member: 8
- Number of RPVC: 8
- Number of TLSPVC: 8
- Number of PAEPVC: 8
- Number of VLAN: 16
- IGMP maximum group per DSL port is 16
- IGMP maximum host IPs per DSL port is 16
- IGMP maximum host IPs per Ethernet port is 1024
- Number of DHCP snooping: 32
- Maximum joined MVLAN: 4
- Maximum ACL profile mapping: 8

System limitations:

- Number of VLAN: 256
- ADSL profile: 24
- ATM profile: 48
- IGMP filter profile: 128
- ADSL ALARM profile: 24
- Dot1X profile: 64

- DHCP relay server: 32
- IP ROUTE: 128
- Static multicast address: 32
- IGMP groups: 256 groups
- MAC learning: 9.5k at most (128 per ADSL port at most, 4k per ENET port at most)
- RPVC gateway IP address: 96
- RPVC routing entry: 96
- ACL profile: 128

The following table shows the specifications for wire gauge.

Note: Make sure you use wires of the specified wire gauge.

Table 124 Wire Gauge Specifications

WIRE TYPE	REQUIRED AWG NO. (DIAMETER)
Ground Wire	18 or larger
Telephone Wire	26 or larger

AWG (American Wire Gauge) is a measurement system for wire that specifies its thickness. As the thickness of the wire increases, the AWG number decreases.

PART VIII
Appendices and Index

The appendices provide general information. Some details may not apply to your AAM1212.

Legal Information (479)
Customer Support (477)
Index (489)

A

Legal Information

Copyright

Disclaimers

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

FCC Warning

This device has been tested and found to comply with the limits for a Class A digital switch, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This device generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this device in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning:

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Taiwanese BSMI (Bureau of Standards, Metrology and Inspection) A Warning:

警告使用者
這是甲類的資訊產品，在居住的環境使用時，
可能造成射頻干擾，在這種情況下，
使用者會被要求採取某些適當的對策。

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Viewing Certifications

1. Go to http://www.zyxel.com.
2. Select your product on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page.

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Viewing Certifications

1. Go to http://www.zyxel.com.
2. Select your product on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com.

A

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device. Regional offices are listed below (see also http://www.zyxel.com/web/contact_us.php). Please have the following information ready when you contact an office.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

"+" is the (prefix) number you dial to make an international telephone call.

Corporate Headquarters (Worldwide)

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-3-578-3942
- Fax: +886-3-578-2439
- Web: www.zyxel.com
- Regular Mail: ZyXEL Communications Corp., 6 Innovation Road II, Science Park, Hsinchu 300, Taiwan

China - ZyXEL Communications (Beijing) Corp.

- Support E-mail: cso.zycn@zyxel.cn
- Sales E-mail: sales@zyxel.cn
- Telephone: +86-010-82800646
- Fax: +86-010-82800587
- Address: 902, Unit B, Horizon Building, No.6, Zhichun Str, Haidian District, Beijing
- Web: http://www.zyxel.cn

China - ZyXEL Communications (Shanghai) Corp.

- Support E-mail: cso.zycn@zyxel.cn
- Sales E-mail: sales@zyxel.cn
- Telephone: +86-021-61199055
- Fax: +86-021-52069033

- Address: 1005F, ShengGao International Tower, No.137 XianXia Rd., Shanghai
- Web: http://www.zyxel.cn

Costa Rica

- Support E-mail: soporte@zyxel.co.cr
- Sales E-mail: sales@zyxel.co.cr
- Telephone: +506-2017878
- Fax: +506-2015098
- Web: www.zyxel.co.cr
- Regular Mail: ZyXEL Costa Rica, Plaza Roble Escazú, Etapa El Patio, Tercer Piso, San José, Costa Rica

Czech Republic

- E-mail: info@cz.zyxel.com
- Telephone: +420-241-091-350
- Fax: +420-241-091-359
- Web: www.zyxel.cz
- Regular Mail: ZyXEL Communications, Czech s.r.o., Modranská 621, 143 01 Praha 4 - Modrany, Ceská Republika

