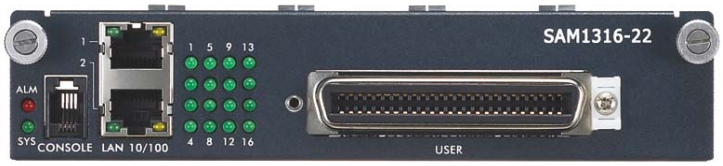
SAM1316-22

SHDSL.bis module of IES-1000

User's Guide



Default Login Details

IP Address	http://192.168.1.1
User Name	admin
Password	1234

Firmware Version 3.53
Edition 1, 4/2010

www.zyxel.com

ZyXEL

About This User's Guide

Intended Audience

This manual is intended for people who want to install, connect, or configure the SAM1316-22.

Related Documentation

- IES-1000 User's Guide

  See this User's Guide for more on the chassis in which you install the SAM1316-22.

- Support Disc

  Refer to the included CD for support documents.

Documentation Feedback

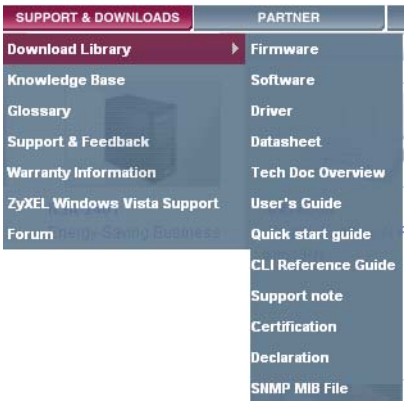
Send your comments, questions or suggestions to: techwriters@zyxel.com.tw

Thank you!

The Technical Writing Team, ZyXEL Communications Corp.,
6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 30099, Taiwan.

Need More Help?

More help is available at www.zyxel.com.



- Download Library

  Search for the latest product updates and documentation from this link. Read the Tech Doc Overview to find out how to efficiently use the documentation in order to better understand how to use your product.

- Knowledge Base

  If you have a specific question about your product, the answer may be here. This is a collection of answers to previously asked questions about ZyXEL products.

- Forum

  This contains discussions on ZyXEL products. Learn from others who use ZyXEL products and share your experiences as well.

Customer Support

Should problems arise that cannot be solved by the methods listed above, 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.

See http://www.zyxel.com/web/contact_us.php for contact information. Please have the following information ready when you contact an office.

- 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.

Document Conventions

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

Syntax Conventions

- The SAM1316-22 may be referred to as the “SAM1316-22”, the “device”, the “system”, the “switch”, or the “product” 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.
- Mouse action sequences are denoted using a comma. For example, “In Windows, click **Start**, **Programs**, **Acrobat Reader**” means first click the **Start** button, then move your mouse pointer to **Programs** and then click **Acrobat Reader**.
- 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 use the following generic icons. The SAM1316-22 icon is not an exact representation of your SAM1316-22.

Graphics in this book may differ slightly from the product due to differences in operating systems, operating system versions, or if you installed updated firmware/software for your device. Every effort has been made to ensure that the information in this manual is accurate.

SAM1316-22 	Computer 	Server 
Computer 	DSLAM 	Gateway 
Central Office/ ISP 	Internet 	Hub/Switch 

Firmware Naming Conventions

A firmware version includes the model code and release number as shown in the following example.

Firmware Version: V3.53 (BVE.0)

"BVE" is the model code.

"0" is this firmware's release number. This varies as new firmware is released. Your firmware's release number may not match what is displayed in this User's Guide.

Safety Warnings

- 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

User's Guide 27

Getting to Know the SAM1316-22 29
Installing and Removing the SAM1316-22 33
Front Panel 37

Technical Reference 43

Introducing the Web Configurator 45
Initial Configuration 53
Home and Port Statistics Screens 59
System Information 71
General Setup 75
User Account 77
Switch Setup 81
IP Setup 87
ENET Port Setup 89
xDSL Port Setup 91
xDSL Profiles Setup 107
xDSL Line Data 123
G.bond 129
VLAN 133
IGMP 141
Static Multicast 153
Multicast VLAN 155
Filtering 161
MAC Filter 165
Spanning Tree Protocol 167
Port Authentication 175
Port Security 181
DHCP Relay 183
DHCP Snoop 189
2684 Routed Mode 193
PPPoA to PPPoE 203
DSCP 209
TLS PVC 213
ACL 217
Downstream Broadcast 225
Syslog 227
Access Control 229

PPPoE Intermediate Agent 237
Maximum MTU Size 241
PVC Upstream Limit 243
OUI Filter 247
Static Routing 249
Alarm 251
Maintenance 261
Diagnostic 265
MAC Table 267
ARP Table 271
Commands 273
Command Examples 297
Alarm Commands 303
DHCP Commands 311
IEEE 802.1Q Tagged VLAN Commands 323
MAC Commands 333
IGMP Commands 339
PPPoE Intermediate Agent Commands 357
OUI Filter Commands 361
Packet Filter Commands 365
IP Commands 369
Firmware and Configuration File Maintenance 375
SNMP 381
DSL Commands 385
Virtual Channel Management 401
ACL Commands 429
Troubleshooting 435
Specifications 445

Table of Contents

About This User's Guide 3

Document Conventions 5

Safety Warnings 7

Contents Overview 9

Table of Contents 11

Part I: User's Guide 27

Chapter 1
Getting to Know the SAM1316-22 29

1.1 Overview 29
1.2 Applications 29
1.2.1 MTU Application 29
1.2.2 Curbside Application 30

Chapter 2
Installing and Removing the SAM1316-22 33

2.1 Overview 33
2.2 Installing the SAM1316-22 in the IES-1000 33
2.3 Removing the SAM1316-22 from the IES-1000 34

Chapter 3
Front Panel 37

3.1 LEDs 37
3.2 Front Panel Ports 38
3.2.1 Console Port 38
3.2.2 LAN (Ethernet) Ports 38
3.2.3 USER Ports 39

Part II: Technical Reference 43

Chapter 4
Introducing the Web Configurator 45

4.1 Overview 45
4.2 Screen Privilege Levels 45
4.3 Accessing the Web Configurator 45
4.4 Navigation Panel 47
4.5 Changing Your Password 50
4.6 Saving Your Configuration 51
4.7 Logging Out of the Web Configurator 51

Chapter 5
Initial Configuration 53

5.1 Overview 53
5.2 Initial Configuration 53

Chapter 6
Home and Port Statistics Screens 59

6.1 Home Screen 59
6.1.1 Ethernet Port Statistics Screen 61
6.1.2 DSL Port Statistics Screen 64
6.1.3 RMON Statistics Screen 66
6.1.4 RMON History Screen 68
6.1.5 RMON History Detail Screen 69

Chapter 7
System Information 71

Chapter 8
General Setup 75

Chapter 9
User Account 77

9.1 User Account Screen 77
9.2 Authentication Screen 78

Chapter 10
Switch Setup 81

10.1 GARP Timer Setup 81
10.2 Switch Modes 81
10.2.1 Standalone Switch Mode 81
10.2.2 Port Isolation with Standalone Switch Mode Example 82
10.2.3 Daisychain Switch Mode 82
10.2.4 Port Isolation with Daisychain Switch Mode Example 83
10.3 Switch Setup Screen 84

Chapter 11
IP Setup 87

Chapter 12
ENET Port Setup 89

Chapter 13
xDSL Port Setup 91

13.1 DSL Profiles 91
13.2 Alarm Profiles 91
13.3 Downstream and Upstream 91
13.4 EFM and ATM Modes 92
13.5 Default Settings 92
13.6 xDSL Port Setup Screen 92
13.6.1 xDSL Port Setting Screen 95
13.7 Virtual Channels 97
13.7.1 Super Channel 97
13.7.2 LLC 98
13.7.3 VC Mux 98
13.7.4 Virtual Channel Profile 98
13.8 VC Setup Screen 98
13.9 Priority-based PVCs 102
13.10 PPVC Setup Screen 103
13.10.1 PPVC Setup Members Screen 104

Chapter 14
xDSL Profiles Setup 107

14.1 Configured Versus Actual SHDSL Rates 107
14.2 N-wire Mode 107
14.3 Port Profile Screen 108
14.4 ATM QoS 110
14.5 Traffic Shaping 110
14.5.1 ATM Traffic Classes 110
14.5.2 Traffic Parameters 111
14.6 Upstream Policing 113
14.7 VC Profile Screen 114
14.8 Alarm Profile Screen 116
14.8.1 Alarm Profile Map Screen 117
14.9 IGMP Filtering 118
14.10 IGMP Filter Profile Screen 119

Chapter 15
xDSL Line Data 123

15.1 xDSL Line Rate Info Screen 123
15.2 xDSL Performance Screen 125

Chapter 16
G.bond 129

16.1 Bonding Overview 129
16.1.1 Cell-level Bonding Process 129
16.1.2 Bonding Standards 129
16.2 G.bond Setup Screen 130
16.2.1 G.bond Status Screen 131

Chapter 17
VLAN 133

17.1 Introduction to VLANs 133
17.2 Introduction to IEEE 802.1Q Tagged VLAN 133
17.2.1 Forwarding Tagged and Untagged Frames 134
17.3 VLAN Status Screen 135
17.4 Static VLAN Setting Screen 136
17.5 VLAN Port Setting Screen 138

Chapter 18
IGMP 141

18.1 IGMP 141
18.2 IP Multicast Addresses 141
18.2.1 IGMP Snooping 141
18.2.2 IGMP Proxy 142
18.3 IGMP Status Screen 143
18.4 IGMP Bandwidth Screen 145
18.4.1 Bandwidth Port Setup Screen 146
18.5 IGMP Setup Screen 147
18.6 IGMP Filter Setup Screen 148
18.7 IGMP Count Screen 149
18.8 IGMP Port Info Screen 150
18.9 IGMP Port Group Screen 151

Chapter 19
Static Multicast 153

19.1 Static Multicast 153
19.2 Static Multicast Screen 153

Chapter 20
Multicast VLAN 155

20.1 Multicast VLAN Overview 155
20.2 MVLAN Status Screen 156
20.3 MVLAN Setup Screen 157
20.4 MVLAN Group Screen 159

Chapter 21
Filtering 161

21.1 Packet Filter Screen 161

Chapter 22
MAC Filter 165

22.1 MAC Filter Introduction 165
22.2 MAC Filter Screen 165

Chapter 23
Spanning Tree Protocol 167

23.1 RSTP and STP 167
23.2 Spanning Tree Protocol Status Screen 170
23.3 Spanning Tree Protocol Screen 172

Chapter 24
Port Authentication 175

24.1 Introduction to Authentication 175
24.1.1 RADIUS 175
24.1.2 Introduction to Local User Database 175
24.2 RADIUS Screen 176
24.3 802.1x Screen 178

Chapter 25
Port Security 181

25.1 Port Security Overview 181
25.2 Port Security Screen 181

Chapter 26
DHCP Relay 183

26.1 DHCP Relay 183
26.2 DHCP Relay Agent Information Option (Option 82) 183
26.2.1 Private Format 183
26.2.2 TR-101 Format 184
26.3 DHCP Relay Screen 185

Chapter 27
DHCP Snoop 189

27.1 DHCP Snoop Overview 189
27.2 DHCP Snoop Screen 189
27.3 DHCP Snoop Status Screen 191
27.4 DHCP Counter Screen 192

Chapter 28
2684 Routed Mode 193

28.1 2684 Routed Mode 193
28.1.1 2684 Routed Mode Example 193
28.2 2684 Routed PVC Screen 195
28.3 2684 Routed Domain Screen 196
28.4 RPVC Arp Proxy Screen 198
28.5 2684 Routed Gateway Screen 199

Chapter 29
PPPoA to PPPoE 203

29.1 PPPoA to PPPoE Overview 203
29.2 PPPoA to PPPoE Screen 203
29.3 PPPoA to PPPoE Status Screen 207

Chapter 30
DSCP 209

30.1 DSCP Overview 209
30.2 DSCP Setup Screen 209
30.3 DSCP Map Screen 210

Chapter 31
TLS PVC 213

31.1 Transparent LAN Service (TLS) Overview 213
31.1.1 TLS Network Example 213
31.2 TLS PVC Screen 214

Chapter 32
ACL 217

32.1 Access Control Logic (ACL) Overview 217
32.1.1 ACL Profile Rules 217
32.1.2 ACL Profile Actions 218
32.2 ACL Setup Screen 219
32.3 ACL Profile Setup Screen 221
32.4 ACL Profile Map Screen 223

Chapter 33
Downstream Broadcast 225

33.1 Downstream Broadcast 225
33.2 Downstream Broadcast Screen 225

Chapter 34
Syslog 227

34.1 Syslog 227
34.2 SysLog Screen 227

Chapter 35
Access Control 229

35.1 Access Control Screen 229
35.2 Access Control Overview 229
35.3 SNMP 229
35.3.1 Supported MIBs 231
35.3.2 SNMP Traps 231
35.4 SNMP Screen 233
35.5 Service Access Control Screen 234
35.6 Remote Management Screen 234

Chapter 36
PPPoE Intermediate Agent 237

36.1 PPPoE Intermediate Agent Tag Format 237
36.2 PPPoE Intermediate Agent Screen 239

Chapter 37
Maximum MTU Size 241

37.1 Maximum MTU Size Screen 241

Chapter 38
PVC Upstream Limit 243

38.1 PVC Upstream Limit and Upstream VC Profiles 243
38.2 PVC Upstream Limit Screen 244

Chapter 39
OUI Filter 247

Chapter 40
Static Routing 249

Chapter 41
Alarm 251

41.1 Alarm 251
41.2 Alarm Status Screen 251
41.3 Alarm Descriptions 252
41.4 Alarm Event Setup Screen 253
41.4.1 Edit Alarm Event Setup Screen 255
41.5 Alarm Port Setup Screen 256
41.6 Alarm History Screen 258

Chapter 42
Maintenance 261

42.1 Maintenance Screen 261
42.2 Firmware Upgrade Screen 261
42.3 Restore Configuration Screen 262
42.4 Backing Up a Configuration File 263
42.5 Load Factory Defaults 263
42.6 Reboot System 264
42.7 Command Line FTP 264

Chapter 43
Diagnostic 265

43.1 Diagnostic Screen 265

Chapter 44
MAC Table 267

44.1 Introduction to MAC Table 267
44.2 MAC Table Screen 268

Chapter 45
ARP Table 271

45.1 Introduction to ARP Table 271
45.1.1 How ARP Works 271
45.2 ARP Table Screen 271

Chapter 46
Commands 273

46.1 Command Line Interface Overview 273
46.2 Command Privilege Levels 273
46.3 Saving Your Configuration 274
46.4 Commands 274

Chapter 47
Command Examples 297

47.1 Command Examples Overview 297
47.2 Sys Commands 297
47.2.1 Log Show Command 297
47.2.2 Log Clear Command 297
47.2.3 Info Show Command 298
47.3 Isolation Commands 298
47.3.1 Isolation Show Command 298
47.3.2 Isolation Enable Command 299
47.3.3 Isolation Disable Command 299

47.3.4 Switch Isolation VLAN Delete Command 299
47.3.5 Switch Isolation VLAN Set Command 300
47.4 Statistics Monitor Command 300
47.5 Statistics Port Command 301

Chapter 48
Alarm Commands 303

48.1 Alarm Commands 303
48.2 General Alarm Command Parameters 303
48.3 Alarm Show Command 304
48.4 Alarm Port Show Command 304
48.5 Alarm Port Set Command 305
48.6 Alarm Tablelist Command 305
48.7 Log Format 307
48.8 Alarm History Show Command 307
48.9 Alarm History Clear Command 308
48.10 Alarm XEdit Command 308
48.11 Alarm Cutoff Command 309
48.12 Alarm Clear Command 310

Chapter 49
DHCP Commands 311

49.1 DHCP Relay Commands 311
49.1.1 Show Command 311
49.1.2 Enable Command 311
49.1.3 Disable Command 312
49.1.4 Server Set Command 312
49.1.5 Server Delete Command 313
49.1.6 Server Active Command 313
49.1.7 Optionmode Command 313
49.1.8 Relaymode Command 314
49.2 DHCP Relay Option 82 (Agent Information) Sub-option 1 (Circuit ID) 315
49.2.1 Option 82 Sub-option 1 Enable Command 315
49.2.2 Option 82 Sub-option 1 Disable Command 315
49.2.3 Option 82 Sub-option 1 Set Command 315
49.3 DHCP Relay Option 82 (Agent Information) Sub-option 2 (Remote ID) 316
49.3.1 Option 82 Sub-option 2 Enable Command 316
49.3.2 Option 82 Sub-option 2 Disable Command 316
49.3.3 Option 82 Sub-option 2 Set Command 317
49.4 DHCP Snoop Commands 317
49.4.1 DHCP Snoop Enable Command 317
49.4.2 DHCP Snoop Disable Command 318
49.4.3 DHCP Snoop Flush Command 318

49.4.4 DHCP Snoop Show Command 318
49.4.5 DHCP Counter Statistics Command 319
49.4.6 DHCP Snoop Statistics Command 320
49.4.7 DHCP Snoop Pool Set Command 320
49.4.8 DHCP Snoop Pool Delete Command 321
49.4.9 DHCP Snoop LAN to LAN Show Command 321
49.4.10 DHCP Snoop LAN to LAN Disable Command 321
49.4.11 DHCP Snoop LAN to LAN Enable Command 322

Chapter 50
IEEE 802.1Q Tagged VLAN Commands 323

50.1 Introduction to VLANs 323
50.2 IEEE 802.1Q Tagging Types 323
50.3 Filtering Databases 324
50.3.1 Static Entries (SVLAN Table) 324
50.4 IEEE VLAN1Q Tagged VLAN Configuration Commands 324
50.4.1 VLAN Port Show Command 324
50.4.2 VLAN PVID Command 325
50.4.3 VLAN Priority Command 325
50.4.4 VLAN Set Command 326
50.4.5 VLAN Frame Type Command 327
50.4.6 VLAN CPU Show Command 328
50.4.7 VLAN CPU Set Command 328
50.4.8 Configuring Management VLAN Example 329
50.4.9 VLAN Delete Command 329
50.5 VLAN Enable 330
50.6 VLAN Disable 330
50.6.1 VLAN Show Command 330

Chapter 51
MAC Commands 333

51.1 MAC Commands Overview 333
51.2 MAC Filter Commands 333
51.2.1 MAC Filter Show Command 333
51.2.2 MAC Filter Enable Command 334
51.2.3 MAC Filter Disable Command 334
51.2.4 MAC Filter Mode Command 335
51.2.5 MAC Filter Set Command 335
51.2.6 MAC Filter Delete Command 336
51.3 MAC Count Commands 336
51.3.1 MAC Count Show Command 336
51.3.2 MAC Count Enable Command 337
51.3.3 MAC Count Disable Command 337

51.3.4 MAC Count Set Command 338

Chapter 52
IGMP Commands 339

52.1 Multicast Overview 339
52.2 IGMP Snoop Commands 339
52.2.1 IGMP Snoop Show Command 339
52.2.2 IGMP Snoop Enable Command 339
52.2.3 IGMP Snoop Disable Command 340
52.2.4 IGMP Snoop qryvid Delete Command 340
52.2.5 IGMP Snoop qryvid Set Command 340
52.2.6 IGMP Snoop qryvid Show Command 341
52.3 IGMP Filter Commands 341
52.3.1 IGMP Filter Show Command 341
52.3.2 IGMP Filter Set Command 342
52.3.3 IGMP Filter Profile Set Command 342
52.3.4 IGMP Filter Profile Delete Command 343
52.3.5 IGMP Filter Profile Show Command 343
52.4 IGMP Bandwidth Commands 344
52.4.1 IGMP Bandwidth Default Command 344
52.4.2 IGMP Bandwidth Set Command 345
52.4.3 IGMP Bandwidth Delete Command 345
52.5 IGMP Bandwidth Port Commands 345
52.5.1 IGMP Bandwidth Port Disable Command 345
52.5.2 IGMP Bandwidth Port Enable Command 346
52.5.3 IGMP Bandwidth Port Set Command 346
52.5.4 IGMP Bandwidth Port Show Command 346
52.6 IGMP Count Limit Commands 347
52.6.1 IGMP Count Disable Command 347
52.6.2 IGMP Count Enable Command 348
52.6.3 IGMP Count Set Command 348
52.6.4 IGMP Count Show Command 349
52.7 IGMP Snoop Statistics Commands 349
52.7.1 IGMP Snoop Info Statistics Command 349
52.7.2 IGMP Group Statistics Command 350
52.7.3 IGMP Port Info Statistics Command 350
52.7.4 IGMP Port Group Statistics Command 351
52.8 Multicast VLAN Commands 351
52.8.1 Multicast VLAN Set Command 352
52.8.2 Multicast VLAN Delete Command 352
52.8.3 Multicast VLAN Disable Command 353
52.8.4 Multicast VLAN Enable Command 353
52.8.5 Multicast VLAN Show Command 353

52.8.6 Multicast VLAN Group Set Command 354
52.8.7 Multicast VLAN Group Delete Command 354
52.8.8 Multicast VLAN Group Show Command 355

Chapter 53
PPPoE Intermediate Agent Commands 357

53.1 PPPoE Agent Information 357
53.1.1 PPPoE Intermediate Agent Clear Info Command 357
53.1.2 PPPoE Intermediate Agent Enable Command 357
53.1.3 PPPoE Intermediate Agent Delete Command 358
53.1.4 PPPoE Intermediate Agent Disable Command 358
53.1.5 PPPoE Intermediate Agent Info Command 359
53.1.6 PPPoE Intermediate Agent Set Command 359
53.1.7 PPPoE Intermediate Agent Show Command 360

Chapter 54
OUI Filter Commands 361

54.1 OUI Filter Commands 361
54.1.1 OUI Filter Disable Command 361
54.1.2 OUI Filter Enable Command 361
54.1.3 OUI Filter Mode Command 361
54.1.4 OUI Filter Set Command 362
54.1.5 OUI Filter Show Command 362

Chapter 55
Packet Filter Commands 365

55.1 Packet Filter Commands 365
55.1.1 Packet Filter Show Command 365
55.1.2 Packet Filter Set Command 366
55.1.3 Packet Filter PPPoE Only Command 367

Chapter 56
IP Commands 369

56.1 IP Commands Introduction 369
56.2 IP Settings and Default Gateway 369
56.3 General IP Commands 370
56.3.1 Show 371
56.3.2 Ping Command 371
56.3.3 Route Set Command 371
56.3.4 Route Delete Command 371
56.3.5 Route Show Command 372
56.3.6 ARP Show Command 372
56.3.7 ARP Flush Command 373

56.4 Statistics IP Command 373

Chapter 57
Firmware and Configuration File Maintenance 375

57.1 Firmware and Configuration File Maintenance Overview 375
57.2 Filename Conventions 375
57.3 Editable Configuration File 376
57.3.1 Editable Configuration File Backup 377
57.3.2 Edit Configuration File 377
57.3.3 Editable Configuration File Upload 378
57.4 Firmware File Upgrade 379

Chapter 58
SNMP 381

58.1 SNMP Commands 381
58.1.1 Get Community Command 381
58.1.2 Set Community Command 381
58.1.3 Trusted Host Set Command 382
58.1.4 Trap Community Command 382
58.1.5 Trap Destination Set Command 382
58.1.6 Show SNMP Settings Command 383

Chapter 59
DSL Commands 385

59.1 DSL Port Commands 385
59.1.1 DSL Port Show Command 385
59.1.2 DSL Port Enable Command 386
59.1.3 DSL Port Disable Command 386
59.1.4 DSL Port Profile Show Command 386
59.1.5 DSL Port Profile Set Command 387
59.1.6 DSL Port Profile Delete Command 389
59.1.7 DSL Port Profile Map Command 389
59.1.8 DSL Port Name Command 389
59.1.9 DSL Port Tel Command 390
59.1.10 DSL Port Loopback Command 390
59.2 Statistics DSL Commands 391
59.2.1 DSL Statistics Show Command 391
59.2.2 DSL Port Lineinfo Command 392
59.2.3 DSL Port Lineperf Command 393
59.2.4 DSL Port 15 Minute Performance Command 394
59.2.5 DSL Port 1 Day Performance Command 395
59.3 Alarm Profile Commands 397
59.3.1 Alarm Profile Show Command 397

59.3.2 Alarm Profile Set Command 397
59.3.3 Alarm Profile Delete Command 398
59.3.4 Alarm Profile Map Command 399
59.3.5 Alarm Profile Showmap Command 399

Chapter 60
Virtual Channel Management 401

60.1 Virtual Channel Management Overview 401
60.2 Virtual Channel Profile Commands 401
60.2.1 Show Virtual Channel Profile Command 401
60.2.2 Set Virtual Channel Profile Command 401
60.2.3 Delete Virtual Channel Profile Command 403
60.3 PVC Channels 403
60.3.1 PVC Show Command 404
60.3.2 PVC Set Command 404
60.3.3 PVC Delete Command 405
60.4 Priority-based PVCs 406
60.4.1 PPVC Set Command 406
60.4.2 PPVC Member Set Command 407
60.5 PPVC Member Delete Command 408
60.6 PPVC Member Show Command 409
60.6.1 PPVC Show Command 409
60.6.2 PPVC Delete Command 410
60.7 2684 Routed Mode Commands 410
60.7.1 2684 Routed Mode Example 411
60.7.2 RPVC Gateway Set Command 413
60.7.3 RPVC Gateway Show Command 413
60.7.4 RPVC Gateway Delete Command 414
60.7.5 RPVC Set Command 414
60.7.6 RPVC Show Command 415
60.7.7 RPVC Delete Command 416
60.7.8 RPVC Route Set Command 417
60.7.9 RPVC Route Show Command 417
60.7.10 RPVC Route Delete Command 418
60.7.11 RPVC ARP Agingtime Set Command 419
60.7.12 RPVC ARP Agingtime Show Command 419
60.7.13 RPVC ARP Show Command 420
60.7.14 RPVC ARP Flush Command 420
60.8 PPPoA to PPPoE (PAE) Commands 420
60.8.1 PAE PVC Delete Command 420
60.8.2 PAE PVC Set Command 421
60.8.3 PAE PVC Show Command 422
60.8.4 PAE PVC Session Command 422

60.8.5 PAE PVC Counter Command 423
60.9 Transparent LAN Service (TLS) Commands 425
60.9.1 TLS PVC Delete Command 425
60.9.2 TLS PVC Set Command 425
60.9.3 TLS PVC Show Command 426

Chapter 61
ACL Commands 429

61.1 ACL Profile Commands 429
61.1.1 ACL Profile Set Command 429
61.1.2 ACL Profile Delete Command 431
61.1.3 ACL Profile Show Map Command 431
61.1.4 ACL Profile Show Command 432
61.2 ACL Assignment Commands 432
61.2.1 ACL Assignment Set Command 432
61.2.2 ACL Assignment Delete Command 433
61.2.3 ACL Assignment Show Command 433

Chapter 62
Troubleshooting 435

62.1 The SYS LED Does Not Turn On 435
62.2 The ALM LED Is On 435
62.3 LAN Port LEDs Do Not Turn On 436
62.4 LAN Port Data Transmission 436
62.5 DSL Data Transmission 437
62.6 Local Server 437
62.7 Data Rate 438
62.8 Configured Settings 438
62.9 Password 438
62.10 System Lockout 438
62.11 SNMP 439
62.12 Telnet 439
62.13 Resetting the Defaults 440
62.13.1 Resetting the Defaults Via Command 440
62.13.2 Uploading the Default Configuration File 441
62.14 Recovering the Firmware 442

Chapter 63
Specifications 445

63.1 Hardware Telco-50 Connector Pin Assignments 451
63.2 Console Cable Pin Assignments 453

Appendix A Legal Information 455

Index..... 459

PART I

User's Guide

1

Getting to Know the SAM1316-22

1.1 Overview

This chapter introduces the main features and applications of your SAM1316-22.

The SAM1316-22 (G.SHDSL.bis Access Module) is a SHDSL multiplexer network module designed to be installed in the IES-1000 IP-based DSLAM chassis. The SAM1316-22 aggregates traffic from 16 SHDSL lines to two Ethernet ports to connect SHDSL subscribers to the Internet.

You can use the built-in web configurator to manage and configure the SAM1316-22. In addition, the SAM1316-22 can also be managed via Telnet, the console port, or third-party SNMP management.

1.2 Applications

These are the main applications for the SAM1316-22:

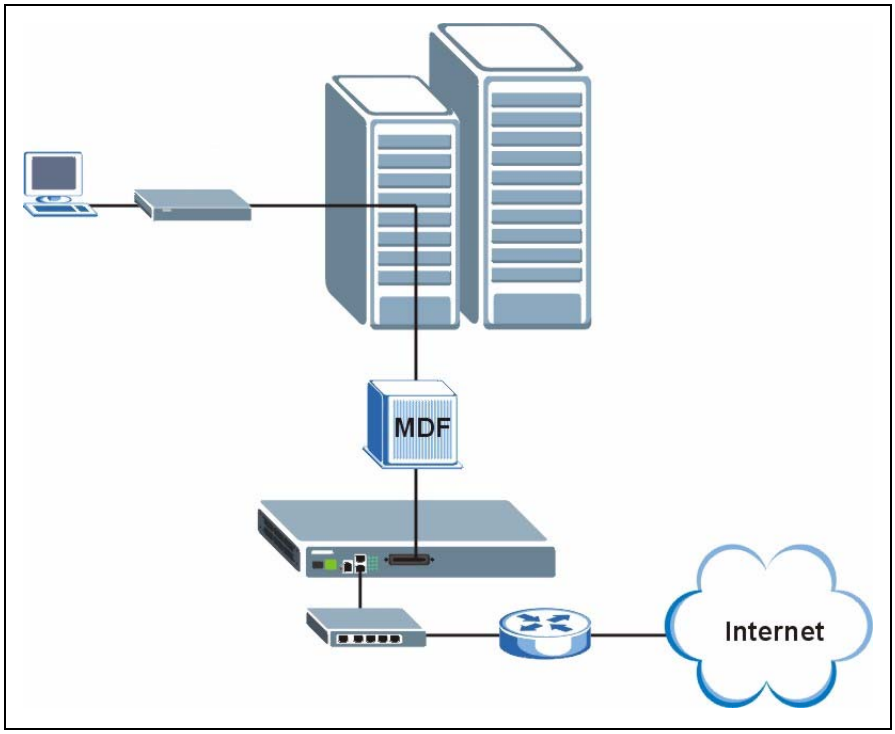
- Provide Internet access and multimedia services for Multiple Tenant Units (MTU).
- Other applications include telemedicine, surveillance systems, remote servers systems, cellular base stations and high-quality teleconferencing.

1.2.1 MTU Application

The following diagram depicts a typical application of the SAM1316-22 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.

Figure 1 MTU Application

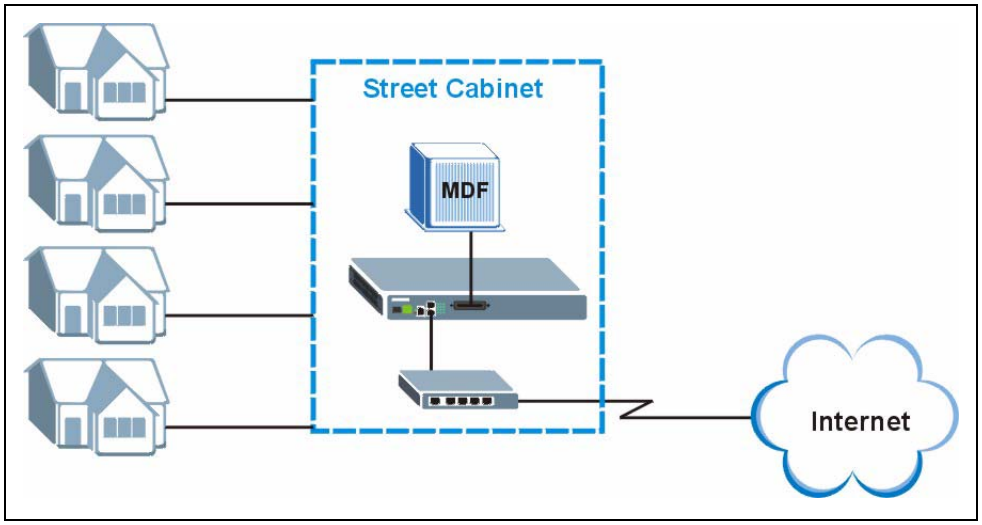


1.2.2 Curbside Application

The SAM1316-22 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 SAM1316-22

2.1 Overview

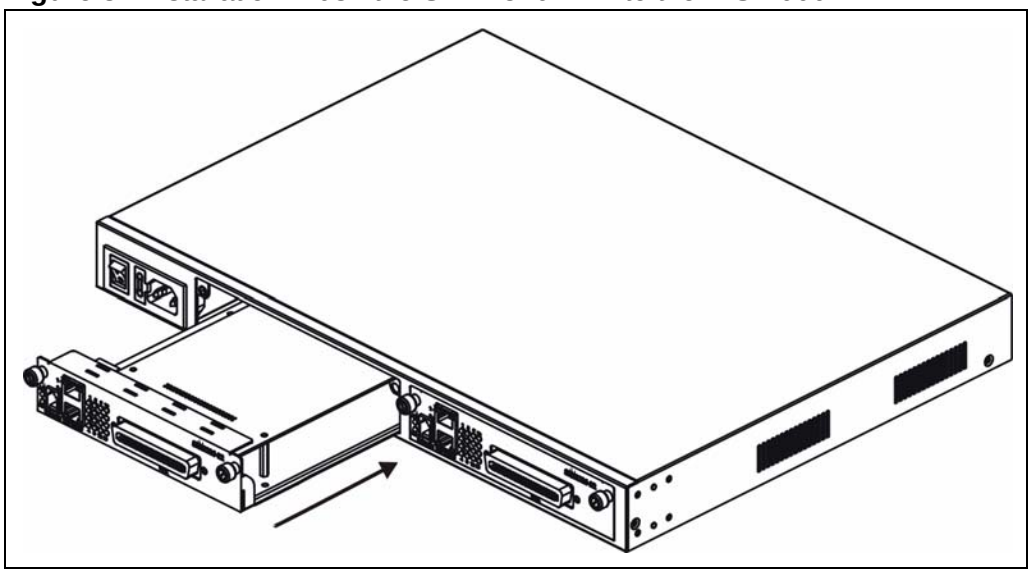
This chapter shows you how to install the SAM1316-22 in the IES-1000 and how to remove it.

2.2 Installing the SAM1316-22 in the IES-1000

1 Hold the SAM1316-22 with the network ports facing you.

2 Insert it into an empty slot on the front of the IES-1000. Push the SAM1316-22 into the IES-1000 until the front of the SAM1316-22 is flush with the IES-1000.

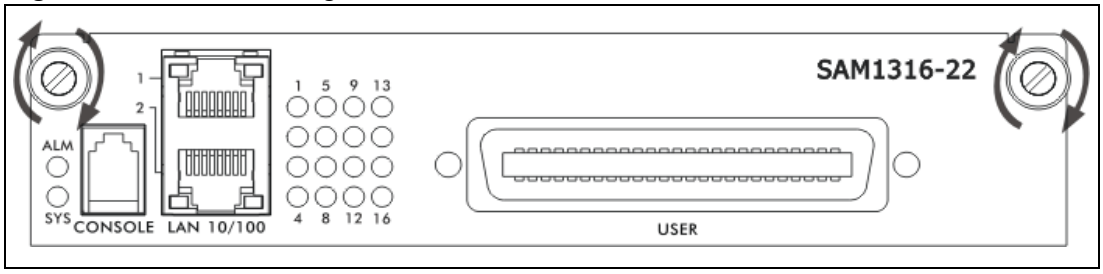
Figure 3 Installation: Push the SAM1316-22 into the IES-1000



Note: The front of the SAM1316-22 must be flush with the front of the IES-1000.

3 Turn the two screws on the front of the SAM1316-22 clockwise to secure the SAM1316-22 to the chassis as shown below.

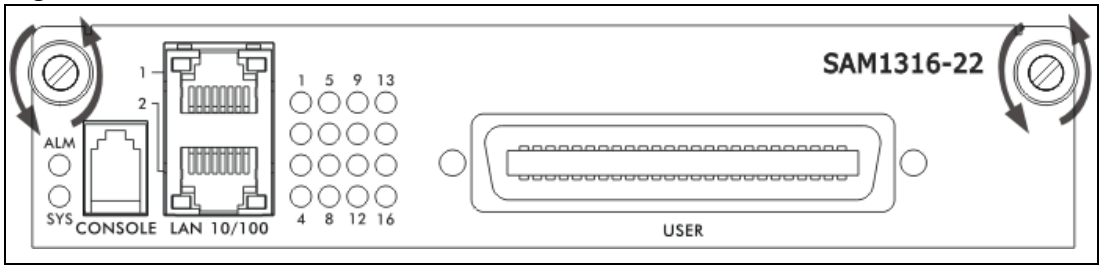
Figure 4 Installation: Tighten Module Screws



2.3 Removing the SAM1316-22 from the IES-1000

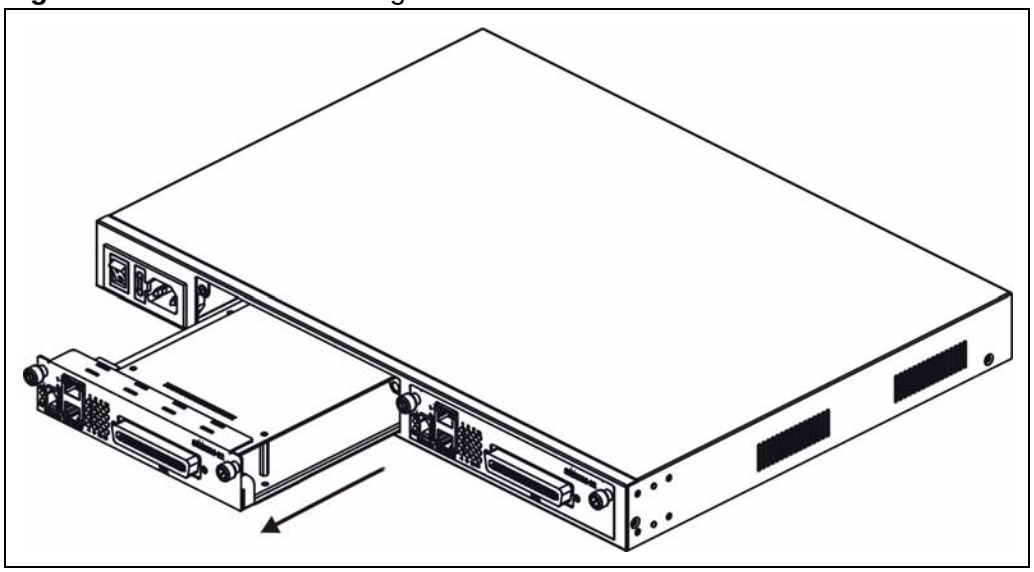
1 Turning the two screws that secure the module to the chassis counter-clockwise to loosen them.

Figure 5 Removal: Loosen Module Screws



2 Gently pull the SAM1316-22 out of the chassis as shown next.

Figure 6 Removal: Removing the SAM1316-22 from the IES-1000

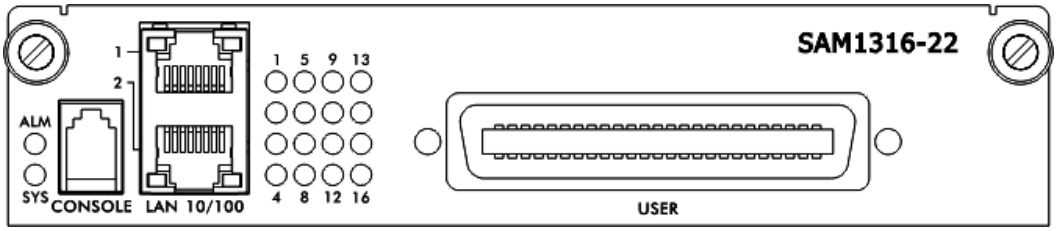


3

Front Panel

This chapter describes the front panel of the SAM1316-22, shown below.

Figure 7 Front Panel



The LEDs and ports are discussed in the following sections.

3.1 LEDs

The following table describes the LED indicators on the SAM1316-22.

Table 1 LEDs

LED	COLOR	STATUS	DESCRIPTION
ALM	Red	On	The temperature or voltage is abnormal.
		Off	The temperature or voltage is normal.
SYS	Green	On	The system is running.
		Blinking	The system is rebooting and performing self-diagnostic tests.
		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.
		Blinking	There is network traffic on a 10 Mbps Ethernet network.
		Off	The link to a 10 Mbps Ethernet network is down.
	Orange	On	The link to a 100 Mbps Ethernet network is up.
		Blinking	There is network traffic on a 100 Mbps Ethernet network.
		Off	The link to a 100 Mbps Ethernet network is down.

Table 1 LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
1-16	Green	On	The DSL link is up.
		Off	The DSL link is down.

3.2 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 SAM1316-22 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	Connect the Telco-50 connector to subscribers.

Each port is discussed further in the following sections.

3.2.1 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 SAM1316-22. Connect the female end to a serial port (COM1, COM2 or other COM port) of your computer.

3.2.2 LAN (Ethernet) Ports

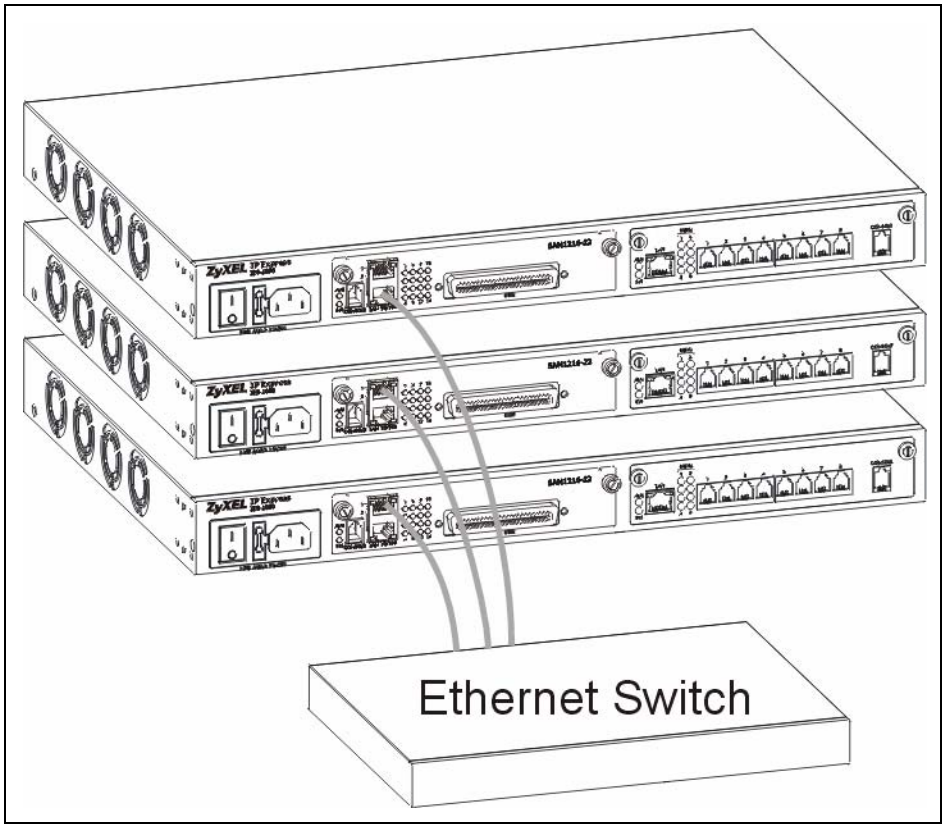
The factory default negotiation settings for the Ethernet ports on the SAM1316-22 are:

- Speed: Auto
- Duplex: Auto

Connect the LAN port of your SAM1316-22 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 an Ethernet switch as shown next.

Figure 8 LAN Ports: Stacking Multiple IES-1000 Units



3.2.3 USER Ports

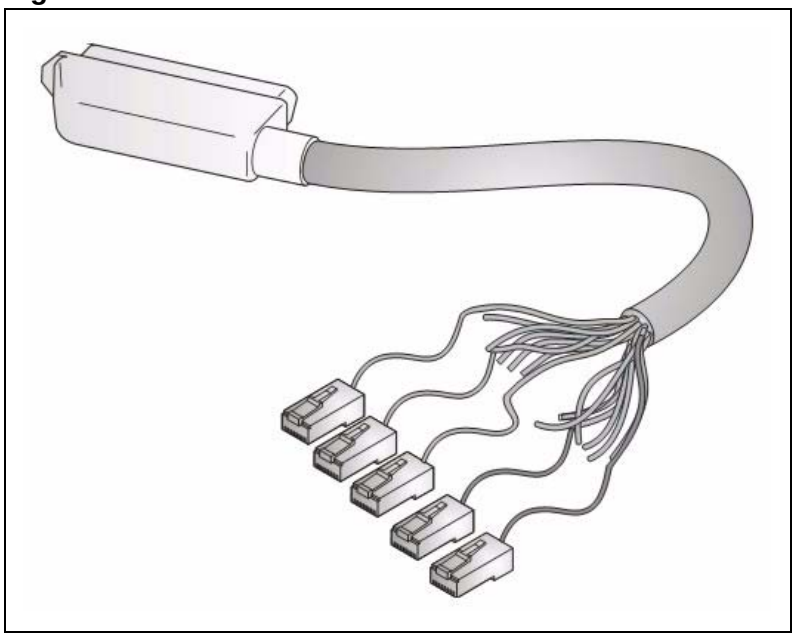
Use a Telco-50 connector to connect the USER ports to other SHDSL devices. The rest of this section introduces Telco-50 cables, MDF (Main Distribution Frames), and explains how to connect the USER ports to MDF.

3.2.3.1 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, RJ-11 connectors or directly to DSL modem(s).

Figure 9 Telco-50 Cable with RJ-11 Connectors



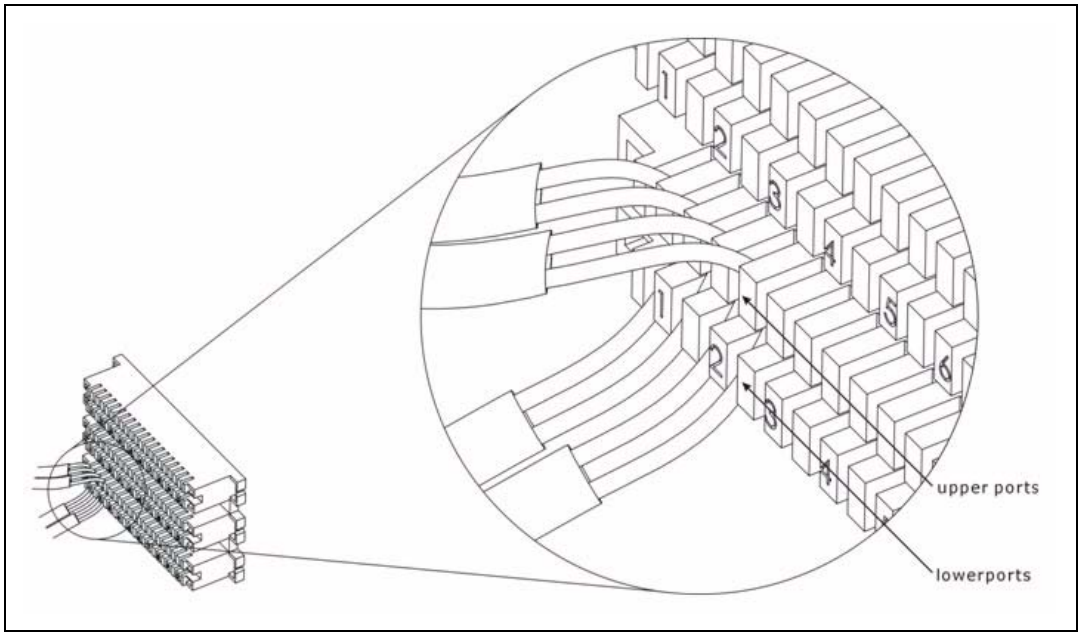
See Appendix C on page 443 for pin assignments.

3.2.3.2 Main Distribution Frame (MDF)

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 10 MDF Wiring



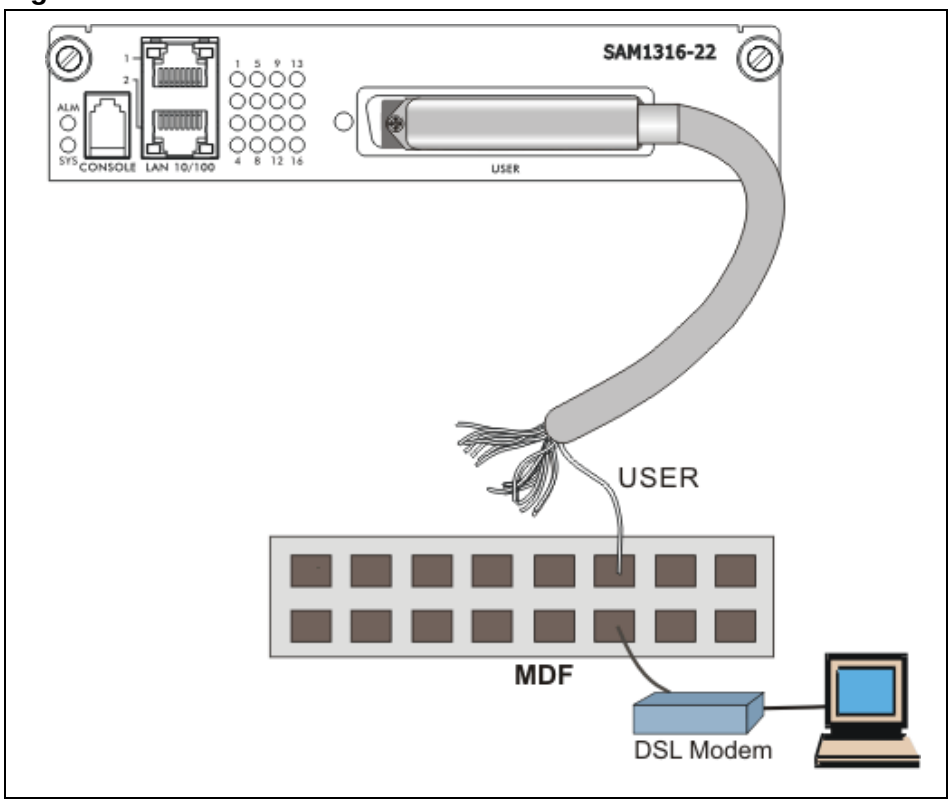
- Connect wiring from end-user equipment to the lower ports of an MDF using a telephone wire. Connect wiring from the telephone company to the upper ports of an MDF (see the previous figure).
- Some MDFs have surge protection circuitry built in between the two banks; thus, do not connect telephone wires from the telephone company directly to the SAM1316-22.
- Use a punch-down tool to seat telephone lines between MDF blocks.

3.2.3.3 Typical MDF Scenario

You want to install the SAM1316-22 in an environment where there are no previously installed MDFs. There is no phone service and you want to install the SAM1316-22 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-SAM1316-22 end of the Telco-50 cable and then connect to DSL modems directly.

Figure 11 MDF Installation Scenario



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.

PART II
Technical Reference

4

Introducing the Web Configurator

4.1 Overview

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

The web configurator allows you to use a web browser to manage the SAM1316-22.

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 SAM1316-22's storage that remains even if the SAM1316-22'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.

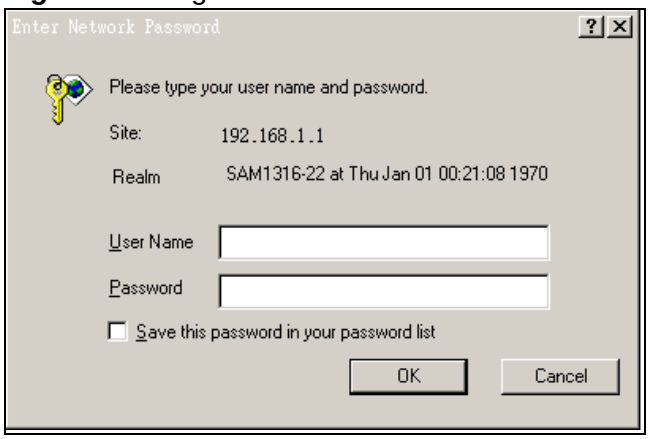
4.3 Accessing the Web Configurator

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 SAM1316-22 (default: **192.168.1.1** is the factory default) in the **Location** or **Address** field. Press **Enter**. The **Login** screen appears.

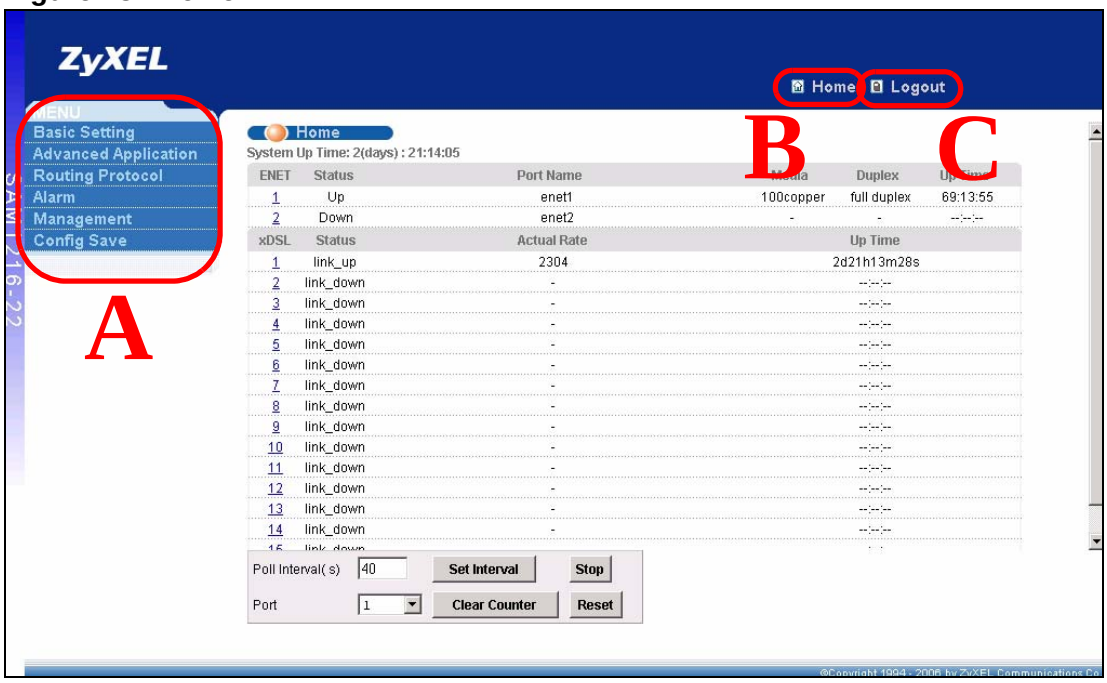
Figure 12 Login



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 13 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 47 for more information.

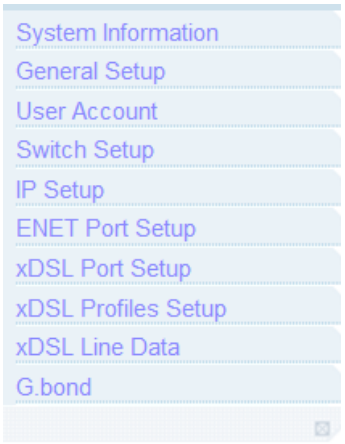
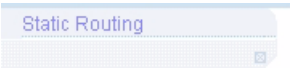
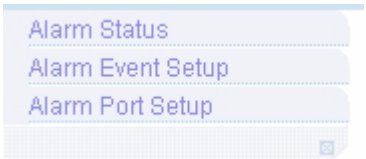
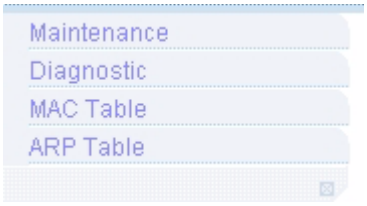
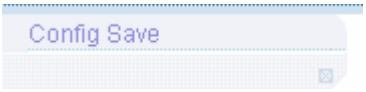
B - Click this to open the **Home** screen. (This is the same screen that is displayed above.) See Chapter 6 on page 59 for more information.

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 3 Navigation Panel Submenu Links

BASIC SETTING	ADVANCED APPLICATION	ROUTING PROTOCOL
		
ALARM	**MANAGEMENT**	**CONFIG SAVE**
		

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

Table 4 Web Configurator Screens

LABEL	DESCRIPTION
Basic Setting	
System Information	Use this screen to display general system and hardware monitoring information.
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	This link takes you to screens where you can 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.

Table 4 Web Configurator Screens (continued)

LABEL	DESCRIPTION
2684 Routed Mode	Use this screen to configure the SAM1316-22 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.
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 SAM1316-22 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 SAM1316-22 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 for sending SNMP traps or sys logs for alarms on an individual port(s).
Alarm History	Use this screen to display the alarms that have been raised by the SAM1316-22, including the severity level of an alarm(s) and the date/time when the alarm occured.
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.

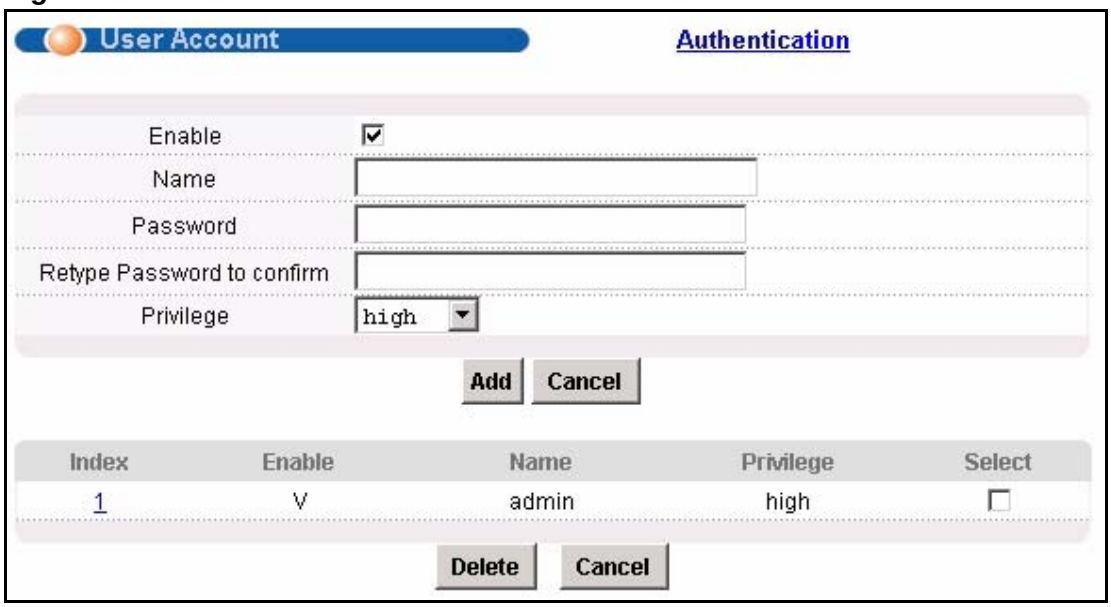
Table 4 Web Configurator Screens (continued)

LABEL	DESCRIPTION
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 SAM1316-22's storage that remains even if the SAM1316-22's power is turned off).

4.5 Changing Your Password

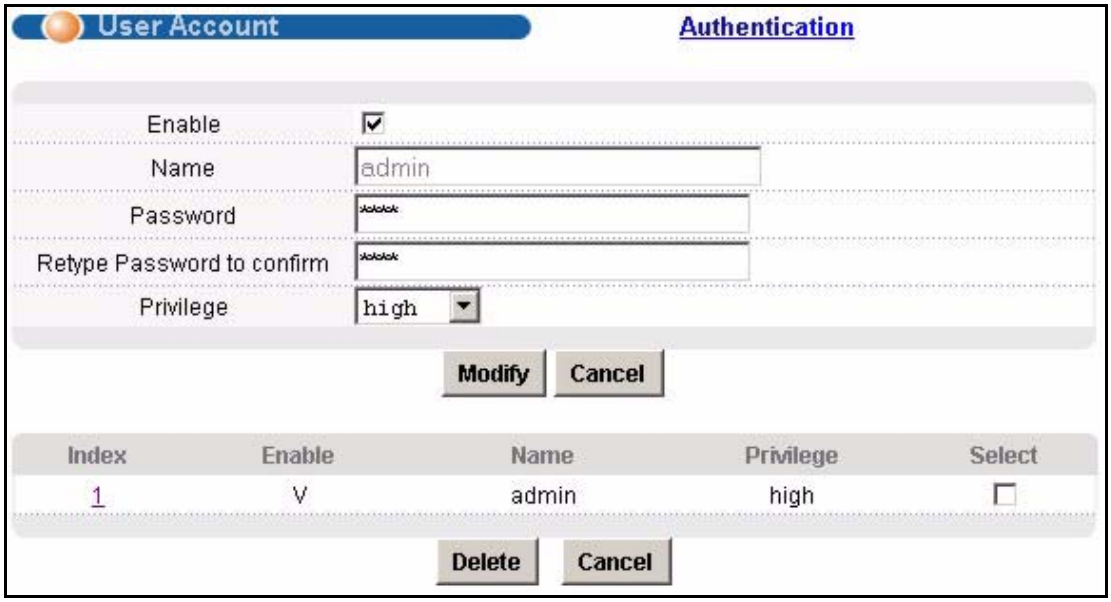
After you log in for the first time, it is recommended you change the default administrator password. Click **Basic Setting** and then **User Account** to display the **User Account** screen.

Figure 14 User Account



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

Figure 15 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 51.

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 SAM1316-22's power is turned off.

Click **Config Save** in the navigation panel to save your configuration to nonvolatile memory. Nonvolatile memory refers to the SAM1316-22's storage that remains even if the SAM1316-22's power is turned off.

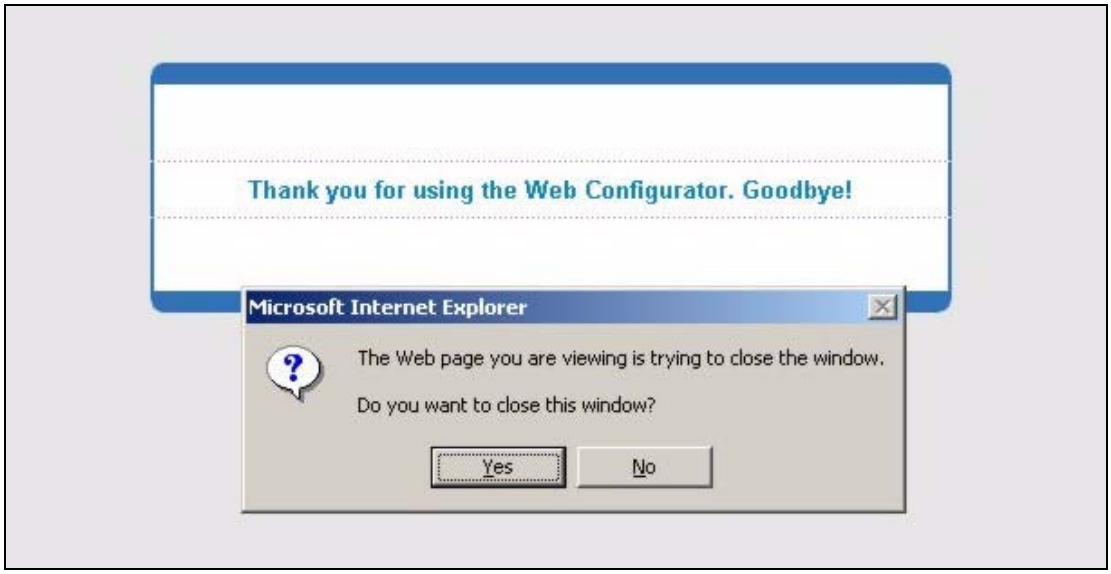
Note: Use **Config Save** when you are done with a configuration session.

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 16 Logout



5

Initial Configuration

5.1 Overview

This chapter describes initial configuration for the SAM1316-22. See Appendix A on page 435 for various default settings of the SAM1316-22.

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

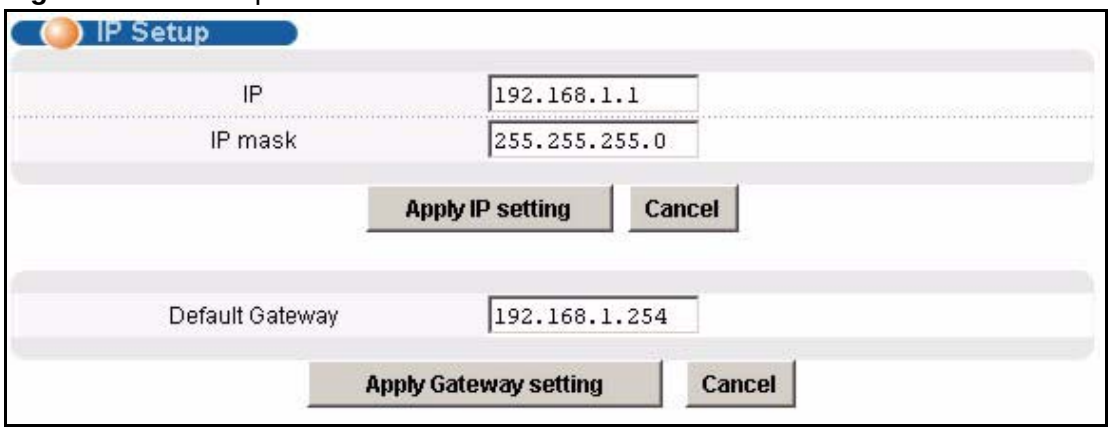
5.2 Initial Configuration

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 45 for instructions.

2 In the navigation panel, click **Basic Setting**, **IP Setup**. The **IP Setup** screen appears.

Figure 17 IP Setup



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

Note: If you change the IP address of the SAM1316-22, after you click **Apply IP setting**, you have to use the new IP address to log into the web configurator again.

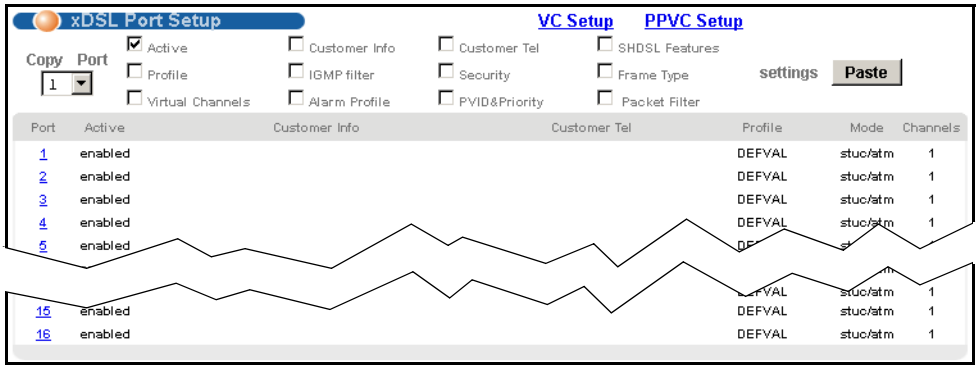
4 If your subscribers use VPI 0 and VCI 33 (the default for all of the DSL ports), go to step 13. Otherwise, use the following steps to change the VPI and VCI settings for all of the DSL ports.

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 SAM1316-22 drops any frames received from the subscriber that are tagged with another VLAN ID.

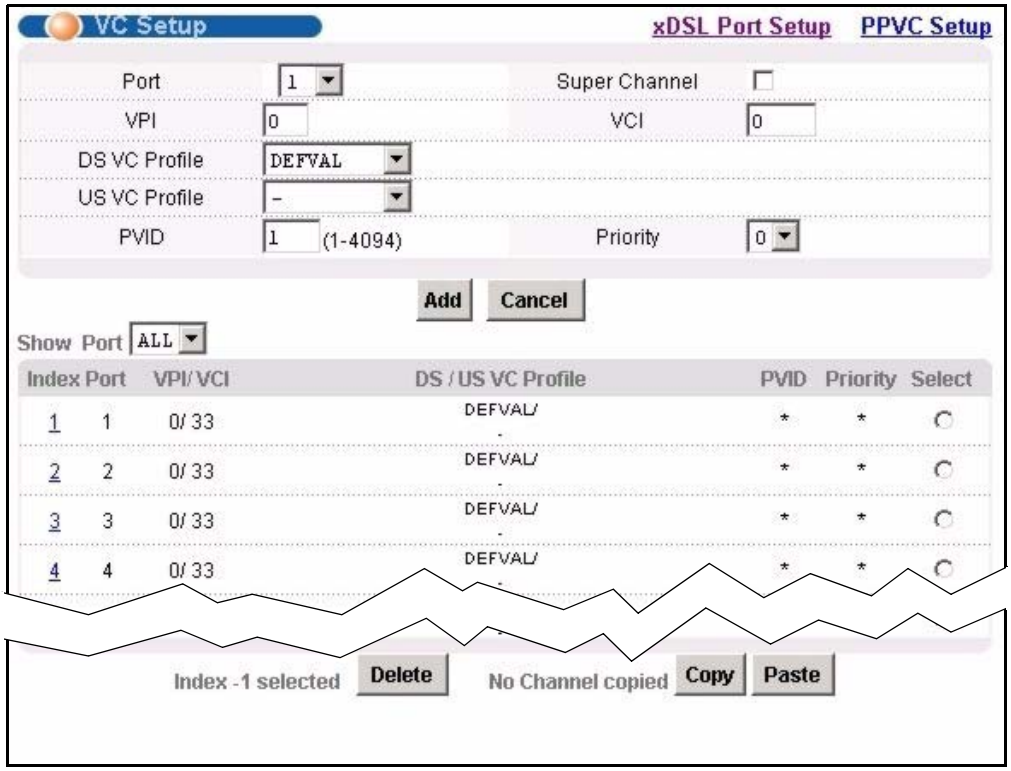
5 In the navigation panel, click **Basic Setting**, **xDSL Port Setup**. The **xDSL Port Setup** screen appears.

Figure 18 xDSL Port Setup



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

Figure 19 VC Setup

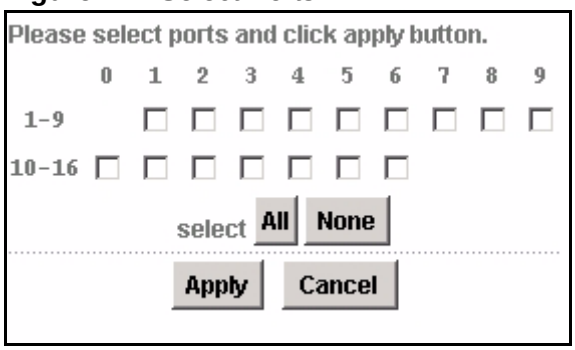


7 Select any virtual channel's **Select** radio button, and click **Delete**. The following screen appears.

Figure 20 VC Setup, Delete

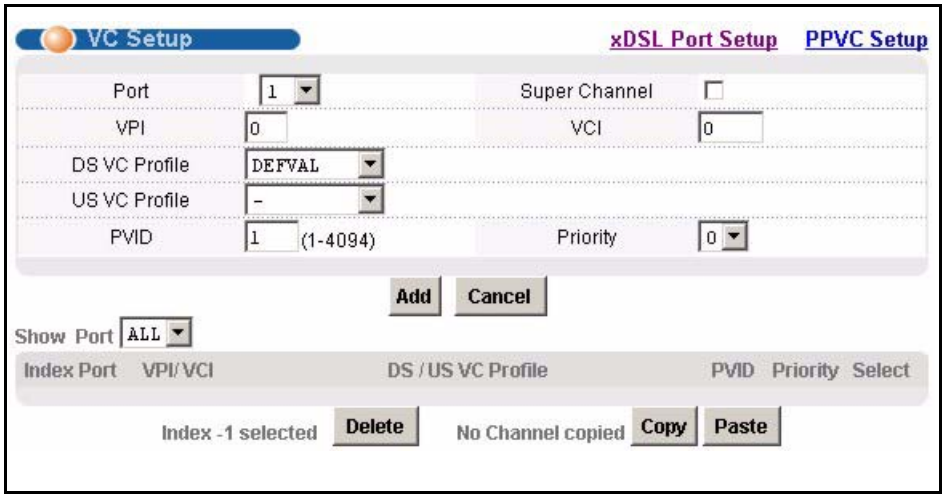
8 Click **OK**. The following screen appears.

Figure 21 Select Ports



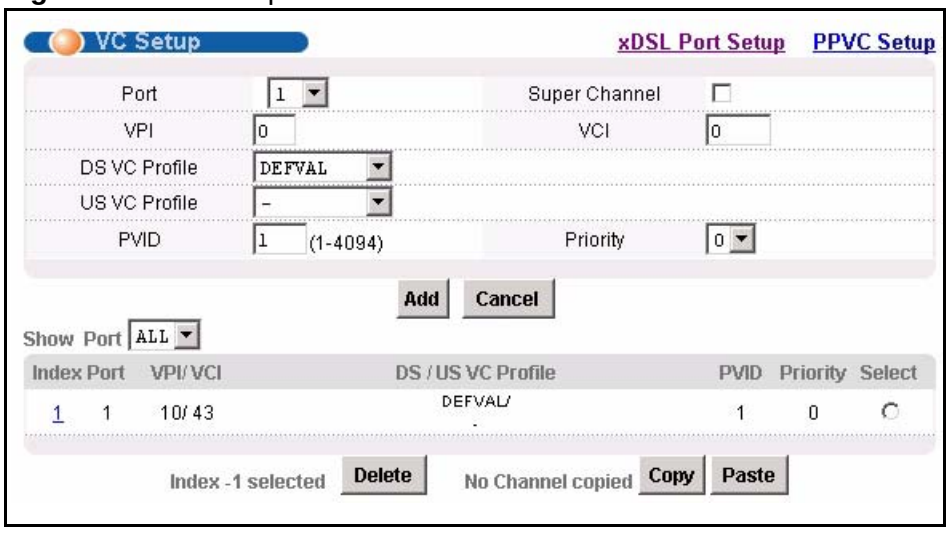
9 Click **All,** and then click **Apply**. The **VC Setup** screen is updated.

Figure 22 VC Setup



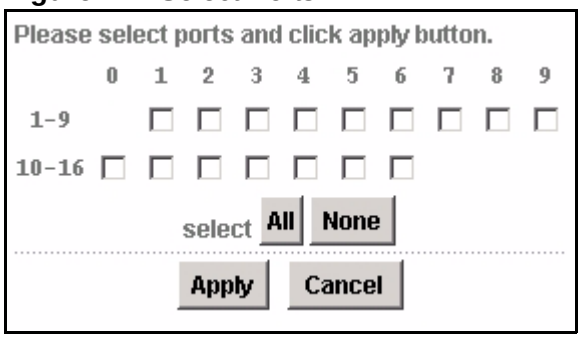
10 Select **Super Channel** to allow the channel to forward frames belonging to multiple VLAN groups (that are not assigned to other channels). Then, enter the VPI and VCI that you use. Leave the other default settings, and click **Add**. The **VC Setup** screen is updated.

Figure 23 VC Setup



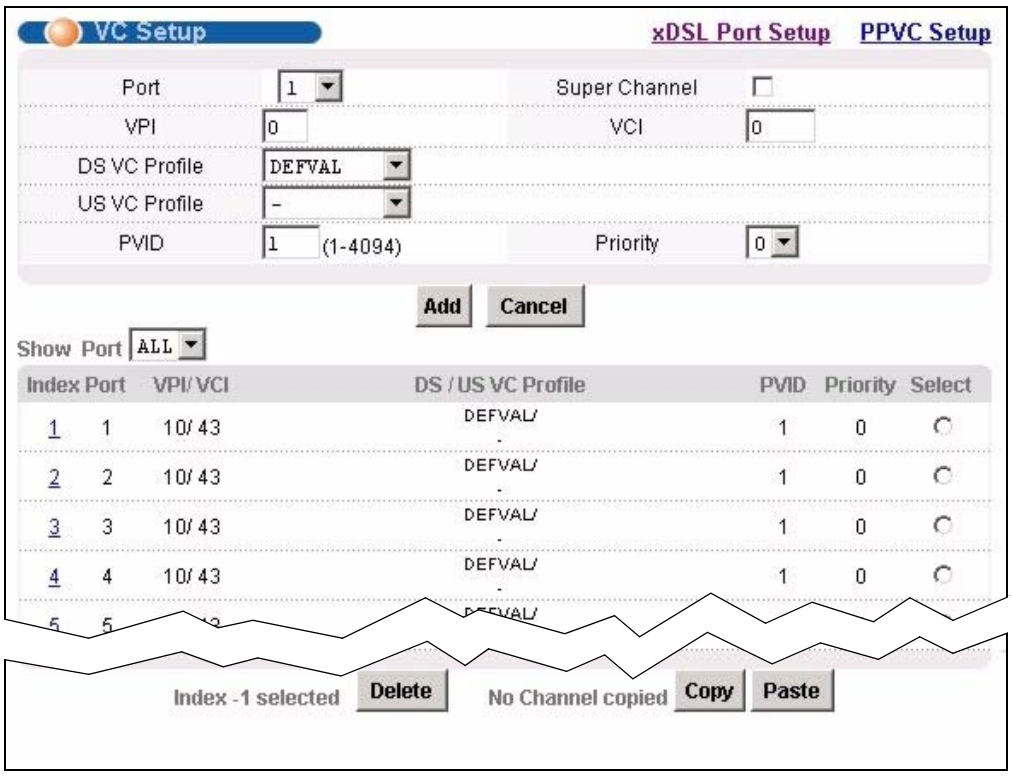
11 Select the new channel's **Select** radio button. Click **Copy**, and then click **Paste**. The following screen appears. The following screen appears.

Figure 24 Select Ports



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

Figure 25 VC Setup



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

Figure 26 Config Save

Note: Clicking **Save** in the **Config Save > Config Save** screen saves any changes, including the new IP address of the SAM1316-22, in the Flash memory. Otherwise, the SAM1316-22 reverts to the default settings (IP address is 192.168.1.1) once it is turned off.

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

Figure 27 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 Appendix A on page 435 for information on other default settings.

6

Home and Port Statistics Screens

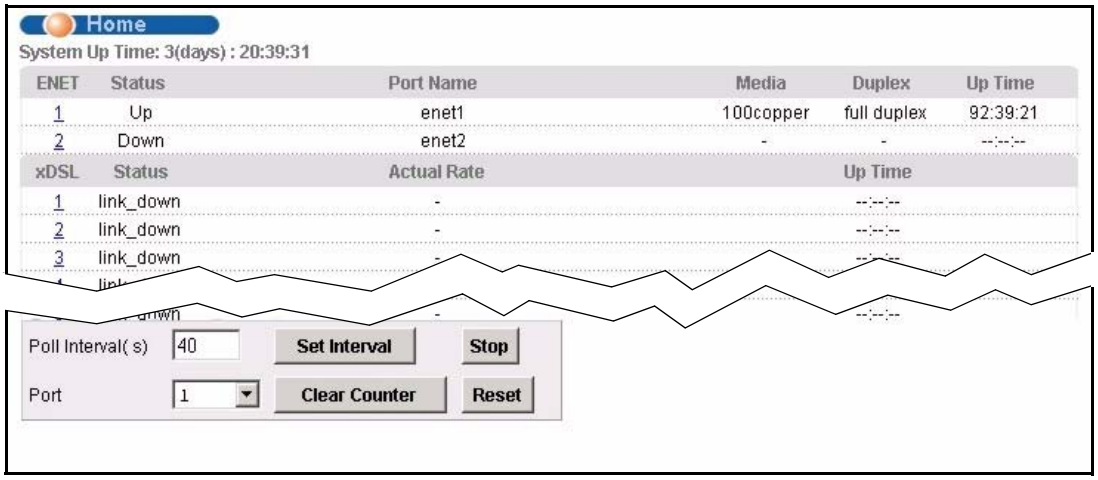
This chapter describes the **Home** (status), **Port Statistics**, and RMON screens.

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 28 Home



The following table describes the labels in this screen.

Table 5 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.

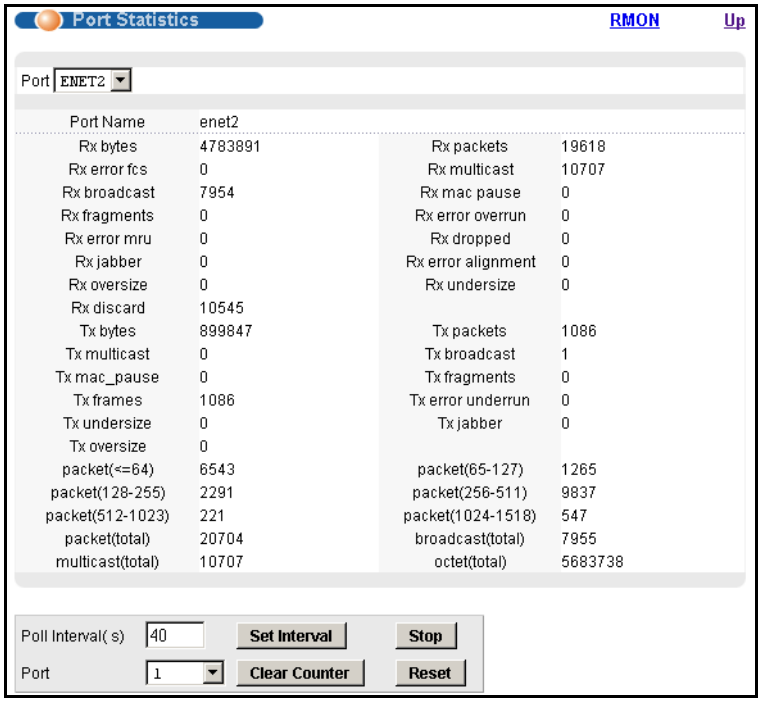
Table 5 Home (continued)

LABEL	DESCRIPTION
ENET	This field displays the number of the Ethernet port. Click a port number to display that port's statistics screen. The Ethernet Port Statistics Screen appears. See Section 6.1.1 on page 61.
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.
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. The DSL Port Statistics Screen appears. See Section 6.1.2 on page 64.
Status	This field shows whether the port is connected (**Up**) or not (**Down**).
Actual Rate	This field shows the interface's current bandwidth in kilobits per second. For interfaces that do not vary in bandwidth or for those where no accurate estimation can be made, this object should contain the nominal bandwidth.
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 29 Port Statistics (Ethernet)



The following table describes the labels in this screen.

Table 6 Port Statistics (Ethernet)

LABEL	DESCRIPTION
RMON	Click this to open the **RMON Statistics** screen.
Up	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.

Table 6 Port Statistics (Ethernet) (continued)

LABEL	DESCRIPTION
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.
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 SAM1316-22, 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.

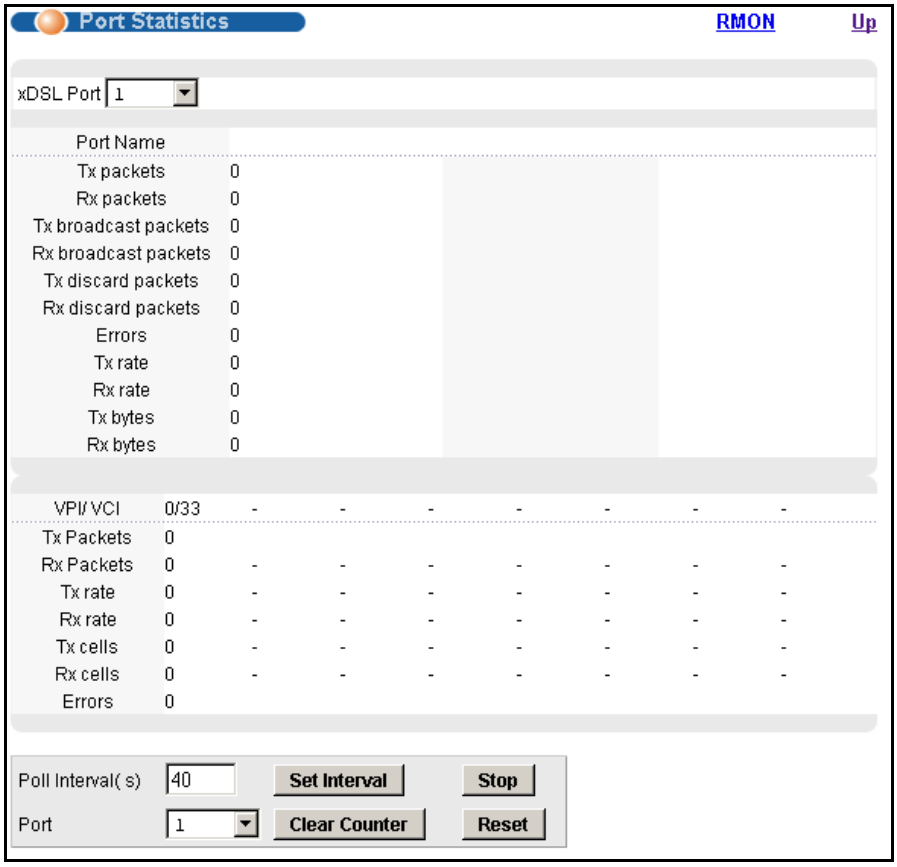
Table 6 Port Statistics (Ethernet) (continued)

LABEL	DESCRIPTION
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).
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 30 Port Statistics (DSL)



The following table describes the labels in this screen.

Table 7 Port Statistics (DSL)

LABEL	DESCRIPTION
RMON	Click this to open the **RMON Statistics** screen.
Up	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.

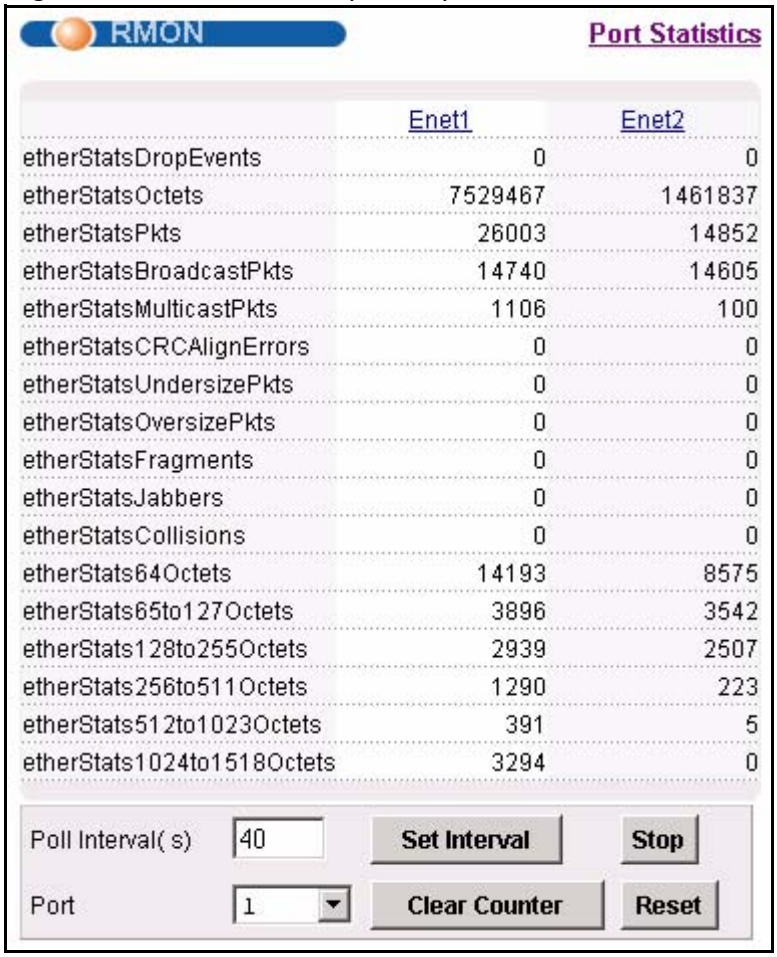
Table 7 Port Statistics (DSL) (continued)

LABEL	DESCRIPTION
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 SAM1316-22 does not discard packets that it sends.
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 SAM1316-22 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 31 Port Statistics (RMON)



The following table describes the labels in this screen.

Table 8 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.

Table 8 Port Statistics (RMON) (continued)

LABEL	DESCRIPTION
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.
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**.

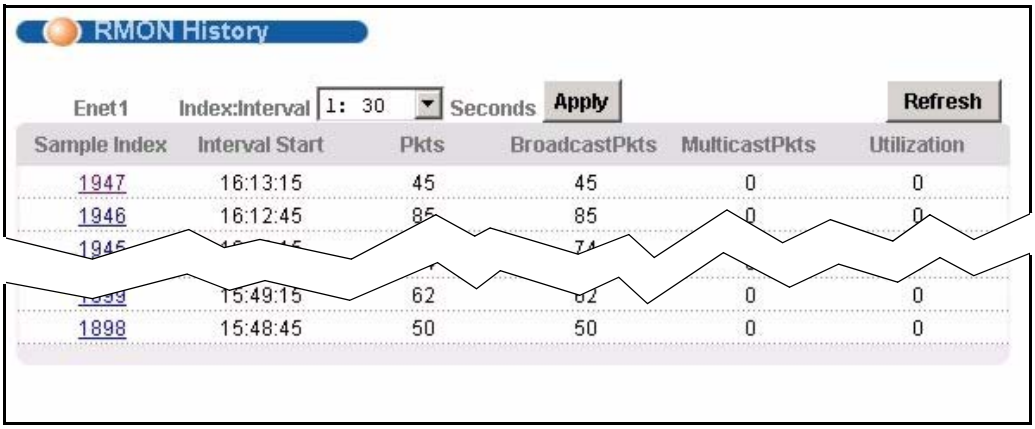
Table 8 Port Statistics (RMON) (continued)

LABEL	DESCRIPTION
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 32 Port Statistics (RMON History))



The following table describes the labels in this screen.

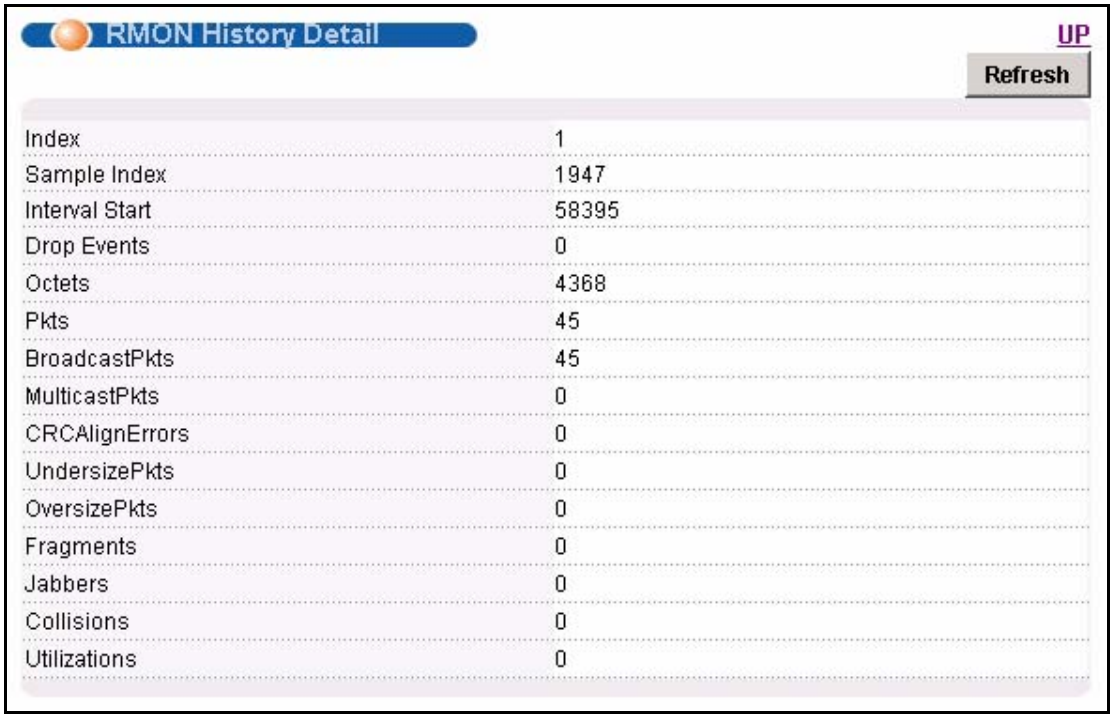
Table 9 Port Statistics (RMON History)

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 33 Port Statistics (RMON History Detail))



The following table describes the labels in this screen.

Table 10 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.

Table 10 Port Statistics (RMON History Detail) (continued)

LABEL	DESCRIPTION
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.
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.

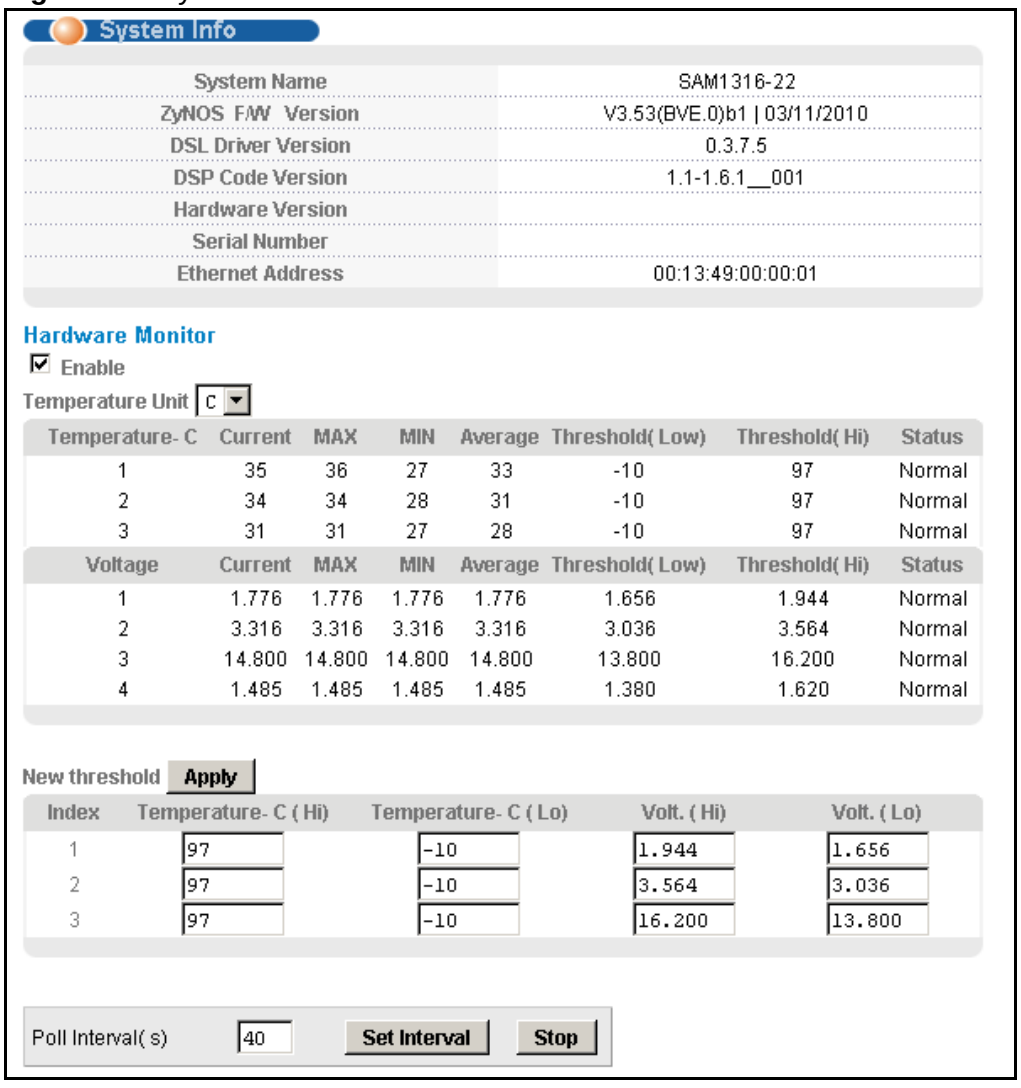
7

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 34 System Info



The following table describes the labels in this screen.

Table 11 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.
DSL Driver Version	This field displays the Digital Subscriber Line firmware version number.
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.

Table 11 System Info (continued)

LABEL	DESCRIPTION
	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.
Index	This field is a sequential value.
Temperature (Hi)	Use these fields to configure the highest temperature limit at each sensor.
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.

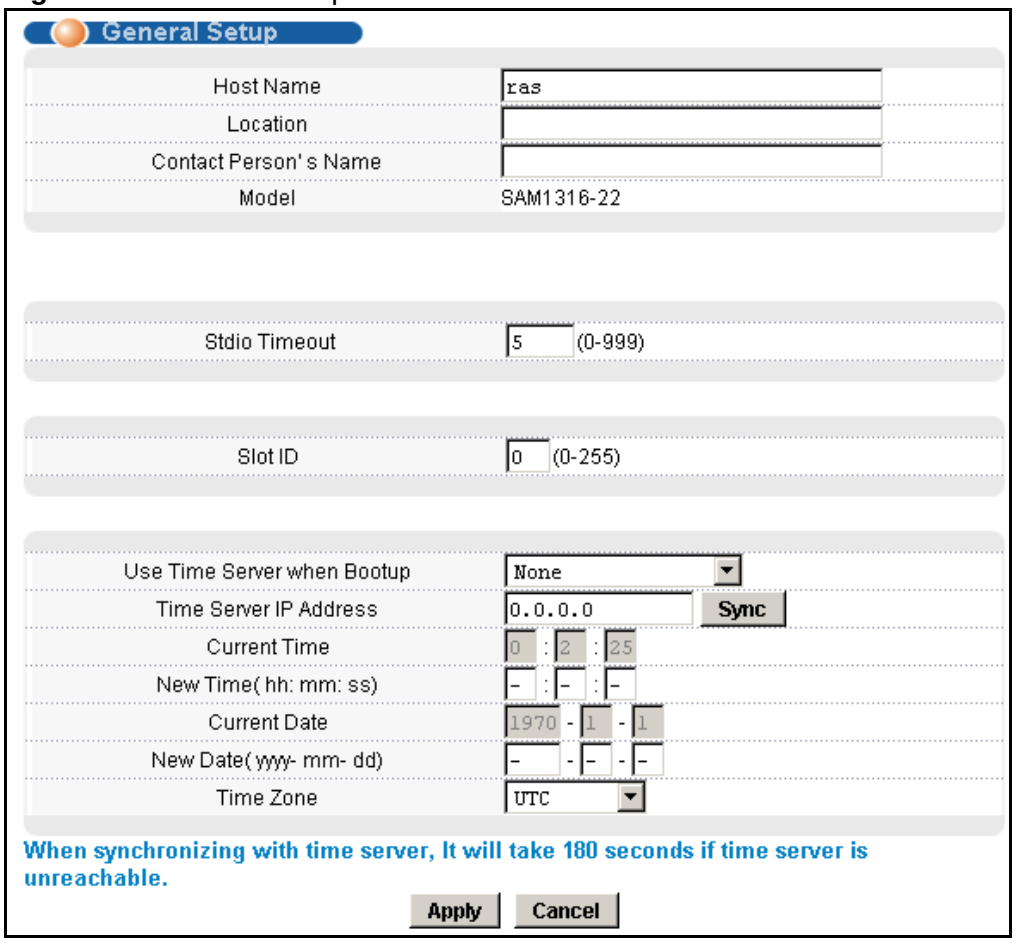
8

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 35 General Setup



The following table describes the labels in this screen.