Denmark

- Support E-mail: support@zyxel.dk
- Sales E-mail: sales@zyxel.dk
- Telephone: +45-39-55-07-00
- Fax: +45-39-55-07-07
- Web: www.zyxel.dk
- Regular Mail: ZyXEL Communications A/S, Columbusvej, 2860 Soeborg, Denmark

Finland

- Support E-mail: support@zyxel.fi
- Sales E-mail: sales@zyxel.fi
- Telephone: +358-9-4780-8411
- Fax: +358-9-4780-8448
- Web: www.zyxel.fi
- Regular Mail: ZyXEL Communications Oy, Malminkaari 10, 00700 Helsinki, Finland

France

- E-mail: info@zyxel.fr
- Telephone: +33-4-72-52-97-97
- Fax: +33-4-72-52-19-20
- Web: www.zyxel.fr
- Regular Mail: ZyXEL France, 1 rue des Vergers, Bat. 1 / C, 69760 Limonest, France

Germany

- Support E-mail: support@zyxel.de
- Sales E-mail: sales@zyxel.de
- Telephone: +49-2405-6909-69
- Fax: +49-2405-6909-99
- Web: www.zyxel.de
- Regular Mail: ZyXEL Deutschland GmbH., Adenauerstr. 20/A2 D-52146, Wuerselen, Germany

Hungary

- Support E-mail: support@zyxel.hu
- Sales E-mail: info@zyxel.hu
- Telephone: +36-1-3361649
- Fax: +36-1-3259100
- Web: www.zyxel.hu
- Regular Mail: ZyXEL Hungary, 48, Zoldlomb Str., H-1025, Budapest, Hungary

India

- Support E-mail: support@zyxel.in
- Sales E-mail: sales@zyxel.in
- Telephone: +91-11-30888144 to +91-11-30888153
- Fax: +91-11-30888149, +91-11-26810715
- Web: http://www.zyxel.in
- Regular Mail: India - ZyXEL Technology India Pvt Ltd., II-Floor, F2/9 Okhla Phase -1, New Delhi 110020, India

Japan

- Support E-mail: support@zyxel.co.jp
- Sales E-mail: zyp@zyxel.co.jp
- Telephone: +81-3-6847-3700
- Fax: +81-3-6847-3705
- Web: www.zyxel.co.jp
- Regular Mail: ZyXEL Japan, 3F, Office T&U, 1-10-10 Higashi-Gotanda, Shinagawa-ku, Tokyo 141-0022, Japan

Kazakhstan

- Support: http://zyxel.kz/support
- Sales E-mail: sales@zyxel.kz
- Telephone: +7-3272-590-698
- Fax: +7-3272-590-689
- Web: www.zyxel.kz
- Regular Mail: ZyXEL Kazakhstan, 43 Dostyk Ave., Office 414, Dostyk Business Centre, 050010 Almaty, Republic of Kazakhstan

Malaysia

- Support E-mail: support@zyxel.com.my
- Sales E-mail: sales@zyxel.com.my
- Telephone: +603-8076-9933
- Fax: +603-8076-9833
- Web: http://www.zyxel.com.my
- Regular Mail: ZyXEL Malaysia Sdn Bhd., 1-02 & 1-03, Jalan Kenari 17F, Bandar Puchong Jaya, 47100 Puchong, Selangor Darul Ehsan, Malaysia

North America

- Support E-mail: support@zyxel.com
- Support Telephone: +1-800-978-7222
- Sales E-mail: sales@zyxel.com
- Sales Telephone: +1-714-632-0882
- Fax: +1-714-632-0858
- Web: www.zyxel.com
- Regular Mail: ZyXEL Communications Inc., 1130 N. Miller St., Anaheim, CA 92806-2001, U.S.A.

Norway

- Support E-mail: support@zyxel.no
- Sales E-mail: sales@zyxel.no
- Telephone: +47-22-80-61-80
- Fax: +47-22-80-61-81
- Web: www.zyxel.no
- Regular Mail: ZyXEL Communications A/S, Nils Hansens vei 13, 0667 Oslo, Norway

Poland

- E-mail: info@pl.zyxel.com
- Telephone: +48-22-333 8250
- Fax: +48-22-333 8251
- Web: www.pl.zyxel.com
- Regular Mail: ZyXEL Communications, ul. Okrzei 1A, 03-715 Warszawa, Poland

Russia

- Support: http://zyxel.ru/support
- Sales E-mail: sales@zyxel.ru
- Telephone: +7-095-542-89-29
- Fax: +7-095-542-89-25
- Web: www.zyxel.ru
- Regular Mail: ZyXEL Russia, Ostrovityanova 37a Str., Moscow 117279, Russia

Singapore

- Support E-mail: support@zyxel.com.sg
- Sales E-mail: sales@zyxel.com.sg
- Telephone: +65-6899-6678
- Fax: +65-6899-8887
- Web: http://www.zyxel.com.sg
- Regular Mail: ZyXEL Singapore Pte Ltd., No. 2 International Business Park, The Strategy #03-28, Singapore 609930

Spain

- Support E-mail: support@zyxel.es
- Sales E-mail: sales@zyxel.es
- Telephone: +34-902-195-420
- Fax: +34-913-005-345
- Web: www.zyxel.es
- Regular Mail: ZyXEL Communications, Arte, 21 5ª planta, 28033 Madrid, Spain

Sweden

- Support E-mail: support@zyxel.se
- Sales E-mail: sales@zyxel.se
- Telephone: +46-31-744-7700
- Fax: +46-31-744-7701
- Web: www.zyxel.se
- Regular Mail: ZyXEL Communications A/S, Sjöporten 4, 41764 Göteborg, Sweden

Taiwan

- Support E-mail: support@zyxel.com.tw
- Sales E-mail: sales@zyxel.com.tw
- Telephone: +886-2-27399889
- Fax: +886-2-27353220
- Web: http://www.zyxel.com.tw
- Address: Room B, 21F., No.333, Sec. 2, Dunhua S. Rd., Da-an District, Taipei

Thailand

- Support E-mail: support@zyxel.co.th
- Sales E-mail: sales@zyxel.co.th
- Telephone: +662-831-5315
- Fax: +662-831-5395
- Web: http://www.zyxel.co.th
- Regular Mail: ZyXEL Thailand Co., Ltd., 1/1 Moo 2, Ratchaphruk Road, Bangrak-Noi, Muang, Nonthaburi 11000, Thailand.

Turkey

- Support E-mail: cso@zyxel.com.tr
- Telephone: +90 212 222 55 22
- Fax: +90-212-220-2526
- Web: http:www.zyxel.com.tr
- Address: Kaptanpasa Mahallesi Piyalepasa Bulvari Ortadogu Plaza N:14/13 K:6 Okmeydani/Sisli Istanbul/Turkey

Ukraine

- Support E-mail: support@ua.zyxel.com
- Sales E-mail: sales@ua.zyxel.com
- Telephone: +380-44-247-69-78
- Fax: +380-44-494-49-32
- Web: www.ua.zyxel.com
- Regular Mail: ZyXEL Ukraine, 13, Pimonenko Str., Kiev 04050, Ukraine

United Kingdom

- Support E-mail: support@zyxel.co.uk
- Sales E-mail: sales@zyxel.co.uk
- Telephone: +44-1344-303044, 0845 122 0301 (UK only)
- Fax: +44-1344-303034
- Web: www.zyxel.co.uk
- Regular Mail: ZyXEL Communications UK Ltd., 11 The Courtyard, Eastern Road, Bracknell, Berkshire RG12 2XB, United Kingdom (UK)

Index

Numerics

2684 routed mode 438

A

Access Control 229
acl ouifilter commands 318
actual rate 108
Address Resolution Protocol. See ARP.
adsl alarmprofile commands 423
adsl commands 393
adsl linediag commands 415
adsl paepvc commands 447
ADSL Port Setup 107, 125
adsl ppvc commands 433
ADSL profiles 108
  default 109
adsl pvc commands 431
adsl rpvc commands 438
ADSL standard 140
adsl tlspvc commands 451
adsl vcprofile commands 429
aging time 100
alarm commands 323
Alarm Profile Screen 133
all digital mode 113
ALM LED
  troubleshooting 463
American Wire Gauge (AWG) 475
Annex I 113
Annex L 113
Annex M 113
ARP 176, 271
  table 271
ATM F5 266
ATM Forum Traffic Management 4.0 Specification 128
ATM QoS 128
ATM traffic class 128, 132
authentication 94
  default privilege level for administrators 95
  modes for administrators 95
  user 94