Table 12 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.
Stdio Timeout	Enter how many minutes of inactivity the SAM1316-22 waits before automatically disconnecting a session. You need to enter the username and password again before accessing the Web Configurator.
Slot ID	If you have several SAM1316-22s in your network, you can use this field to identify them. This may be required by some services such as DHCP or PPPoE. If it's not required, you can leave the default value **0**.
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 SAM1316-22's volatile memory. The SAM1316-22 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

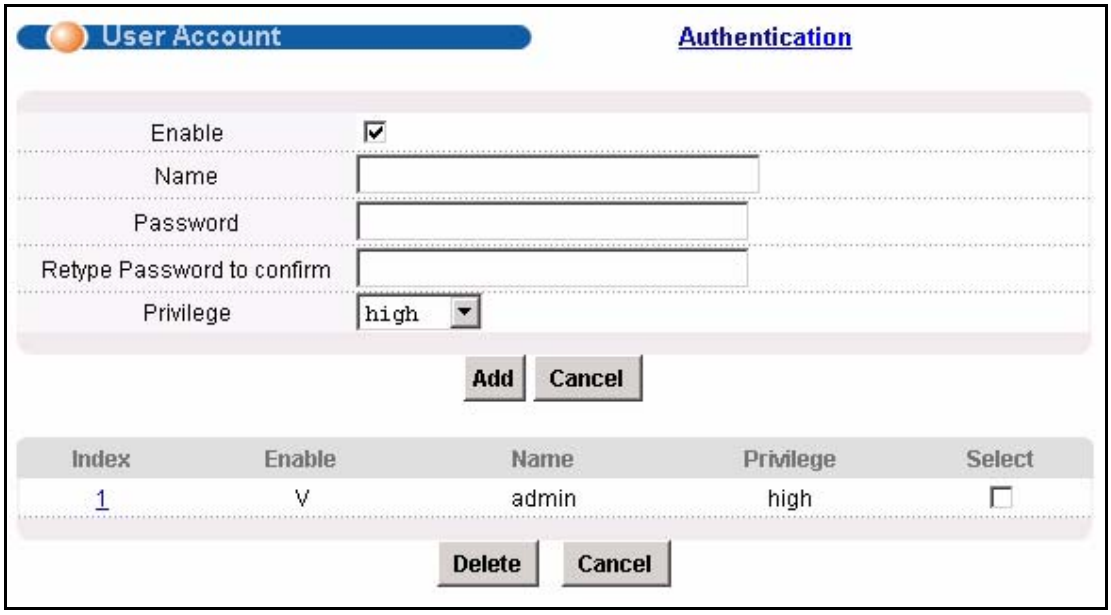
The **User Account** screens allows you to set up and configure system administrator accounts for the SAM1316-22. You can also configure the authentication policy for SAM1316-22 administrators. This is different than port authentication in Chapter 24 on page 175.

See Chapter 24 on page 175 for background information on authentication.

9.1 User Account Screen

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

Figure 36 User Account



The following table describes the labels in this screen.

Table 13 User Account

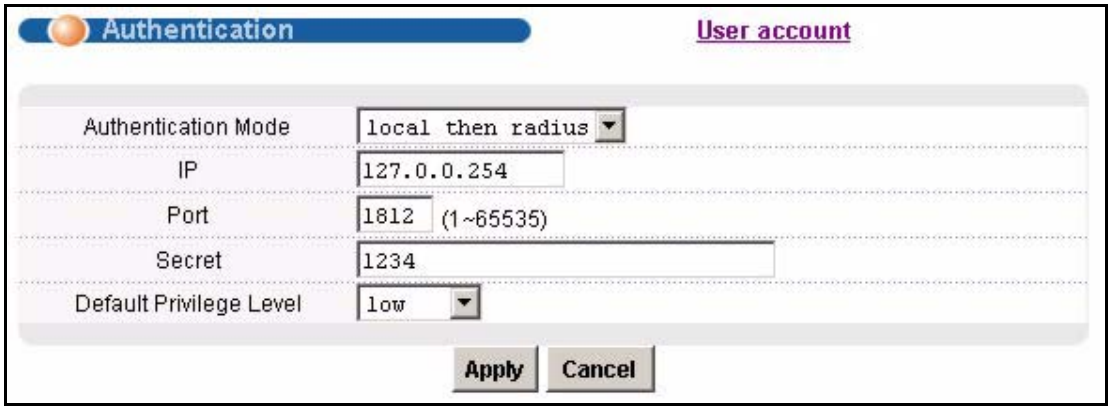
LABEL	DESCRIPTION
Authentication	Click this to open the **Authentication** screen. See Section 9.2 on page 78.
Enable	Select this check box to turn on the administrator account.
Name	Enter a user name for the administrator account.
Password	Enter a password for the administrator account.
Retype Password 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 SAM1316-22's volatile memory. The SAM1316-22 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 SAM1316-22.

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

Figure 37 Authentication



The following table describes the labels in this screen.

Table 14 User Account

LABEL	DESCRIPTION
User account	Click this to open the **User Account** screen. See Section 9.1 on page 77.
Authentication Mode	Select the process by which the SAM1316-22 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.

Table 14 User Account (continued)

LABEL	DESCRIPTION
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 SAM1316-22. 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 SAM1316-22.

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 SAM1316-22 supports standalone and daisychain switch modes.

10.2.1 Standalone Switch Mode

“Standalone switch mode” relates to the SAM1316-22’s operational behavior, not a standalone network topology. The standalone switch mode allows either or both of the SAM1316-22’s Ethernet ports to connect to the backbone Ethernet network. You can also connect one of the SAM1316-22’s Ethernet ports to the Ethernet network and the other to another SAM1316-22 (see Figure 38 on page 82 for an example). When the SAM1316-22 is in standalone mode, you can use it in a network topology that uses loops (you should also enable RSTP). You can have multiple SAM1316-22 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.

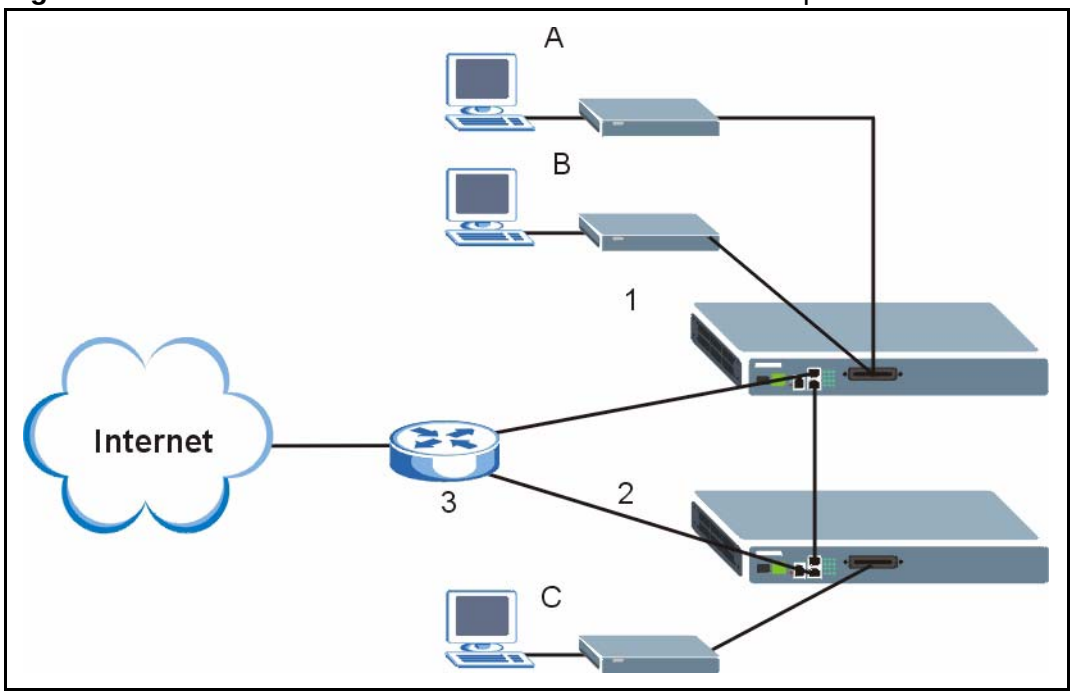
Standalone switch mode with port isolation enabled blocks communications between subscriber ports on an individual SAM1316-22. However, one SAM1316-22's subscribers can communicate with another SAM1316-22's subscribers if the two SAM1316-22's Ethernet ports are connected to each other (see Figure 38 on page 82 for an example). If you have multiple SAM1316-22 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 SAM1316-22 **1** and **2** connected to each other and the Ethernet backbone switch (**3**) in a network topology that creates a loop. The SAM1316-22 are using the standalone switch mode and have RSTP enabled.

In this example, both SAM1316-22 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 38 Port Isolation with Standalone Switch Mode Example



10.2.3 Daisychain Switch Mode

Daisychain switch mode sets the SAM1316-22 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) SAM1316-22. The daisychain switch mode is recommended for use in a network topology that does

not have loops. When you daisychain multiple SAM1316-22 they must all be set to daisychain mode.

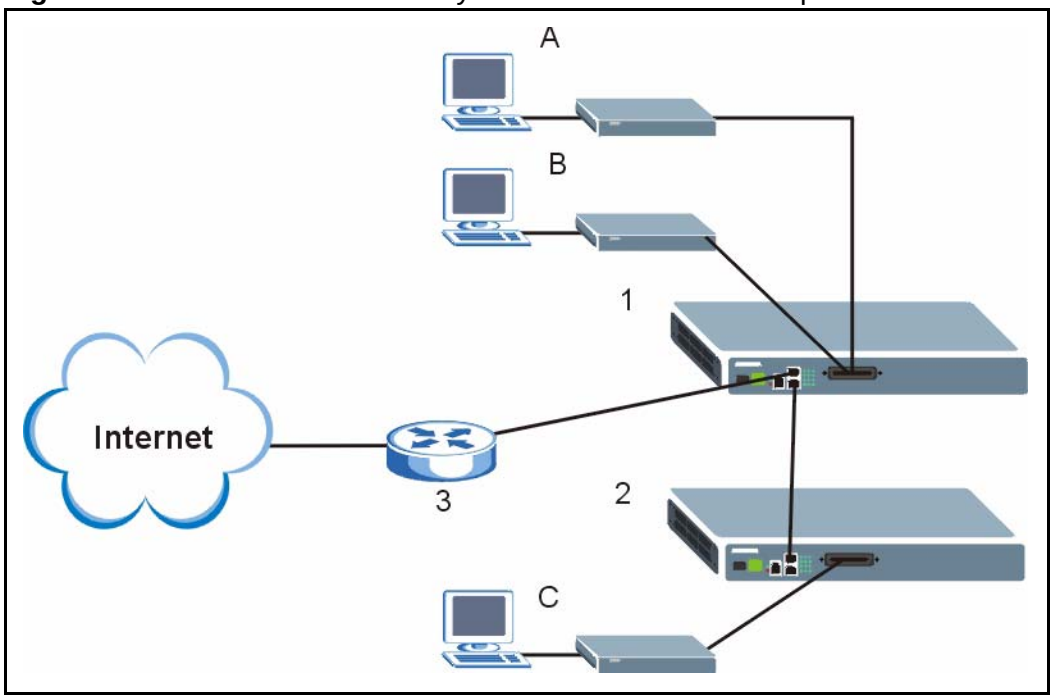
Daisychain switch mode with port isolation enabled blocks communications between subscriber ports on an individual SAM1316-22 and between the subscribers of any daisychained SAM1316-22 (see Figure 39 on page 83 for an example). Use the same port isolation setting on all SAM1316-22 that you set up in a daisychain.

10.2.4 Port Isolation with Daisychain Switch Mode Example

In the example below, the SAM1316-22 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 SAM1316-22 (**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.

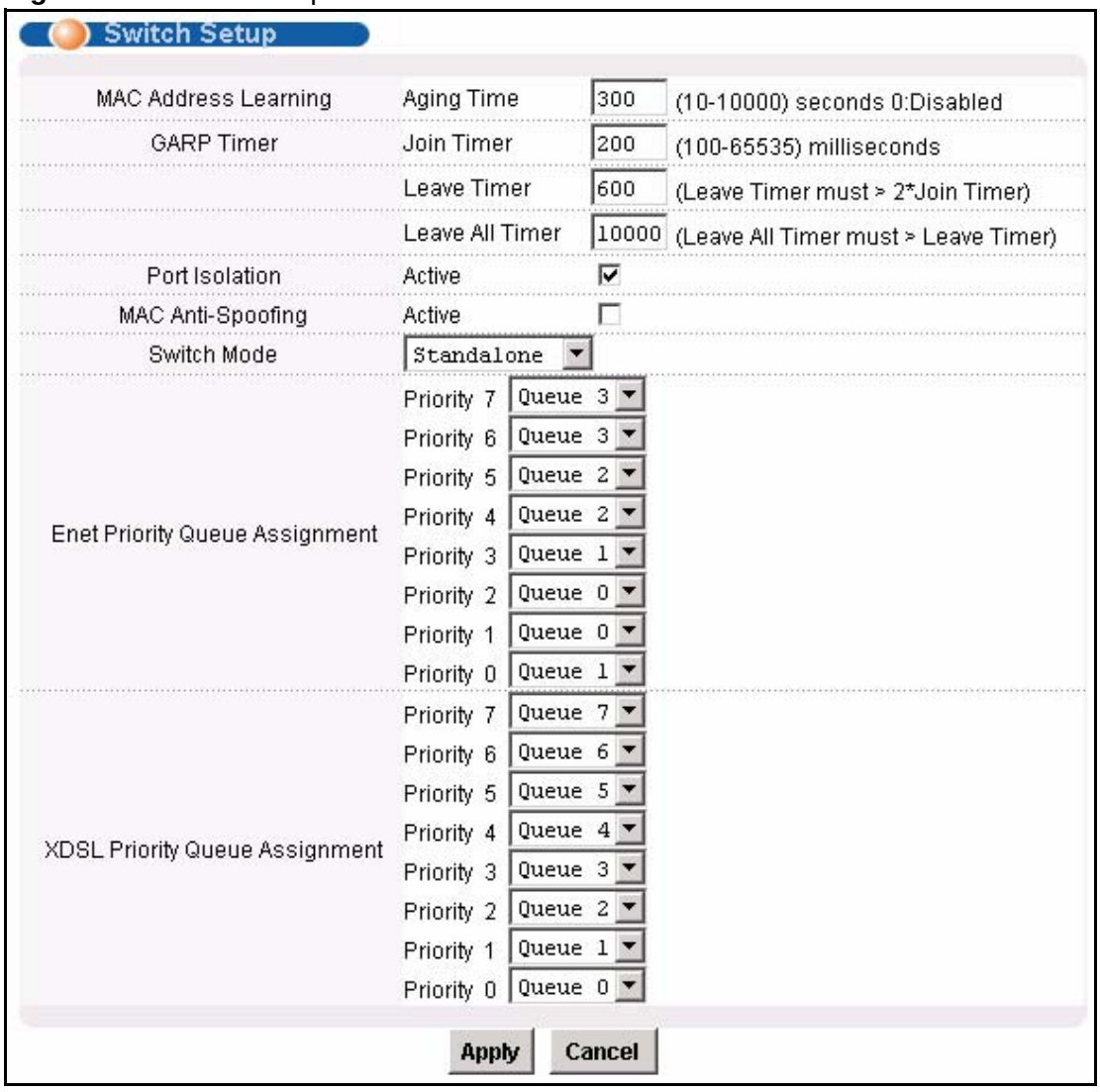
Figure 39 Port Isolation with Daisychain Switch Mode Example



10.3 Switch Setup Screen

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

Figure 40 Switch Setup



The following table describes the labels in this screen.

Table 15 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.
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 SAM1316-22 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 SAM1316-22'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 SAM1316-22. The SAM1316-22 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) SAM1316-22. Note: Daisychain mode is recommended for network topologies that do not use loops.

Table 15 Switch Setup (continued)

LABEL	DESCRIPTION
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 SAM1316-22’s volatile memory. The SAM1316-22 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.

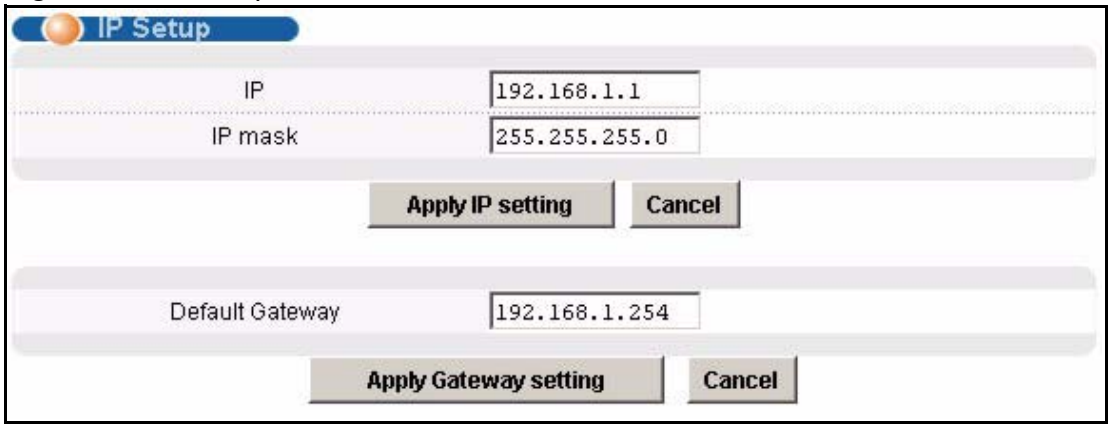
11

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 41 IP Setup



The following table describes the labels in this screen.

Table 16 IP Setup

LABEL	DESCRIPTION
IP	Enter the IP address of your SAM1316-22 in dotted decimal notation for example 1.2.3.4.
IP Mask	Enter the IP subnet mask of your SAM1316-22 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 SAM1316-22's volatile memory. The SAM1316-22 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 16 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 SAM1316-22's volatile memory. The SAM1316-22 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.

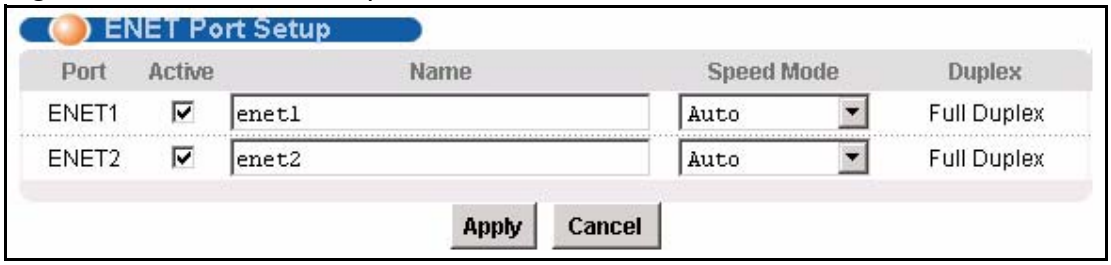
12

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 42 ENET Port Setup



The following table describes the labels in this screen.

Table 17 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 SAM1316-22 automatically determine the type of connection that the Ethernet port has. When the peer Ethernet device has auto-negotiation turned on, the SAM1316-22 negotiates with the peer to determine the connection speed. If the peer Ethernet port does not have auto-negotiation turned on, the SAM1316-22 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 SAM1316-22 uses full duplex Ethernet connections by default.

Table 17 ENET Port Setup (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the SAM1316-22's volatile memory. The SAM1316-22 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 DSL ports. It also covers how to configure virtual channels and virtual channel profiles.

13.1 DSL Profiles

A DSL profile is a table that contains a list of pre-configured DSL settings. Each DSL 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 DSL ports efficiently. You can configure all of the DSL ports with the same profile, thus removing the need to configure the DSL ports one-by-one. You can also change an individual DSL 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 a DSL 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.

13.2 Alarm Profiles

Alarm profiles define DSL port alarm thresholds. The SAM1316-22 sends an alarm trap and generates a syslog entry when the thresholds of the alarm profile are exceeded. See Section 14.8 on page 116 for how to configure alarm profiles.

13.3 Downstream and Upstream

Downstream refers to traffic going out from the SAM1316-22 to the subscriber's DSL modem or router. Upstream refers to traffic coming into the SAM1316-22 from the subscriber's DSL modem or router.

13.4 EFM and ATM Modes

The SAM1316-22 can operate in two modes: Ethernet in the First Mile (EFM) and Asynchronous Transfer Mode (ATM).

- IEEE 802.3-2004's EFM (Ethernet First Mile) lets you run Ethernet protocol over G.SHDSL. EFM framing has less overhead than ATM encapsulation, thus allowing better data transmission rates. If the CPE device supports EFM, select **efm** to use Ethernet frames over SHDSL. For ports set to EFM mode you can use PAF (PHY Aggregation Function) to bundle EFM PHYs to either increase the data rate of one logical EFM link for a given loop length or increase the maximum achievable loop length for a given data rate. This bundling is configured in the SHDSL profile's **Wire Pair** setting (see Chapter 14 on page 108).
- If the CPE device only supports ATM, select **atm** to use ATM cells over SHDSL. For ports set to ATM mode, you can use G.bond to create bundles of up to 16 wires (see Chapter 16 on page 129).

13.5 Default Settings

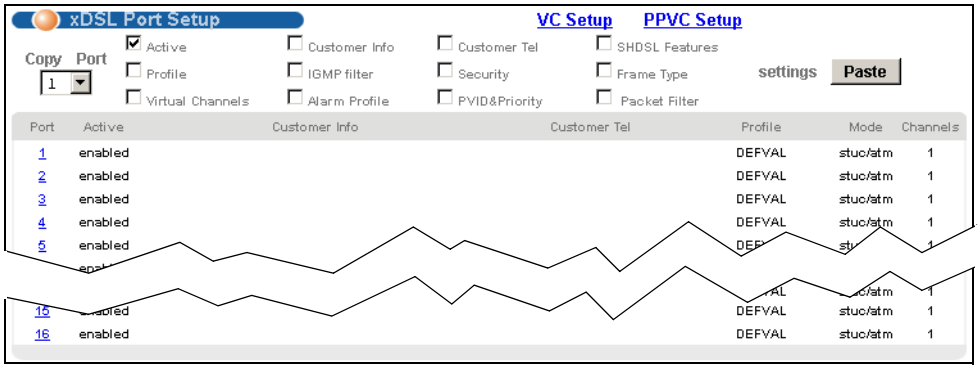
The default profile always exists and all of the DSL ports use the default profile settings when the SAM1316-22 is shipped. The default profile's name is set to DEFVAL.

See Appendix A on page 435 for the settings of the default profile and DSL port default settings.

13.6 xDSL Port Setup Screen

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

Figure 43 xDSL Port Setup



The following table describes the labels in this screen.

Table 18 xDSL Port Setup

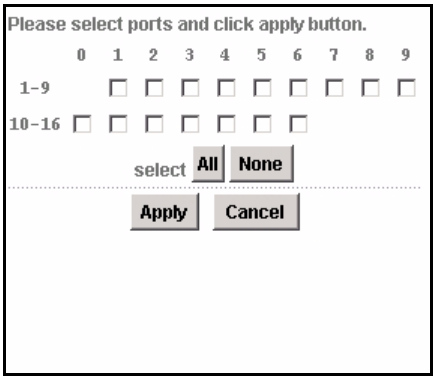
LABEL	DESCRIPTION
VC Setup	Click **VC Setup** to open the **VC Setup** screen where you can configure VC settings for the DSL ports (see Section 13.8 on page 98).
PPVC Setup	Click **PPVC Setup** to open the **PPVC Setup** screen where you can configure priority PVC settings for the DSL ports (see Section 13.10 on page 103).
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 44** 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 13.6.1 on page 95).
Customer Info	Select this check box to copy this port's subscriber information. This is configured in the **xDSL Port Setting** screen (see Section 13.6.1 on page 95).
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 13.6.1 on page 95).
SHDSL Features	Select this check box to copy this port's SHDSL feature settings. These are configured in the **xDSL Port Setting** screen (see Section 13.6.1 on page 95).
Profile	Select this check box to copy this port's port profile settings. These are configured in the **xDSL Port Profile Setup** screens (see Chapter 14 on page 107).

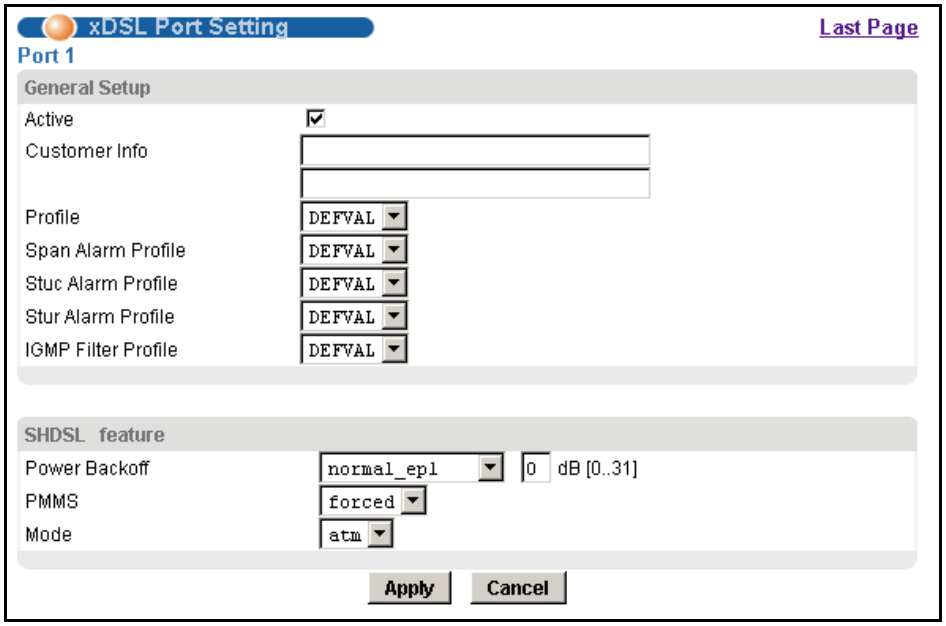
Table 18 xDSL Port Setup (continued)

LABEL	DESCRIPTION
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 14.10 on page 119).
Security	Select this check box to copy this port's security settings. This is configured in the **Port Security** screen (see Chapter 25 on page 181).
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 23 on page 167).
Virtual Channels	Select this check box to copy this port's virtual channel settings. These are configured in the **VC Setup** screen (see Section 13.8 on page 98).
Alarm Profile	Select this check box to copy this port's alarm profile. This is configured in the **Alarm Profile Setup** screen (see Section 14.8 on page 116).
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 17 on page 133).
Packet Filter	Select this check box to copy this port's packet filter settings. These are configured in the **Packet Filtering** screen (see Chapter 21 on page 161).
Paste	See **Copy Port**.
Port	This field shows each DSL 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 13.6.1 on page 95).
Customer Info	This field shows the customer information provided for this port. This is configured in the **xDSL Port Setting** screen (see Section 13.6.1 on page 95).
Customer Tel	This field shows the customer telephone number provided for this port. This is configured in the **xDSL Port Setting** screen (see Section 13.6.1 on page 95).
Profile	This field shows which profile is assigned to this port. This is configured in the **xDSL Port Setting** screen (see Section 13.6.1 on page 95).
Mode	This field shows which DSL operational mode the port is set to use. This is configured in the **xDSL Port Setting** screen (see Section 13.6.1 on page 95).
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 13.8 on page 98).

13.6.1 xDSL Port Setting Screen

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

Figure 45 xDSL Port Setting



The following table describes the labels in this screen.

Table 19 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 DSL port.
Customer Info	Enter information to identify the subscriber connected to this DSL port. You can use up to 31 printable ASCII characters (including spaces and hyphens).
Profile	Select a profile of DSL settings (such as the transfer rate, wire pair 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 107)
Span Alarm Profile	Select an alarm profile to define the thresholds that trigger an alarm on the port when exceeded. This alarm profile is for the whole span. This is the entire connection including any SHDSL regenerators that might be located between the STU-C (SHDSL Termination Unit - Central) and STU-R (SHDSL Termination Unit - Remote) end points. An SHDSL regenerator amplifies the SHDSL signal in order to increase the connection distance. Use the **Alarm Profile** screen to configure alarm profiles. (See Section 14.8 on page 116).

Table 19 xDSL Port Setting (continued)

LABEL	DESCRIPTION
Stuc Alarm Profile	Select an alarm profile to define the thresholds that trigger an alarm on the port when exceeded. This alarm profile is for the STU-C (SHDSL Termination Unit - Central) end point. Use the **Alarm Profile** screen to configure alarm profiles. (See Section 14.8 on page 116).
Stur Alarm Profile	Select an alarm profile to define the thresholds that trigger an alarm on the port when exceeded. This alarm profile is for the STU-R (SHDSL Termination Unit - Remote) end point. Use the **Alarm Profile** screen to configure alarm profiles. (See Section 14.8 on page 116).
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 14.10 on page 119).
SHDSL feature	
Power Backoff	Power backoff calculates how much power is needed for the connection. This allows the STU-C and STU-R to use only enough power for the port's maximum transmission rate (configured in the DSL profile). You can normally just leave the default setting (**NORMAL_EPL**). You only need to use this if the STU-R does not support EPL or you need to configure the port to use a specific power backoff setting. Select **NORMAL_EPL** to use power backoff with EPL (Estimated Power Loss). Each end calculates an EPL and uses it in determining a power backoff value for the other end to use. Select **FORCED_EPL** to use forced power backoff with EPL. The STU-C calculates an EPL and uses it in determining the power backoff values for both ends. This can be used when the STU-R device does not support EPL. Select **FORCED_NO_EPL** to use forced power backoff without EPL. The STU-C uses the value you specify in determining the power backoff values for both ends. This can be used when you have prior knowledge about the physical line (loop). Set the power backoff value (0~31 in dBm). When using **NORMAL_EPL** or **FORCED_EPL**, this sets the maximum power backoff value. When using **FORCED_NO_EPL**, this sets the power backoff value.
PMMS	Specify how the target noise margin value is acquired. Select **normal** to have each end of the connection determine the target noise margin to be used by the other end. Select **forced** to set the upstream and downstream parameters according to the target noise margin value set in the DSL profile.
Mode	Select the port's operational mode. Select **efm** to use Ethernet frames inside SHDSL framing. This option has less overhead and better data transmission rates. Select **atm** to use ATM cells inside SHDSL framing. Select this when your CPE device only supports this mode.

Table 19 xDSL Port Setting (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the SAM1316-22's volatile memory. The SAM1316-22 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.

13.7 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 DSL ports.

Use the **Edit Static VLAN** screen to configure a static VLAN on the SAM1316-22 for voice on the port.

Use the **DSL 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.

13.7.1 Super Channel

The SAM1316-22 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.

13.7.2 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.

13.7.3 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.

13.7.4 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.

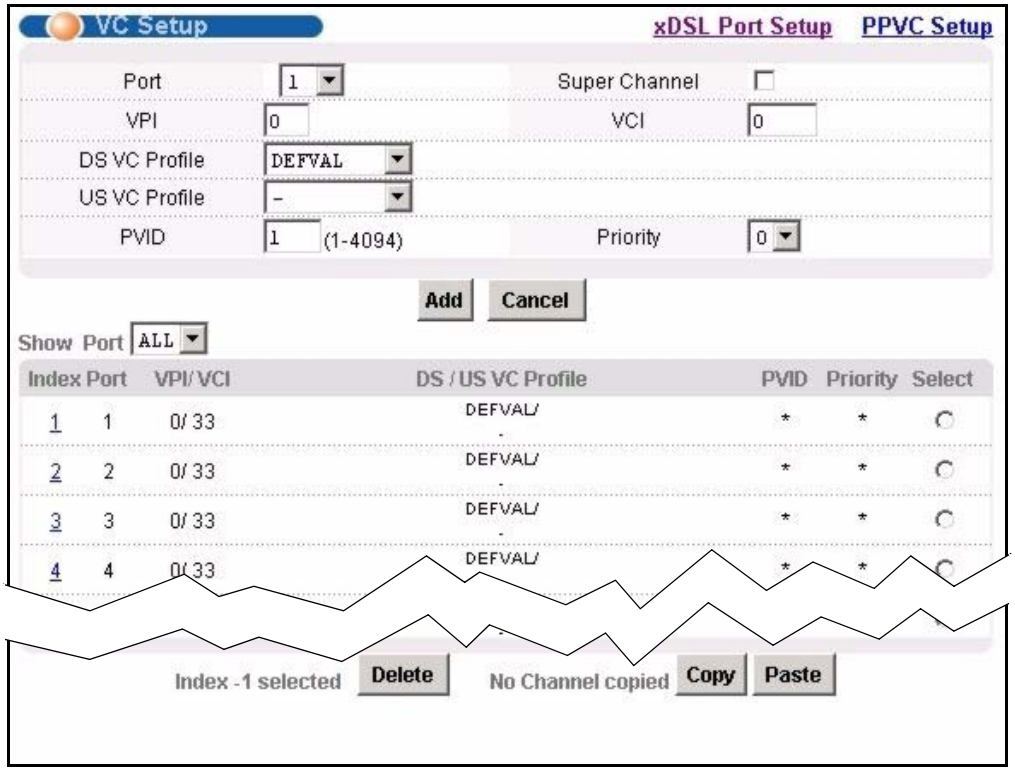
The SAM1316-22 provides two default virtual channel profiles: **DEFVAL** (for LLC encapsulation) and **DEFVAL_VC** (for VC encapsulation). By default, all virtual channels are associated to **DEFVAL**.

13.8 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 46 VC Setup



The following table describes the labels in this screen.

Table 20 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 13.6 on page 92).
PPVC Setup	Click **PPVC Setup** to open the **PPVC Setup** screen where you can configure priority PVC settings for the DSL ports (see Section 13.10 on page 103).
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 SAM1316-22 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.

Table 20 VC Setup (continued)

LABEL	DESCRIPTION
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 SAM1316-22 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 SAM1316-22's volatile memory. The SAM1316-22 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 a DSL 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 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.
US / DS 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 20 VC Setup (continued)

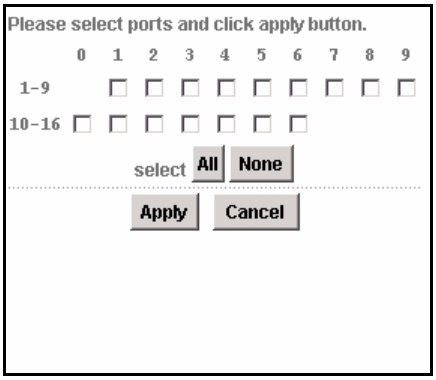
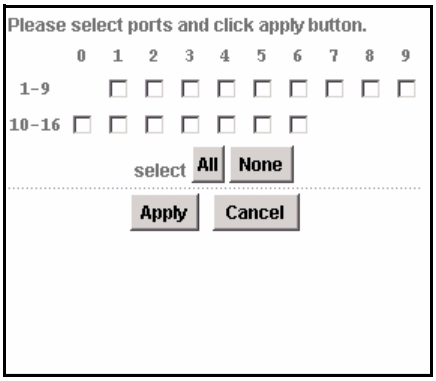
LABEL	DESCRIPTION
Select Delete	Do the following to remove one or more PVCs. 1. Select a PVC's **Select** radio button. 2. Click **Delete**. 3. Click **OK** if you want to remove the PVC from other ports. Click **Cancel** to only remove the one you selected. **Figure 47** Basic Setting, xDSL Port Setup, 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 48** Select Ports 

Table 20 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 49** Select Ports 

13.9 Priority-based PVCs

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

The SAM1316-22 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 21 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

Table 21 IEEE 802.1p Priority to PPVC Mapping (continued)

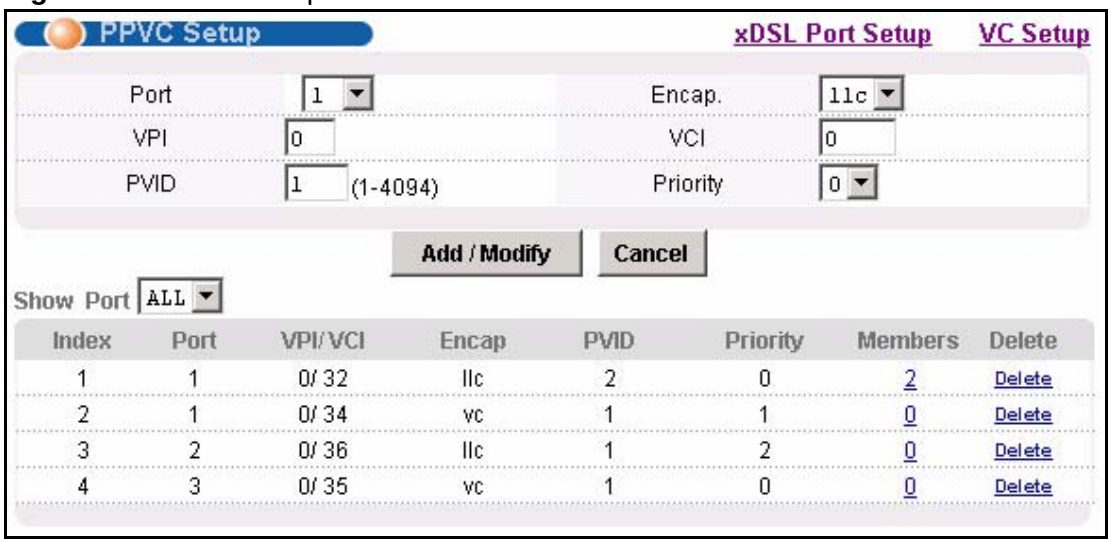
IEEE 802.1 PRIORITY	MAPS TO:	PPVC 0/33, PRIORITY QUEUE
2	->	level 2
1	->	level 1
0	>	level 0

13.10 PPVC Setup Screen

Use this screen to view and configure PPVCs.

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

Figure 50 PPVC Setup



The following table describes the labels in this screen.

Table 22 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 13.6 on page 92).
VC Setup	Click **VC Setup** to open the **VC Setup** screen where you can configure VC settings for the DSL ports (see Section 13.8 on page 98).
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 SAM1316-22 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.

Table 22 PPVC Setup (continued)

LABEL	DESCRIPTION
PVID	Type a PVID (Port VLAN ID) to assign to untagged frames received on this PPVC.
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 SAM1316-22's volatile memory. The SAM1316-22 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 a DSL 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 DSL 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 SAM1316-22 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 SAM1316-22's volatile memory. The SAM1316-22 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.

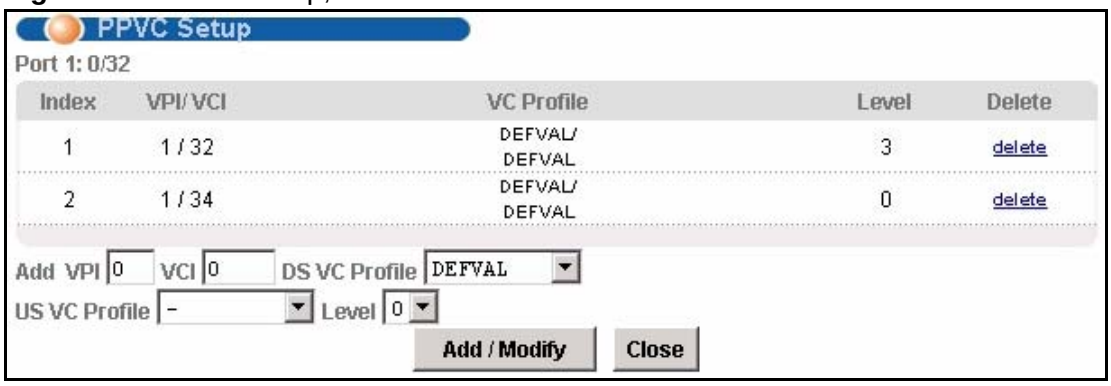
13.10.1 PPVC Setup Members Screen

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 51 PPVC Setup, Edit



The following table describes the labels in this screen.

Table 23 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 SAM1316-22's volatile memory. The SAM1316-22 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 SAM1316-22 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 23 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 SAM1316-22's volatile memory. The SAM1316-22 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 91.

14.1 Configured Versus Actual SHDSL Rates

You configure the maximum and minimum rates of individual SHDSL ports using the set profile command. 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 in the set profile command, the actual rate is always a multiple of 64 Kbps. If you enter a rate that is not a multiple of 64 Kbps, the actual value will be the next lower multiple of 64Kbps. For instance, if you specify 2100 Kbps for a port, the actual value will be 2048 Kbps, and if you specify 2120 Kbps, the actual value will be 2112 Kbps.

Note that when you configure a DSL profile, the upstream and downstream speeds are the same. The minimum rate must be less than or equal to the maximum rate.

14.2 N-wire Mode

The n-wire mode allows you to physically bundle two SHDSL ports into a single 4-wire connection. The 4-wire mode is described in ITU-T G.991.2. You can use it to connect to SHDSL modems or routers that also support 4-wire mode. N-wire mode also allows you to physically bundle four SHDSL ports into a single 8-wire connection. The 8-wire group is called mpair4.

N-wire mode can increase the reach of a particular data rate without having to regenerate the signal. It can also give increased bandwidth for LAN-to-LAN applications.

When using 4 or 8-wire groups, you must apply the same DSL profile to every port in a specific set of ports. For example, a profile for a 4-wire group can be used

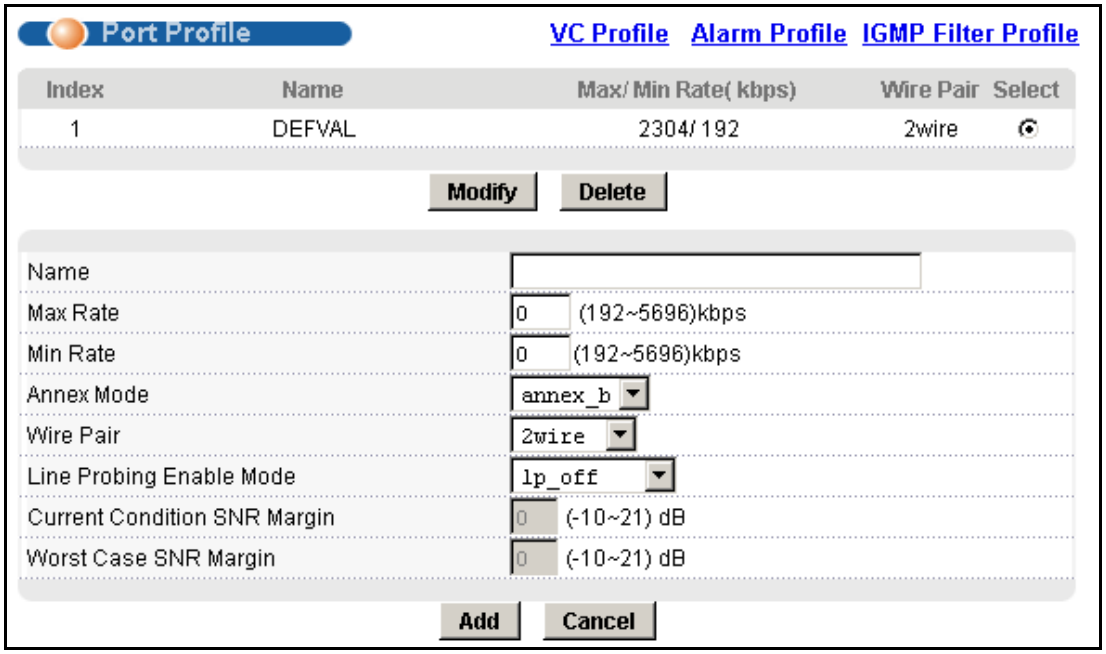
with ports 1,2 or 3,4 but not with ports 2,3 or 4,5. A profile for an 8-wire group can be used with ports 1,2,3,4 or 5,6,7,8 but not with ports 2,3,4,5 or 4,5,6,7.

After you assign the same DSL profile to all the ports in the set, you only have to configure the one with the highest port number. Its settings apply to all the ports in the set. For example, if you create an 8-wire group with ports 5, 6, 7, and 8, all the settings for port 8 apply to ports 5, 6, and 7 (regardless of whatever settings might already exist for ports 5, 6, and 7).

14.3 Port Profile Screen

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

Figure 52 Port Profile



The following table describes the labels in this screen.

Table 24 Port Profile

LABEL	DESCRIPTION
VC Profile	Click **VC Profile** to open the **VC Profile** screen where you can configure virtual channel profiles (see Section 14.7 on page 114).
Alarm Profile	Click **Alarm Profile** to open the **Alarm Profile** screen where you can configure limits that trigger an alarm when exceeded (see Section 14.8 on page 116)
IGMP Filter Profile	Click **IGMP Filter Profile** to open the **IGMP Filter Profile** screen where you can configure IGMP multicast filter profiles (see Section 14.10 on page 119).
Index	This is the port profile index number.

Table 24 Port Profile (continued)

LABEL	DESCRIPTION
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.
Max/Min Rate	This field displays the maximum and minimum transfer rate for this profile.
Wire Pair	This field displays how many pairs of wires the profile uses.
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.
Max Rate	Type a maximum transfer rate for this profile.
Min Rate	Type the minimum upstream transfer rate for this profile.
Annex Mode	Select the region setting. Select **annex_a** to use DSL over POTS (G.992.1 Annex A). Select **annex_b** to use DSL over ISDN (G.992.1 Annex B).
Wire Pair	Select a wire pair number. Select **2wire** for a normal connection using a single SHDSL port's two wires, this is the default. Select **4wire** for a 4-wire n-wire group (two SHDSL ports grouped together). Select **mpair4** for an 8-wire n-wire group (four SHDSL ports grouped together).
Line Probing Enable Mode	The SAM1316-22 and subscriber modem use line probes to determine the best possible transmission rate. This is used in rate adaptation. Select **lp_off** to have the SAM1316-22 skip the rate adaptation phase to shorten connection set up time. Select **lp_on_cur** to enable line probing using the current target Signal to Noise Ratio margin. Select **lp_on_wc** to enable line probing using the worst case target Signal to Noise Ratio margin.
Current Condition SNR Margin	Type the current condition target Signal to Noise Ratio margin, -10 ~ 21 in dB.
Worst Case SNR Margin	Type the worst case Signal to Noise Ratio margin, -10 ~ 21 in dB.

Table 24 Port Profile (continued)

LABEL	DESCRIPTION
Add	Click **Add** to save your changes to the SAM1316-22's volatile memory. The SAM1316-22 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.

14.4 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 14.5 on page 110). This allows you to fine-tune the levels of services on the priority of the traffic flow.

14.5 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).

14.5.1 ATM Traffic Classes

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

14.5.1.1 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.

14.5.1.2 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.

14.5.1.3 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.

14.5.2 Traffic Parameters

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

14.5.2.1 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.

14.5.2.2 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.

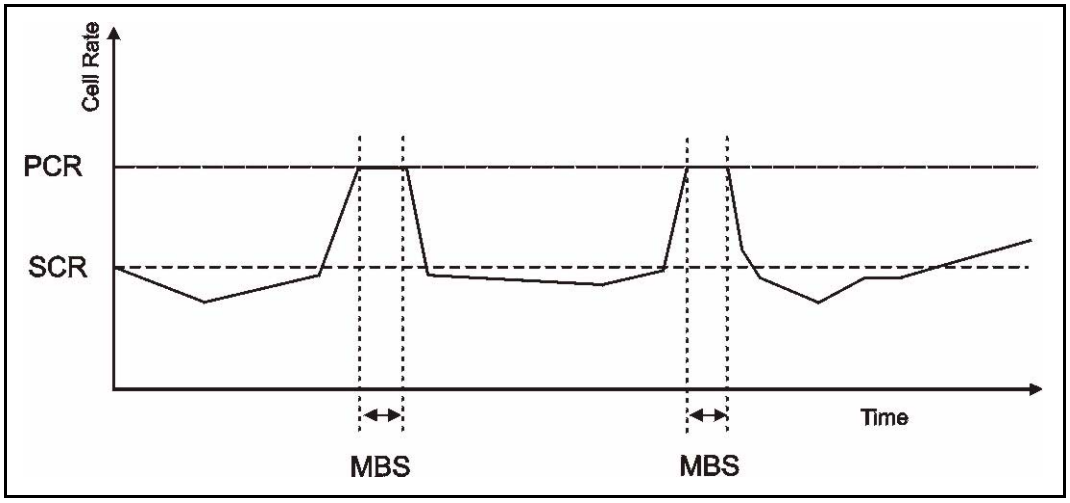
14.5.2.3 Maximum Burst Size (MBS)

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 53 PCR, SCR and MBS in Traffic Shaping



14.5.2.4 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.

14.5.2.5 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.

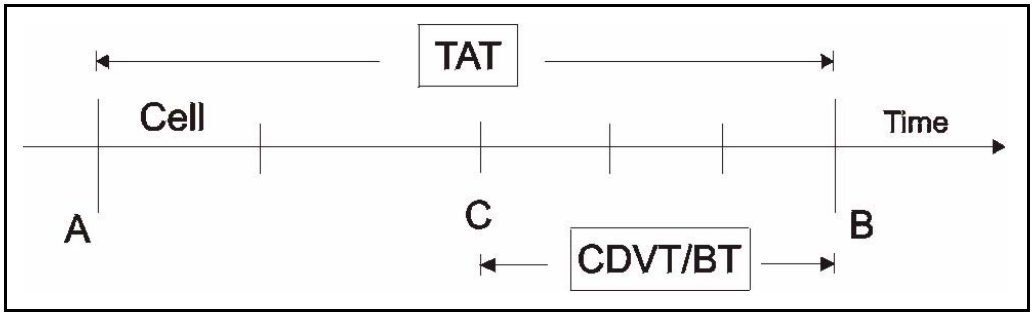
14.5.2.6 Theoretical Arrival Time (TAT)

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 54 TAT, CDVT and BT in Traffic Shaping



14.6 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 SAM1316-22.

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 SAM1316-22'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.

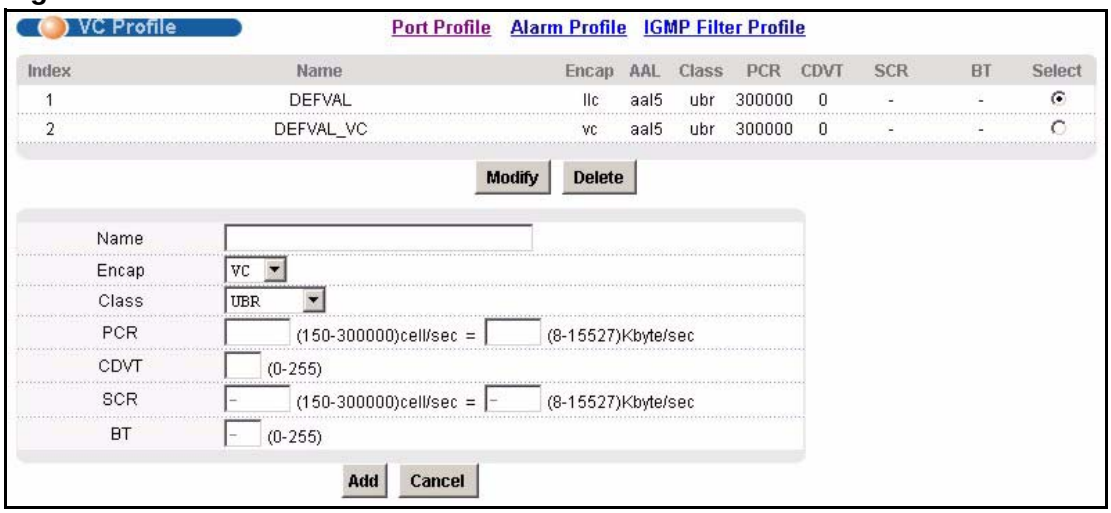
Note that since the SAM1316-22 uses ATM QoS, if the subscriber device's upstream shaping rate is larger than the SAM1316-22's upstream policing rate, some ATM cells will be discarded. In the worst case, none of the Ethernet packets from the CPE will be able to be reassembled from AAL5, so no packets from the subscriber's device can be received by the SAM1316-22.

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 SAM1316-22 will drop any upstream traffic that violates the specified ATM VC profile.

14.7 VC Profile Screen

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

Figure 55 VC Profile



The following table describes the labels in this screen.

Table 25 VC Profile

LABEL	DESCRIPTION
Port Profile	Click **Port Profile** to configure port profiles and assign them to individual ports (see Section 14.3 on page 108).
Alarm Profile	Click **Alarm Profile** to open the **Alarm Profile** screen where you can configure limits that trigger an alarm when exceeded (see Section 14.8 on page 116)
IGMP Filter Profile	Click **IGMP Filter Profile** to open the **IGMP Filter Profile** screen where you can configure IGMP multicast filter profiles (see Section 14.10 on page 119).
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.

Table 25 VC Profile (continued)

LABEL	DESCRIPTION
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.
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 SAM1316-22's volatile memory. The SAM1316-22 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.

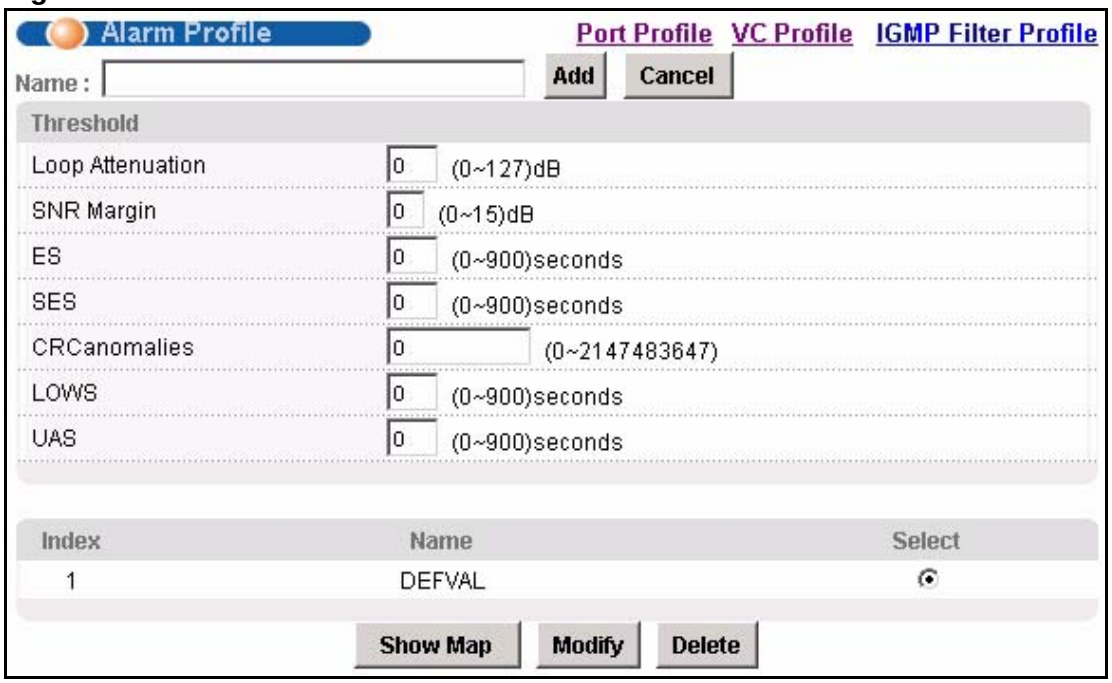
14.8 Alarm Profile Screen

Alarm profiles define DSL port alarm thresholds. The SAM1316-22 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 56 Alarm Profile



The following table describes the labels in this screen.

Table 26 Alarm Profile

LABEL	DESCRIPTION
Port Profile	Click **Port Profile** to open the **Port Profile** screen (see Section 14.3 on page 108). Use the **Port Profile** screen to configure profiles of DSL 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 14.7 on page 114).
IGMP Filter Profile	Click **IGMP Filter Profile** to open the **IGMP Filter Profile** screen where you can configure IGMP multicast filter profiles (see Section 14.10 on page 119).
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.

Table 26 Alarm Profile (continued)

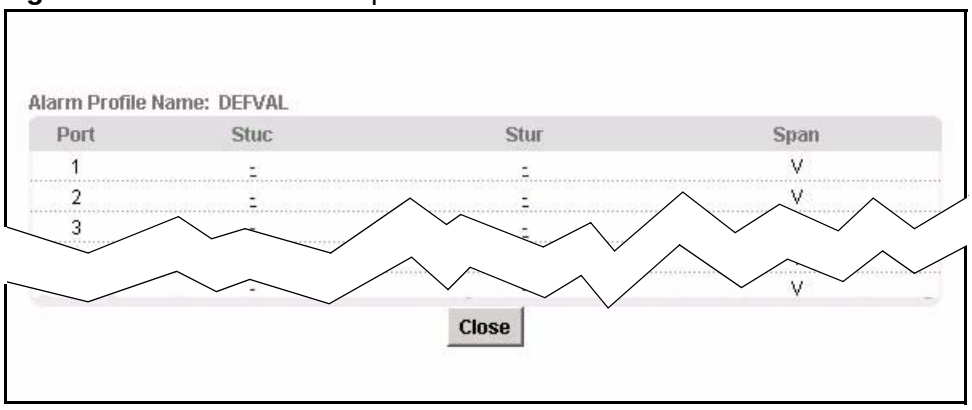
LABEL	DESCRIPTION
Add	Click **Add** to save your changes to the SAM1316-22's volatile memory. The SAM1316-22 loses these changes if it is turned off or loses power, so use the **Config Save** link on the navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click **Cancel** to start configuring the screen again.
Threshold	Specify limits for the individual performance counters. The SAM1316-22 sends an alarm trap and generates a syslog entry when one of these thresholds is exceeded. A value of 0 disables the alarm threshold.
Loop Attenuation	The permitted attenuation (reduction of signal amplitude) of a port's connection.
SNR Margin	The permitted signal to noise ratio margin.
ES	The number of Errored Seconds (0~900) that are permitted to occur within 15 minutes.
SES	The number of Severely Errored Seconds (0~900) that are permitted to occur within 15 minutes.
CRCanomalies	The number of Cyclic Redundancy Checking anomalies that are permitted to occur within 15 minutes.
LOWS	The number of Loss Of Sync Word Seconds (0~900) that are permitted to occur within 15 minutes.
UAS	The number of UnAvailable Seconds (0~900) that are permitted to occur within 15 minutes.
Index	This is the index number of the alarm profile.
Name	This is the name of the alarm profile.
Show Map	
Select Modify	Select a profile's **Select** radio button and click **Modify** to edit the profile
Delete	Select a profile's **Select** radio button and click **Delete** to remove the profile

14.8.1 Alarm Profile Map Screen

Use this screen to look at and to assign the ports to which alarm profiles are assigned. The SAM1316-22 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.

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

Figure 57 Alarm Profile Map



The following table describes the labels in this screen.

Table 27 Alarm Profile Map

LABEL	DESCRIPTION
Alarm Profile Name	This field displays the name of the alarm profile displayed in this screen.
Port	This field displays the DSL port number.
Stuc	This field displays whether or not the alarm profile is assigned to this port as the alarm profile for the STU-C end point. It displays **V** if it is assigned, and it displays **-** if it is not assigned. Click **-** to assign this profile to the port for the STU-C end point.
Stur	This field displays whether or not the alarm profile is assigned to this port as the alarm profile for the STU-R end point. It displays **V** if it is assigned, and it displays **-** if it is not assigned. Click **-** to assign this profile to the port for the STU-R end point.
Span	This field displays whether or not the alarm profile is assigned to this port as the alarm profile for the whole span. It displays **V** if it is assigned, and it displays **-** if it is not assigned. Click **-** to assign this profile to the port for the whole span.
Close	Click **Close** to close this screen.

14.9 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.

14.10 IGMP Filter Profile Screen

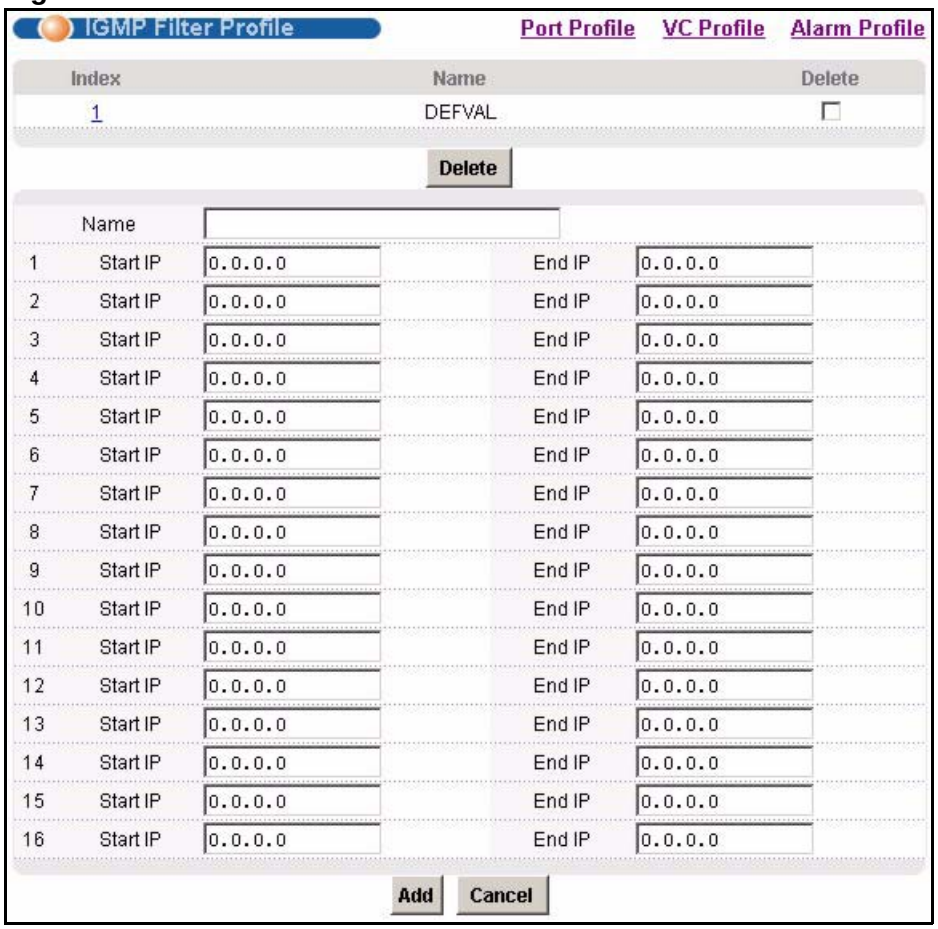
You can use the IGMP filter profiles to control access to a service that uses a specific multicast group (like a SIP server for example). Configure an IGMP filter profile that allows access to that multicast group. Then assign the IGMP filter profile to DSL ports that are allowed to use the service.

The **DEFVAL** IGMP filter profile is assigned to all of the DSL 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 a DSL 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 DSL port in the **XDSL Port Setting** screen (see Section 13.6.1 on page 95).

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 58 IGMP Filter Profile



The following table describes the labels in this screen.

Table 28 IGMP Filter Profile

LABEL	DESCRIPTION
Port Profile	Click **Port Profile** to configure port profiles and assign them to individual ports (see Section 14.3 on page 108).
VC Profile	Click **VC Profile** to open the **VC Profile** screen where you can configure virtual channel profiles (see Section 14.7 on page 114).
Alarm Profile	Click **Alarm Profile** to open the **Alarm Profile** screen where you can configure limits that trigger an alarm when exceeded (see Section 14.8 on page 116)
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.

Table 28 IGMP Filter Profile (continued)

LABEL	DESCRIPTION
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 SAM1316-22's volatile memory. The SAM1316-22 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

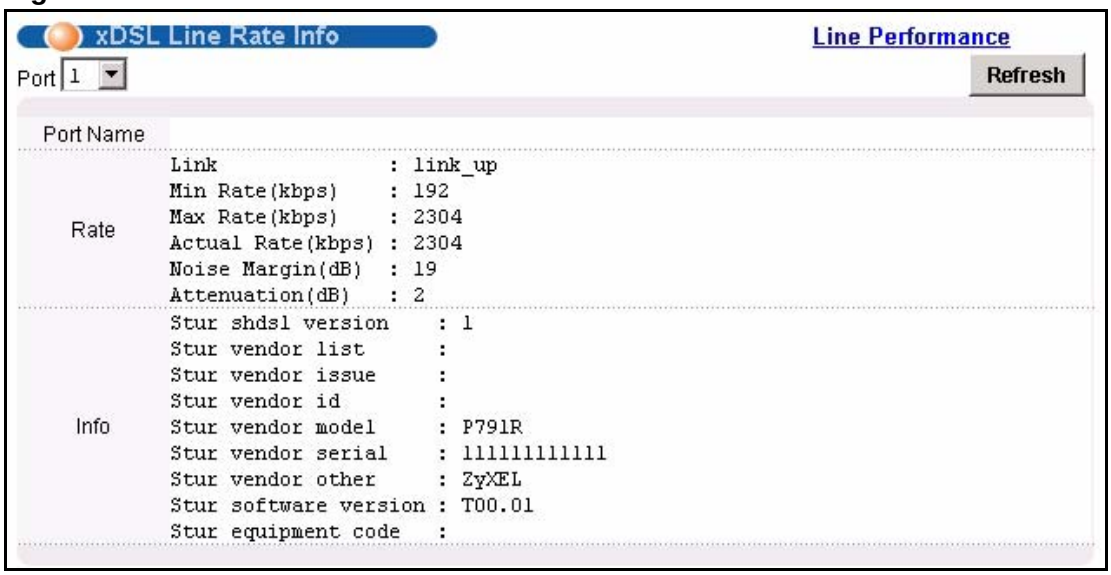
xDSL Line Data

15.1 xDSL Line Rate Info Screen

This screen displays a DSL 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 59 xDSL Line Rate Info



The following table describes the labels in this screen.

Table 29 xDSL Line Rate Info

LABEL	DESCRIPTION
Line Performance	Click **Line Performance** to display a DSL port's line performance counters (see Section 15.2 on page 125).
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.
Rate	The rate fields display the transmission rates. "Line Down" indicates that the DSL port is not connected to a subscriber.

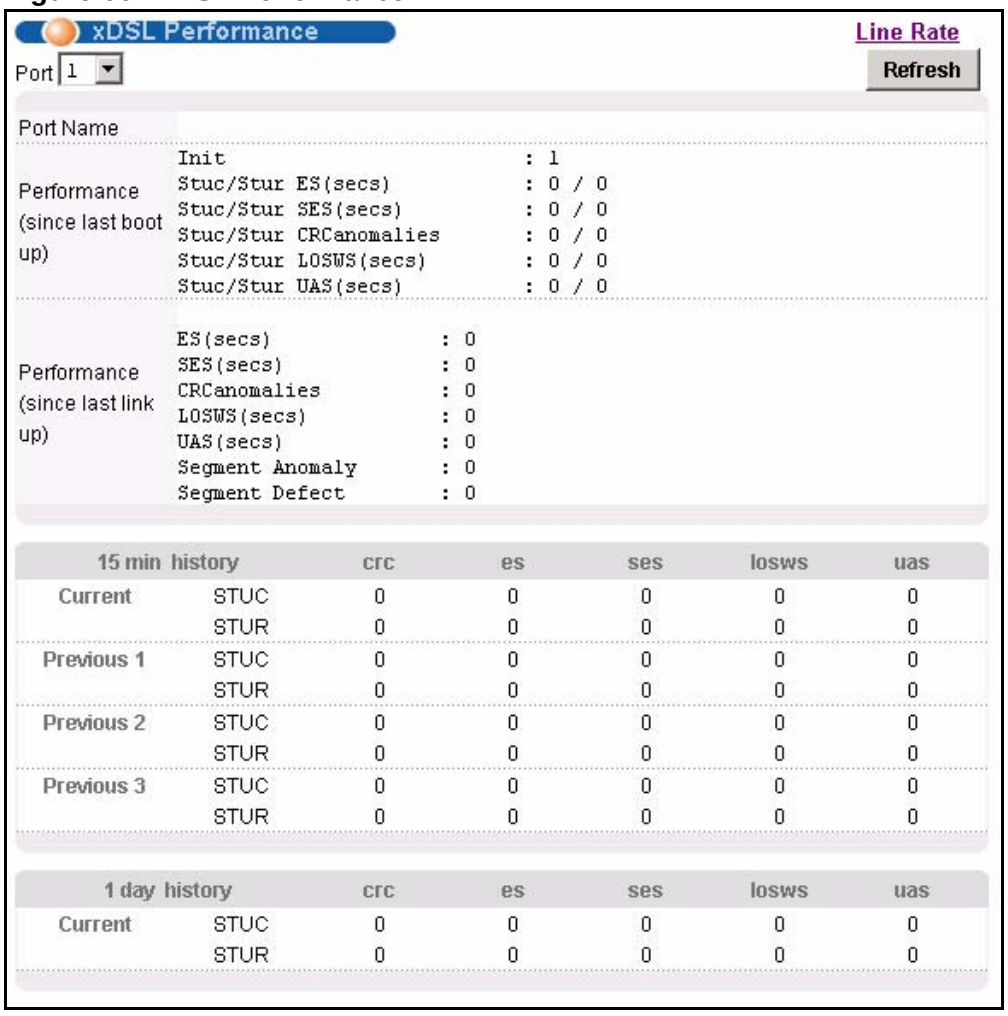
Table 29 xDSL Line Rate Info (continued)

LABEL	DESCRIPTION
Link	This displays the connection status of the DSL link.
Min Rate(kbps)	This is the minimum rate (in Kbps) of the DSL line.
Max Rate(kbps)	This is the maximum rate (in Kbps) of the DSL line.
Actual Rate(kbps)	This is the rate (in Kbps) at which the port has been sending and receiving data.
Noise Margin(dB)	This is the DSL line's noise margin measured in decibels (dB).
Attenuation(dB)	This is the reduction in amplitude of the DSL signals, measured in decibels (dB).
Info	This section displays the information that is reported by the STU-R in an Inventory Response message. If information is not provided, the field is blank.
Stur shdsl version	This field displays the version of the HDSL2/SHDSL standard implemented.
Stur vendor list	This field displays the vendor list number.
Stur vendor issue	This field displays the vendor issue number.
Stur vendor id	This field displays the vendor ID.
Stur vendor model	This field displays the vendor model number.
Stur vendor serial	This field displays the vendor serial number.
Stur vendor other	This field displays the other vendor information.
Stur software version	This field displays the vendor software version.
Stur equipment code	This field displays the equipment code conforming to ANSI T1.213, Coded Identification of Equipment Entities.

15.2 xDSL Performance Screen

These counters display line performance data that has been accumulated since the system started. To open this screen, click **Basic Setting**, **xDSL Line Data**, **Line Performance**.

Figure 60 xDSL Performance



The following table describes the labels in this screen.

Table 30 xDSL Performance

LABEL	DESCRIPTION
Line Rate	Click **Line Rate** to display a DSL port's line operating values (see Section 15.1 on page 123).
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.

Table 30 xDSL Performance (continued)

LABEL	DESCRIPTION
Performance (since last boot up)	There is a mechanism in SHDSL for the STU-C and STU-R to exchange information about line performance. As a result, the SAM1316-22 can report the errors detected by the STU-C and the STU-R. Stuc: This refers to what is detected by the Central Office (CO) end point. Stur: This refers to what is detected by the Remote (R) end point.
Init	This field displays the number of link-ups and link-downs.
Stuc/Stur ES	The number of Errored Seconds detected by the STU-C and the STU-R on this DSL port. An Errored Second is defined as a count of 1-second intervals during which one or more CRC anomalies are declared and/or one or more LOSW defects are declared.
Stuc/Stur SES	The number of Severely Errored Seconds detected by the STU-C and the STU-R on this DSL port. A Severely Errored Second is defined as a count of 1-second intervals during which at least 50 CRC anomalies are declared or one or more LOSW defects are declared. (50 CRC anomalies during a 1-second interval is equivalent to a 30% errored frame rate for a nominal frame length.)
Stuc/Stur CRCanomalies	The number of CRC anomalies detected by the STU-C and the STU-R on this DSL port.
Stuc/Stur LOSWS	The number of Loss of Sync Word Failure Seconds detected by the STU-C and the STU-R on this DSL port.
Stuc/Stur UAS	The number of UnAvailable Seconds.detected by the STU-C and the STU-R on this DSL port. An Unavailable Second is a count of 1-second intervals for which the SHDSL line is unavailable. The SHDSL line becomes unavailable at the onset of 10 contiguous SESs. The 10 SESs are included in the unavailable time. Once unavailable, the SHDSL line becomes available at the onset of 10 contiguous seconds with no SESs. The 10 s with no SESs are excluded from unavailable time.
Stuc/Stur Segment Anomaly	The number of Segment Anomalies that have occurred since the last bootup. A segment anomaly indicates that a regenerator operating on a segment has received corrupted data and therefore the regenerated data is unreliable.
Stuc/Stur Segment Defect	The number of Segment Defects that have occurred since the last bootup. A segment defect indicates that a regenerator has lost SHDSL synchronization and therefore the regenerated data is unavailable.
Performance (since last link up)	
ES	The number of Errored Seconds that have occurred since the last connection was established.
SES	The number of Severely Errored Seconds that have occurred since the last connection was established.
CRCanomalies	The number of CRC anomalies that have occurred since the last connection was established.
LOSWS	The number of Loss of Sync Word Seconds that have occurred since the last connection was established.

Table 30 xDSL Performance (continued)

LABEL	DESCRIPTION
UAS	The number of UnAvailable Seconds.that have occurred since the last connection was established.
Segment Anomaly	The number of Segment Anomalies that have occurred since the last connection was established. A segment anomaly indicates that a regenerator operating on a segment has received corrupted data and therefore the regenerated data is unreliable.
Segment Defect	The number of Segment Defects that have occurred since the last connection was established. A segment defect indicates that a regenerator has lost SHDSL synchronization and therefore the regenerated data is unavailable.
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. STUC: This refers to what is detected by the Central Office (CO) end point. STUR: This refers to what is detected by the Remote (R) end point.
crc	The number of CRC anomalies detected within the period.
es	The number of Errored Seconds detected within the period.
ses	The number of Severely Errored Seconds detected within the period.
losws	The number of Loss of Sync Word Seconds detected within the period.
uas	The number of UnAvailable Seconds detected within the period.

16

G.bond

This chapter explains how to combine multiple ports into a logical link.

16.1 Bonding Overview

Bonding combines multiple ports into a logical link. This lets the SAM1316-22 transmit at higher bandwidths over longer distances. In addition, bonding is a cheaper alternative than installing fiber.

Bonding can occur at the physical level or at the cell/packet level. The SAM1316-22 can bond ports at the ATM-cell level.

16.1.1 Cell-level Bonding Process

This process depends on an 8-bit or 12-bit sequence ID (SID). If the SID is eight bits, it uses the first eight bits of the VCI field. If the SID is twelve bits, it uses the GFC field and the first eight bits of the VCI field.

This process consists of these steps.

1. The sender breaks up the message into several segments and assigns a sequence ID to each segment.
2. Each segment is transmitted over one of the ports in the bond.
3. The receiver uses the sequence ID to reconstruct the original message.

16.1.2 Bonding Standards

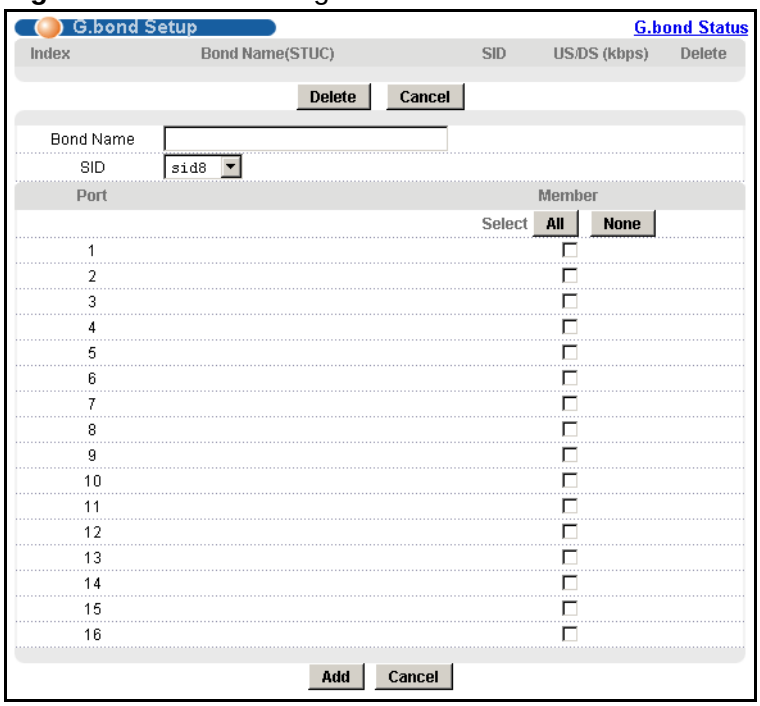
ITU G.998.1 defines bonding standards for ATM networks.

16.2 G.bond Setup Screen

Use this screen to bond one or more ports into a logical link.

To open this screen, click **Basic Setting** > **G.bond**.

Figure 61 Basic Setting > G.bond



The following table describes the labels in this screen.

Table 31 Basic Setting > G.bond

LABEL	DESCRIPTION
G.bond Status	Click **G.bond Status** to look at the status of each port in each bond (see Section 16.2.1 on page 131).
Index	This is the number of the bond. Click a profile's index number to edit the profile. You cannot edit the **DEFVAL** profile.
Bond Name (STUC)	This is the name of the bond.
SID	This is the length of the sequence ID used in this bond.
US/DS (kbps)	This is the maximum upstream bandwidth and maximum downstream bandwidth available through this bond. This is calculated from the maximum rate available through each port.
Delete	Select the check box for one or more bonds, and click **Delete** to remove the selected bond(s).
Cancel	Select this to clear the fields in this screen without saving any changes.
Bond Name	Enter the name of the bond. You can use up to 31 English keyboard characters; double quotation marks (") and spaces are not allowed.

Table 31 Basic Setting > G.bond (continued)

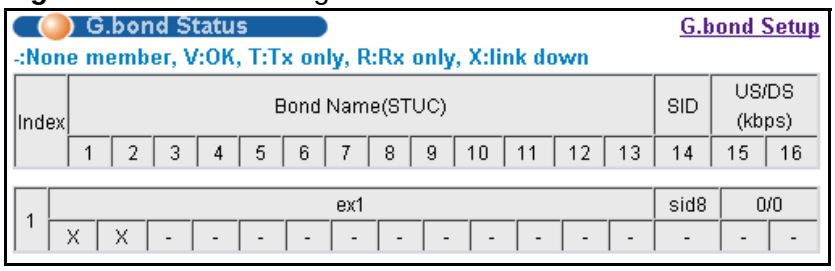
LABEL	DESCRIPTION
SID	Select the length of the sequence ID used in this bond. The STU-C specifies this value. **sid8**: The sequence ID is 8 bits long. **sid12**: The sequence ID is 12 bits long.
Port	This field displays the DSL port number.
Member	Select this to include this port in the bond. Clear this to remove this port from the bond. Select **All** to include all of the ports in the bond. Select **None** to include none of the ports in the bond.
Add	Select this to add or update the bond.
Cancel	Select this to clear the fields in this screen without saving any changes.

16.2.1 G.bond Status Screen

Use this screen to look at the status of each port in each bond.

To open this screen, click **Basic Setting** > **G.bond > G.bond Status**.

Figure 62 Basic Setting > G.bond > G.bond Status



The following table describes the labels in this screen.

Table 32 Basic Setting > G.bond > G.bond Status

LABEL	DESCRIPTION
G.bond Setup	Click **G.bond Setup** to bond one or more ports into a logical link (see Section 16.2 on page 130).
Index	This is the number of the bond.
Bond Name (STUC/STUR)	This is the name of the bond.
SID	This is the length of the sequence ID used in this bond. The STU-C specifies this value.

Table 32 Basic Setting > G.bond > G.bond Status (continued)

LABEL	DESCRIPTION
US/DS (kbps)	This is the current upstream bandwidth and current downstream bandwidth used in this bond.
	This field displays the role of each port in the bond. **-**: This port is not a member of the bond. **V**: This port is sending and receiving information in the bond. **T**: This port is only sending information in the bond. **R**: This port is only receiving information in the bond. **X**: This port does not have a DSL connection.

17

VLAN

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

17.1 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.

17.2 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 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 SAM1316-22 handles up to 4094 VLANs (VIDs 1-4094). The device accepts incoming frames with VIDs 1-4094.

17.2.1 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 SAM1316-22 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 SAM1316-22 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.

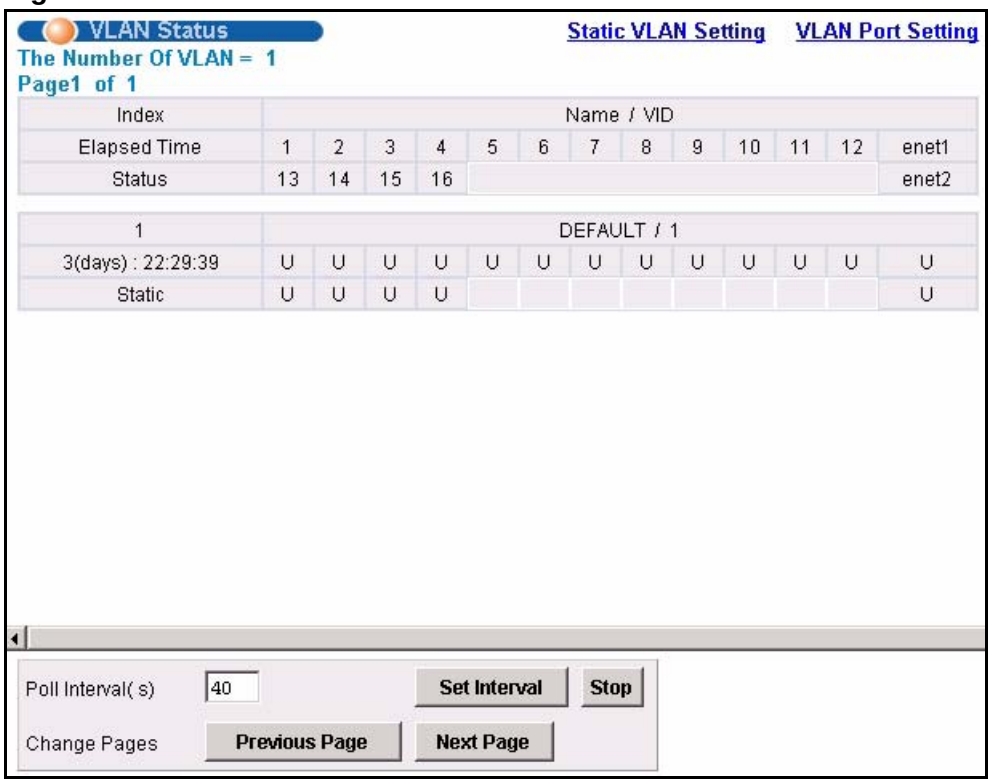
1. GVRP (GARP VLAN Registration Protocol) defines a way for switches to automatically configure switches in a VLAN network.

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.

17.3 VLAN Status Screen

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

Figure 63 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 17.4 on page 136).
VLAN Port Setting	Click **VLAN Port Setting** to specify Port VLAN IDs (PVIDs). See Section 17.5 on page 138.
The Number of VLAN	This is the number of VLANs configured on the SAM1316-22.
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.

Table 33 VLAN Status (continued)

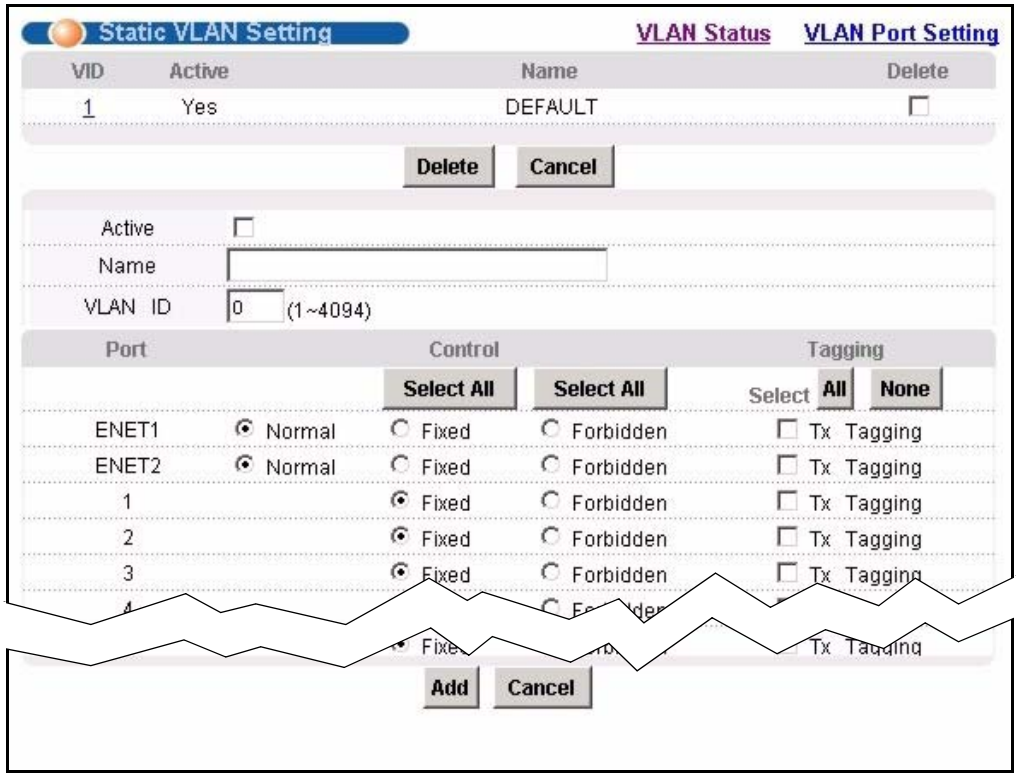
LABEL	DESCRIPTION
	The first table displays the names of the fields. The subsequent tables show the settings of the VLANs.
Index	This is the VLAN index number.
Name / VID	The name identifies an individual VLAN. The vid is the PVID, the Port VLAN ID assigned to untagged frames or priority-tagged frames received on this port.
1~16, 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 SAM1316-22 statically, that is, added as a permanent entry.
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.

17.4 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 64 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 SAM1316-22's ports are members of which VLANs (see Section 17.3 on page 135)
VLAN Port Setting	Click **VLAN Port Setting** to specify Port VLAN IDs (PVIDs). See Section 17.5 on page 138.
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.

Table 34 Static VLAN Setting (continued)

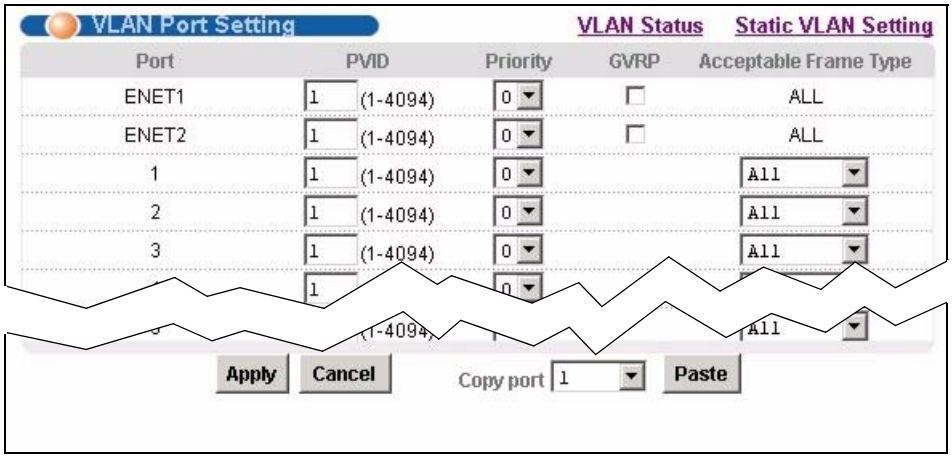
LABEL	DESCRIPTION
Name	Enter a descriptive name for this VLAN group for identification purposes. Spaces are not allowed.
VLAN ID	Enter the VLAN ID for this static VLAN entry; the valid range is between 1 and 4094.
Port	The port numbers identify the SAM1316-22's ports.
Control	Select **Fixed** for the 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 SAM1316-22's volatile memory. The SAM1316-22 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.

17.5 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 65 VLAN Port Setting

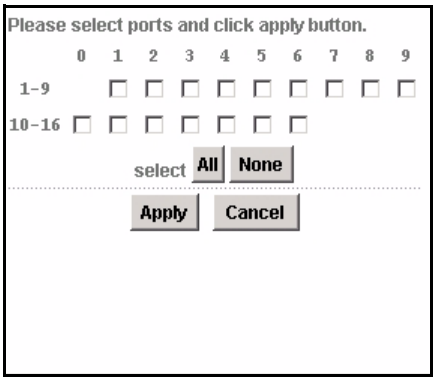


The following table describes the labels in this screen.

Table 35 VLAN Port Setting

LABEL	DESCRIPTION
VLAN Status	Click **VLAN Status** to see which of the SAM1316-22's ports are members of which VLANs (see Section 17.3 on page 135).
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 17.4 on page 136).
Port	The port numbers identify the SAM1316-22's ports.
PVID	Type the Port VLAN ID (PVID) from 1 to 4094. The SAM1316-22 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 SAM1316-22 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 SAM1316-22's volatile memory. The SAM1316-22 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 66** Select Ports 

A. At the time of writing, the **VLAN Acceptable Frame Type** field is read-only for the Ethernet ports. The SAM1316-22 accepts both tagged and untagged incoming frames on the Ethernet ports.

18

IGMP

This chapter describes the **IGMP** screens.

18.1 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.

18.2 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).

18.2.1 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 SAM1316-22 to learn multicast groups without you having to manually configure them.

The SAM1316-22 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 SAM1316-22 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.

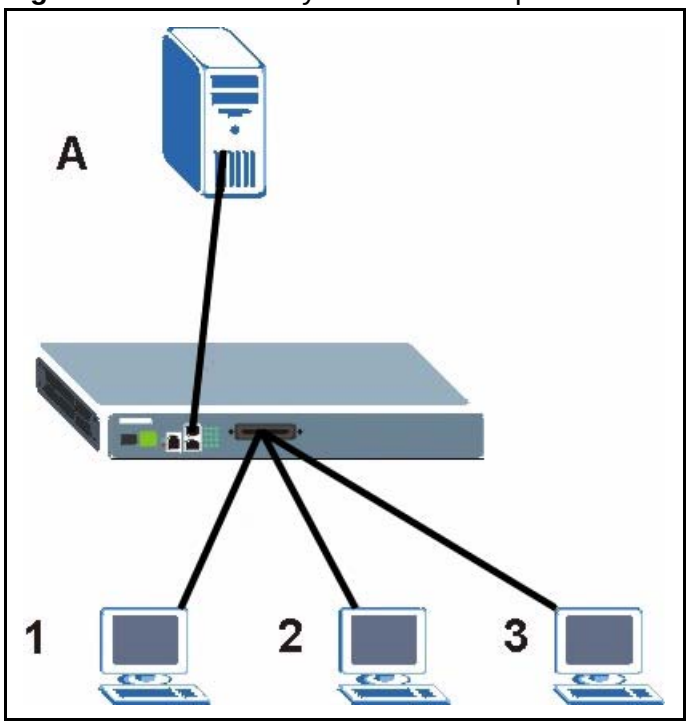
18.2.2 IGMP Proxy

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 SAM1316-22. 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 67 IGMP Proxy Network Example



The SAM1316-22 will not respond to IGMP join and leave messages on the upstream interface. The SAM1316-22 only responds to IGMP query messages on the upstream interface. The SAM1316-22 sends IGMP query messages to the hosts that are members of the query VLAN.

The SAM1316-22 only sends an IGMP leave messages via the upstream interface when the last host leaves a multicast group.

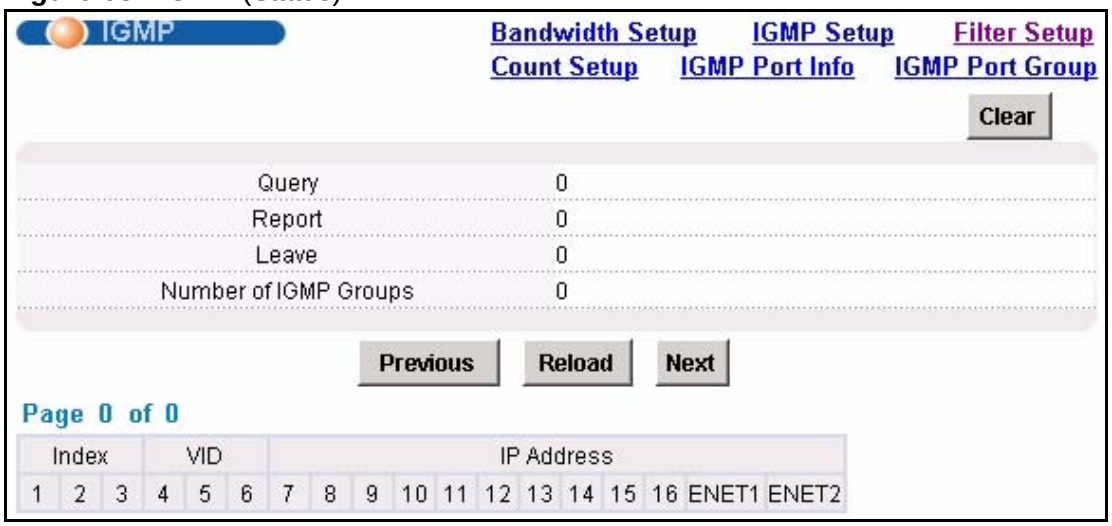
In daisychain mode, Ethernet interface 1 is set as the upstream interface and Ethernet interface 2 and the DSL ports are set as downstream interfaces.

18.3 IGMP Status Screen

Use this screen to view current IGMP information.

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

Figure 68 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 18.4 on page 145). You can also open the **Bandwidth Port Setup** screen to set up multicast bandwidth requirements for selected ports (see Section 18.4.1 on page 146).
IGMP Setup	Click **IGMP Setup** to open the **IGMP Setup** screen where you can configure IGMP settings (see Section 18.5 on page 147).
Filter Setup	Click **Filter Setup** to open the **IGMP Filter Profile** screen where you can configure IGMP multicast filter profiles (see Section 18.6 on page 148).
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 18.7 on page 149).

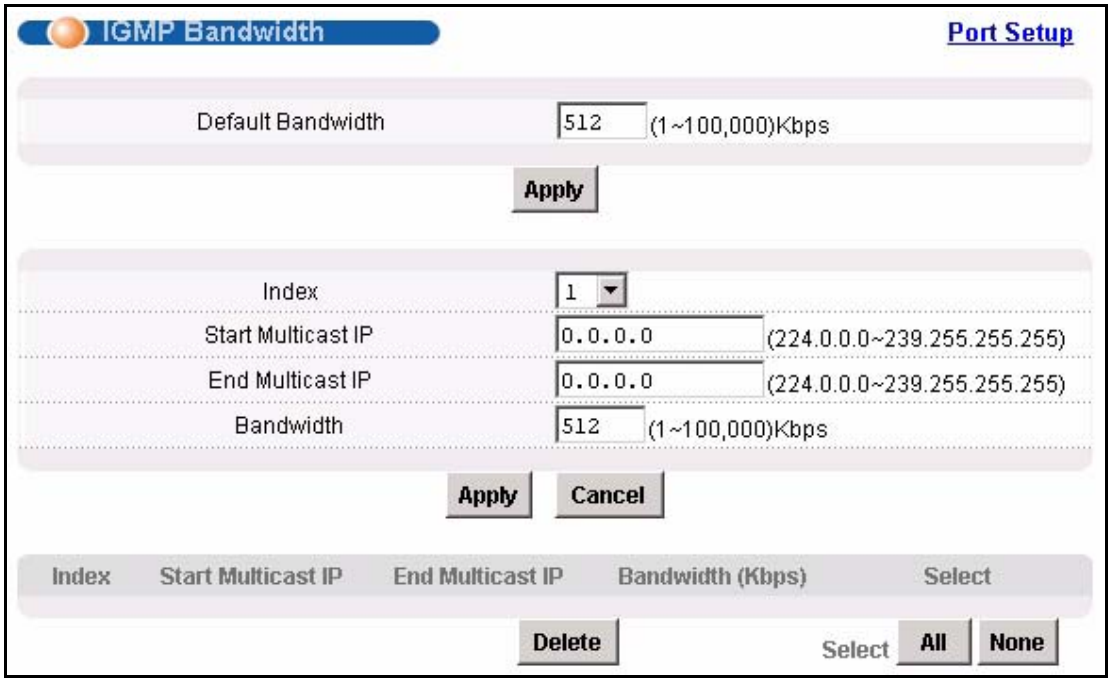
Table 36 IGMP (Status) (continued)

LABEL	DESCRIPTION
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 18.8 on page 150).
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 18.9 on page 151).
Clear	Click **Clear** to delete the information the SAM1316-22 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.
Number of IGMP Groups	This is how many IGMP groups the SAM1316-22 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.
1~16, enet1, enet2	These columns indicate whether or not each port is a member of the IGMP snooping group.

18.4 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 69 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 18.4.1 on page 146).
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 SAM1316-22's volatile memory. The SAM1316-22 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.

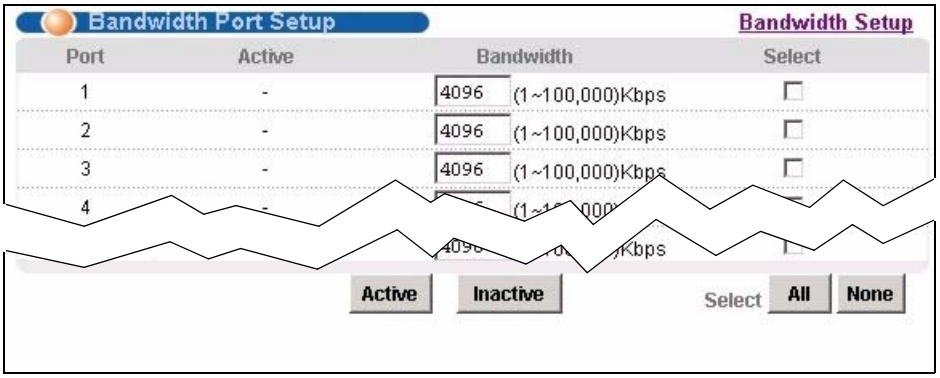
Table 37 IGMP Bandwidth (continued)

LABEL	DESCRIPTION
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 SAM1316-22's volatile memory. The SAM1316-22 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.

18.4.1 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 70 Bandwidth Port Setup



The following table describes the labels in this screen.

Table 38 Bandwidth Port Setup

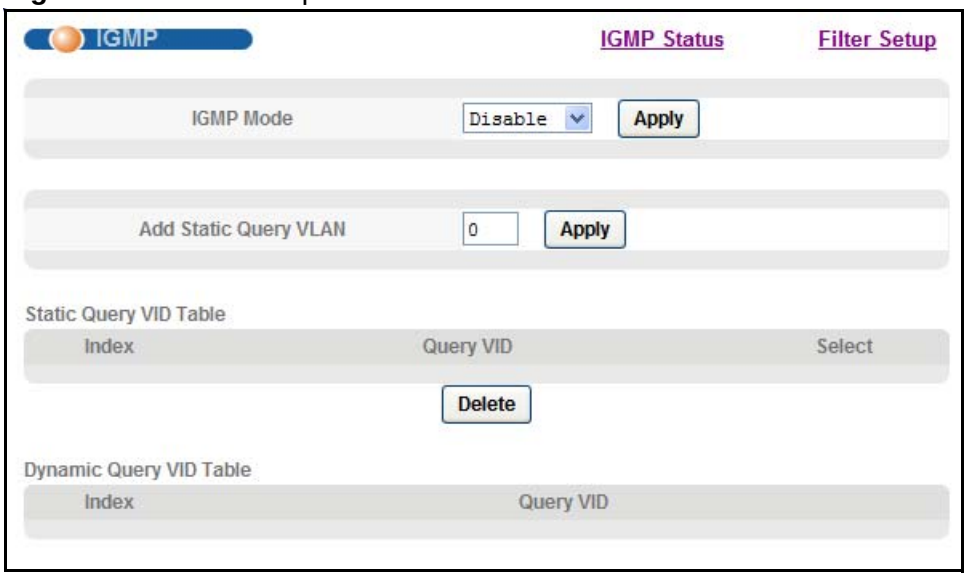
LABEL	DESCRIPTION
Bandwidth Setup	Click **Bandwidth Setup** to open the **IGMP Bandwidth** screen where you can set up bandwidth requirements for multicast channels (see Section 18.4 on page 145).
Port	This field shows each DSL port number.
Active	This field shows whether or not multicast bandwidth requirements 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.

18.5 IGMP Setup Screen

Use this screen to configure your IGMP settings.

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

Figure 71 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 18.3 on page 143).
Filter Setup	Click **Filter Setup** to open the **IGMP Filter Profile** screen where you can configure IGMP multicast filter profiles (see Section 18.6 on page 148).
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 not use either IGMP proxy or snooping.
Apply	Click **Apply** to save your IGMP mode settings. Clicking **Apply** saves your changes to the SAM1316-22's volatile memory. The SAM1316-22 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 SAM1316-22.
Index	This is the index number of an existing static IGMP query VLAN on the SAM1316-22.
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.
Index	This is the dynamic IGMP query VLAN.
Query VID	This is the dynamic IGMP query VLAN's VLAN ID.

18.6 IGMP Filter Setup Screen

To open this screen, click **Advanced Application**, **IGMP**, **Filter Setup**. This screen is discussed in Section 14.9 on page 118.