B

back up configuration 263
bit allocation 145
Bridge Protocol Data Units (BPDU) 180
Burst Tolerance (BT) 130

C

Canonical Format Indicator (CFI) 149
Cell Delay Variation Tolerance (CDVT) 130
certifications 479
  notices 480
  viewing 480
CI 275
CI commands. See commands.
CLI 275
CLI commands. See commands.
Command Line Interface. See CI or CLI.
Commands 276
commands 275, 276
  abbreviations 275
  acl ouifilter disable 318
  acl ouifilter enable 318
  acl ouifilter mode 318
  acl ouifilter set 319
  acl ouifilter show 319
config save 276
configuration
  back up 263, 383
  file names 383
  restore 262, 383
  using FTP 383
configured rate 108
console port 471
  settings 48
Constant Bit Rate (CBR) 128
contact information 483
contact person's name 92
copyright 479
customer support 483

D

Daytime (RFC 867) 92
default gateway 103
default privilege level 95
DEFVAL 116
DEFVAL_VC 116
DHCP 176, 191
DHCP relay 191
  option 82 191
Diagnostic 265
disclaimer 479
Discrete Multi-Tone. See DMT.
DMT 143
double upstream mode 113
double-tagged frames 215
downstream (traffic) 107
DSL LED
  troubleshooting 465
DSL port statistics 77
duplex 105
Dynamic Host Configuration Protocol. See DHCP.

E

EAPoL 176
encapsulation
  LLC 116
  VC Mux 116
Errored Seconds (ES) 142
Ethernet address. See MAC address.
Ethernet port
  default settings 48
  statistics 75
Extensible Authentication Protocol. See EAPoL.

F

factory defaults 263, 469
Far End Block Errors (FEBE) 142
fast channel 108
fast mode 108, 126
FCC interference statement 479
filtering databases 341
firmware upgrade 261, 383
  file names 383
  using FTP 383
  when unable to use FTP 471
firmware version 88
front panel 47
FTP 264, 383
full duplex 105

G

GARP 97
GARP timer 100
GARP timer setup 97
General Setup 91
Generic Attribute Registration Protocol. See GARP.

H

hardware installation 45
Home screen 60, 73
host name 92

I

IEEE 802.1D. See STP.
IEEE 802.1Q. See VLAN.
IEEE 802.1w. See RSTP.
IEEE 802.1x 185, 187
IEEE 802.1x. See also RADIUS.
IGMP 176
  leave packets 159
  modes 163
  query packets 159
  report packets 159
IGMP Filter Profile Screen 136
IGMP snooping 157
initial configuration 67
interleave delay 108, 126
interleave mode 126
Internet Explorer 59, 67
Internet Group Multicast Protocol. See IGMP.
Internet Protocol. See IP.
IP 176
ip commands 375
IP Setup 103

L

LAN LED
  troubleshooting 464
latency mode 126
LDM test 266
line bit allocation 296
Line Data 143
line operating values 139
Line Performance 141
line type 142
LLC 116
location 92
log format 314, 326
log messages 314
logging out 65
Login screen 60
loopback test 266

M

MAC address 88
MAC address learning 100
MAC filter 177
Management Information Base (MIB) 230
Maximum Burst Size (MBS) 129
Media Access Control. See MAC address.
metric 252
model 92
multicast MAC address 168
Multicast VLAN. See MVLAN.
MVLAN 169

N

Near End Block Errors (NEBE) 142
NetBIOS 176
Network Basic Input/Output System. See NetBIOS.
non real-time Variable Bit Rate (nrt-VBR) 128
NTP (RFC-1305) 92

O

OAM F5 Loopback 266
Operational Mode 281
option 82 191
Organizationally Unique Identifier, See OUI 247
OUI 247
  filter 247

P

packet filter 175
password 63
Peak Cell Rate (PCR) 129
Permanent Virtual Circuit. See PVC.
ping 266
PMM 267
Point-to-Point Protocol over Ethernet, See PPPoE. 305
Point-to-Point Protocol over Ethernet. See PPPoE.
Port Security 189
Port Setup 105
Port VLAN ID. See PVID.
PPPoE 176, 305
PPVC 433
PPVC Setup 121
PPVC Setup Members 122
priority queue assignment 101
product registration 481
PVC 115, 431
PVID 118
  default 150