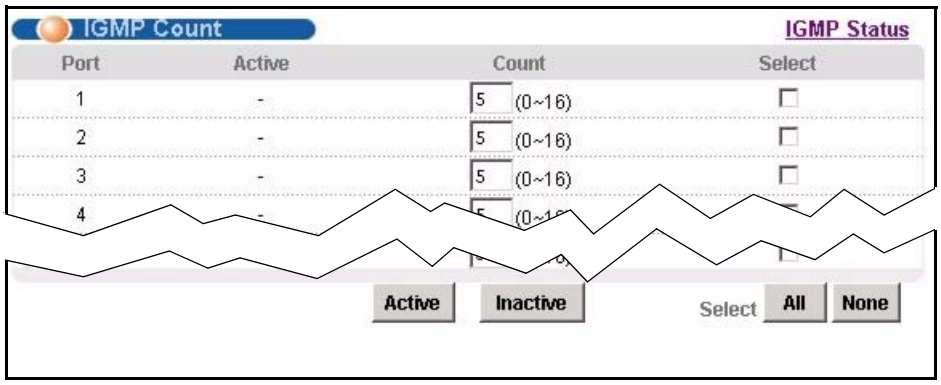
18.7 IGMP Count Screen

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 72 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 18.3 on page 143).
Port	This field shows each DSL port number.
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.

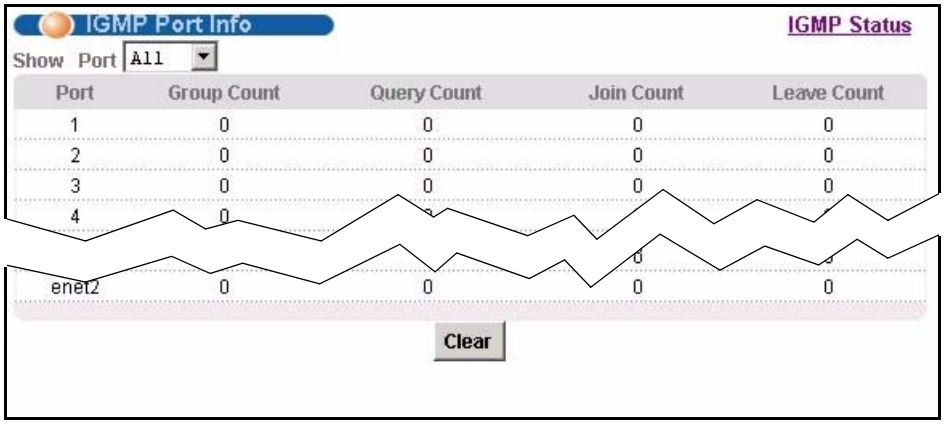
Table 40 IGMP Count (continued)

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.

18.8 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 73 IGMP Port Info



The following table describes the labels in this screen.

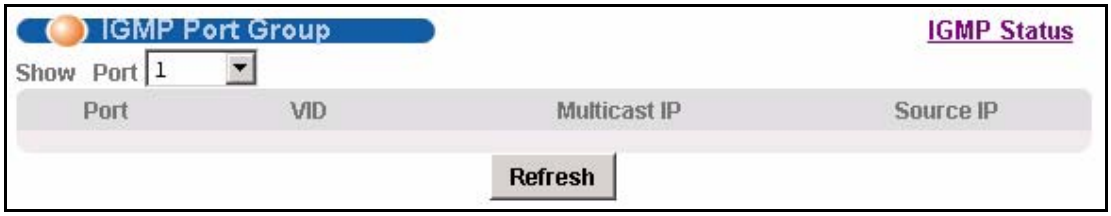
Table 41 IGMP Port Info

LABEL	DESCRIPTION
IGMP Status	Click **IGMP Status** to open the **IGMP Setup** screen where you can view current IGMP information (see Section 18.3 on page 143).
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.
Leave Count	This is the total number of Leave packets received on this port.
Clear	Click **Clear** to delete the information the SAM1316-22 has learned about multicast groups. This resets every counter in this screen.

18.9 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 74 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 18.3 on page 143).
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.

19

Static Multicast

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

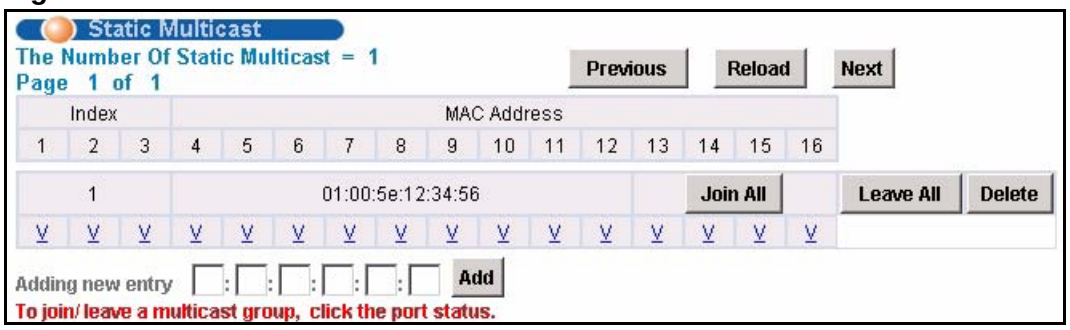
19.1 Static Multicast

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.

19.2 Static Multicast Screen

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

Figure 75 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 SAM1316-22.
Page X of X	This identifies which page of information is displayed and the total number of pages of information.

Table 43 Static Multicast (continued)

LABEL	DESCRIPTION
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.
	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.
1~16	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 SAM1316-22's volatile memory. The SAM1316-22 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.

20

Multicast VLAN

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

20.1 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 SAM1316-22 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 SAM1316-22 uses the super channel instead. This applies to all downstream traffic, not just multicast traffic.

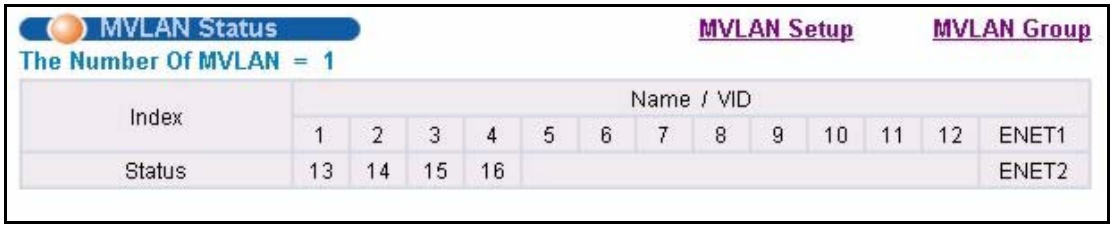
It is suggested to use a super channel for multicast VLAN. If a normal PVC is used and the multicast VLAN ID is not the same as the PVC's VID, the SAM1316-22 does not forward traffic to this PVC even if the subscriber's port has joined the multicast VLAN.

Since the SAM1316-22 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.

20.2 MVLAN Status Screen

Use this screen to look at a summary of all multicast VLAN on the SAM1316-22. To open this screen, click **Advanced Application**, **Multicast VLAN**.

Figure 76 MVLAN Status



The following table describes the labels in this screen.

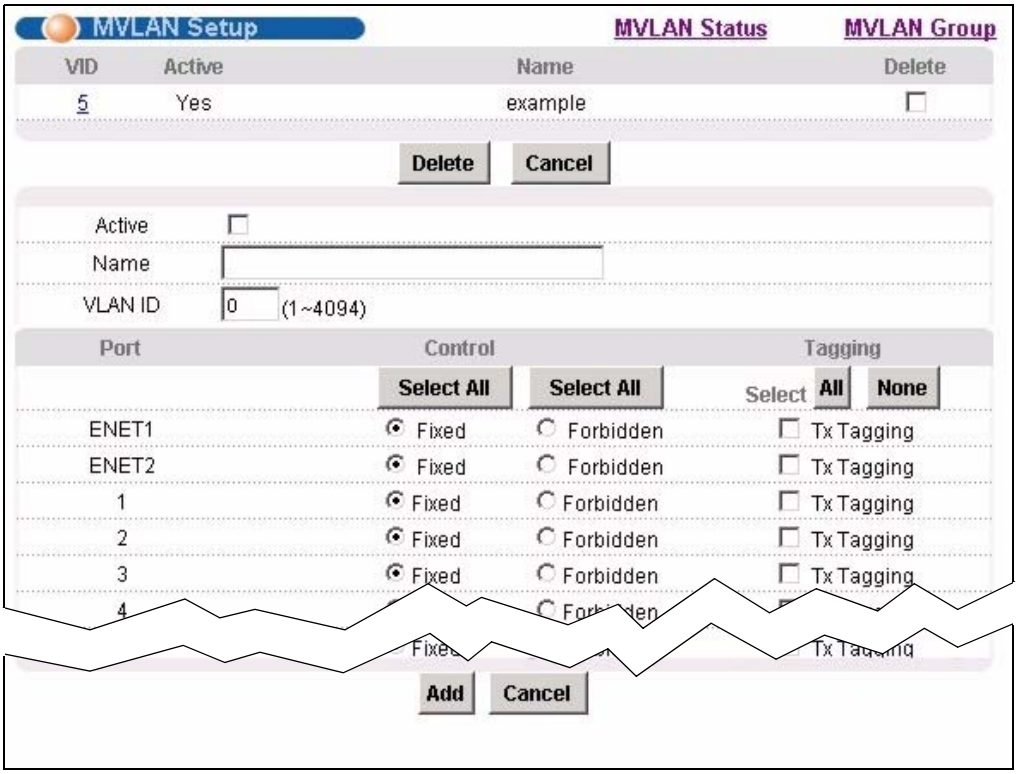
Table 44 MVLAN Status

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 20.3 on page 157).
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 20.4 on page 159).
The Number of MVLAN	This is the number of multicast VLAN configured on the SAM1316-22.
	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.
1~16 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**).

20.3 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 77 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 SAM1316-22 (see Section 20.2 on page 156).
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 20.4 on page 159).
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.

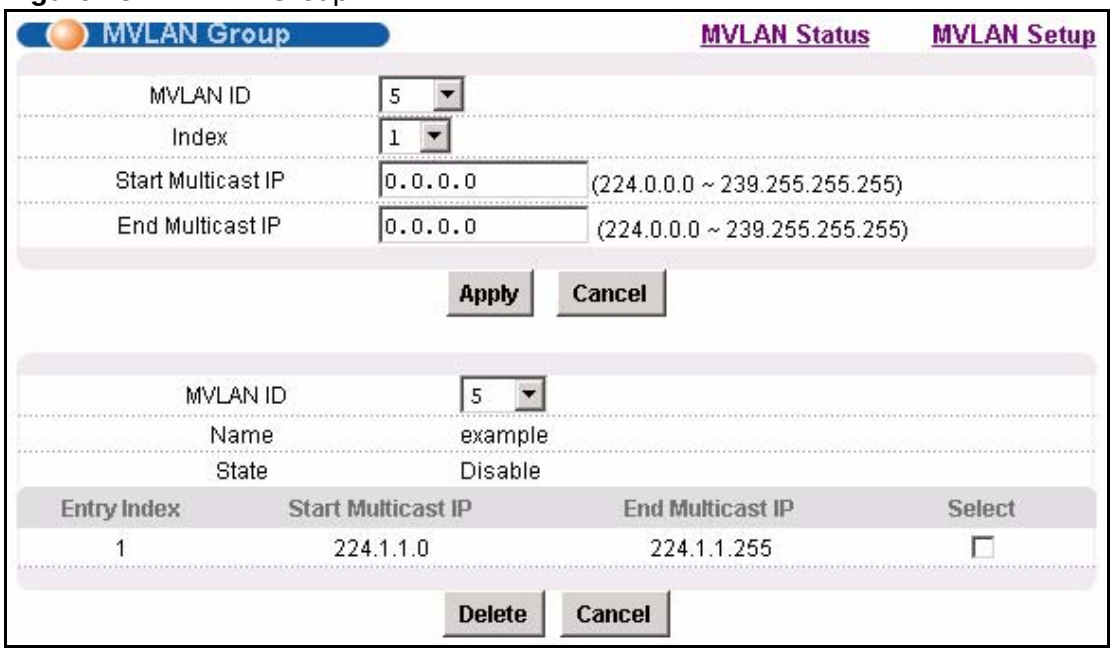
Table 45 MVLAN Setup (continued)

LABEL	DESCRIPTION
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.
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 SAM1316-22's volatile memory. The SAM1316-22 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.

20.4 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 78 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 SAM1316-22 (see Section 20.2 on page 156).
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 20.3 on page 157).
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.

Table 46 MVLAN Group (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the SAM1316-22's volatile memory. The SAM1316-22 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.

21

Filtering

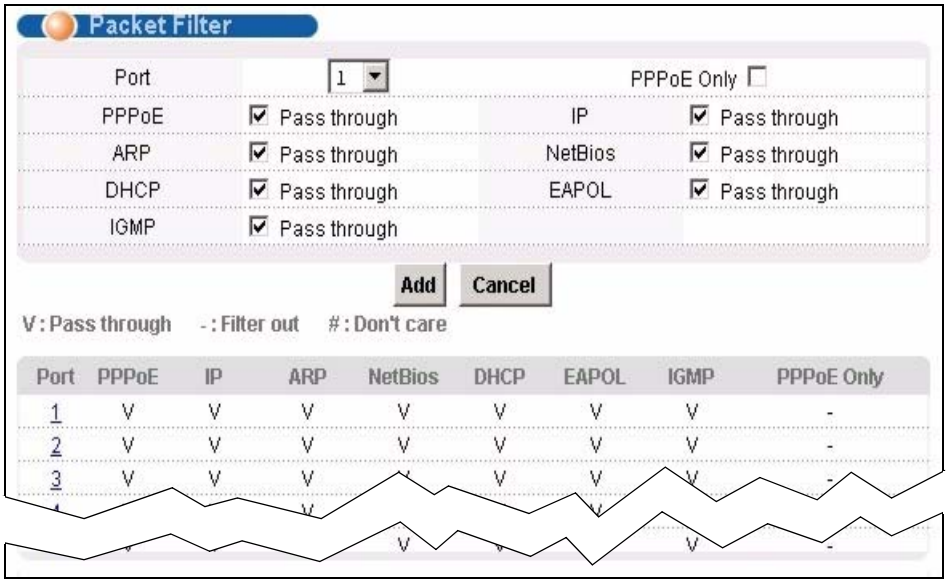
This chapter describes how to configure the **Packet Filter** screen.

21.1 Packet Filter Screen

Use this screen to set which types of packets the SAM1316-22 accepts on individual DSL ports.

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

Figure 79 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.
	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 SAM1316-22’s volatile memory. The SAM1316-22 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.

Table 47 Packet Filter (continued)

LABEL	DESCRIPTION
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 SAM1316-22 is to accept on the port. "-" displays for packet types that the SAM1316-22 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 SAM1316-22 rejects all packet types except for PPPoE (packet types that are not listed are also rejected).

22

MAC Filter

This chapter introduces the MAC filter.

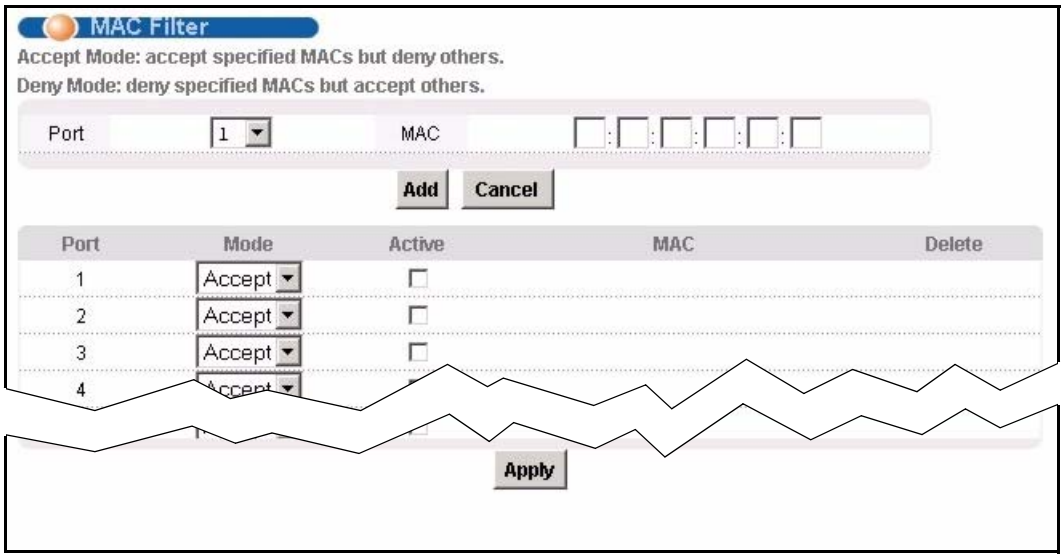
22.1 MAC Filter Introduction

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

22.2 MAC Filter Screen

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

Figure 80 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 SAM1316-22's volatile memory. The SAM1316-22 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 SAM1316-22's volatile memory. The SAM1316-22 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.

23

Spanning Tree Protocol

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

23.1 RSTP and STP

RSTP adds rapid reconfiguration capability to STP. The SAM1316-22 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

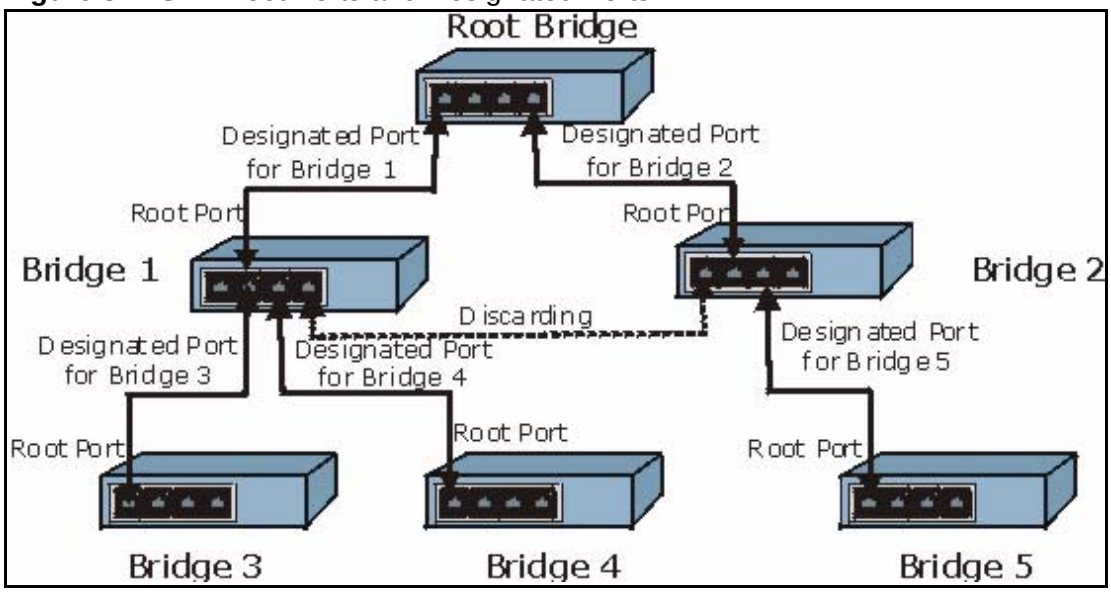
	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	4Mbps	250	100 to 1000	1 to 65535
Path Cost	10Mbps	100	50 to 600	1 to 65535
Path Cost	16Mbps	62	40 to 400	1 to 65535
Path Cost	100Mbps	19	10 to 60	1 to 65535
Path Cost	1Gbps	4	3 to 10	1 to 65535
Path Cost	10Gbps	2	1 to 5	1 to 65535

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 81 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 169). 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

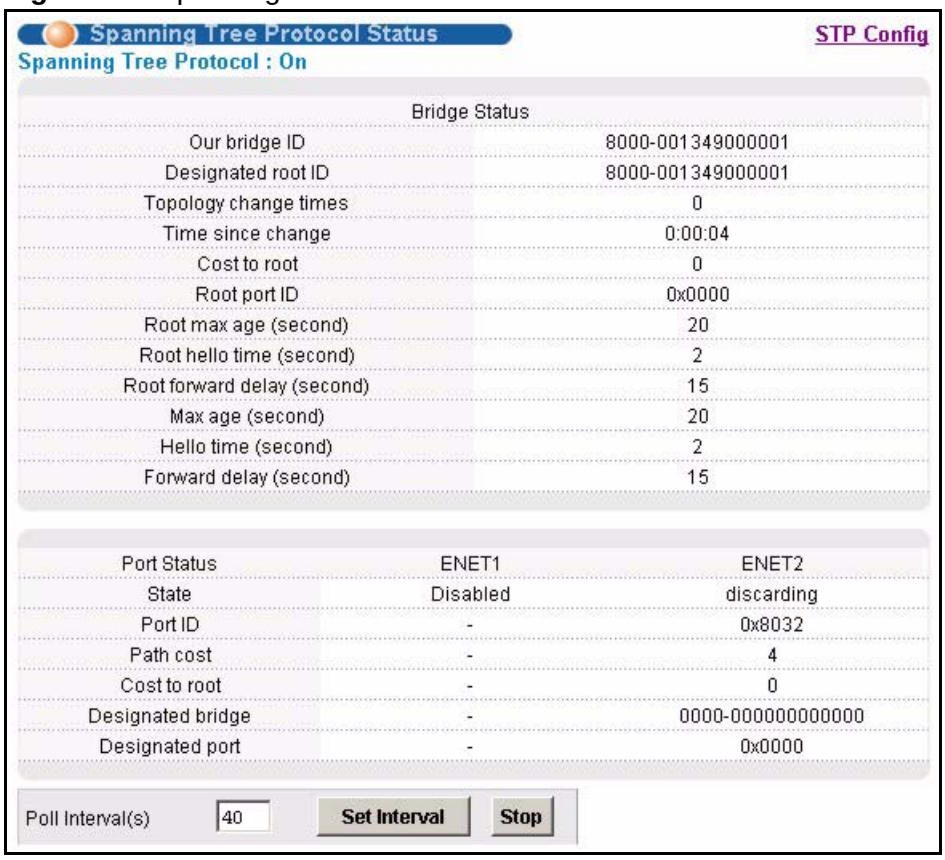
RSTP PORT STATE	STP PORT STATE	DESCRIPTION
Discarding	Disabled	RSTP or STP is disabled (default).
Discarding	Blocking	In RSTP, BPDUs are discarded. In STP, only configuration and management BPDUs are received and processed.
Discarding	Listening	In RSTP, BPDUs are discarded. In STP, all BPDUs are received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

23.2 Spanning Tree Protocol Status Screen

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

Figure 82 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 SAM1316-22's STP settings (see Section 23.3 on page 172).
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 SAM1316-22 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 SAM1316-22 is the root switch.
Topology change times	This is the number of times the spanning tree has been reconfigured.

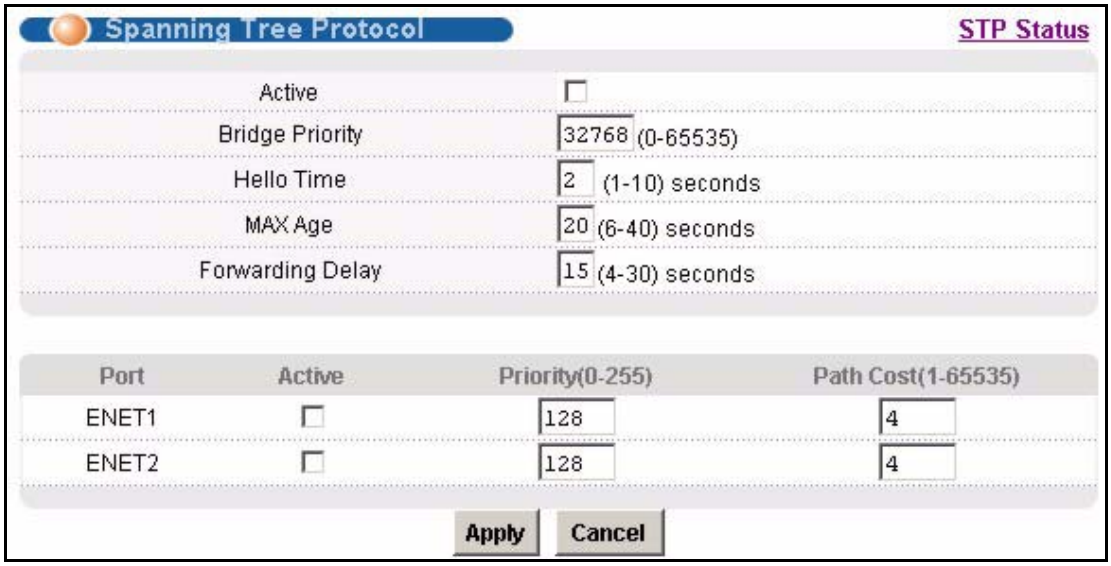
Table 51 Spanning Tree Protocol Status (continued)

LABEL	DESCRIPTION
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 SAM1316-22 can wait without receiving a configuration message before attempting to reconfigure.
Hello time (second)	This is the time interval (in seconds) at which the SAM1316-22 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 SAM1316-22 will wait before changing states (that is, listening to learning to forwarding).
Port Status	This identifies the SAM1316-22’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.
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.

23.3 Spanning Tree Protocol Screen

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

Figure 83 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 SAM1316-22's STP status (see Section 23.2 on page 170).
Active	Select this check box to turn on RSTP. Note: It is recommended that you only use STP when you use the SAM1316-22 in standalone mode with a network topology that has loops.
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.

Table 52 Spanning Tree Protocol (continued)

LABEL	DESCRIPTION
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 SAM1316-22's volatile memory. The SAM1316-22 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 Authentication

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

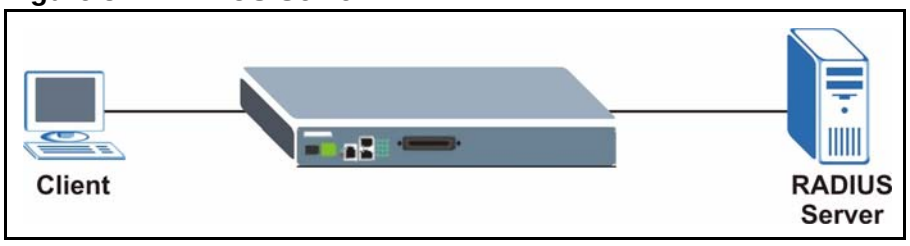
24.1 Introduction to Authentication

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.

24.1.1 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 84 RADIUS Server



24.1.2 Introduction to Local User Database

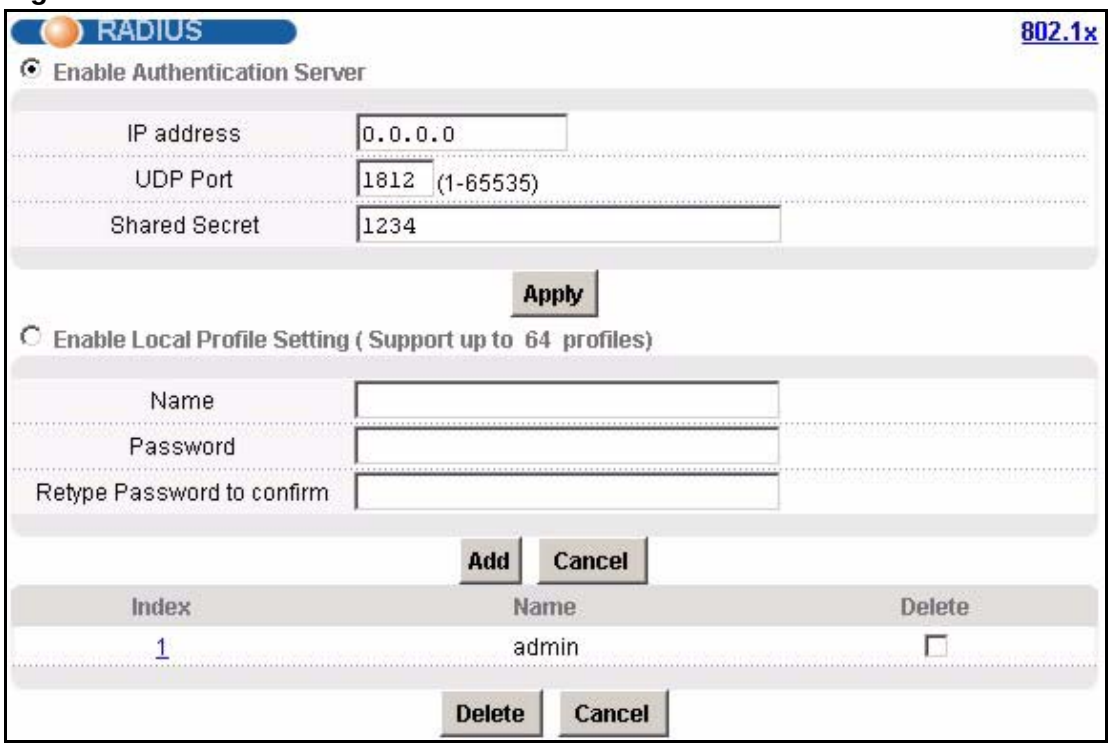
By storing user profiles locally on the SAM1316-22, your SAM1316-22 is able to authenticate users without interacting

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.

24.2 RADIUS Screen

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

Figure 85 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 24.3 on page 178).
Enable Authentication Server	Select this check box to have the SAM1316-22 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.

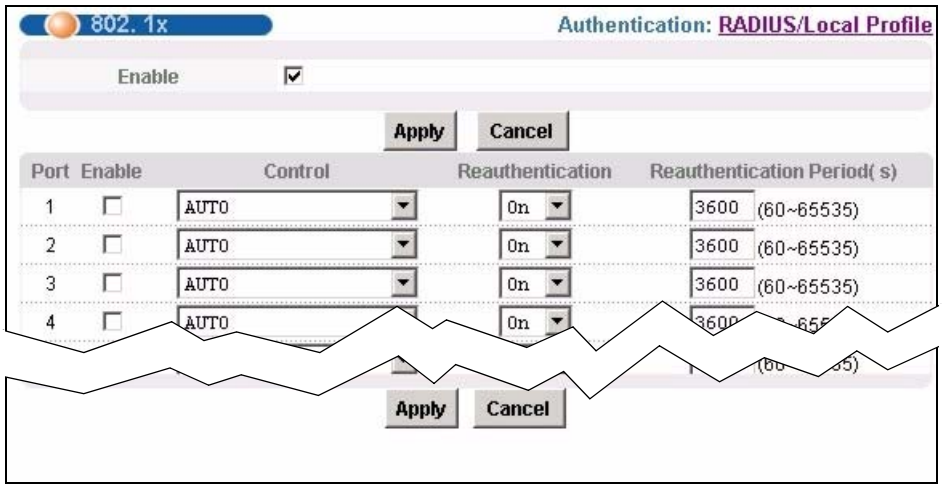
Table 53 RADIUS (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes to the SAM1316-22's volatile memory. The SAM1316-22 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 SAM1316-22 use its internal database of user names and passwords to authenticate users.
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 SAM1316-22's volatile memory. The SAM1316-22 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.

24.3 802.1x Screen

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

Figure 86 802.1x



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 24.2 on page 176).
Enable	Select this check box to turn on IEEE 802.1x authentication on the switch.
Apply	Click **Apply** to save your changes to the SAM1316-22's volatile memory. The SAM1316-22 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.

Table 54 802.1x (continued)

LABEL	DESCRIPTION
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 SAM1316-22's volatile memory. The SAM1316-22 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.

25

Port Security

This chapter shows you how to set up port security.

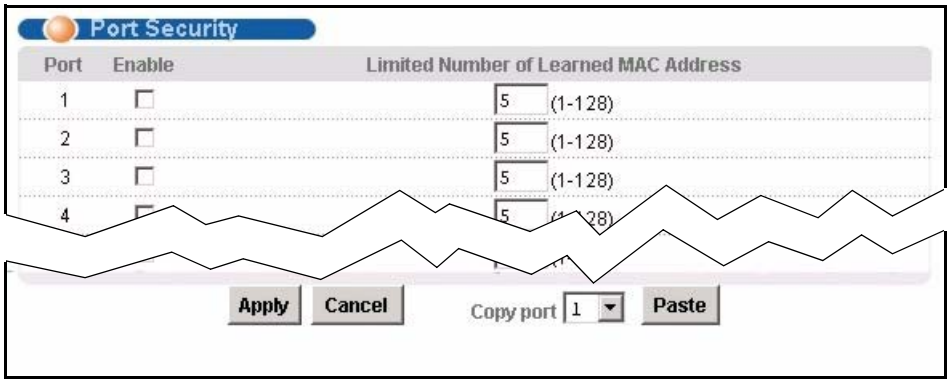
25.1 Port Security Overview

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

25.2 Port Security Screen

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

Figure 87 Port Security

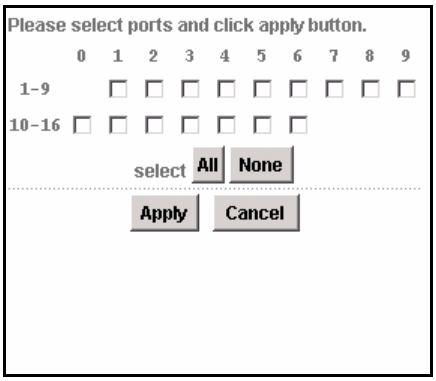


The following table describes the labels in this screen.

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 SAM1316-22 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 SAM1316-22's volatile memory. The SAM1316-22 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 88** Select Ports 

26

DHCP Relay

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

26.1 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 SAM1316-22 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.

26.2 DHCP Relay Agent Information Option (Option 82)

The SAM1316-22 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 SAM1316-22 to add to the DHCP requests that it relays to the DHCP server. Please see RFC 3046 for more details.

26.2.1 Private Format

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 SAM1316-22 relays to a DHCP server. The Agent Information field that the SAM1316-22 adds contains an "Agent Circuit-ID sub-option" that includes the slot and port numbers, VLAN ID and optional information about the slot and port on which the DHCP request was received.

The following table shows the format of the private Agent Circuit ID sub-option. The (binary) "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 1-byte **Slot No** field

specifies the ingress slot number, and a 1-byte **Port No** field specifies the ingress port number (both 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 1 to 24 bytes (including a one-byte termination character) and is optional information (that you specify) about this relay agent.

Table 56 DHCP Relay Agent Circuit ID Sub-option Format: Private

1	N	Slot No	Port No	VLAN ID	A

The Agent Information field that the SAM1316-22 adds also contains an "Agent Remote-ID sub-option" of information that you specify.

The following table shows the format of the private 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 port number (in plain text format) upon which the DHCP client request was received. Next, the extra information field (**A** in the table) contains from 0 to 23 bytes of optional information (that you specify) with no spaces and no termination character (if you do not specify any information, this field contains no data). This is followed by a slash (/), the port name, a slash (/) and the telephony port.

Table 57 DHCP Relay Agent Remote ID Sub-option Format: Private

2	N	Port Number	/	A	/	Port Name	/	Port Tel

26.2.2 TR-101 Format

The Agent Information field that the management switch card adds contains an "Agent Circuit-ID sub-option" that 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 Agent Circuit ID 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 58 DHCP Relay Agent Circuit ID Sub-option Format: TR-101 (VID on)

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

Table 59 DHCP Relay Agent Circuit ID Sub-option Format: TR-101 (VID off)

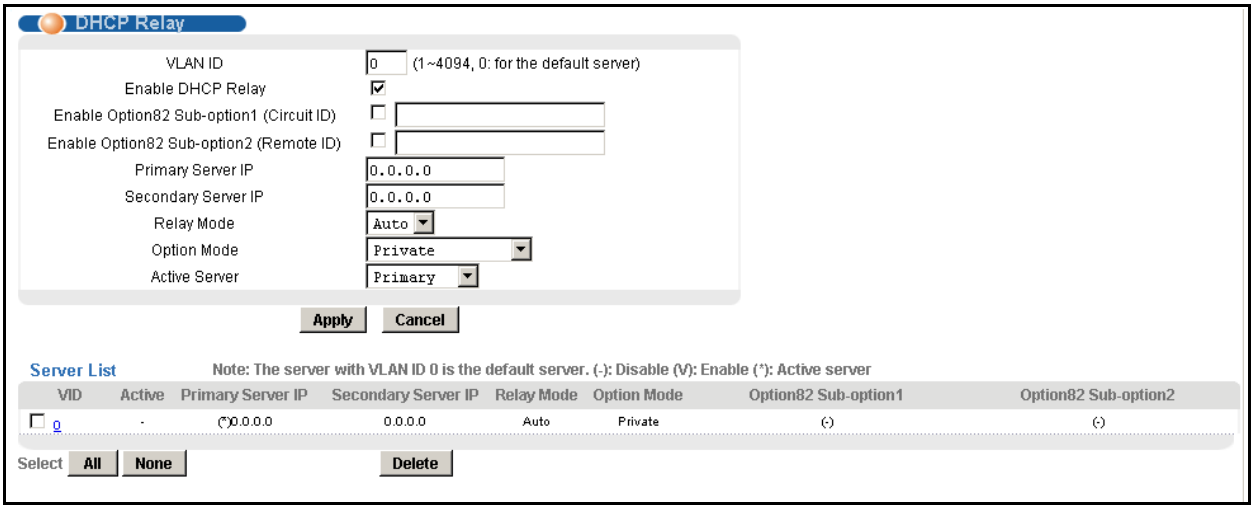
1	N	hostname / A / IP	“atm “	Slot ID	/	Port No.	:	VPI	.	VCI

TR-101 uses the same remote ID sub-option format as the Private format.

26.3 DHCP Relay Screen

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

Figure 89 DHCP Relay



The following table describes the labels in this screen.

Table 60 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 SAM1316-22 relay DHCP requests to a DHCP server and the server’s responses back to the clients.

Table 60 DHCP Relay (continued)

LABEL	DESCRIPTION
Enable Option 82 sub option 1 (Circuit ID)	Select this to have the SAM1316-22 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 SAM1316-22 to add to the DHCP requests that the SAM1316-22 relays to a DHCP server. Examples of information you could add would be the system name of the SAM1316-22 or the ISP's name.
Enable Option 82 sub option 2 (Remote ID)	Select this to have the SAM1316-22 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 SAM1316-22 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 SAM1316-22 relays DHCP requests. **Auto** - The SAM1316-22 routes DHCP requests to the active server for each VLAN. **Both** - The SAM1316-22 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 SAM1316-22 should relay DHCP requests for the selected VLAN.
Apply	Click **Apply** to save your changes to the SAM1316-22's volatile memory. The SAM1316-22 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.
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.
VID	This field displays the ID of the VLAN served by the specified DHCP relay(s).
Active	This field displays whether or not the SAM1316-22 relays DHCP requests in the selected VLAN to a DHCP server and the server's responses back to the clients.
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 60 DHCP Relay (continued)

LABEL	DESCRIPTION
Relay Mode	This field displays how the SAM1316-22 relays DHCP requests for the selected VLAN. **Auto** - The SAM1316-22 routes DHCP requests to the active server for the VLAN. **Both** - The SAM1316-22 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 SAM1316-22 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 SAM1316-22 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**.

27

DHCP Snoop

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

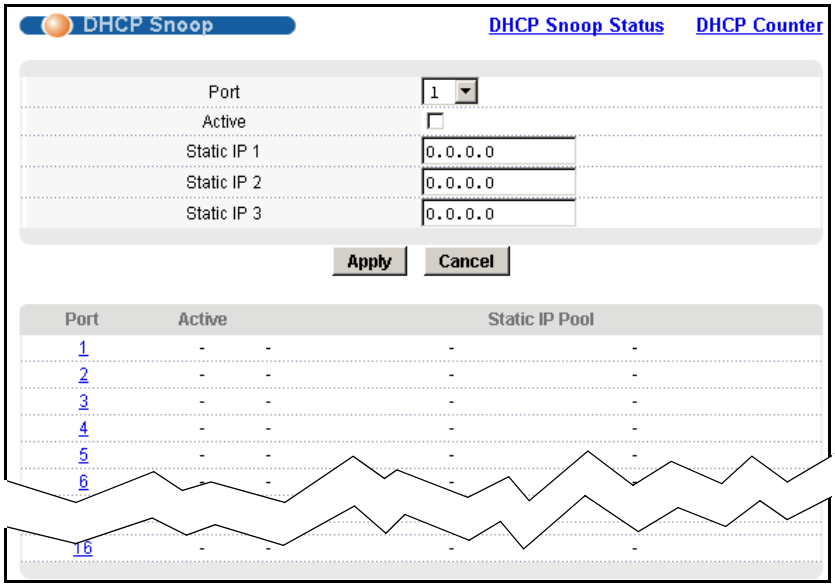
27.1 DHCP Snoop Overview

DHCP snooping prevents clients from assigning their own IP addresses. The SAM1316-22 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.

27.2 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 90 DHCP Snoop



The following table describes the labels in this screen.

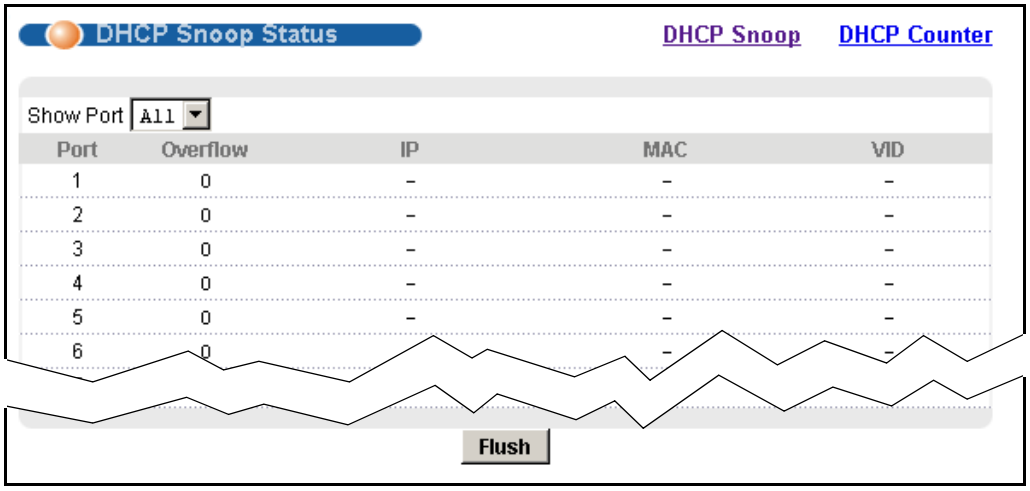
Table 61 DHCP Snoop

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 27.3 on page 191).
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 27.4 on page 192).
Port	This field displays each DSL port number.
Active	This field displays whether DHCP snooping is active (“V”) or inactive (“-”) 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 SAM1316-22 should forward packets, even if the IP address is not assigned by the DHCP server. The SAM1316-22 drops packets from other unknown IP addresses on this port. To delete an existing IP address, enter **0.0.0.0**.
Apply	Click **Apply** to save your changes to the SAM1316-22’s volatile memory. The SAM1316-22 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 each DSL port number.
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 SAM1316-22 should forward packets, even if the IP address is not assigned by the DHCP server. **0.0.0.0** is a blank value.

27.3 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 91 DHCP Snoop Status



The following table describes the labels in this screen.

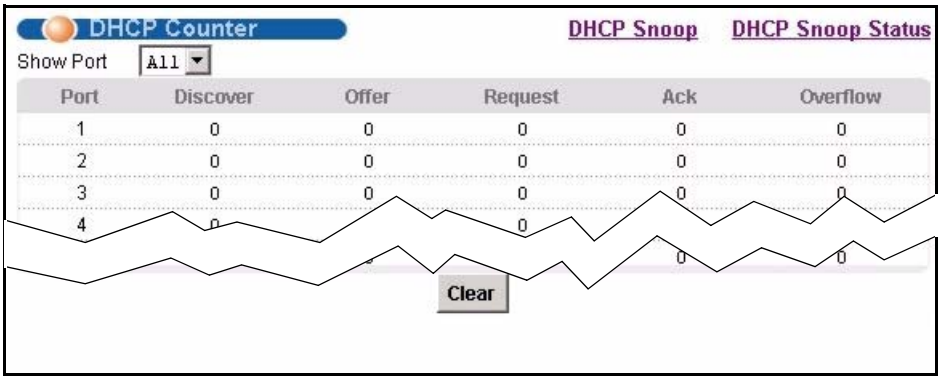
Table 62 DHCP Snoop Status

LABEL	DESCRIPTION
DHCP Snoop	Click **DHCP Snoop** to open the screen where you can activate or deactivate DHCP snooping on each port (see Section 27.2 on page 189).
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 27.4 on page 192).
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 VID assigned to a client on this port.
Flush	Click **Flush** to remove all of the entries from the DHCP snooping table for the selected port(s).

27.4 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 92 DHCP Counter



The following table describes the labels in this screen.

Table 63 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 27.2 on page 189).
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 27.3 on page 191).
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 SAM1316-22 has learned about DHCP packets. This resets every counter in this screen.

28

2684 Routed Mode

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

28.1 2684 Routed Mode

Use the 2684 (formerly 1483) routed mode to have the SAM1316-22 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 SAM1316-22 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.

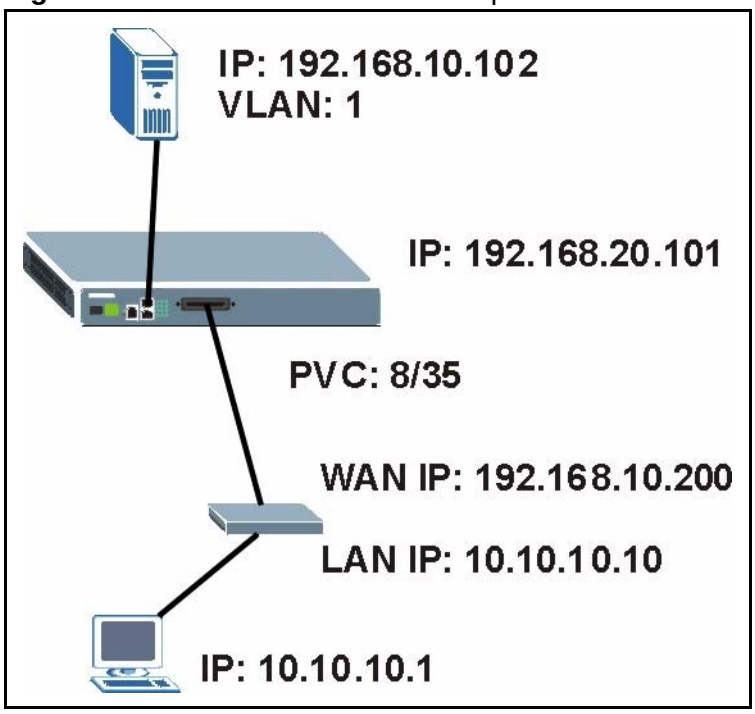
- Use the 2684 Routed PVC Screen to configure PVCs for 2684 routed mode traffic.
- Use the 2684 Routed Domain Screen to configure domains for 2684 routed mode traffic. The domain is the range of IP addresses behind the subscriber's device (the CPE or Customer Premises Equipment). This includes the CPE 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 SAM1316-22 reassembles the Ethernet packets from the AAL5 ATM cells, the SAM1316-22 will append the routed mode gateway's MAC address and the SAM1316-22's MAC address as the destination/source MAC address.
- For downstream traffic: When the SAM1316-22 sees the destination IP address is specified in the RPVC (or RPVC domain), the SAM1316-22 will strip out the MAC header and send them to the corresponding RPVC.

28.1.1 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 SAM1316-22 uses IP address 192.168.20.101. The subscriber's device (the CPE) is connected to DSL port 1 on the SAM1316-22 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 93 2684 Routed Mode Example



Note the following.

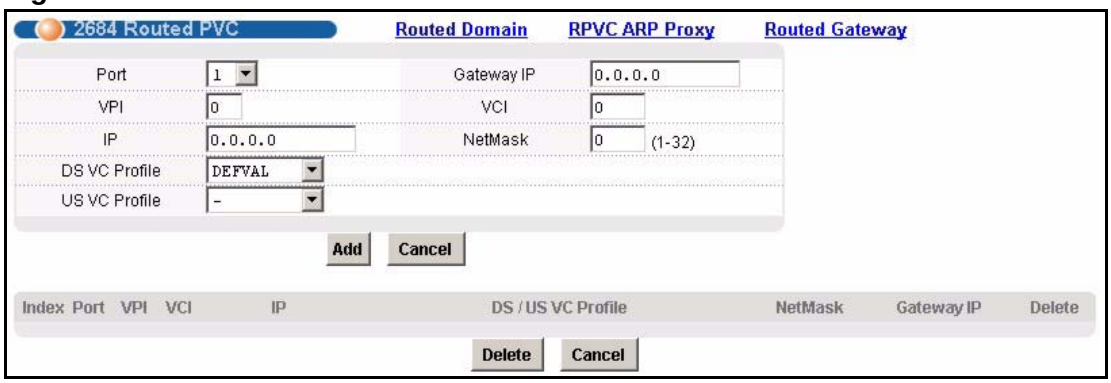
- The CPE device's WAN IP (192.168.10.200 in this example) must be in the same subnet as the gateway's IP address (192.168.10.102 in this example).
- The SAM1316-22's management IP address can be any IP address, it doesn't have any relationship to the WAN IP address or routed gateway IP address.
- The SAM1316-22'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 SAM1316-22's management IP address should not be in the same subnet range of any RPVC and RPVC domain. It will make the SAM1316-22 confused if the SAM1316-22 receives a packet with this IP as destination IP.
- The SAM1316-22'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.

28.2 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 94 2684 Routed PVC



The following table describes the labels in this screen.

Table 64 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 28.3 on page 196).
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 28.4 on page 198).
Routed Gateway	Click **Routed Gateway** to go to the screen where you can configure gateway settings (see Section 28.5 on page 199).
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 SAM1316-22's IP address.

Table 64 2684 Routed PVC (continued)

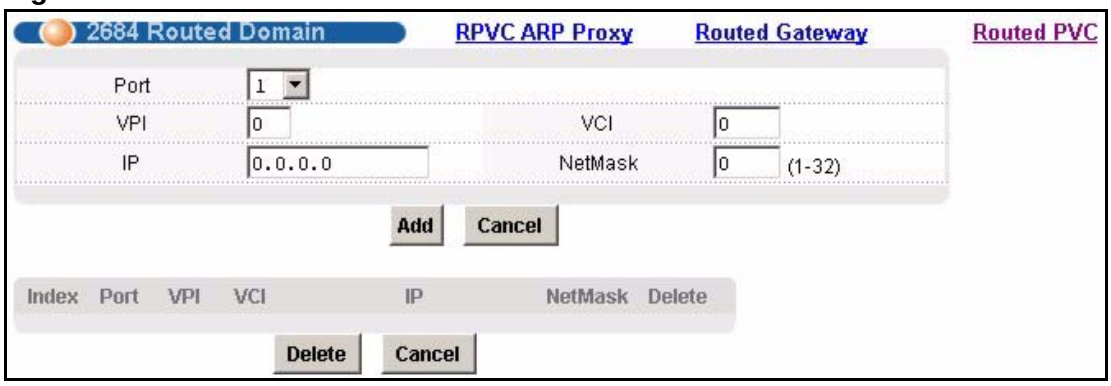
LABEL	DESCRIPTION
DS VC Profile	Use the drop-down list box to select a VC profile to use for this channel's downstream traffic shaping.
US VC Profile	Use the drop-down list box to select a VC profile to use for this channel's upstream traffic. The SAM1316-22 does not perform upstream traffic policing if you do not specify an upstream VC profile.
Add	Click **Add** to save your changes to the SAM1316-22's volatile memory. The SAM1316-22 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 SAM1316-22's volatile memory. The SAM1316-22 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.

28.3 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 95 2684 Routed Domain



The following table describes the labels in this screen.

Table 65 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 28.4 on page 198).
Routed Gateway	Click **Routed Gateway** to go to the screen where you can configure gateway settings (see Section 28.5 on page 199).
Routed PVC	Click **Routed PVC** to go to the screen where you can configure routed PVC settings (see Section 28.2 on page 195).
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 SAM1316-22's volatile memory. The SAM1316-22 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.

Table 65 2684 Routed Domain (continued)

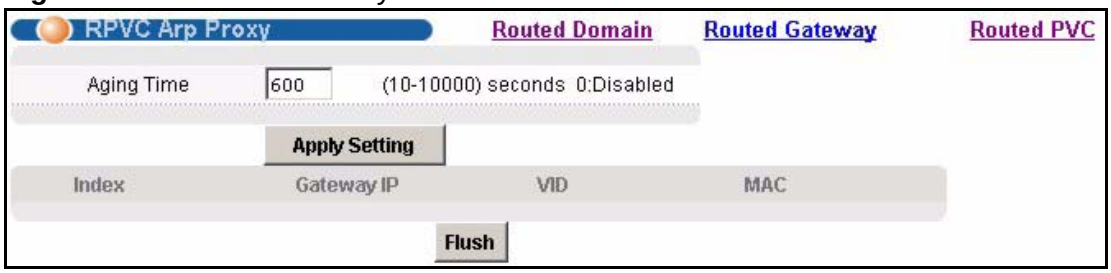
LABEL	DESCRIPTION
VPI	This field displays the Virtual Path Identifier (VPI) The VPI and VCI identify a channel on this port.
VCI	This field displays the Virtual Circuit Identifier (VCI). The VPI and VCI identify a channel on this port.
IP	This field displays the subscriber's IP address.
NetMask	This field displays the bit number of the subnet mask of the subscriber's LAN IP address.
Delete	Select an entry's **Delete** check box and click **Delete** to remove the entry. Clicking **Delete** saves your changes to the SAM1316-22's volatile memory. The SAM1316-22 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.

28.4 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 96 RPVC ARP Proxy



The following table describes the labels in this screen.

Table 66 RPVC ARP Proxy

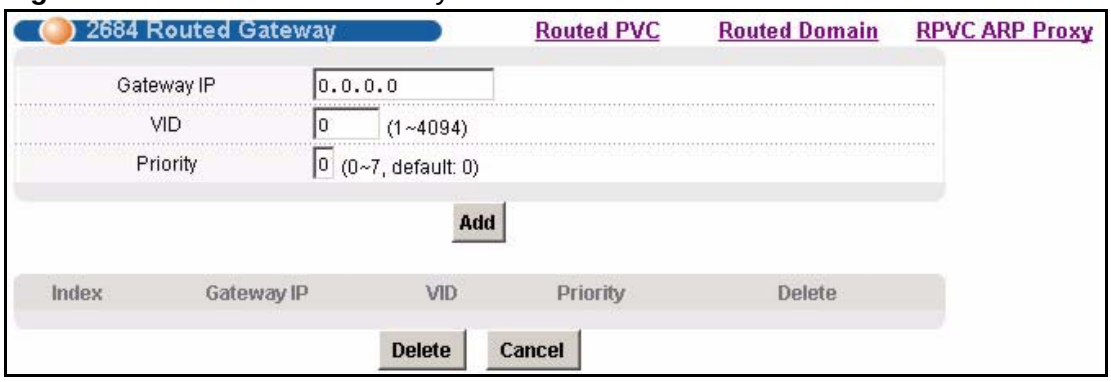
LABEL	DESCRIPTION
Routed Domain	Click **Routed Domain** to open this screen where you can configure domains for 2684 routed mode traffic (see Section 28.3 on page 196).
Routed Gateway	Click **Routed Gateway** to go to the screen where you can configure gateway settings (see Section 28.5 on page 199).
Routed PVC	Click **Routed PVC** to go to the screen where you can configure routed PVC settings (see Section 28.2 on page 195).
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 SAM1316-22's volatile memory. The SAM1316-22 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.
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.

28.5 2684 Routed Gateway Screen

Use this screen to configure gateway settings.

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

Figure 97 2684 Routed Gateway



The following table describes the labels in this screen.

Table 67 2684 Routed Gateway

LABEL	DESCRIPTION
Routed PVC	Click **Routed PVC** to go to the screen where you can configure routed PVC settings (see Section 28.2 on page 195).
Routed Domain	Click **Routed Domain** to open this screen where you can configure domains for 2684 routed mode traffic (see Section 28.3 on page 196).
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 28.4 on page 198).
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.
Add	Click **Add** to save your changes to the SAM1316-22's volatile memory. The SAM1316-22 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.

Table 67 2684 Routed Gateway (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 SAM1316-22's volatile memory. The SAM1316-22 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.

29

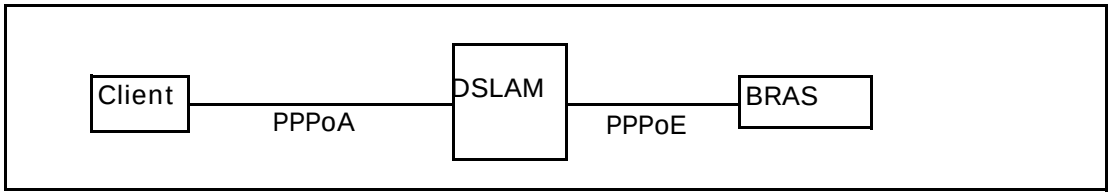
PPPoA to PPPoE

This chapter shows you how to set up the SAM1316-22 to convert PPPoA frames to PPPoE traffic and vice versa.

29.1 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 98 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 SAM1316-22) to translate PPPoA frames to PPPoE packets and vise versa.

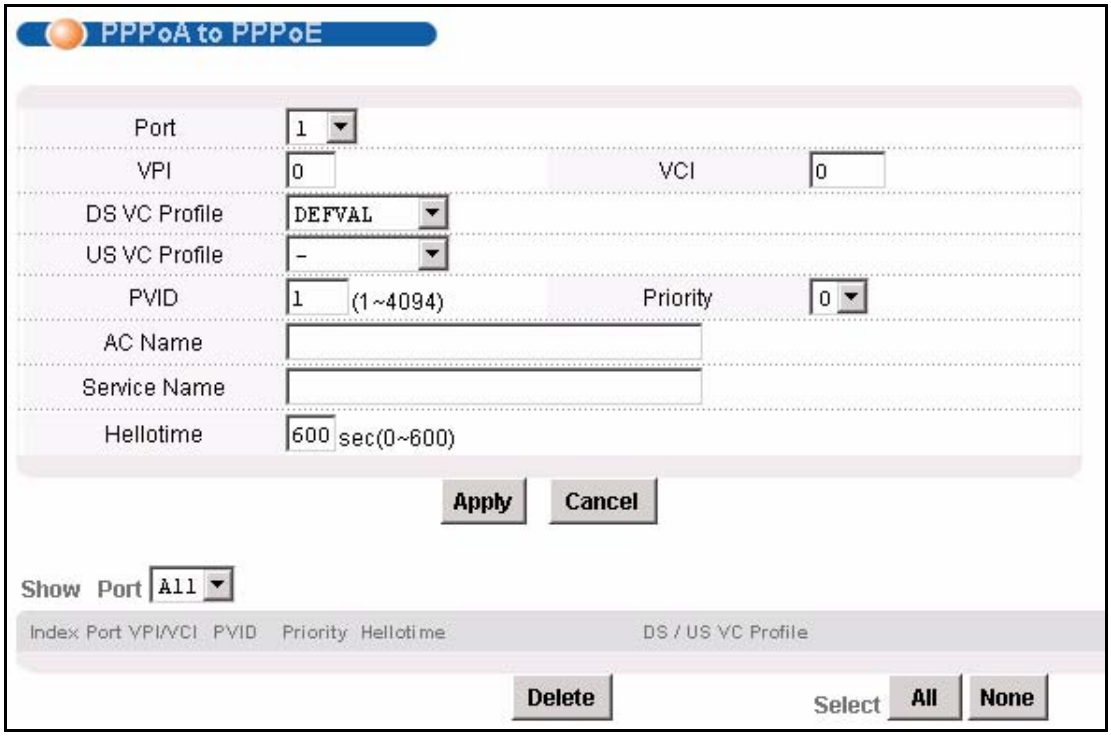
When PPPoA packets are received from the CPE, the ATM headers are removed and the SAM1316-22 adds PPPoE and Ethernet headers before sending the packets to the BRAS. When the SAM1316-22 receives PPPoE packets from the BRAS, PPPoE and Ethernet headers are stripped and necessary PVC information (such as encapsulation type) is added before forwarding to the designated CPE.

29.2 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 91 for

background information about creating PVCs. To open this screen, click **Advanced Application**, **PPPoA to PPPoE**.

Figure 99 PPPoA to PPPoE



The following table describes the labels in this screen.

Table 68 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 SAM1316-22 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.

Table 68 PPPoA to PPPoE (continued)

LABEL	DESCRIPTION
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.
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 SAM1316-22 checks the AC name field in the BRAS's reply PDU. If there is a mismatch, the SAM1316-22 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 SAM1316-22's volatile memory. The SAM1316-22 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 29.3 on page 207.) 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.

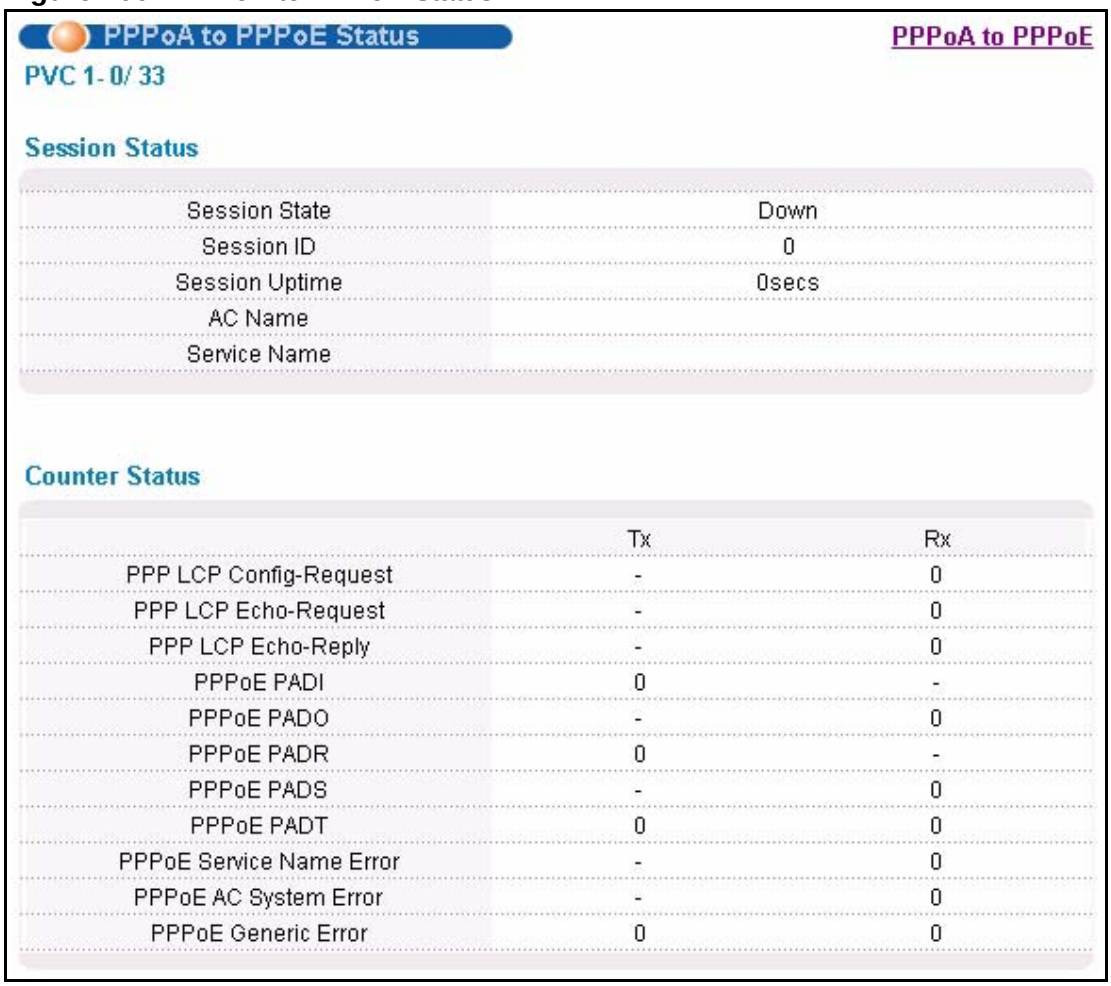
Table 68 PPPoA to PPPoE (continued)

LABEL	DESCRIPTION
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.

29.3 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 100 PPPoA to PPPoE Status


PPPoA to PPPoE Status

PPPoA to PPPoE

PVC 1- 0/ 33

Session Status

Session State	Down
Session ID	0
Session Uptime	0secs
AC Name	
Service Name	

Counter Status

	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 Service Name Error	-	0
PPPoE AC System Error	-	0
PPPoE Generic Error	0	0

The following table describes the labels in this screen.

Table 69 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 29.2 on page 203).
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.

Table 69 PPPoA to PPPoE Status (continued)

LABEL	DESCRIPTION
Session Uptime	This field displays how long the current session has been up.
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 SAM1316-22.
PPP LCP Config-Request	This field displays the number of config-request PDUs received by the SAM1316-22 from the CPE (client) device.
PPP LCP Echo-Request	This field displays the number of echo-request PDUs received by the SAM1316-22 from the CPE (client) device.
PPP LCP Echo-Reply	This field displays the number of echo-reply PDUs received by the SAM1316-22 from the CPE (client) device.
PPPoE PADI	This field displays the number of padi PDUs sent by the SAM1316-22 to the BRAS.
PPPoE PADO	This field displays the number of pado PDUs sent by the BRAS to the SAM1316-22.
PPPoE PADR	This field displays the number of padr PDUs sent by the SAM1316-22 to the BRAS.
PPPoE PADS	This field displays the number of pads PDUs sent by the BRAS to the SAM1316-22.
PPPoE PADT	This field displays the number of padt PDUs sent and received by the SAM1316-22.
PPPoE Service Name Error	This field displays the number of service name errors; for example, the SAM1316-22'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 SAM1316-22 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 SAM1316-22 and the BRAS.

30

DSCP

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

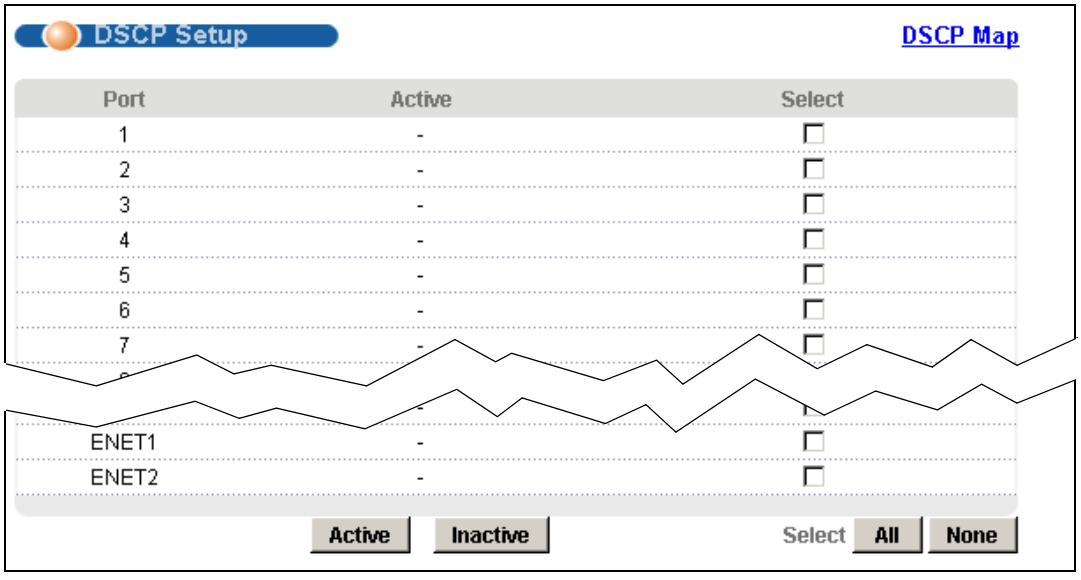
30.1 DSCP Overview

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.

30.2 DSCP Setup Screen

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

Figure 101 DSCP Setup



The following table describes the labels in this screen.

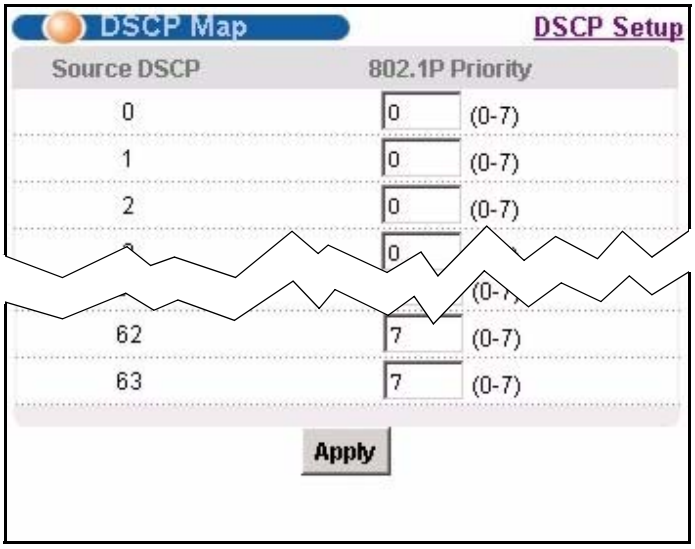
Table 70 DSCP Setup

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 30.3 on page 210).
Port	This field displays each port number.
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.

30.3 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 102 DSCP Map



The following table describes the labels in this screen.

Table 71 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 30.2 on page 209).
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 SAM1316-22's volatile memory. The SAM1316-22 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.

31

TLS PVC

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

31.1 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.

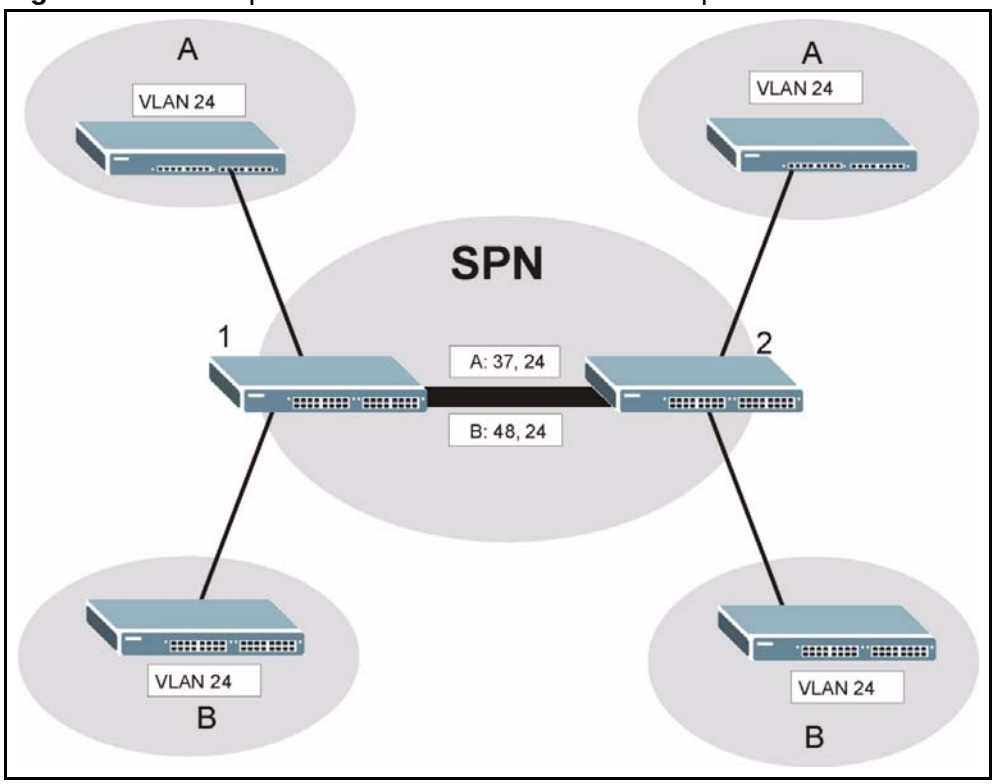
Before the SAM1316-22 sends the frames from the customers, the VLAN ID is added to the frames. When packets intended for specific customers are received on the SAM1316-22, the outer VLAN tag is removed before the traffic is sent.

31.1.1 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 103 Transparent LAN Service Network Example

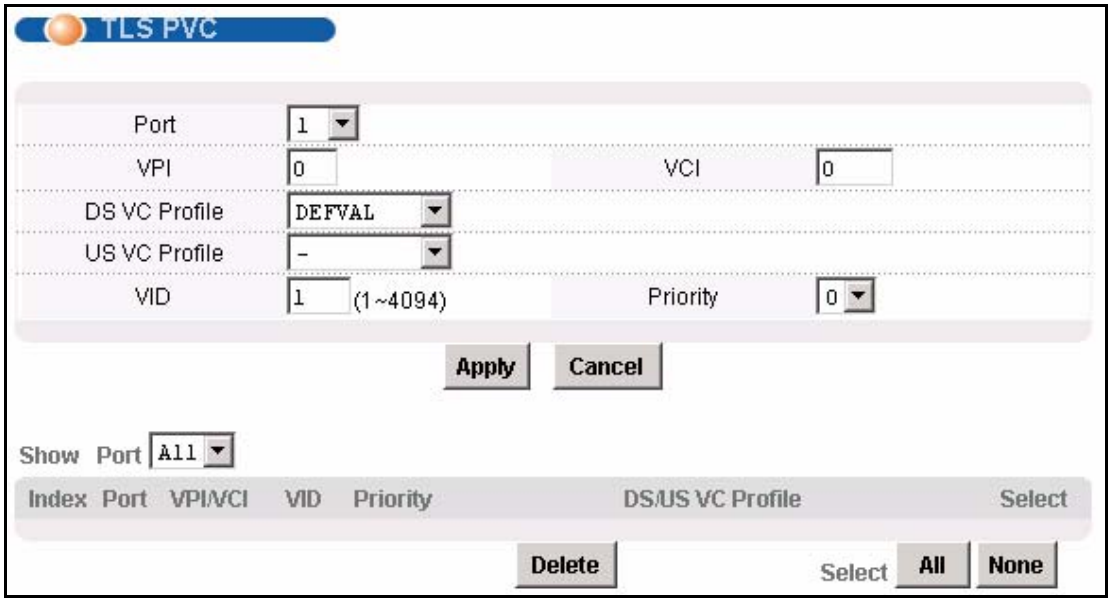


31.2 TLS PVC Screen

Use this screen to set up Transparent LAN Services on each port. This is set up by creating a TLS PVC. See Chapter 13 on page 91 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 104 TLS PVC



The following table describes the labels in this screen.

Table 72 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 SAM1316-22 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.

Table 72 TLS PVC (continued)

LABEL	DESCRIPTION
Apply	Click this to add or save channel settings on the selected port. This saves your changes to the SAM1316-22's volatile memory. The SAM1316-22 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 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.

32 ACL

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

32.1 Access Control Logic (ACL) Overview

An ACL (Access Control Logic) profile allows the SAM1316-22 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.

32.1.1 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 SAM1316-22 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 SAM1316-22 checks Profile1 first. If the traffic is VLAN ID 100, the SAM1316-22 follows the action in Profile1 and does not check Profile2. You cannot assign profiles that have the same rule numbers to the same PVC.

32.1.2 ACL Profile Actions

The SAM1316-22 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 SAM1316-22 can apply more than one action to a packet, unless you select deny.

If you select the rvlan action, the SAM1316-22 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

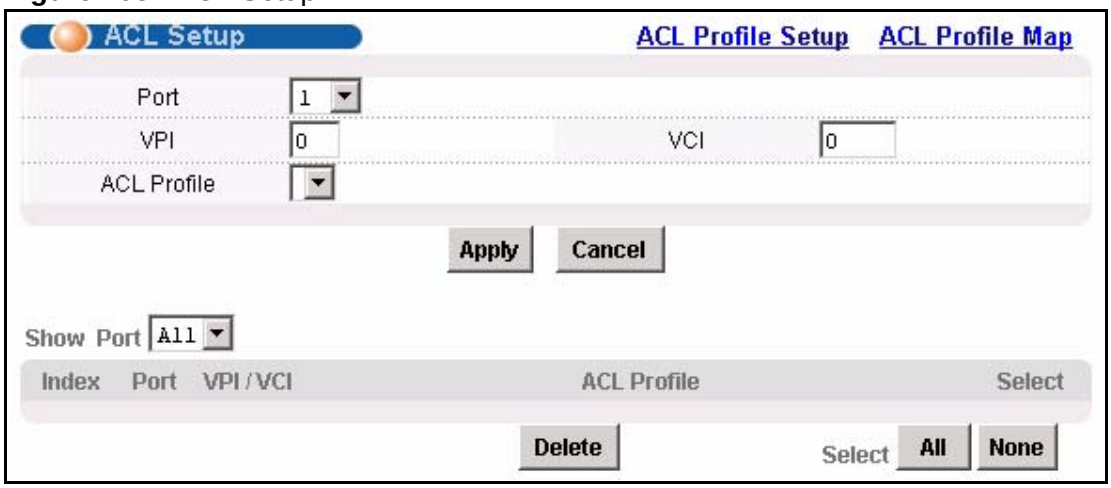
PVC, the SAM1316-22 drops the traffic because the new VLAN ID does not match the VID of the PVC. This is illustrated in the following scenario.

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 SAM1316-22 checks the ACL rule and changes the traffic to VLAN 901. When the SAM1316-22 finally compares the VLAN ID of the traffic (901) to the VID of the PVC (900), the SAM1316-22 drops the packets because they do not match.

32.2 ACL Setup Screen

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

Figure 105 ACL Setup



The following table describes the labels in this screen.

Table 73 ACL Setup

LABEL	DESCRIPTION
ACL Profile Setup	Click **ACL Profile Setup** to open the screen where you can set up ACL profiles (see Section 32.3 on page 221).
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 32.4 on page 223).
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.

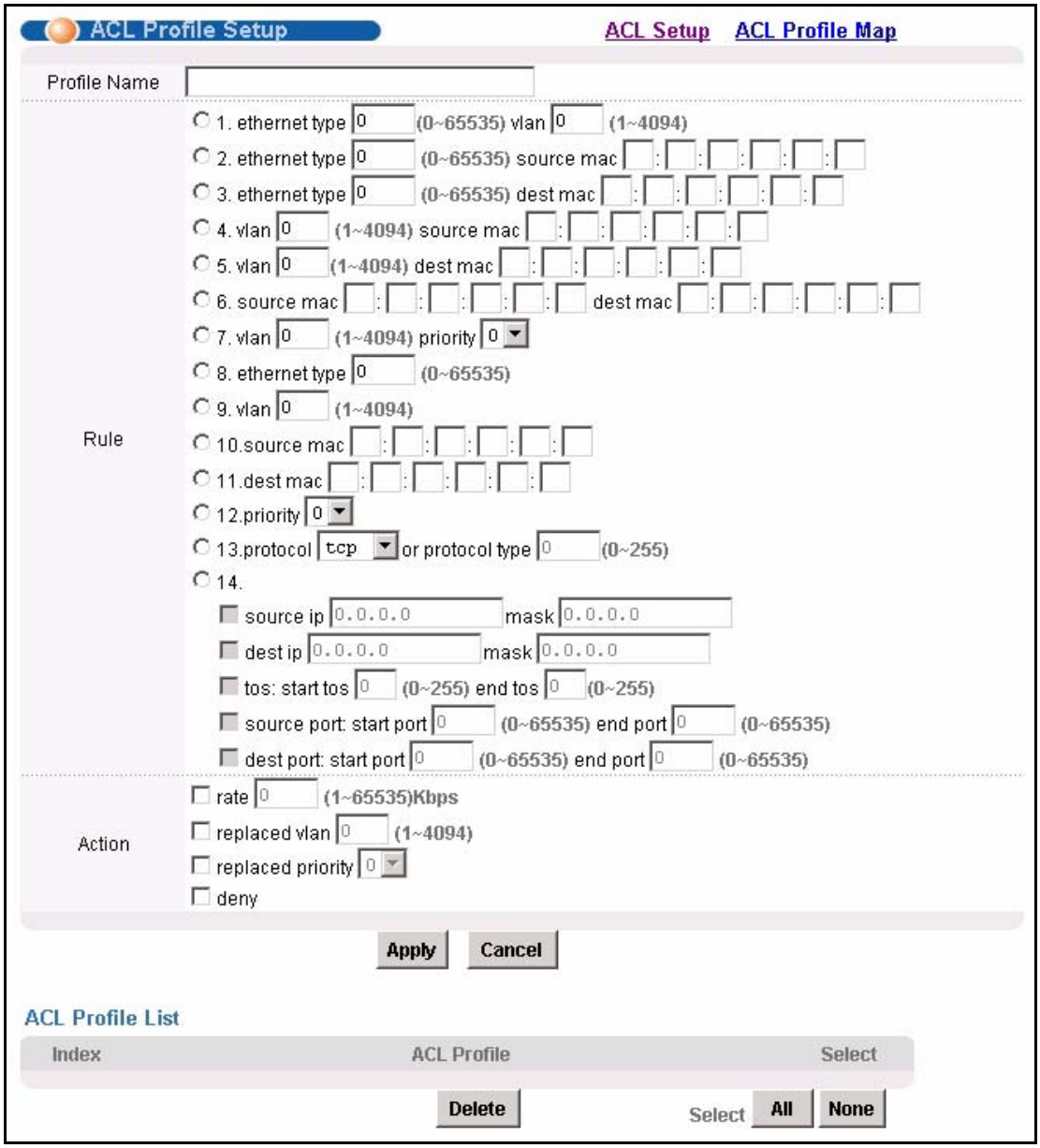
Table 73 ACL Setup (continued)

LABEL	DESCRIPTION
Apply	Click this to save your changes to the SAM1316-22's volatile memory. The SAM1316-22 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.
Select All	Click this to select all entries in the table.
Select None	Click this to un-select all entries in the table.

32.3 ACL Profile Setup Screen

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

Figure 106 ACL Profile Setup



The following table describes the labels in this screen.

Table 74 ACL Profile Setup

LABEL	DESCRIPTION
ACL Setup	Click **ACL Setup** to open the screen where you can assign ACL profiles to PVCs (see Section 32.2 on page 219).
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 32.4 on page 223).
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 SAM1316-22 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 SAM1316-22 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.

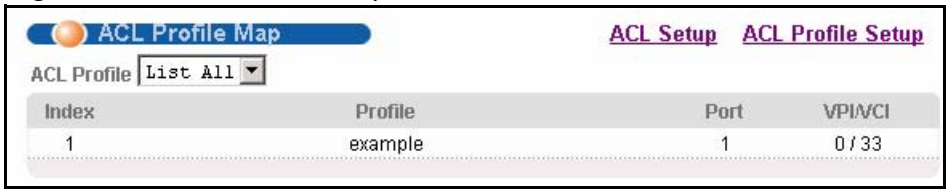
Table 74 ACL Profile Setup (continued)

LABEL	DESCRIPTION
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.

32.4 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 107 ACL Profile Map



The following table describes the labels in this screen.

Table 75 ACL Profile Map

LABEL	DESCRIPTION
ACL Setup	Click **ACL Setup** to open the screen where you can assign ACL profiles to PVCs (see Section 32.2 on page 219).
ACL Profile Setup	Click **ACL Profile Setup** to open the screen where you can set up ACL profiles (see Section 32.3 on page 221).
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.

33

Downstream Broadcast

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

33.1 Downstream Broadcast

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

33.2 Downstream Broadcast Screen

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

Figure 108 Downstream Broadcast

The following table describes the labels in this screen.

Table 76 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.

Table 76 Downstream Broadcast (continued)

LABEL	DESCRIPTION
Add	Click **Add** to save your changes to the SAM1316-22's volatile memory. The SAM1316-22 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.
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 SAM1316-22's volatile memory. The SAM1316-22 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.

34

Syslog

This chapter explains how to set the syslog parameters.

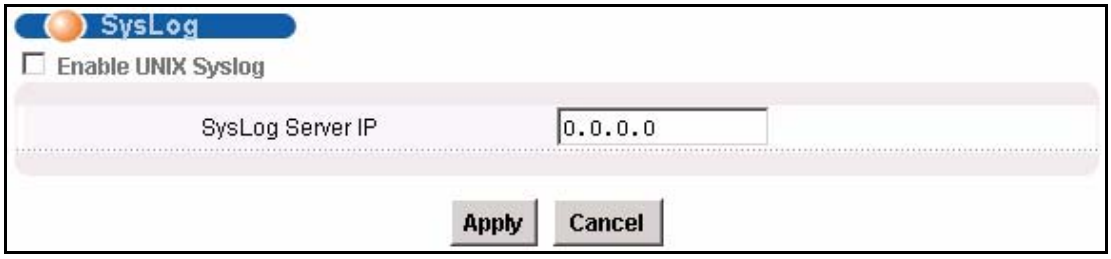
34.1 Syslog

The syslog feature sends logs to an external syslog server.

34.2 SysLog Screen

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

Figure 109 SysLog



The following table describes the labels in this screen.

Table 77 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 41.4 on page 253.)
Apply	Click **Apply** to save your changes to the SAM1316-22's volatile memory. The SAM1316-22 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

Access Control

This chapter describes how to configure access control.

35.1 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 110 Access Control

35.2 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 78 Access Control Summary

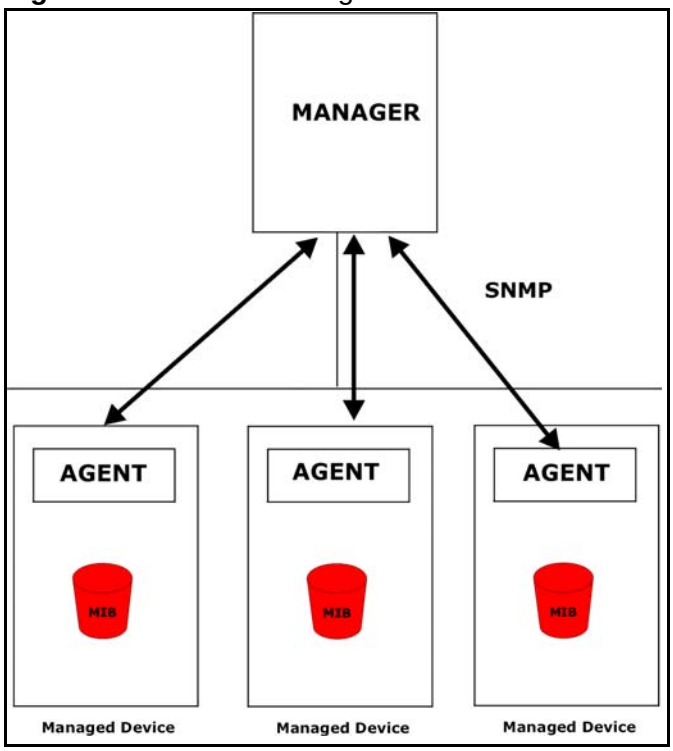
	CONSOLE PORT	TELNET	FTP	WEB	SNMP
Number of sessions allowed	1	5	1	No limit	No limit

35.3 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 SAM1316-22

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 111 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 SAM1316-22). 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 79 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.
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.

35.3.1 Supported MIBs

MIBs let administrators collect statistics and monitor status and performance. See Appendix on page 437 for the list of MIBs the SAM1316-22 supports.

35.3.2 SNMP Traps

The SAM1316-22 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 SAM1316-22 to the subscriber). ATUR refers to the upstream channel (for traffic coming from the subscriber to the SAM1316-22).

Table 80 SNMP Traps

TRAP NAME	DESCRIPTION	OID
coldStart	System Cold Start	1.3.6.1.6.3.1.1.5.1
warmStart	System Warm Start	1.3.6.1.6.3.1.1.5.2
linkDown	Both Ethernet and DSL link Down	1.3.6.1.6.3.1.1.5.3
linkUp	Both Ethernet and DSL link UP	1.3.6.1.6.3.1.1.5.4
hdsl2ShdslLoopAttenCrossing	This notification indicates that the loop attenuation threshold (as per the hdsl2ShdslEndpointThreshLoopAttenuation value) has been reached/exceeded for the HDSL2/SHDSL segment endpoint.	1.3.6.1.2.1.10.48.0.1
hdsl2ShdslSNRMarginCrossing	This notification indicates that the SNR margin threshold (as per the hdsl2ShdslEndpointThreshSNRMargin value) has been reached/exceeded for the HDSL2/SHDSL segment endpoint.	1.3.6.1.2.1.10.48.0.2

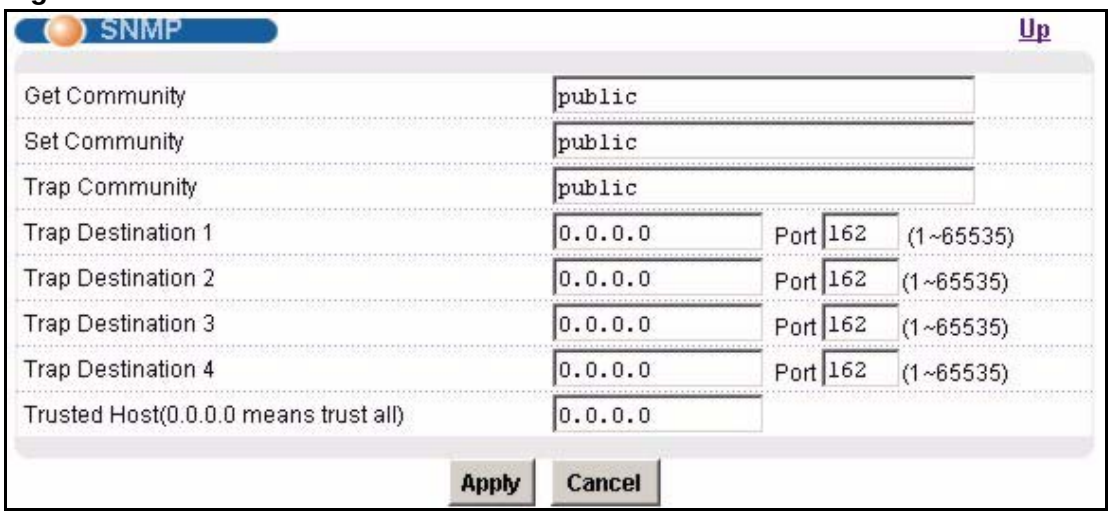
Table 80 SNMP Traps (continued)

TRAP NAME	DESCRIPTION	OID
hdsl2ShdslPerfESThresh	This notification indicates that the errored seconds threshold (as per the hdsl2ShdslEndpointThreshES value) has been reached/ exceeded for the HDSL2/ SHDSL segment endpoint.	1.3.6.1.2.1.10.48.0.3
hdsl2ShdslPerfSESThresh	This notification indicates that the severely errored seconds threshold (as per the hdsl2ShdslEndpointThreshSES value) has been reached/exceeded for the HDSL2/SHDSL Segment Endpoint.	1.3.6.1.2.1.10.48.0.4
hdsl2ShdslPerfCRCanomalies Thresh	This notification indicates that the CRC anomalies threshold (as per the hdsl2ShdslEndpointThreshCRCanomalies value) has been reached/exceeded for the HDSL2/SHDSL Segment Endpoint.	1.3.6.1.2.1.10.48.0.5
hdsl2ShdslPerfLOSWSThresh	This notification indicates that the LOSW seconds threshold (as per the hdsl2ShdslEndpointThreshLOSWS value) has been reached/exceeded for the HDSL2/SHDSL segment endpoint.	1.3.6.1.2.1.10.48.0.6
hdsl2ShdslPerfUASThresh	This notification indicates that the unavailable seconds threshold (as per the hdsl2ShdslEndpointThreshUAS value) has been reached/exceeded for the HDSL2/ SHDSL segment endpoint.	1.3.6.1.2.1.10.48.0.7
reboot	Send a message to the manager that the system is going to reboot. The variable is the reason why the system reboots.	1.3.6.1.4.1.890.1.5.13.0.1
overheat	Send a message to the manager that the system is overheated. The variable in the binding list is the current temperature in Celsius of the system.	1.3.6.1.4.1.890.1.5.13.0.3
overheatOver	Send a message to the manager that the overheated condition is over. The variable in the binding list is the current temperature in Celsius of the system.	1.3.6.1.4.1.890.1.5.13.0.4
voltageOutOfRange	Send a message to the manager that the voltage of the system is out of range. The variable in the binding list is the current voltage in volt of the system.	1.3.6.1.4.1.890.1.5.13.0.8
voltageNormal	Send a message to the manager that the low-voltage condition is over. The variable in the binding list is the current voltage in volt of the system.	1.3.6.1.4.1.890.1.5.13.0.9
thermalSensorFailure	The trap signifies that the thermal sensor failed.	1.3.6.1.4.1.890.1.5.13.0.22
sysMacAntiSpoofing	MAC Anti-spoofing.	1.3.6.1.4.1.890.1.5.5.6.12.4.1

35.4 SNMP Screen

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

Figure 112 SNMP



The following table describes the labels in this screen.

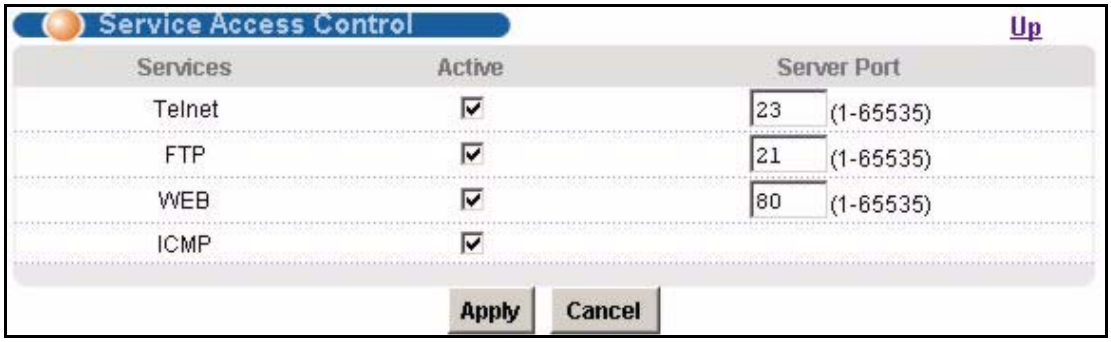
Table 81 SNMP

LABEL	DESCRIPTION
Up	Click **Up** 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 SAM1316-22. **0.0.0.0** allows any computer to use SNMP to access the SAM1316-22. Specify an IP address to allow only the computer with that IP address to use SNMP to access the SAM1316-22.
Apply	Click **Apply** to save your changes to the SAM1316-22’s volatile memory. The SAM1316-22 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.

35.5 Service Access Control Screen

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

Figure 113 Service Access Control



The following table describes the labels in this screen.

Table 82 Service Access Control

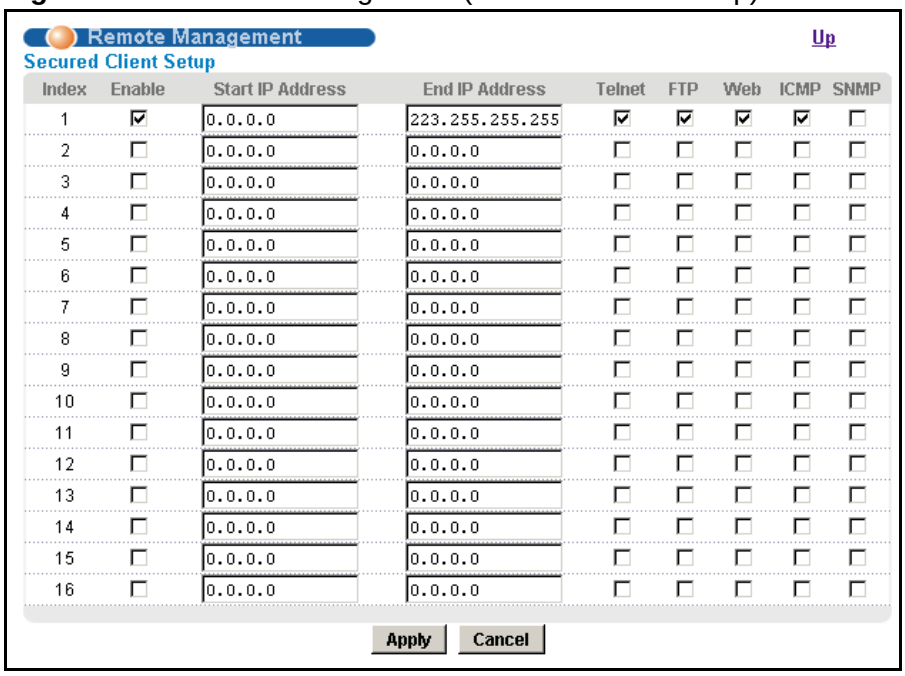
LABEL	DESCRIPTION
Up	Click **Up** to go back to the previous screen.
Services	Services you may use to access the SAM1316-22 are listed here.
Active	Select the **Active** check boxes for the corresponding services that you want to allow to access the SAM1316-22.
Server Port	For Telnet, FTP or web services, 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 SAM1316-22's volatile memory. The SAM1316-22 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.

35.6 Remote Management Screen

Use this screen to configure the IP address ranges of trusted computers that may manage the SAM1316-22.

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

Figure 114 Remote Management (Secured Client Setup)



The following table describes the labels in this screen.

Table 83 Remote Management (Secured Client Setup)

LABEL	DESCRIPTION
Up	Click **Up** 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 SAM1316-22.
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 SAM1316-22. The SAM1316-22 checks if the client IP address of a computer requesting a service or protocol matches the range set here. The SAM1316-22 immediately disconnects the session if it does not match.
Telnet/FTP/Web/ ICMP/SNMP	Select services that may be used for managing the SAM1316-22 from the specified trusted computers.
Apply	Click **Apply** to save your changes to the SAM1316-22’s volatile memory. The SAM1316-22 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.

36

PPPoE Intermediate Agent

This chapter describes how the SAM1316-22 gives a PPPoE termination server additional information that the server can use to identify and authenticate a PPPoE client.

36.1 PPPoE Intermediate Agent Tag Format

If the PPPoE Intermediate Agent is enabled, the SAM1316-22 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 84 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 SAM1316-22 supports two formats for the PPPoE intermediate agent sub-options: private and TR-101.

36.1.0.1 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 85 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 86 PPPoE Intermediate Agent Remote ID Sub-option Format

SubOpt (0x02)	Length	MAC (6 bytes)

The SAM1316-22 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 SAM1316-22 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 SAM1316-22 adds extra information, it does not append a trailing 0x00 (00h).

36.1.0.2 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 87 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 88 PPPoE Intermediate Agent Sub-option Format: TR-101 (VID off)

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

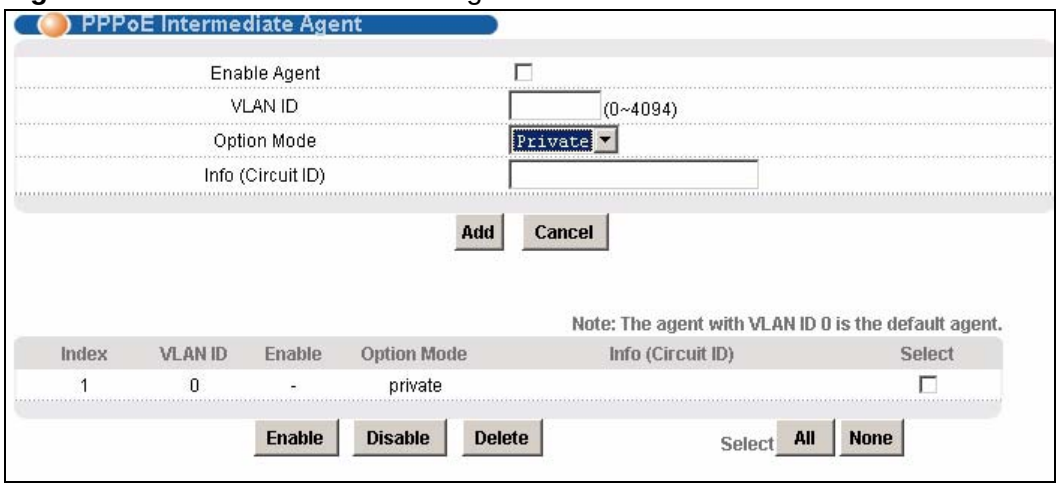
Unlike the private format for PPPoE intermediate agent, the TR-101 format for PPPoE intermediate agent does not include the Remote ID sub-option.

36.2 PPPoE Intermediate Agent Screen

Use this screen to configure the SAM1316-22 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 115 PPPoE Intermediate Agent



The following table describes the labels in this screen.

Table 89 PPPoE Intermediate Agent

LABEL	DESCRIPTION
Enable Agent	Select this if you want the SAM1316-22 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 SAM1316-22 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 SAM1316-22 adds to PADI and PADR packets in the specified VLAN. You can enter up to 23 printable English keyboard characters or spaces.

Table 89 PPPoE Intermediate Agent (continued)

LABEL	DESCRIPTION
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 SAM1316-22's volatile memory. The SAM1316-22 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 SAM1316-22 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 SAM1316-22 adds to PADI and PADR packets in the specified VLAN, if the PPPoE intermediate agent is turned on.
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.

37

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.