Q

Q-in-Q. See TLS.
Quality of Service (QOS) 128

R

RADIUS 185
  shared secret 186
RADIUS Setup 186
Rapid Spanning Tree Protocol. See RSTP.
reach extended ADSL2 113
real-time Variable Bit Rate (rt-VBR) 128
reboot 263
Reed-Solomon 108, 126

registration
product 481
related documentation 3
Remote Authentication Dial In User Service. See RADIUS.
Remote Management screen 234
restart 263
restore configuration 262
RFC 1305. See NTP.
RFC 2131. See DHCP.
RFC 2132. See DHCP.
RFC 2138. See RADIUS.
RFC 2139. See RADIUS.
RFC 2486. See EAPoL.
RFC 3046. See Option 82.
RFC 867. See Daytime.
RFC 868. See Time.
RSTP 179
port states 180
See also STP.

S

safety warnings 6
save configuration 64
Secured Client Setup screen 234
SELT 266
Service Access Control 233
Service Provider’s Network (SPN) 215
Severely Errored Seconds (SES) 142
shared secret 95
Simple Network Management Protocol. See SNMP.
Single End Loop Test. See SELT.
SNMP 229
commands 230
Get 230
GetNext 230
manager 230
MIBs 231
supported versions 229
Trap 231
traps 231
SNMP screen 233
Spanning Tree Protocol. See STP.
static multicast filter 167
static route 251
metric 252
Static VLAN. See SVLAN.
statistics
DSL port 77
Ethernet port 75
statistics adsl commands 409
statistics dhcp commands 337
statistics igmpsnoop commands 364
statistics ip commands 378
statistics monitor command 319
statistics port command 320
STP 179
Bridge Protocol Data Units (BPDU) 180
designated bridge 179
hello time 180
max age 180
path cost 179
port path cost 184
port priority 184
port states 180
root bridge 179
root port 179
super channel 115
Sustained Cell Rate (SCR) 129
SVLAN 341
switch acl commands 458
switch acl profile commands 455
switch dhcprelay commands 331
switch dhcpsnoop commands 335
switch igmpfilter commands 356
switch igmpsnoop bandwidth commands 359
switch igmpsnoop commands 355
switch igmpsnoop igmpcount commands 362
switch igmpsnoop mvlan commands 366
switch isolation commands 317
switch mac count commands 352
switch mac filter commands 349
switch pktfilter commands 371
Switch Setup 99
switch vlan commands 342
syntax conventions 4
sys commands 313
SYS LED
troubleshooting 463
sys snmp commands 389
syslog 227
System Information 87
system log 266
system up time 73

T

Tag Control Information (TCI) 149
Tag Protocol Identifier (TPID) 149

tagged VLAN. See VLAN.
temperature 88
terminal emulation 471
Theoretical Arrival Time (TAT) 130
Time (RFC-868) 92
time server protocols supported 92
time zone 92
TLS 215
ToneDiag 267
tones 143
trademarks 479
traffic parameters 129
traffic shaping 128
transmission error correction 108, 126
Transparent LAN Service. See TLS.
Trellis encoding 140
troubleshooting 463

U

UnAvailable Seconds (UAS) 142
UNIX syslog 227
Unspecified Bit Rate (UBR) 129
up time 74
upstream (traffic) 107
User Account 93

V

Variable Bit Rate (VBR) 128
VC 116
VC Mux 116
VC Profile Screen 131
VC Setup 116
vendor information 140
virtual channel 115
  downstream profile 117
  profile 116
  upstream profile 118
Virtual Circuit Identifier (VCI)
Virtual Circuit. See VC.
Virtual Local Area Network. See VLAN.
Virtual Path Identifier (VPI)
VLAN 149
  explicit tagging 341
  forwarding 150
  implicit tagging 341
  priority frame 150
  registration information 341
  VLAN ID 149
  VLAN ID, maximum number of 149
  when VLAN ID is zero 150
VLAN stacking. See TLS.
voltage 88

W

warranty 481
  note 481

X

XMODEM upload 471, 472