37.1 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 116 Maximum MTU

The following table describes the labels in this screen.

Table 90 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 SAM1316-22's volatile memory. The SAM1316-22 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.

38

PVC Upstream Limit

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

Note: 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 SAM1316-22 does not check the p-bit of incoming packets from subscribers when it discards the packet.

These limits are completely managed by the SAM1316-22, regardless of the CPE device's settings, which makes this approach more flexible and easier for operators to deploy.

38.1 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 SAM1316-22. 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 SAM1316-22 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 SAM1316-22.

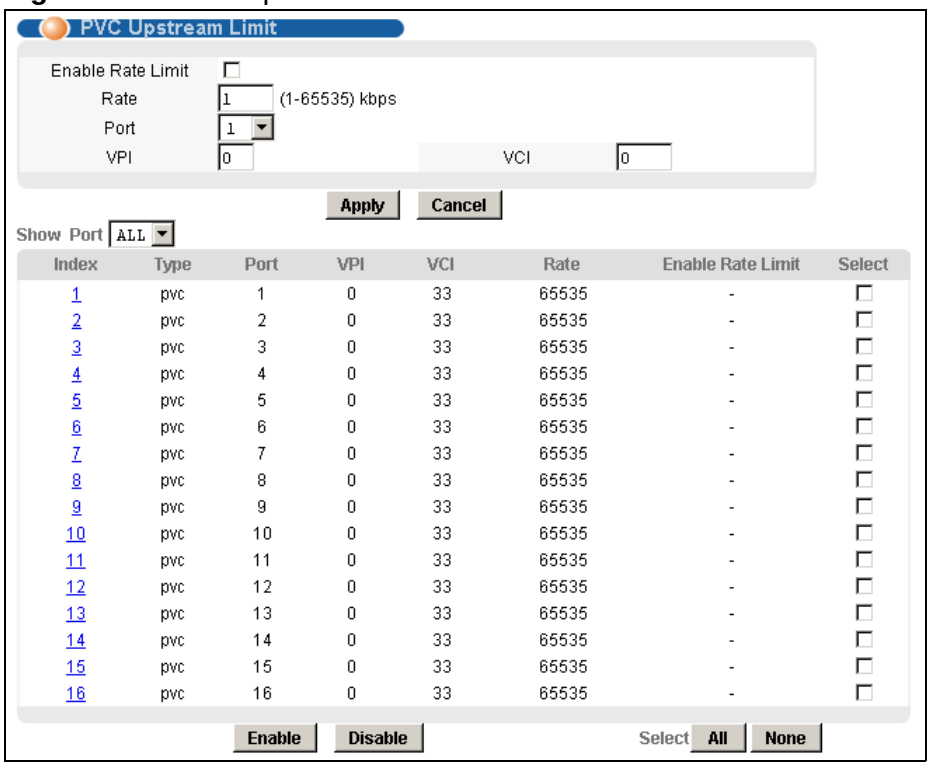
If there are limits on the transmission rate for upstream traffic both in upstream VC profiles and in this feature, the SAM1316-22 enforces the limit in the upstream VC profile first.

38.2 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 117 PVC Upstream Limit



The following table describes the labels in this screen.

Table 91 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.

Table 91 PVC Upstream Limit (continued)

LABEL	DESCRIPTION
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 SAM1316-22's volatile memory. The SAM1316-22 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.
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.
Enable Rate Limit	This shows "V" when the SAM1316-22 applies a limit on the upstream transmission rate for the specified PVC. It shows "-" when there is not limit applied.
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.

39

OUI Filter

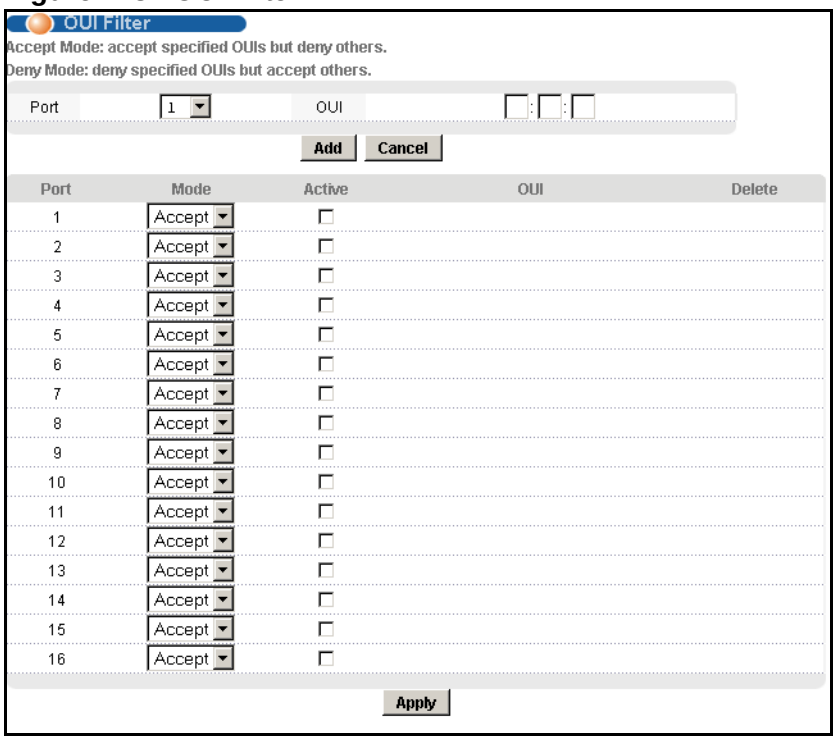
This chapter describes the **OUI Filter** screen.

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 118 OUI Filter



The following table describes the labels in this screen.

Table 92 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 SAM1316-22's port number.
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.

40

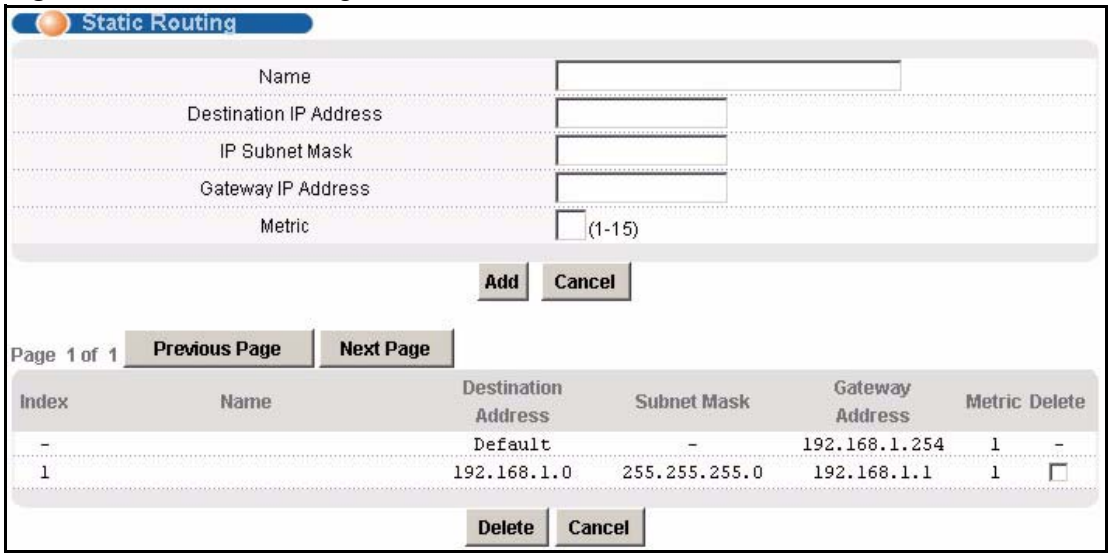
Static Routing

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

Static routes tell the SAM1316-22 how to forward the SAM1316-22'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 119 Static Routing



The following table describes the labels in this screen.

Table 93 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.

Table 93 Static Routing (continued)

LABEL	DESCRIPTION
IP Subnet Mask	Enter the subnet mask for this destination.
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 SAM1316-22’s volatile memory. It then displays in the summary table at the bottom of the screen. The SAM1316-22 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 SAM1316-22.
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.

41

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.

41.1 Alarm

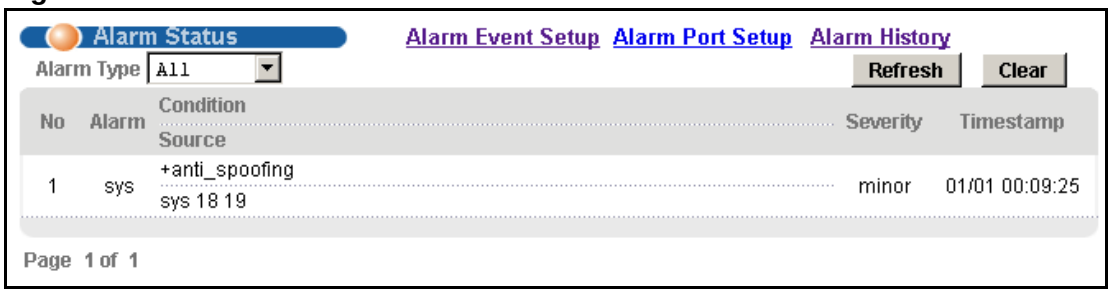
The SAM1316-22 monitors for equipment, DSL and system alarms and can report them via SNMP or syslog. You can specify the severity level of an alarm(s) and where the system is to send the alarm(s). You can also set the alarm severity threshold for recording alarms on an individual port(s). The system reports an alarm on a port if the alarm has a severity equal to or higher than the port's threshold.

41.2 Alarm Status Screen

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

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

Figure 120 Alarm Status



The following table describes the labels in this screen.

Table 94 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 41.4 on page 253.
Alarm Port Setup	Click **Alarm Port Setup** to go to a screen where you can configure the alarm severity threshold for sending SNMP traps or sys logs for alarms on an individual port(s). See Section 41.5 on page 256.
Alarm History	Click **Alarm History** to go to a screen that displays the alarms that have been raised by the SAM1316-22, including the severity level of an alarm(s) and the date/time when the alarm occured.
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.
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.

41.3 Alarm Descriptions

This table describes alarms that the system can send.

ATUC refers to the downstream channel (for traffic going from the SAM1316-22 to the subscriber). ATUR refers to the upstream channel (for traffic coming from the

subscriber to the SAM1316-22). A “V” in the **CLEARABLE** column indicates that an administrator can remove the alarm.

Table 95 Alarm Descriptions

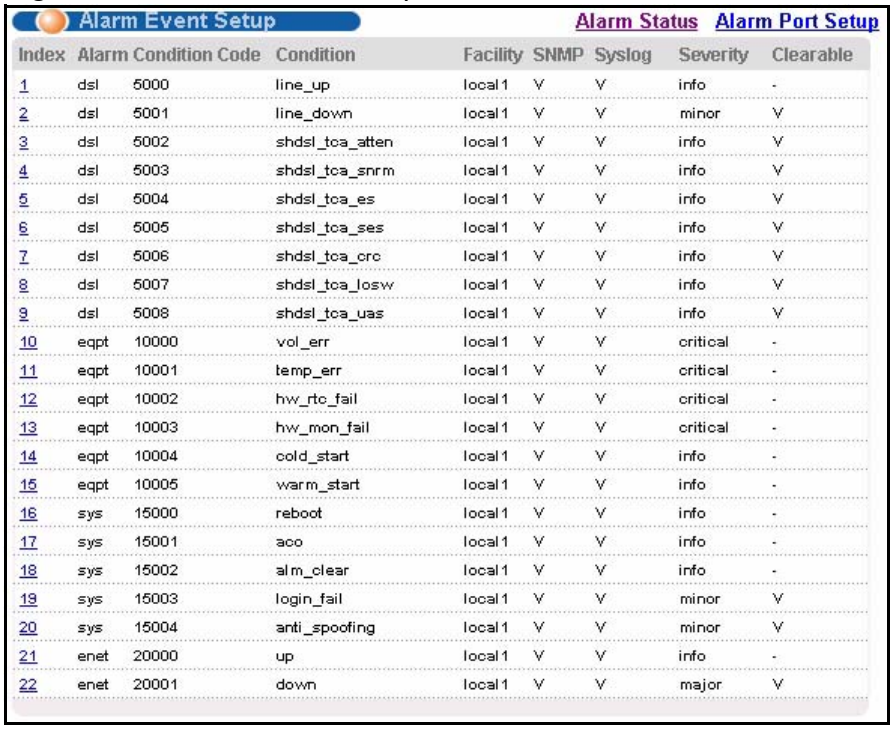
NO	ALARM	CONDITION	FACILITY	SNMP	SYSLOG	SEVERITY	CLEARABLE
1	dsl	(5000)line_up	local1	V	V	info	-
2	dsl	(5001)line_down	local1	V	V	minor	V
3	dsl	(5002)shdsl_tca_atten	local1	V	V	info	V
4	dsl	(5003)shdsl_tca_snrm	local1	V	V	info	V
5	dsl	(5004)shdsl_tca_es	local1	V	V	info	V
6	dsl	(5005)shdsl_tca_ses	local1	V	V	info	V
7	dsl	(5006)shdsl_tca_crc	local1	V	V	info	V
8	dsl	(5007)shdsl_tca_losw	local1	V	V	info	V
9	dsl	(5008)shdsl_tca_uas	local1	V	V	info	V
10	eqpt	(10000)vol_err	local1	V	V	critical	-
11	eqpt	(10001)temp_err	local1	V	V	critical	-
12	eqpt	(10002)hw_rtc_fail	local1	V	V	critical	-
13	eqpt	(10003)hw_mon_fail	local1	V	V	critical	-
14	eqpt	(10004)cold_start	local1	V	V	info	-
15	eqpt	(10005)warm_start	local1	V	V	info	-
16	sys	(15000)reboot	local1	V	V	info	-
17	sys	(15001)aco	local1	V	V	info	-
18	sys	(15002)alm_clear	local1	V	V	info	-
19	sys	(15003)login_fail	local1	V	V	minor	V
20	sys	(15004)anti_spoofing	local1	V	V	minor	V
21	enet	(20000)up	local1	V	V	info	-
22	enet	(20001)down	local1	V	V	major	V

41.4 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 121 Alarm Event Setup



Alarm Event Setup — Alarm Status | Alarm Port 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	shdsl_tca_atten	local1	V	V	info	V
4	dsl	5003	shdsl_tca_snrm	local1	V	V	info	V
5	dsl	5004	shdsl_tca_es	local1	V	V	info	V
6	dsl	5005	shdsl_tca_ses	local1	V	V	info	V
7	dsl	5006	shdsl_tca_crc	local1	V	V	info	V
8	dsl	5007	shdsl_tca_losw	local1	V	V	info	V
9	dsl	5008	shdsl_tca_uas	local1	V	V	info	V
10	eqpt	10000	vol_err	local1	V	V	critical	-
11	eqpt	10001	temp_err	local1	V	V	critical	-
12	eqpt	10002	hw_rtc_fail	local1	V	V	critical	-
13	eqpt	10003	hw_mon_fail	local1	V	V	critical	-
14	eqpt	10004	cold_start	local1	V	V	info	-
15	eqpt	10005	warm_start	local1	V	V	info	-
16	sys	15000	reboot	local1	V	V	info	-
17	sys	15001	aco	local1	V	V	info	-
18	sys	15002	alm_clear	local1	V	V	info	-
19	sys	15003	login_fail	local1	V	V	minor	V
20	sys	15004	anti_spoofing	local1	V	V	minor	V
21	enet	20000	up	local1	V	V	info	-
22	enet	20001	down	local1	V	V	major	V

The following table describes the labels in this screen.

Table 96 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 41.2 on page 251).
Alarm Port Setup	Click **Alarm Port Setup** to go to a screen where you can configure the alarm severity threshold for sending SNMP traps or sys logs for alarms on an individual port(s). See Section 41.5 on page 256.
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 41.4.1 on page 255.
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.

Table 96 Alarm Event Setup (continued)

LABEL	DESCRIPTION
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.
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.

41.4.1 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 122 Alarm Event Setup Edit

The following table describes the labels in this screen.

Table 97 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.

Table 97 Alarm Event Setup Edit (continued)

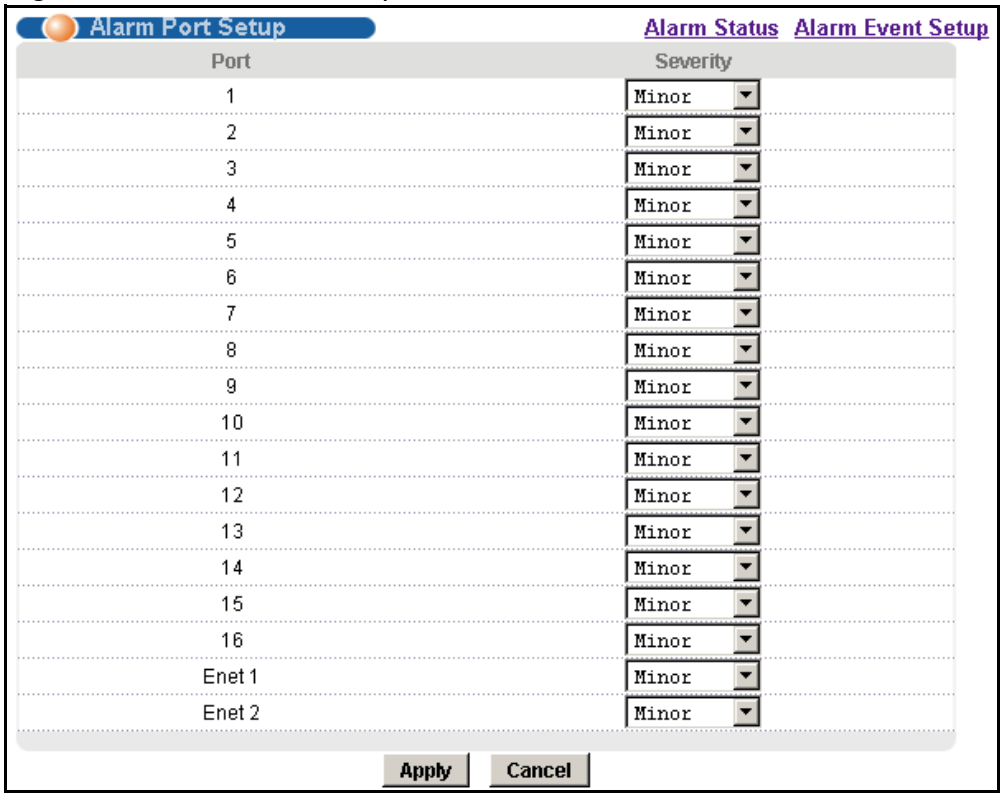
LABEL	DESCRIPTION
Facility	The log facility (local1~local7) has the device log the syslog messages to a particular file in the syslog server. Select a log facility (local1~local7) from the drop-down list box if this entry is for sending alarms to a syslog server. See your syslog program's documentation 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.
Apply	Click **Apply** to save your changes to the SAM1316-22's volatile memory. The SAM1316-22 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.

41.5 Alarm Port Setup Screen

Use this screen to set the alarm severity threshold for sending SNMP traps or sys logs in response to alarms on an individual port(s). The system sends SNMP traps or sys logs 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 123 Alarm Port Setup



The following table describes the labels in this screen.

Table 98 Alarm Port Setup

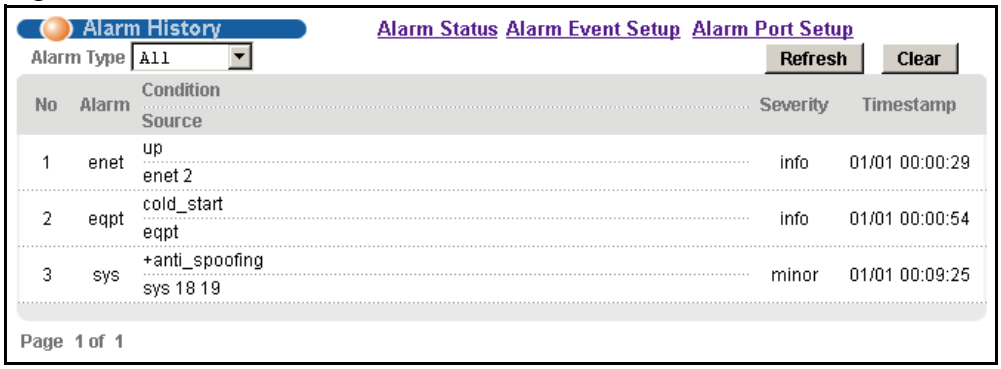
LABEL	DESCRIPTION
Alarm Status	Click **Alarm Status** to go to a screen that displays the alarms that are currently in the system (see Section 41.2 on page 251).
Alarm Event Setup	Click **Alarm Event Setup** to go to a screen where you can configure the severity level of an alarm(s) and where the system is to send the alarm(s). See Section 41.4 on page 253.
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 events on this port that trigger the SAM1316-22 to send SNMP traps or sys logs. 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 SAM1316-22's volatile memory. The SAM1316-22 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.

41.6 Alarm History Screen

This screen displays the alarms that have been raised by the SAM1316-22, including the severity level of an alarm(s) and the date/time when the alarm occured.

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

Figure 124 Alarm Status



The following table describes the labels in this screen.

Table 99 Alarm Status

LABEL	DESCRIPTION
Alarm Status	Click **Alarm Status** to go to a screen that displays the alarms that are currently in the system (see Section 41.2 on page 251).
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 41.4 on page 253.
Alarm Port Setup	Click **Alarm Port Setup** to go to a screen where you can configure the alarm severity threshold for sending SNMP traps or sys logs for alarms on an individual port(s). See Section 41.5 on page 256.
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.
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.

Table 99 Alarm Status (continued)

LABEL	DESCRIPTION
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.

42

Maintenance

This chapter explains how to use the maintenance screens.

42.1 Maintenance Screen

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

Figure 125 Maintenance

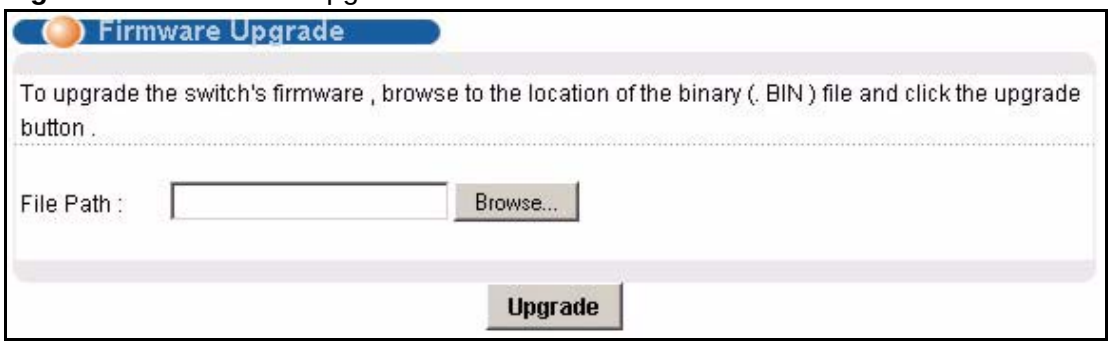
42.2 Firmware Upgrade Screen

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 126 Firmware Upgrade



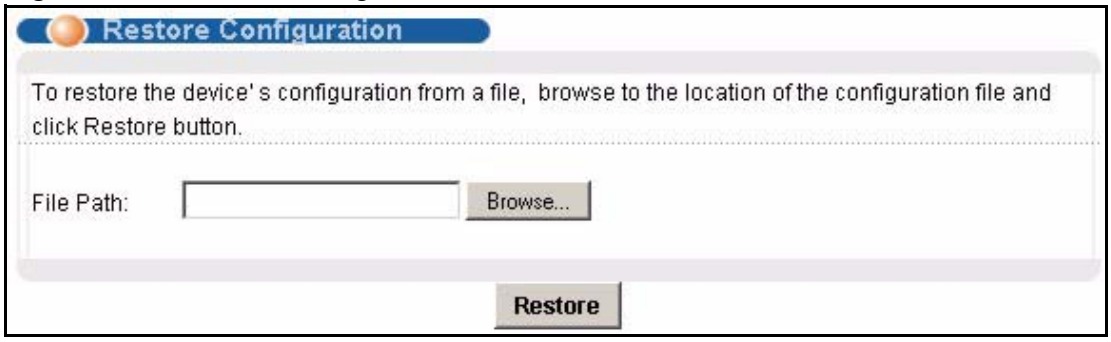
Type the path and file name of the firmware file you wish to upload to the device in the **File Path** text box or click **Browse** to locate it. After you have specified the file, click **Upgrade**.

42.3 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 127 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.

42.4 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 SAM1316-22.

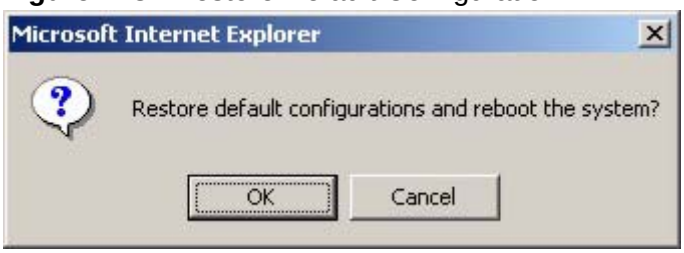
42.5 Load Factory Defaults

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 128 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 129 Restore Factory Default Settings, Reboot

42.6 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 130 Reboot System

Click **OK**. You then see the screen as shown in Figure 129 on page 264. Click **OK** again and wait for the device to restart. This takes up to two minutes. This does not affect the device's configuration.

42.7 Command Line FTP

See Chapter 57 on page 375 for how to upload or download files to or from the device using FTP commands.

43

Diagnostic

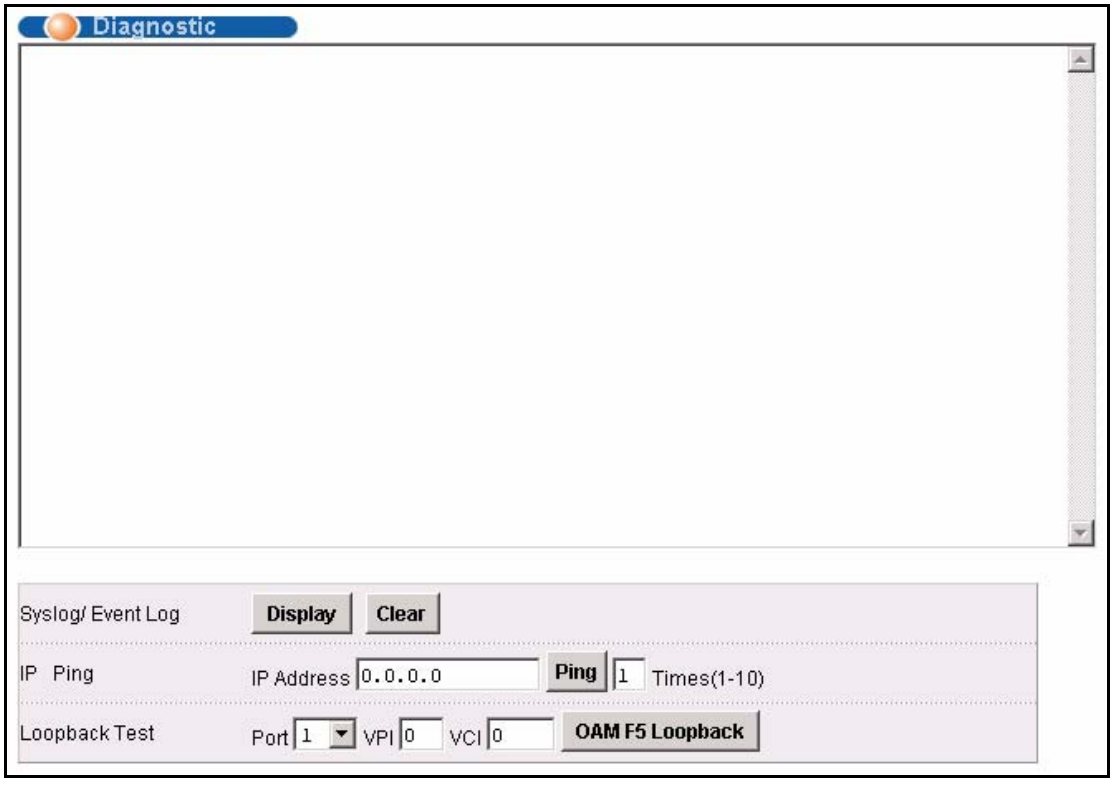
This chapter explains the Diagnostic screens.

43.1 Diagnostic Screen

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

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

Figure 131 Diagnostic



The following table describes the labels in this screen.

Table 100 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.

44

MAC Table

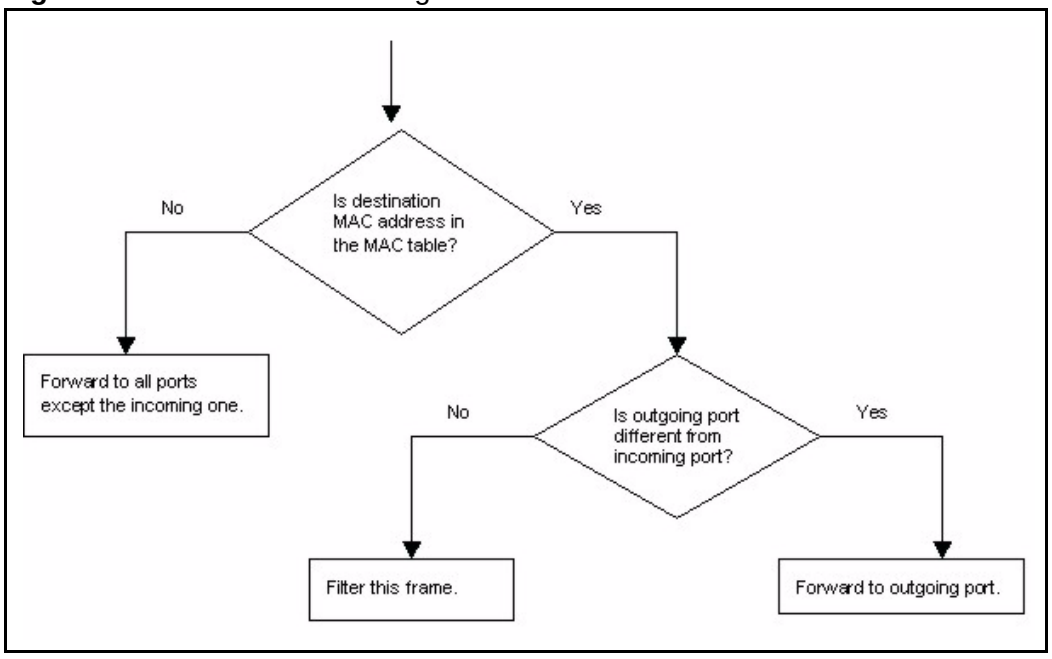
This chapter introduces the MAC Table.

44.1 Introduction to MAC Table

The MAC table lists device MAC addresses that are dynamically learned by the SAM1316-22. 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 132 MAC Table Filtering Flowchart



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

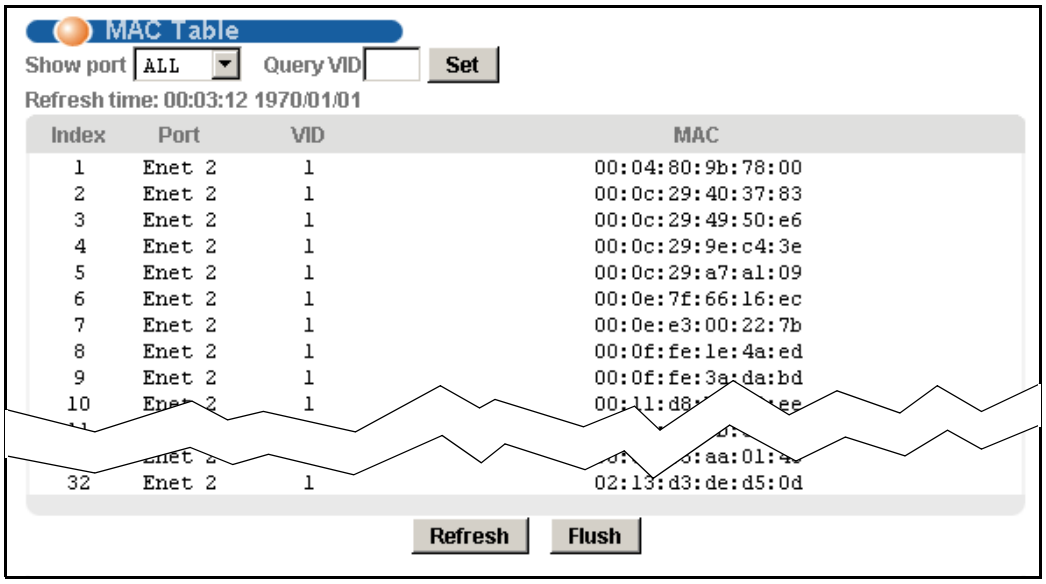
2 The device checks to see if the frame's destination MAC address matches a source MAC address already learned in the MAC table.

- 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.

44.2 MAC Table Screen

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

Figure 133 MAC Table



The following table describes the labels in this screen.

Table 101 MAC Table

LABEL	DESCRIPTION
Show port	Select a port for which to display learned MAC addresses (or display all of them).
Query VID	Enter the VID for which you want to see the MAC table.
Refresh Time	This shows the time of the MAC table update.
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.

Table 101 MAC Table (continued)

LABEL	DESCRIPTION
Index	This is the number of the MAC table entry.
Port	This is the port to which the MAC address is associated.
VID	This shows the VID 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.

45

ARP Table

This chapter describes the ARP Table.

45.1 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.

45.1.1 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.

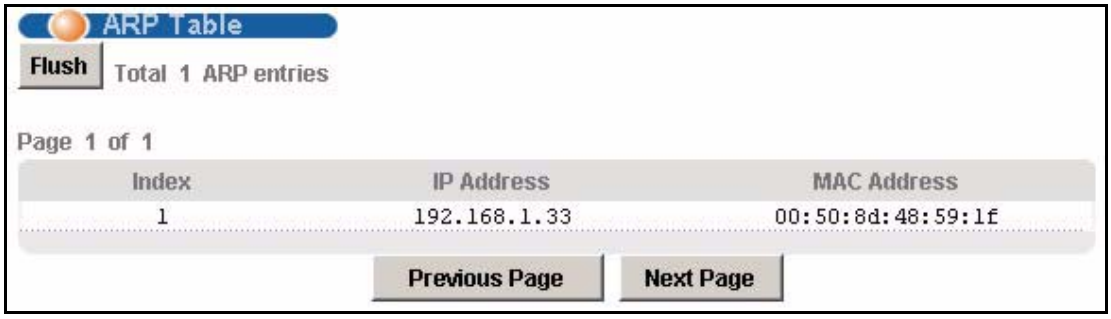
If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The device fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the device puts all ones in the target 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.

45.2 ARP Table Screen

The ARP table can hold up to 500 entries.

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

Figure 134 ARP Table



The following table describes the labels in this screen.

Table 102 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.

46

Commands

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

46.1 Command Line Interface Overview

Note: See the previous chapters for background information on features configurable by 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.

46.2 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.

46.3 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 SAM1316-22 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 SAM1316-22 returns to its default settings when it is restarted. Save your changes after each configuration session.

Nonvolatile memory refers to the SAM1316-22's storage that remains even if the SAM1316-22's power is turned off. Run-time (memory) is lost when the SAM1316-22's power is turned off.

46.4 Commands

The following table lists commands that you can use with the SAM1316-22.

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 103 Commands

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
sys				
	info show		Displays general system information.	L/L

Table 103 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	info hostname	<hostname>	Sets the system name.	M/L
	info location	<location>	Sets location information.	M/L
	info contact	<contact>	Sets contact person information.	M/L
	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
	snmp show		Displays SNMP settings.	M/L
	snmp getcommunity	<community>	Sets the SNMP GetRequest community.	H/H
	snmp setcommunity	<community>	Sets the SNMP SetRequest community.	H/H
	snmp trapcommunity	<community>	Sets the SNMP Trap community.	H/H
	snmp trusthost	<ip>	Sets the SNMP trusted host. Set 0.0.0.0 to trust all hosts.	H/H
	snmp trapdst set	<index> <ip> [<port>]	Sets the SNMP trap server and listening port. Set 0.0.0.0 to not send any SNMP traps.	H/H
	snmp trapdst del	<index>	Deletes the SNMP trap server	H/H
	server show		Displays the device's service status and port numbers.	M/L
	server enable	<telnet|ftp|web|icmp>	Turns on a service.	H/H
	server disable	<telnet|ftp|web|icmp>	Turns off a service.	H/H
	server port	<telnet|ftp|web|icmp>	Sets a port for a service.	H/H
	client show		Displays the device's secured client settings.	M/L
	client enable	<index>	Turns on a secure client.	H/H
	client disable	<index>	Turns off a secure client.	H/H
	client set	<index> <start ip> <end ip> [[telnet] [ftp] [web] [icmp] [snmp]]	Sets a secured client set: a range of IP addresses from which you can manage the device and the protocols that can be used.	H/H
	syslog show		Displays the syslog settings.	M/L
	syslog enable		Turns on the syslog logging.	H/H
	syslog disable		Turns off the syslog logging.	H/H
	syslog server	<ip>	Sets the IP address of the syslog server.	H/H

Table 103 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	stdio show		Displays Current Stdio Timeout.	L/L
	stdio set	<minute|0:no timeout>	Sets Current Stdio Timeout.	H/H
	time show		Displays the system's current time.	L/L
	time set	<hh> [<mm> [ss]]	Sets the system's time.	H/H
	date show		Displays the system's current date.	L/L
	date set	<yyyy mm dd>	Sets the system's date.	H/H
	timeserver show		Displays the system's time server.	M/L
	timeserver set	<none>	Sets the system to not use a time server.	H/H
	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	<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 sync		Retrieves the date and time from the time server.	H/H
	log show		Displays the device's logs.	M/L
	log clear		Clears the device's logs.	H/H
	wdog show		Displays the current watchdog firmware protection feature status and timer.	H/~
	wdog set	<msec|0:disable>	Sets the watchdog count. 0 turns the watchdog off.	H/~
	monitor show		Displays the hardware monitor's statistics.	L/L
	monitor enable		Turns the hardware monitor on.	H/H
	monitor disable		Turns the hardware monitor off.	H/H

Table 103 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	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=1.8v, 2=3.3v, 3=15v	H/H
	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
	user online		Displays online user info.	M/~
	user enable	<name>	Turns on the specified user name of multi-login.	H/H
	user disable	<name>	Turns off the specified user name of multi-login.	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 delete	<name>	Removes the specified user name of multi-login.	H/H
	user show		Displays the authentication mode, RADIUS server settings and user info.	M/L
	user auth	<local|radius|landr>	Set authentication method.	H/H
	user server	<ip> <port> <secret> [high|middle|low|deny]	Set remote authentication server IP address and secret	H/H
shdsl				
	show	[portlist]	Displays the DSL settings.	L/L
	enable	<portlist>	Turns on the specified DSL ports.	M/H
	disable	<portlist>	Turns off the specified DSL ports.	M/H

Table 103 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	mode set	<portlist> <mode>	Sets the Transmission Convergence Mode of the SHDSL port.	M/H
	mode show	[portlist]	Displays the Transmission Convergence Mode of the SHDSL port.	L/L
	profile show	[profile]	Displays profile contents.	L/L
	profile set	<profile> <min-rate> <max-rate> [annexa|annexb 2wire|4wire|mpair4 [lp_off | lp_on_cur [curr-margin] | lp_on_wc [worst-margin]]]	Creates a DSL line profile.	H/H
	profile delete	<profile>	Removes a DSL profile.	H/H
	profile map	<portlist> <profile>	Assigns a specific profile to a port(s).	H/H
	gbond set	<name> <portlist> <sid>	Create a bonding group	M/H
	gbond del	<name>	Delete a bonding group	M/H
	gbond show	[name]	Displays a bonding group's status	L/L
	name	<portlist> <name>	Sets the name of a port(s).	M/L
	tel	<portlist> <tel>	Records a DSL port(s) subscriber's telephone number.	M/L
	loopback	<portlist> <f5> <vpi> <vci>	Performs an OAMF5 loopback test.	H/H
	uslimit disable	<portlist> <vpi> <vci>	Disables the upstream rate-limit setting	M/H
	uslimit enable	<portlist> <vpi> <vci>	Enables the upstream rate-limit setting	M/H
	uslimit set	<portlist> <vpi> <vci> <rate>	Sets an upstream rate limit to a PVC (PVC could be pvc, ppvc, ipbpvc or tlspvc)	M/H
	uslimit show	[<portlist>[<vpi><vci>]]	Displays the current rate-limit settings of pvcs	L/L
	vcprofile show	[vcprofile]	Shows a virtual channel profile's contents.	L/L
	vcprofile set	<vcprofile> <vc|llc> <ubr|cbr> <pcr> <cdvt>	Creates a UBR or CBR virtual channel profile (with encapsulation).	H/H

Table 103 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	vcprofile set	<vcprofile> <vc|llc> <vbr(rt-vbr)|nrt-vbr> <pcr> <cdvt> <scr mcr> <bt nrm>	Creates a VBR virtual channel profile (with encapsulation).	H/H
	vcprofile delete	<vcprofile>	Removes a virtual channel profile.	H/H
	pvc show	[portlist] [<vpi> <vci>]	Displays PVC settings.	M/L
	pvc set	<portlist> <vpi> <vci> <super |vid = 1..4094 <priority>> <DS vcprofile[,US vcprofile]>	Creates or modifies a PVC setting.	H/H
	pvc delete	<portlist> <vpi> <vci>	Removes a PVC setting.	H/H
	ppvc show	[portlist] [<vpi> <vci>]	Display priority PVC settings	M/L
	ppvc set	<portlist> <vpi> <vci> <encap> <pvid> <priority>	Set priority PVC.	H/H
	ppvc member show	[portlist] [<vpi> <vci>]	Display PPVC member settings.	M/L
	ppvc member set	<portlist> <vpi> <vci> <member vpi> <member vci> <DS vcprofile[,US vcprofile]> <level>	Set PPVC member.	H/H
	ppvc member delete	<portlist> <vpi> <vci> <member vpi> <member vci>	Remove PPVC member.	H/H
	ppvc delete	<portlist> <vpi> <vci>	Remove Priority PVC.	H/H
	rpvc gateway set	<gateway ip> <vlan id> [<priority>]	Set gateway for RPVC.	H/H
	rpvc gateway delete	<gateway ip>	Delete gateway for RPVC	H/H
	rpvc gateway show		Display gateway for RPVC	M/L
	rpvc set	<portlist> <vpi> <vci> <DS vcprofile[,US vcprofile]> <ip>/<netmask> <gateway ip>	Set RPVC on a port	H/H
	rpvc delete	<portlist> <vpi> <vci>	Delete RPVC on a port	H/H

Table 103 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	rpvc show	<portlist>	Display RPVC on a port	M/L
	rpvc route set	<port number> <vpi> <vci> <ip>/ <netmask>	Set RPVC routing subnet on a port	H/H
	rpvc route delete	<port number> <vpi> <vci> <ip>/ <netmask>	Delete RPVC routing subnet on a port	H/H
	rpvc route show	<portlist>	Display RPVC routing subnet on a port	M/L
	rpvc arp agingtime show		Display RPVC ARP proxy aging time	H/H
	rpvc arp agingtime set	<sec, 10..10000|0:disabled>	Set RPVC ARP proxy aging time	M/L
	rpvc arp flush		Flush RPVC ARP proxy table	H/H
	rpvc arp show		Show RPVC ARP proxy table	M/L
	paepvc delete	<portlist> <vpi> <vci>	Delete a PPPoAoE PVC	M/H
	paepvc set	<portlist> <vpi> <vci> <DS vcprofile[,US vcprofile]> <pvid> <priority> [acname <string32>] [srvcname <string32>] [hellotime <time>]	Create/modify a PPPoAoE PVC <acname>: access concentrator name <srvcname>: service name, <time>: 0~600 in unit of second Default: acname="", srvcname="", <time>=600	M/H
	paepvc show	[<portlist> [<vpi> <vci>]]	Display PPPoAoE PVC setting by	L/L
	paepvc session	<portlist> [<vpi> <vci>]	Display PPPoAoE PVC session status	L/L
	paepvc counter	<portlist> [<vpi> <vci>]	Display PPPoAoE PVC counter	L/L
	tlspvc delete	<portlist> <vpi> <vci>	Delete a TLS PVC	M/H
	tlspvc set	<portlist> <vpi> <vci> <DS vcprofile[,US vcprofile]> <pvid> <priority>	Create/modify a TLS PVC <profile>: <vid>: s-tag VLAN id <priority>: priority for s-tag	M/H
	tlspvc show	[<portlist> [<vpi> <vci>]]	Display TLS PVC setting by 'port'	L/L
	queuemap show		Displays the xDSL priority level to physical queue mapping.	M/L

Table 103 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	queuemap set	<priority> <queue>	Set the xDSL priority level to physical queue mapping.	H/H
	alarmprofile show	[profile]	Displays alarm profiles and their settings.	L/L
	alarmprofile set	<profile> [atten <atten>] [snrmgn <snrmgn>] [es <es>] [ses <ses>] [crc <crc>] [losws <losws>] [uas <uas>]	Configures an alarm profile.	H/H
	alarmprofile delete	<profile>	Removes an alarm profile.	H/H
	alarmprofile map	<portlist> <profile> <span|stuc|stur|*>	Maps specified DSL ports to an alarm profile.	H/H
	alarmprofile showmap	[port number]	Displays alarm profile to DSL port mapping.	L/L
	alarmprofile showport	<port number>	Displays which alarm profile parameters are mapped to a DSL port.	L/~
	dsbcast enable	<port number> <vlanlist>	Enable downstream broadcast on xDSL port	H/H
	dsbcast disable	<port number> <vlanlist>	Disable downstream broadcast on xDSL port	H/H
	dsbcast show	<portlist>	Show downstream broadcast on xDSL port	M/L
	reset	<portlist>	Reset xDSL port	H/H
	pmms show	<portlist>	Displays the PMMS mode for the specified port(s).	L/L
	pmms set	<portlist> <normal|forced>	Sets the PMMS mode	H/H
	pbo show	<portlist>	Displays the PMMS mode for the specified port(s).	M/L
	pbo set	<portlist> <normal_epl|forced_epl|forced_no_epl <value>>	Sets the PBO(Power back off) mode	H/H
alarm				
	clear		Clear current alarm	M/L
	cutoff		Alarm cutoff	M/~
	xedit	<alarm>|all <cond>|<condcode> <severity> <fac> <target>[,<target>] [clearable]	Edit system alarm table	M/L

Table 103 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	history clear	<alarm>|all <condition>|all	Clear history alarm	M/~
	history clear	<severity>	Clear history alarm	M/~
	history show	[<severity>|all] [<alarm>|all] [<condition>|all] [<sdate>|all] [<edate>|all] [for|rev] [detail]	Display history alarm	L/~
	show	[<severity>|all] [<alarm>|all] [<condition>|all] [<sdate>|all] [<edate>|all] [for|rev] [detail]	Display history alarm	L/L
	port show		Display xDSL port threshold of severity which will issue an alarm	L/L
	port set	<all|enet1|enet2|port> <severity>	Set xDSL port threshold of severity which will send SNMP traps and sys logs.	M/L
	tablelist	[<alarm>|all] [<severity>|all] [<fac>|all] [<target>[,<target>]] [<condition>|all]	Display system alarm table	L/L
switch				
	igmpsnoop show		Displays the IGMP snooping setting.	M/L
	igmpsnoop enable	<proxy|snooping>	Sets IGMP snooping mode.	H/H
	igmpsnoop disable		Turns off IGMP snooping.	H/H
	igmpsnoop bandwidth default	<bandwidth>	Set default bandwidth for multicast IP channels	M/H
	igmpsnoop bandwidth delete	<index>	Delete an entry of bandwidth budget setting specified in <index> field.	M/H
	igmpsnoop bandwidth port disable	<portlist>	Disable bandwidth budget control for a port	M/H
	igmpsnoop bandwidth port enable	<portlist>	Enable bandwidth budget control for a port	L/H
	igmpsnoop bandwidth port set	<portlist> <bandwidth>	Set bandwidth threshold for a port <bandwidth>: 1..100,000, in unit of kbps	M/H

Table 103 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	igmpsnoop bandwidth port show	<portlist>	Show bandwidth control setting for a port	L/L
	igmpsnoop bandwidth set	<index> <start-mcast-ip> <end-mcast-ip> <bandwidth>	Set bandwidth budget for a range of multicast IP channels specified in <index> field. <index>: 1~96 <start-mcast-ip>: <ip>, start multicast IP address <end-mcast-ip>: <ip>, end multicast IP address	M/H
	igmpsnoop bandwidth show		Show bandwidth budget for a range of multicast IP channels	L/L
	igmpsnoop igmpcount disable	<portlist>	Disable IGMP count limiting to subscriber port	H/H
	igmpsnoop igmpcount enable	<portlist>	Enable IGMP count limiting to subscriber port	H/H
	igmpsnoop igmpcount set	<portlist> <count>	Set IGMP count limiting number to subscriber port	H/H
	igmpsnoop igmpcount show	[portlist]	Display IGMP count limiting setting status on the specified slot	M/L
	igmpsnoop mvlan set	<vid> <portlist>:<F<T|U>|X> [<portlist>:<F<T|U>|X> ...] [name]	Configures a MVLAN entry.	H/H
	igmpsnoop mvlan show	<vlanlist>	Show multicast VLANs, Include group information	M/L
	igmpsnoop mvlan disable	<vid>	Turns off a MVLAN entry.	H/H
	igmpsnoop mvlan enable	<vid>	Turns on a MVLAN entry.	H/H
	igmpsnoop mvlan delete	<vlanlist>	Removes a MVLAN entry.	H/H
	igmpsnoop mvlan group set	<vid> <index> <start_mcast_ip> <end_mcast_ip>	Create a multicast to VLAN translation entry. up to 16 entries <index>: 1~16, Note: IP address in each entry should be disjointed	H/H
	igmpsnoop mvlan group delete	<vid> <index>	Delete a multicast to VLAN translation entry.	H/H

Table 103 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	igmpsnoop mvlan group show	<vlanlist>	Show a multicast to VLAN translation entry.	M/L
	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
	igmpfilter set	<portlist> <name>	Sets a DSL port(s) to use an IGMP filter profile.	H/H
	igmpfilter show	[portlist]	Displays which IGMP filter profile a DSL port(s) is using.	M/L
	igmpfilter profile set	<name> <index> <startip> <endip>	Configures an IGMP filter profile.	H/H
	igmpfilter profile delete	<name>	Removes an IGMP filter profile.	H/H
	igmpfilter profile show	[name]	Displays an IGMP filter profile's settings.	M/L
	queuemap show		Displays the system's priority level to ENET queue mapping.	M/L
	queuemap set	<priority> <queue>	Maps a priority level to a ENET queue.	H/H
	garptimer show		Display the system's garp settings.	M/L
	garptimer join	<join msec>	Set system's garp join time.	H/H
	garptimer leave	<leave msec>	Set system's garp leave time.	H/H
	garptimer leaveall	<leaveall msec>	Set system's garp leaveall time.	H/H
	rstp show		Display the system's rstp settings.	M/L
	rstp enable		Turn system's rstp on.	H/H
	rstp disable		Turn system's rstp off.	H/H
	rstp priority	<priority>	Set system rstp's priority.	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

Table 103 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	rstp fwdelay	<fwdelay sec>	Set system rstp's forward delay time.	H/H
	rstp port show		Display enet port rstp status.	M/L
	rstp port enable	<portlist>	Set enet port to enable rstp.	H/H
	rstp port disable	<portlist>	Set enet port to disable rstp.	H/H
	rstp port priority	<portlist> <priority>	Set enet port's rstp priority.	H/H
	rstp port pathcost	<portlist> <pathcost>	Set enet port's rstp pathcost.	H/H
	dhcprelay enable	<vid>|all	Turns on DHCP relay for the specified VLAN(s).	H/H
	dhcprelay disable	<vid>|all	Turns off DHCP relay for the specified VLAN(s).	H/H
	dhcprelay opt82sub2 disable	<vid>|all	Turns off option 82 sub-option 2 for the specified VLAN(s).	M/H
	dhcprelay opt82sub2 enable	<vid>|all	Turns on option 82 sub-option 2 for the specified VLAN(s).	M/H
	dhcprelay opt82sub2 set	<vid>|all <relay info>	Adds the specified information for sub-option 2.	M/H
	dhcprelay option82 disable	<vid>|all	Turns off the DHCP relay agent information (Option 82) feature for the specified VLAN(s).	M/H
	dhcprelay option82 enable	<vid>|all	Turns on the DHCP relay agent information (Option 82) feature for the specified VLAN(s).	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

Table 103 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	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
	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 SAM1316-22 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

Table 103 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	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
	acl profile delete	<name>	delete an acl profile	M/H
	acl profile set	<name> <rule> <action>	Create/modify a acl profile. See Section 61.1.1 on page 429 for details.	M/H
	acl profile show	[<name>]	Display an acl profile	L/L
	acl profile showmap	<name>	Display acl profile reference	L/L
	acl delete	<portlist> <vpi> <vci> <profile>	Remove an acl profile from PVC <profile>: string32 up to 8 profiles if only one PVC has profiles	M/H
	acl set	<portlist> <vpi> <vci> <profile>	Apply an acl profile to a PVC Max. 8 profiles per port	M/H
	acl show	[portlist] [<vpi> <vci>]	Show acl profile setting for a PVC	L/L
	dhcpsnoop disable	< portlist >	Disable ip spoofing for a port	M/H
	dhcpsnoop enable	< portlist >	Enable ip spoofing for a port	M/H
	dhcpsnoop flush	< portlist >	Flush DHCP snooping table for a port	M/H
	dhcpsnoop show	<portlist>	Display DHCP snooping result on a port	L/L
	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 lan2lan show		This command displays whether LAN to LAN DHCP services are enabled or disabled.	L/~
	dhcpsnoop lan2lan disable		This command disables LAN to LAN DHCP services.	M/~

Table 103 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	dhcpsnoop lan2lan enable		This command enables LAN to LAN DHCP services.	M/~
	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
	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 SAM1316-22 to not add line information to PPPoE discover packets.	H/H
	poeagent enable	<<vid>|all>	Sets the SAM1316-22 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

Table 103 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	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
	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
	dscp show	[portlist]	Displaying per port DSCP setting	L/L
	dscp enable	< portlist >	Enable DSL/ENET ports to use DSCP mapping	M/H
	dscp disable	< portlist >	Disable DSL/ENET ports to use DSCP mapping	M/H
	dscp map show		Displaying the DSCP code to 802.1p mapping table	L/L
	dscp map set	<srccp> <mappri> <srccp>: source code point, 0~63, example: 1,3~5,10~15 <mappri> : mapping priority, 0~7	Setting the DSCP code to 802.1p mapping table	M/H

Table 103 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	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
	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 SAM1316-22 to not add line information to PPPoE discover packets.	H/H
	poeagent enable	<<vid>|all>	Sets the SAM1316-22 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

Table 103 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	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
	vlan show	<vlanlist>	Displays VLAN settings.	M/L
	vlan portshow	[portlist]	Displays the port(s) VLAN settings.	M/L
	vlan set	<vid> <portlist>:<F<T|U> |X|N> [<portlist>: <F<T|U>|X|N> ...] [name]	Configures a VLAN entry.	H/H
	vlan enable	<vid>	Turns on a VLAN entry.	H/H
	vlan disable	<vid>	Turns off a VLAN entry.	H/H
	vlan delete	<vlanlist>	Removes a VLAN entry.	H/H
	vlan pvid	<portlist> <pvid>	Sets the PVID (Port VLAN ID) assigned to untagged frames or priority frames (0 VID) received on this port(s).	H/H
	vlan priority	<portlist> <priority>	Sets a port's default IEEE 802.1p priority.	H/H
	vlan gvrp	<portlist> <enable|disable>	Set the port(s) to enable or disable gvrp.	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

Table 103 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	vlan cpu show		Displays the VLAN ID of the Management VLAN.	M/~
	vlan cpu set	<vid>	Sets the VLAN ID of the Management VLAN.	H/~
	mac flush		Clears learned MAC addresses from the forwarding table.	H/H
	mac agingtime show		Displays the MAC aging out time period.	M/L
	mac agingtime set	<sec, 10..10000|0:disabled>	Sets the MAC aging out time period.	H/H
	mac antispoofing show		Show the MAC antispoofing status	M/L
	mac antispoofing enable		Turns on the MAC antispoofing	H/H
	mac antispoofing disable		Turns off the MAC antispoofing	H/H
	mac count show	[portlist]	Displays the system's current MAC address count settings.	M/L
	mac count enable	<portlist>	Turns on the MAC address count filter for a DSL port(s).	H/H
	mac count disable	<portlist>	Turns off the MAC address count filter for a DSL port(s).	H/H
	mac count set	<portlist> <count>	Sets the MAC address count filter for a DSL port(s).	H/H
	mac filter show	[portlist]	Displays MAC filter settings.	M/L
	mac filter enable	[portlist]	Turns on the MAC filter.	H/H
	mac filter disable	[portlist]	Turns off 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 a DSL port(s).	H/H
	mac filter delete	<port> <mac> [<mac> <mac> ...]	Removes a MAC filter MAC entry on a DSL port(s).	H/H
	pktfilter show	[portlist]	Display packet filter settings.	M/L
	pktfilter set	set <portlist> <filter>	Set packet filter for port	H/H
	pktfilter pppoeonly	pppoeonly <portlist>	Set packet filter to PPPoE only for port.	H/H
	dot1x show	[portlist]	Display dot1x settings.	M/L
	dot1x enable		Turn on dot1x.	H/H
	dot1x disable		Turn off dot1x.	H/H
	dot1x auth	<profile|radius>	Set authentication method to profile or radius.	H/H

Table 103 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	dot1x port enable	<portlist>	Turn on dot1x on port.	H/H
	dot1x port disable	<portlist>	Turn off dot1x on port.	H/H
	dot1x port control	<portlist> <auto|auth|unauth>	Set port authentication status.	H/H
	dot1x port reauth	<portlist> <on|off>	Turn on or turn off port to do reauthentication.	H/H
	dot1x port peroid	<portlist> <period>	Set port reauth period.	H/H
	dot1x radius show		Display radius server settings.	M/L
	dot1x radius ip	<ip>	Set Radius server IP.	H/H
	dot1x radius port	<port>	Set Radius server port.	H/H
	dot1x radius secret	<secret>	Set Radius server secret.	H/H
	dot1x profile show		Display accounts for profile mode.	M/L
	dot1x profile set	<name> <password>	Set account and password for profile mode.	H/H
	dot1x profile delete	<name>	Remove account for profile mode.	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
	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 enable	<portlist>	Turns on the specified Ethernet port(s).	H/H
	enet disable	<portlist>	Turns off the specified Ethernet port(s).	H/H
	enet reset	<portlist>	Reset the ENET interface	H/H
	smcast show		Display all MAC addresses joined to DSL ports.	M/L
	smcast set	<dsl_port> <mac> <join|leave>	Use join/leave to add/ remove multicast MAC addresses on specified DSL ports, a range of DSL ports or all DSL ports. MAC example: 01005E010203	H/H

Table 103 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	smcast delete	<mac>	Removes a static multicast filter entry by deleting the associated MAC address.	H/H
	isolation show		Displays the subscriber isolation feature's current setting.	M/L
	isolation enable		Turns the subscriber isolation feature on.	H/H
	isolation disable		Turns the subscriber isolation feature off.	H/H
	isolation daisychain		Set switch mode to daisychain mode	H/H
	isolation standalone		Set 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
ip				
	show		Displays the Management IP address settings.	M/L
	arp show		Displays the device's IP Address Resolution Protocol(ARP) table.	M/L
	arp flush		Clears the device's IP Address Resolution Protocol(ARP) table.	H/H
	set	<ip>[/netmask]	Sets the Management IP address and subnet mask.	H/H
	gateway	<gateway ip>	Sets the IP address of the device's default gateway.	H/H
	route show		Displays the routing table.	M/L
	route set	<dst ip>[/netmask] <gateway ip> [metric] <name>	Adds a routing table entry.	H/H
	route set	default <gateway ip> <metric>	Sets the device's default route.	H/H
	route delete	<dst ip>[/netmask]	Removes a routing table entry.	H/H
	route flush		Clears the routing table.	H/~
	ping	<ip> [count]	Pings a remote host.	M/L
statistics				
	monitor		Displays hardware monitor status.	M/L

Table 103 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	shdsl show	[portlist]	Displays DSL port connection status.	M/L
	shdsl linedata	<portlist>	Displays the line data load per symbol (tone).	M/L
	shdsl lineinfo	<portlist>	Displays the info of the specified DSL ports.	M/L
	shdsl lineperf	<portlist>	Displays the performance statistics of the specified DSL port.	M/L
	shdsl linerate	<portlist>	Displays the line rate.	M/L
	shdsl 15mperf	<portlist> [count <0..96>]	Displays line performance statistics for the current and previous 15-minute periods.	M/L
	shdsl 1dayperf	<portlist>	Displays line performance statistics for the current and previous 24 hours.	M/L
	igmpsnoop info	[clear]	Display protocol packets counters & number of learned groups	L/L
	igmpsnoop group	[<vid> [<mcast_ip>]]	Display IGMP learned group member information	L/L
	igmpsnoop port info	[<portlist> [clear]]	Display received protocol packets counters, number of joined groups.	L/L
	igmpsnoop port group	<portlist>	Display joined groups in this port	L/L
	dhcp counter	[<portlist> [clear]]	Display DHCP statistics for a port	L/L
	dhcp snoop	<portlist>	Display snooping	L/L
	rmon	Stats|history <giga-port>	Display uplink/subtending link RMON information	M/L
	rstp			M/L
	vlan		Displays current VLANs.	M/L
	mac		Displays current MAC address forwarding table.	M/L
	port	<portlist> [<vpi> <vci>] [clear]	This command displays and/ or erases port statistics.	M/L
	dot1x	[portlist]		M/L
	enet		Displays Ethernet port settings and statistics.	M/L
	ip		Displays a Management port's status and performance data.	M/~
config				
	show	<sys|sw|ip|stat|all> [nopause]	Displays the device's configuration.	M/L

Table 103 Commands (continued)

CLASS	COMMAND	PARAMETERS	DESCRIPTION	P
	save		Saves the current configuration.	H/H
	restore		Reloads the factory default configuration.	H/H
exit			Ends the console or telnet session.	L/L

47

Command Examples

This chapter gives some examples of commands.

47.1 Command Examples Overview

These are commands that you may use frequently in configuring and maintaining your SAM1316-22. See Chapter 50 on page 323 for commands that deal with the IEEE 802.1Q Tagged VLAN.

47.2 Sys Commands

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

47.2.1 Log Show Command

Syntax:

```
ras> sys log show
```

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

Figure 135 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!
```

47.2.2 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.

47.2.3 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 136 Info Show Example

```
ras> sys info show
        Hostname:
        Location:
         Contact:
           Model: SAM1316-22
   ZyNOS version: V3.53(BVE.0) | 04/23/2010
        F/W size: 2396478
     MAC address: 00:13:49:00:00:34
  System up time:   3(days) :   23:12:13
Bootbase version: VAIO1.01 | 04/23/2010
  F/W build date: Apr 22 2010 15:32:13
  Driver version: 0.3.7.5
DSP code version: 1.1-1.6.1__001
Hardware version:
   Serial number:
```

47.3 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.

47.3.1 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 137 Isolation Show Example

```
ras> switch isolation show
system isolation: enabled
system switch mode : stand alone
```

47.3.2 Isolation Enable Command

Syntax:

```
ras> switch isolation enable
```

This command turns on the subscriber isolation feature.

47.3.3 Isolation Disable Command

Syntax:

```
ras> switch isolation disable
```

This command turns off the subscriber isolation feature.

47.3.4 Switch Isolation VLAN Delete Command

Syntax:

`switch isolation vlan delete <vid>`

where

`<vid>` = The VLAN ID [1 – 4094].

This command turns off per-VLAN isolation for the specified VLAN.

Note: Per-VLAN isolation only works when the regular switch isolation feature is disabled (see Section 47.3.3 on page 299).

The following example turns off per-VLAN isolation for VLAN 5.

```
ras> switch isolation vlan delete 5
ras> switch isolation show
port isolation :disabled
isolated vlan list:
----
938
```

47.3.5 Switch Isolation VLAN Set Command

Syntax:

```
switch isolation vlan set <vid>
```

where

```
<vid>  =  The VLAN ID [1 – 4094].
```

This command turns on per-VLAN isolation for the specified VLAN.

Note: Per-VLAN isolation only works when the regular switch isolation feature is disabled (see Section 47.3.3 on page 299).

The following example turns on per-VLAN isolation for VLAN 5.

```
ras> switch isolation vlan set 5
ras> switch isolation show
port isolation :disabled
isolated vlan list:
----
5
938
```

47.4 Statistics Monitor Command

Syntax:

```
ras> statistics monitor
```

This command shows the current hardware status.

An example is shown next.

Figure 138 Statistics Monitor Command Example

```
ras> statistics monitor
Hardware monitor status: enabled
      nominal limit(hi) limit(lo)   current      min      max      avg status
      ------- --------- --------- --------- -------- -------- -------- ----
----
v1(v)   1.800     1.944     1.656     1.740    1.740    1.754    1.740 Normal
v2(v)   3.300     3.564     3.036     3.334    3.334    3.334    3.334 Normal
v3(v)  15.000    16.200    13.800    14.922   14.922   14.922   14.922 Normal

      limit(hi) limit(lo)   current       min       max       avg status
      --------- --------- --------- --------- --------- --------- --------
t1(c)    97.000   -10.000    42.000    38.000    42.000    39.000 Normal
t2(c)    97.000   -10.000    38.000    34.000    38.000    35.000 Normal
t3(c)    97.000   -10.000    40.000    36.000    40.000    37.000 Normal
```

47.5 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 <1,5,6~8,enet1>.
`<vpi> <vci>`	=	The VPI and VCI of an individual PVC.
`[clear]`	=	Use `clear` to have the SAM1316-22 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 139 Statistics Port Command Example

```
ras> statistics port 1
[xdsl 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 59 for details on the other port statistics fields.

48

Alarm Commands

This chapter describes the alarm management commands.

48.1 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.

48.2 General Alarm Command Parameters

The following table describes commonly used alarm command parameter notation.

Table 104 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.

48.3 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 140 Alarm Show Command Example

```
ras> alarm show

[current alarm list]
    no alarm   condition            severity timestamp      source
------ ------  -------------------- -------- -------------- -------
     1 dsl    +line_down            minor    01/04 17:57:49 1
```

48.4 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 141 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 ================================
```

48.5 Alarm Port Set Command

Syntax:

```
ras> alarm port set <all|enet1|enet2|port> <severity>
```

where

<all|enet1|enet2|port>	= Ports on the SAM1316-22.

This command sets the alarm severity threshold for sending SNMP traps or sys logs in response to alarms on an individual port(s). The system sends SNMP traps or sys logs if the alarm has a severity equal to or higher than the port’s threshold.

The following example has the SAM1316-22 only record critical alarms on DSL port 7.

Figure 142 Alarm Port Set Command Example

```
ras> alarm port set 7 critical
```

48.6 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 143 Alarm Tablelist 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)shdsl_tca_atten      local1    V     V    info       V
  4   dsl  ( 5003)shdsl_tca_snrm       local1    V     V    info       V
  5   dsl  ( 5004)shdsl_tca_es         local1    V     V    info       V
  6   dsl  ( 5005)shdsl_tca_ses        local1    V     V    info       V
  7   dsl  ( 5006)shdsl_tca_crc        local1    V     V    info       V
  8   dsl  ( 5007)shdsl_tca_losw       local1    V     V    info       V
  9   dsl  ( 5008)shdsl_tca_uas        local1    V     V    info       V
 10  eqpt  (10000)vol_err              local1    V     V    critical   -
 11  eqpt  (10001)temp_err             local1    V     V    critical   -
 12  eqpt  (10002)hw_rtc_fail          local1    V     V    critical   -
 13  eqpt  (10003)hw_mon_fail          local1    V     V    critical   -
 14  eqpt  (10004)cold_start           local1    V     V    info       -
 15  eqpt  (10005)warm_start           local1    V     V    info       -
 16   sys  (15000)reboot               local1    V     V    info       -
 17   sys  (15001)aco                  local1    V     V    info       -
 18   sys  (15002)alm_clear            local1    V     V    info       -
 19   sys  (15003)login_fail           local1    V     V    minor      V

    Press any key to continue, 'e' to exit, 'n' for nopause
```

48.7 Log Format

The following table describes the columns in the list.

Table 105 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.
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.

48.8 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 major and critical level alarms.

Figure 144 Alarm History Show Command Example

```
ras> alarm history show major
    no alarm   condition            severity timestamp      source
------ ------  -------------------- -------- -------------- -------
     1 enet   +down                 major    01/01 00:00:08 enet 1
     2 enet   -down                 major    01/01 00:00:11 enet 1
```

48.9 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 145 Alarm History Clear Command Example

```
ras> alarm history clear minor
```

48.10 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 146 Alarm Xedit Command Example

```
ras> alarm xedit sys all major local3 syslog
```

48.11 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.

48.12 Alarm Clear Command

Syntax:

```
ras> alarm clear
```

This command erases the clearable alarm entries.

49

DHCP Commands

This chapter describes how to use the DHCP Relay and DHCP Snoop commands.

49.1 DHCP Relay Commands

Use these commands to configure the DHCP relay feature. See Chapter 26 on page 183 for background information on DHCP relay.

49.1.1 Show Command

Syntax:

```
ras> switch dhcprelay show
```

This command displays whether or not the DHCP relay feature is activated, which relay mode the SAM1316-22 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 147 Show Command Example

```
ras> switch dhcprelay show

 vid enable relay mode primary-server     secondary-server
---- ------ ---------- ------------------ ------------------
   0   -       auto    0.0.0.0            0.0.0.0

     option82                                 option82
 vid optmode sub-opt1 info (Circuit ID)       sub-opt2 info (Remote ID)
---- ------- -------- ---------------------- -------- ----------------------
   0   tr101    -                                 -
```

49.1.2 Enable Command

Syntax:

```
ras> switch dhcprelay enable <vid>|all
```

where

<*vid*> = ID of the VLAN to which this setting applies.

This command turns on the DHCP relay feature for the specified VLAN(s).

The following example enables DHCP relay on VLAN 1.

```
ras> switch dhcprelay enable 1
```

49.1.3 Disable Command

Syntax:

```
ras> switch dhcprelay disable <vid>|all
```

where

<*vid*> = ID of the VLAN to which this setting applies.

This command turns off the DHCP relay feature for the specified VLAN(s).

The following example turns off DHCP relay on VLAN 1.

```
ras> switch dhcprelay disable 1
```

49.1.4 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 SAM1316-22

routes DHCP requests to the specified DHCP server(s) according to the `relaymode`. See Section 49.1.8 on page 314.

Use VLAN ID 0 to set up the default DHCP server(s) for all non-listed VLAN.

49.1.5 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.

49.1.6 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 SAM1316-22 should relay DHCP requests for the selected VLAN.

49.1.7 Optionmode Command

Syntax:

```
ras> switch dhcprelay optionmode [<vid>|all] private|tr101
```

where

<*vid*> = ID of the VLAN to which this setting applies.

This command selects the method (Private or TR-101) in which DHCP relay information is sent and whether or not the VLAN ID is transmitted within the packet on the specified VLAN.

The following example sets the DHCP relay feature on VLAN 10 to use TR-101 encoding, and to transmit the VLAN ID.

```
ras> acl dhcprelay82 optionmode 10 tr101 vid on
```

49.1.8 Relaymode Command

Syntax:

```
ras> switch dhcprelay relaymode <vid>|all <mode>
```

where

<vid> = The ID of the VLAN served by the specified DHCP server(s).

<mode> = relay process mode; it controls to which DHCP server(s) the SAM1316-22 relays DHCP requests.

auto - the SAM1316-22 relays DHCP requests to the active server for each VLAN

both - the SAM1316-22 relays DHCP requests to the primary and secondary server for each VLAN, regardless of which one is active

This command controls how the SAM1316-22 routes DHCP requests for the specified VLAN. The SAM1316-22 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.

49.2 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.

49.2.1 Option 82 Sub-option 1 Enable Command

Syntax:

```
ras> switch dhcprelay option82 enable <vid>|all
```

where

<*vid*> = ID of the VLAN to which this setting applies.

This command turns on the DHCP relay agent information (Option 82 Sub-option 1) feature for the specified VLAN.

49.2.2 Option 82 Sub-option 1 Disable Command

Syntax:

```
ras> switch dhcprelay option82 disable <vid>|all
```

where

<*vid*> = ID of the VLAN to which this setting applies.

This command turns off the DHCP relay agent information (Option 82, Sub-option 1) feature for the specified VLAN.

49.2.3 Option 82 Sub-option 1 Set Command

Syntax:

```
ras> switch dhcprelay option82 set <vid>|all [<relay info>]
```

where

<vid> = The ID of the VLAN served by the specified DHCP server(s).

`[<relay info>]` = Up to 23 ASCII characters of additional information for the SAM1316-22 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 SAM1316-22 or the ISP.

This command adds the specified information for the relay agent for the specified VLAN.

49.3 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.

49.3.1 Option 82 Sub-option 2 Enable Command

Syntax:

```
ras> switch dhcprelay opt82sub2 enable <vid>|all
```

where

<vid> = ID of the VLAN to which this setting applies.

This command turns on the DHCP relay agent information (Option 82, Sub-option 2) feature for the specified VLAN.

49.3.2 Option 82 Sub-option 2 Disable Command

Syntax:

```
ras> switch dhcprelay opt82sub2 disable <vid>|all
```

where

<vid> = ID of the VLAN to which this setting applies.

This command turns off the DHCP relay agent information (Option 82, Sub-option 2) feature for the specified VLAN.

49.3.3 Option 82 Sub-option 2 Set Command

Syntax:

```
ras> switch dhcprelay opt82sub2 set <vid>|all [<relay info>]
```

where

<vid>	=	The ID of the VLAN served by the specified DHCP server(s).
[<relay info>]	=	Up to 23 ASCII characters of additional information for the SAM1316-22 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 SAM1316-22 or the ISP.

This command adds the specified information for the relay agent for the specified VLAN.

49.4 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.

49.4.1 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 <1,5,6~8,enet1>.

This command activates the DHCP snooping feature on the specified port(s). The following example enables DHCP snooping on port 1.

Figure 148 DHCP Snoop Enable Command Example

```
ras> switch dhcpsnoop enable 1
```

49.4.2 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 <1,5,6~8,enet1>.

This command disables the DHCP snooping feature on the specified port(s).

49.4.3 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 <1,5,6~8,enet1>.

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.

49.4.4 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 <1,5,6~8,enet1>.

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 149 DHCP Snoop Show Command Example

```
ras> switch dhcpsnoop show 1~5
 port  enable
----- --------
    1  V
    2  -
    3  -
    4  -
    5  -
```

49.4.5 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 <1,5,6~8,enet1>.

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 150 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.

49.4.6 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 <1,5,6~8,enet1>.

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 151 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.

49.4.7 DHCP Snoop Pool Set Command

Syntax:

```
ras> switch dhcpsnoop pool set <slot-port> <ip-address>
```

This command adds a static IP address to the DHCP snooping table on a port.

The following example adds two static IP addresses (192.168.1.10 and 192.168.1.11) to the DHCP snooping table on port 10 of the line card in slot 2.

```
ras> acl dhcpsnoop pool set 2-10 192.168.1.10
ras> acl dhcpsnoop pool set 2-10 192.168.1.11
ras> acl dhcpsnoop show 2-10
 port enable static ip pool
----- ------ ------------------------------------------------
 2-10   -    192.168.1.10    192.168.1.11
ras>
```

49.4.8 DHCP Snoop Pool Delete Command

Syntax:

```
ras> switch dhcpsnoop pool delete <slot-port> <ip-address>
```

This command removes a static IP address from the DHCP snooping table of a port on the specified line card. The following example removes the static IP address of 192.168.1.11 from the port 10 on the line card in slot 2.

```
ras> acl dhcpsnoop pool delete 2-10 192.168.1.11
ras> acl dhcpsnoop show 2-10
 port enable static ip pool
----- ------ ------------------------------------------------
 2-10   -    192.168.1.10
ras>
```

49.4.9 DHCP Snoop LAN to LAN Show Command

Syntax:

```
ras> switch dhcpsnoop lan2lan show
```

This command displays whether LAN to LAN DHCP services are enabled or disabled.

49.4.10 DHCP Snoop LAN to LAN Disable Command

Syntax:

```
ras> switch dhcpsnoop lan2lan disable
```

This command disables LAN to LAN DHCP services. By default, the LAN to LAN DHCP service should be disabled except if you have the DHCP server connected to one of the DSL ports.

If LAN to LAN DHCP service is disabled, the SAM1316-22 forwards DHCP Discover and DHCP Request packets to the uplink port.

49.4.11 DHCP Snoop LAN to LAN Enable Command

Syntax:

```
ras> switch dhcpsnoop lan2lan enable
```

This command enables LAN to LAN DHCP services. The LAN to LAN DHCP service can be enabled in special cases where you have the DHCP server connected to one of the DSL ports. This has the SAM1316-22 forward DHCP Discover and DHCP Request packets to the DSL ports.

50

IEEE 802.1Q Tagged VLAN Commands

This chapter describes the IEEE 802.1Q Tagged VLAN commands.

50.1 Introduction to VLANs

See Chapter 17 on page 133 for more background information on VLANs.

50.2 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 SAM1316-22 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).

50.3 Filtering Databases

A filtering database stores and organizes VLAN registration information useful for switching frames to and from the SAM1316-22. A filtering database consists of static entries (Static VLAN or SVLAN table).

50.3.1 Static Entries (SVLAN Table)

Static entry registration information is added, modified and removed by administrators only.

50.4 IEEE VLAN1Q Tagged VLAN Configuration Commands

These switch commands allow you to configure and monitor the IEEE 802.1Q Tagged VLAN.

50.4.1 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 <1,5,6~8,enet1>.

This command displays the port's IEEE 802.1Q VLAN tag settings.

The following example shows the settings for DSL port 3.

Figure 152 VLAN Port Show Command Example

```
ras> switch vlan portshow 3
 port pvid priority frametype
----- ---- -------- ---------
    3    1        0       all
```

50.4.2 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 <1,5,6~8,enet1>.
<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 153 VLAN PVID Command Example

```
ras> switch vlan pvid 1 200
```

50.4.3 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: <1,5,6~8,enet1>.
<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 154 VLAN CPU Set Command Example

```
ras> switch vlan priority 2 3
```

50.4.4 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: <1,5,6~8,enet1>.
<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.

50.4.4.1 Modify a Static VLAN Table Example

The following is an example of how to modify a static VLAN table.

Figure 155 Modifying the Static VLAN Example

```
ras> switch vlan set 2000 1:FU
ras> switch vlan set 2001 2:FU
```

50.4.4.2 Forwarding Process Example

Tagged Frames

1. First the SAM1316-22 checks the VLAN ID (VID) of tagged frames or assigns temporary VIDs to untagged frames (see Section 50.4.2 on page 325).
2. The SAM1316-22 checks the frame's source MAC address against the MAC filter.
3. The SAM1316-22 then checks the VID in a frame's tag against the SVLAN table.
4. The SAM1316-22 notes what the SVLAN table says (that is, the SVLAN tells the SAM1316-22 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 SAM1316-22 checks the frame's source MAC address against the MAC filter.
3. The SAM1316-22 checks the PVID table and assigns a VID and IEEE 802.1Q priority.
4. The SAM1316-22 ignores the port from which the frame came, because the SAM1316-22 does not send a frame to the port from which it came. The SAM1316-22 also does not forward frames to "forbidden" ports.
5. If after looking at the SVLAN, the SAM1316-22 does not have any ports to which it will send the frame, it drops the frame.

50.4.5 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 <1,5,6~8>.

<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 SAM1316-22 accepts both tagged and untagged incoming frames on the Ethernet ports.

The following example sets the SAM1316-22 to accept only VLAN tagged Ethernet frames on DSL port 3.

Figure 156 VLAN Frame Type Command Example

```
ras> switch vlan frametype 3 tag
```

50.4.6 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 SAM1316-22.

The following example sets VLAN ID 2 to be the CPU (management) VLAN.

Figure 157 VLAN CPU Set Command Example

```
ras> switch vlan cpu set 2
```

50.4.7 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 SAM1316-22.

The following example sets VLAN ID 2 to be the CPU (management) VLAN.

Figure 158 VLAN CPU Set Command Example

```
ras> switch vlan cpu set 2
```

50.4.8 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 SAM1316-22'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 SAM1316-22 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 SAM1316-22 (the "management" or "CPU" VLAN).

Figure 159 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 160 Deleting Default VLAN Example

```
ras> switch vlan cpu set 3
```

50.4.9 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: <1,5,6~8>.

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 161 VLAN Delete Command Example

```
ras> switch vlan delete 2
```

50.5 VLAN Enable

Syntax:

```
ras> switch vlan enable <vid>
```

This command enables the specified VLAN ID in the SVLAN (Static VLAN) table.

50.6 VLAN Disable

Syntax:

```
ras> switch vlan disable <vid>
```

This command disables the specified VLAN ID in the SVLAN (Static VLAN) table.

50.6.1 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: <1,5,6~8>.

This command shows information about the specified port's VLAN settings.

The following example shows the settings for all VIDs.

Figure 162 VLAN Show Command Example

```
ras> switch vlan show *
 vid name             F:fixed X:forbidden N:normal   U:untag T:tag
---- ---------------- ----------------------------------------------------
   1 DEFAULT
     enabled          1234567890123456 12
                      FFFFFFFFFFFFFFFF FF
                      UUUUUUUUUUUUUUUU UU
```

51

MAC Commands

This chapter describes how to configure the SAM1316-22's MAC commands.

51.1 MAC Commands Overview

Use the MAC commands to configure MAC filtering or limit the MAC count.

51.2 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.

51.2.1 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 <1,5,6~8>.

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 163 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
```

51.2.2 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 <1,5,6~8>.

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 164 MAC Filter Enable Command Example

```
ras> switch mac filter enable 5
```

51.2.3 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 <1,5,6~8>.

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 165 MAC Filter Disable Command Example

```
ras> switch mac filter disable 5
```

51.2.4 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 SAM1316-22 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 166 MAC Filter Mode Command Example

```
ras> switch mac filter mode 5 accept
```

51.2.5 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 167 MAC Filter Set Command Example

```
ras> switch mac filter set 5 00:a0:c5:12:34:56
```

51.2.6 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 168 MAC Filter Delete Command Example

```
ras> switch mac filter delete 5 00:a0:c5:12:34:56
```

51.3 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 51.2 on page 333), the SAM1316-22 ignores the MAC count setting and accepts all of the MAC addresses listed for the port in the MAC filter settings.

51.3.1 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 <1,5,6~8>.

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 169 MAC Count Show Command Example

```
ras> switch mac count show 4
port status count
---- ------ -----
   4   V     128
```

51.3.2 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 <1,5,6~8>.

This command enables the MAC count filter on the specified DSL port(s). When the MAC filter accept mode is enabled (see Section 51.2 on page 333), the SAM1316-22 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 170 MAC Count Enable Command Example

```
ras> switch mac count enable 4
```

51.3.3 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 <1,5,6~8>.

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 171 MAC Count Disable Command Example

```
ras> switch mac count disable 4
```

51.3.4 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 <1,5,6~8>.
<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 172 MAC Count Set Command Example

```
ras> switch mac count set 7 50
```

52

IGMP Commands

This chapter describes the IGMP snooping and filtering commands.

52.1 Multicast Overview

See Chapter 18 on page 141 for background information on this feature.

52.2 IGMP Snoop Commands

Use the IGMP snoop commands to enable or disable IGMP proxy or IGMP snooping.

52.2.1 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 173 IGMP Snoop Show Command Example

```
ras> switch igmpsnoop show
IGMP Snooping/Proxy is Disable
```

52.2.2 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 174 IGMP Snoop Enable Command Example

```
ras> switch igmpsnoop enable proxy
```

52.2.3 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 175 IGMP Snoop Disable Command Example

```
ras> switch igmpsnoop disable
```

52.2.4 IGMP Snoop qryvid Delete Command

Syntax:

```
ras> switch igmpsnoop qryvid delete <vid>
```

This command deletes an IGMP query VLAN ID in IGMP proxy mode. The following example deletes VLAN 10.

```
ras> switch igmpsnoop qryvid 10
```

52.2.5 IGMP Snoop qryvid Set Command

Syntax:

```
ras> switch igmpsnoop qryvid set <vid>
```

This command configures an IGMP query VLAN ID in IGMP proxy mode. The following example configures VLAN 10 as an IGMP query VLAN.

```
ras> switch igmpsnoop qryvid 10
```

52.2.6 IGMP Snoop qryvid Show Command

Syntax:

```
ras> switch igmpsnoop qryvid show
```

This command displays information about the SAM1316-22's IGMP query VLAN IDs, as follows.

```
ras> switch igmpsnoop qryvid show
igmp proxy query vlan table
vid  static/dynamic
---- --------------
  10 static
 120 static
```

52.3 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.

52.3.1 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 <1,5,6~8>.

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 176 IGMP Filter Show Command Example

```
ras> switch igmpfilter show 5
port                           profile
-------------------------------------
   5                            DEFVAL
```

52.3.2 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 177 IGMP Filter Set Command Example

```
ras> switch igmpfilter set 5 voice
```

52.3.3 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 178 IGMP Filter Profile Set Command Example

```
ras> switch igmpfilter profile set test1 1 224.1.1.10 224.1.1.44
```

52.3.4 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 179 IGMP Filter Profile Delete Command Example

```
ras> switch igmpfilter profile delete voice
```

52.3.5 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 180 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
```

52.4 IGMP Bandwidth Commands

Use the IGMP bandwidth commands to set up bandwidth budgets for specific multicast channels.

52.4.1 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.

52.4.2 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).

52.4.3 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.

52.5 IGMP Bandwidth Port Commands

Use the IGMP bandwidth port commands to set up bandwidth budgets for multicast traffic on specific ports.

52.5.1 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 <1,5,6~8>.

This command deactivates multicast bandwidth settings of the specified port.

52.5.2 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 <1,5,6~8>.

This command activates multicast bandwidth setting on the specified port.

52.5.3 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 <1,5,6~8>.
<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.

52.5.4 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 <1,5,6~8>.

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 181 IGMP Bandwidth Port Show Command Example

```
ras> switch igmpsnoop bandwidth port show 1
 port  enable   bandwidth
------ ------ -----------
    1     -        4096
```

52.6 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.

52.6.1 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 <1,5,6~8>.

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 182 IGMP Count Disable Command Example

```
ras> switch igmpsnoop igmpcount disable 4
```

52.6.2 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 <1,5,6~8>.

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 183 IGMP Count Enable Command Example

```
ras> switch igmpsnoop igmpcount enable 4
```

52.6.3 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 <1,5,6~8>.
<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 184 IGMP Count Set Command Example

```
ras> switch igmpsnoop igmpcount set 4 2
```

52.6.4 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 <1,5,6~8>.

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 185 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
```

52.7 IGMP Snoop Statistics Commands

Use the IGMP Snoop Statistics commands to display current IGMP settings and statistics.

52.7.1 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 186 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
```

52.7.2 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 187 IGMP Group Statistics Command Example

```
ras> statistics igmpsnoop group
[group info]
group            vid port
--------------- ---- ------------------------------------------------ --
```

52.7.3 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 <1,5,6~8>.

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 188 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
```

52.7.4 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 <1,5,6~8>.

This command displays the IGMP groups a port joins. The following figure shows an example for port 1.

Figure 189 IGMP Port Group Statistics Command Example

```
ras> statistics igmpsnoop port group 1
port   vid mcast_ip        source ip
----- ---- -------------- --------------
```

52.8 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.

52.8.1 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: <1,5,6~8,enet1>.
<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 50.4.4 on page 326 for examples and more information.

52.8.2 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: <1,5,6~8>.

This command removes the specified multicast VLAN configuration(s).

52.8.3 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 190 Multicast VLAN Disable Command Example

```
ras> switch igmpsnoop mvlan disable 12
```

52.8.4 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.

52.8.5 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: <1,5,6~8>.

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 191 Multicast VLAN Show Command Example

```
ras> switch igmpsnoop mvlan show 1
 vid name             F:fixed X:forbidden    U:untag T:tag
---- ---------------- ----------------------------------------
```

52.8.6 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 192 Multicast VLAN Group Set Command Example

```
ras> switch igmpsnoop mvlan group set 10 1 224.224.224.1
224.224.224.10
```

52.8.7 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.

52.8.8 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.

53

PPPoE Intermediate Agent Commands

53.1 PPPoE Agent Information

Use these commands if you want the SAM1316-22 to add a vendor-specific tag to PADI (PPPoE Active Discovery Initialization) 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 use to identify and authenticate a PPPoE client.

53.1.1 PPPoE Intermediate Agent Clear Info Command

Syntax:

```
ras> switch poeagent clearinfo <vid>|all
```

where

`<vid>|all`	=	The ID of the VLAN to which to apply the setting. Type `all` to apply the setting to all VLAN.

This command clears any extra information the SAM1316-22 adds to PADI and PADR packets in the specified VLAN or for all VLAN.

53.1.2 PPPoE Intermediate Agent Enable Command

Syntax:

```
ras> switch poeagent enable <vid>|all
```

where

`<vid>|all`	=	The ID of the VLAN to which to apply the setting. Type `all` to apply the setting to all VLAN.

This command adds a vendor-specific tag to PADI and PADR packets for PPPoE clients in the selected VLAN(s) or for all VLAN. This tag contains information that a PPPoE termination server can use to identify and authenticate a PPPoE client.

The following example activates the PPPoE agent setting for VLAN 100.

Figure 193 PPPoE Intermediate Agent Enable Command Example

```
ras> switch poeagent enable 100
ras> switch poeagent show
 vid enable  info
---- ------  ----------------------------
   0   -
 100   V
 101   -
 102   -
Note: vid 0 is the default agent.
```

53.1.3 PPPoE Intermediate Agent Delete Command

Syntax:

```
ras> switch poeagent delete <vid>|all
```

where

`<vid>|all`	=	The ID of the VLAN to which to apply the setting. Type `all` to apply the setting to all VLAN.

This command deletes the PPPoE intermediate agent settings for the specified VLAN or for all VLAN. You cannot delete the setting for VLAN 0.

53.1.4 PPPoE Intermediate Agent Disable Command

Syntax:

```
ras> switch poeagent disable <vid>|all
```

where

`<vid>|all`	=	The ID of the VLAN to which to apply the setting. Type `all` to apply the setting to all VLAN.

This command removes the vendor-specific tag from PADI and PADR packets for PPPoE clients in the selected VLAN(s) or for all VLAN.

53.1.5 PPPoE Intermediate Agent Info Command

Syntax:

```
ras> switch poeagent info <vid>|all <description>
```

where

<vid>|all	=	The ID of the VLAN to which to apply the setting. Type all to apply the setting to all VLAN.
<description>	=	The PPPoE line information the switch is to add to PPPoE discover packets from the specified VLAN or from all VLAN. Enter a description (up to 24 alphanumerical characters).

This command specifies the extra information the SAM1316-22 adds to PADI and PADR packets in the specified VLAN or in all VLANs, if the PPPoE intermediate agent is enabled.

Note: Before you can configure PPPoE intermediate agent information, you must first create a entry using the poeagent set command.

The following example sets the switch to add “testing” to PADI and PADR packets on VLAN 100.

Figure 194 PPPoE Intermediate Agent Info Command Example

```
ras> switch poeagent info 100 testing
ras> switch poeagent show
 vid enable  info
---- ------  ----------------------------
   0   -
 100   V     testing
 101   -
 102   -
Note: vid 0 is the default agent.
```

53.1.6 PPPoE Intermediate Agent Set Command

Syntax:

```
ras> switch poeagent set <vid>
```

This command 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. The following example creates an entry for VLAN 10.

Figure 195 PPPoE Intermediate Agent Set Command Example

```
ras> switch poeagent set 10
ras> switch poeagent show
 vid enable  info
---- ------  ----------------------------
   0   -
  10   -
 100   V     testing
 101   -
 102   -
Note: vid 0 is the default agent.
```

53.1.7 PPPoE Intermediate Agent Show Command

Syntax:

```
ras> switch poeagent 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 displays PPPoE intermediate agent settings for the specified VLAN or for all VLAN. The following example shows the PPPoE intermediate agent settings for all VLAN.

Figure 196 PPPoE Intermediate Agent Show Command Example

```
ras> switch poeagent show
 vid enable  info
---- ------  ----------------------------
   0   -
  10   -
 100   V     testing
 101   -
 102   -
Note: vid 0 is the default agent.
```

54

OUI Filter Commands

54.1 OUI Filter 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.

54.1.1 OUI Filter Disable Command

Syntax:

```
switch ouifilter disable <port>
```

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

54.1.2 OUI Filter Enable Command

Syntax:

```
switch ouifilter enable <port>
```

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

54.1.3 OUI Filter 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
```

54.1.4 OUI Filter 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
```

54.1.5 OUI Filter 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   -    -
```

55

Packet Filter Commands

This chapter describes the packet filter commands.

55.1 Packet Filter Commands

Use the following packet filter commands to filter out specific types of packets on specific ports.

55.1.1 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 <1,5,6~8>.

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 SAM1316-22 is to accept on the port. “-“ displays for packet types that the SAM1316-22 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 SAM1316-22 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
```

55.1.2 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 <1,5,6~8>.
`[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
```

55.1.3 Packet Filter PPPoE Only Command

Syntax:

```
ras> switch pktfilter pppoeonly <portlist>
```

This command sets the SAM1316-22 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
```

56

IP Commands

This chapter shows you how to use the (standard shell) IP commands to configure the IP (Internet Protocol) parameters.

56.1 IP Commands Introduction

Use the SAM1316-22's management IP addresses to manage it through the network.

56.2 IP Settings and Default Gateway

Use the following command sequence to set the SAM1316-22'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 SAM1316-22 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 SAM1316-22.

</netmask>	=	The bit number of the subnet mask of the IP address you want to configure for SAM1316-22's uplink, downlink and SAM1316-22 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 SAM1316-22.

The first command changes the IP settings for the SAM1316-22's uplink, downlink and SAM1316-22 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 SAM1316-22 where to send packets that have a destination IP address that is not on the same subnet as the SAM1316-22's IP address.

The third command saves the new configuration to the nonvolatile memory.

For example, use the following command sequence sets the SAM1316-22 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 SAM1316-22 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 SAM1316-22 to the network, otherwise, you may interrupt services already running.

56.3 General IP Commands

The following is a list of general IP commands that help with the management of the IP parameters.

56.3.1 Show

Syntax:

```
ras> ip show
```

Use the command to display the current management IP settings.

56.3.2 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.

56.3.3 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 SAM1316-22's default route.

This command defines a new, static IP forwarding route or edits an existing one.

56.3.4 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.

56.3.5 Route Show Command

Syntax:

```
ras> ip route show
```

This command displays the SAM1316-22'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
```

56.3.6 ARP Show Command

Syntax:

```
ras> ip arp show
```

This command displays the SAM1316-22's IP Address Resolution Protocol table. This is the list of IP addresses and matching MAC addresses that the SAM1316-22 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
```

56.3.7 ARP Flush Command

Syntax:

```
ras> ip arp flush
```

This command clears the SAM1316-22's IP Address Resolution Protocol table.

56.4 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
```

57

Firmware and Configuration File Maintenance

This chapter tells you how to upload a new firmware and/or configuration file for the SAM1316-22.

57.1 Firmware and Configuration File Maintenance Overview

The SAM1316-22's built-in FTP server allows you to use any FTP client (for example, ftp.exe in Windows) to upgrade SAM1316-22 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 SAM1316-22 during the file transfer process, as it may permanently damage your SAM1316-22.

Note: The SAM1316-22 automatically restarts when the upgrade process is complete.

57.2 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 SAM1316-22.

Figure 206 FTP Get Configuration File Example

```
ftp> get config-0 config.txt
```

This is a sample from a FTP session to transfer the SAM1316-22's current configuration file (including the configuration files of all the SAM1316-22) 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 SAM1316-22 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 SAM1316-22 and the external filename refers to the filename not on the SAM1316-22, 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 SAM1316-22 to confirm that you have uploaded the correct firmware version.

Table 106 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	`config-0`	`*.dat`	This is the configuration filename for the SAM1316-22.
Firmware	`ras`	`*.bin`	This is the Operating System firmware on the SAM1316-22.

57.3 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 SAM1316-22.

Note: You can change the ".dat" file to a ".txt" file and still upload it back to the SAM1316-22.

Note: Do not upload any invalid files to the SAM1316-22's configuration file, as it may permanently damage your SAM1316-22.

57.3.1 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 SAM1316-22.

Figure 207 Example: Use an FTP Client to Connect to the SAM1316-22

```
C:\> ftp <SAM1316-22 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
```

57.3.2 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 SAM1316-22 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.

57.3.3 Editable Configuration File Upload

You can upload the configuration file by following the steps below.

Use an FTP client to connect to the SAM1316-22.

Figure 212 Example: Use an FTP Client to Connect to the SAM1316-22

```
C:\> ftp <SAM1316-22 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.

57.4 Firmware File Upgrade

Use the following procedure to upload firmware to the SAM1316-22.

Use an FTP client to connect to the SAM1316-22.

Figure 216 Example: Use an FTP Client to Connect to the SAM1316-22

```
C:\> ftp <SAM1316-22 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 SAM1316-22. The firmware file on your computer (that you want to put onto the SAM1316-22 is named firmware.bin. The internal firmware file on the SAM1316-22 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 SAM1316-22 restarts automatically.

58

SNMP

This chapter covers Simple Network Management Protocol (SNMP) with the SAM1316-22.

58.1 SNMP Commands

Use these commands to configure SNMP settings. See Chapter 35 on page 229 for more information about SNMP.

58.1.1 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.

58.1.2 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.

58.1.3 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 SAM1316-22 will only respond to SNMP messages from this address. If you leave the trusted host set to 0.0.0.0 (default), the SAM1316-22 will respond to all SNMP messages it receives, regardless of source.

58.1.4 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.

58.1.5 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 SAM1316-22 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 SAM1316-22 sends SNMP traps. If you leave the trap destination set to 0.0.0.0 (default), the SAM1316-22 will not send any SNMP traps.

58.1.6 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.

59

DSL Commands

This chapter describes some of the commands that allow you to configure and monitor the DSL ports.

59.1 DSL Port Commands

Use these commands to configure the DSL ports. See Chapter 13 on page 91 for background information on DSL and SHDSL.

59.1.1 DSL Port Show Command

Syntax:

```
ras> shdsl 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 <1,5,6~8>.

This command shows the activation status, DSL mode, maximum upstream and downstream rate settings, and DSL profile of each DSL port. It also provides subscriber information for the port.

The following example displays information on DSL port 1.

Figure 220 DSL Port Show Command Example

```
ras> shdsl show 1
port enable mode min/max rate  profile
---- ------ ---- ------------ --------------------------------
   1   V    stuc    192/  2304 DEFVAL

Subscriber Info:
port name                            tel
---- ------------------------------- ----------------
   1 -                               -
```

59.1.2 DSL Port Enable Command

Syntax:

```
ras> shdsl 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 <1,5,6~8>.

This command forcibly enables the specified DSL port(s).

59.1.3 DSL Port Disable Command

Syntax:

```
ras> shdsl 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 <1,5,6~8>.

This command forcibly disables the specified DSL port(s).

Note: The factory default of all ports is enabled.

59.1.4 DSL Port Profile Show Command

Syntax:

```
ras> shdsl 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 Port Profile Show Command Example

```
ras> shdsl profile show DEFVAL
01. DEFVAL
  max rate      (Kbps): 2304
  min rate      (Kbps): 192
  annex mode          : annexb
  wire pair           : 2wire
  line probe          : lp_off
  curr margin     (dB): 0
  worst margin    (dB): 0
```

See Section 59.1.5 on page 387 for a description of each attribute.

59.1.5 DSL Port Profile Set Command

Syntax:

```
shdsl profile set <profile> <min-rate> <max-rate>
 [annexa|annexb 2wire|4wire|mpair4
 [lp_off | lp_on_cur [curr-margin] | lp_on_wc [worst-margin]]]
```

where

`<profile>`	=	The descriptive name for the profile.
`<min-rate>`	=	The minimum transmission rate in Kbps. (192~4096)
`<max-rate>`	=	The maximum transmission rate in Kbps. (192~4096)
`annexa|annexb`	=	The region setting, annexb is the default. annexa = DSL over POTS (G.992.1 Annex A). annexb = DSL over ISDN (G.992.1 Annex B).
`2wire|4wire|mpair4`	=	The wire pair number. 2wire = a normal connection using a single DSL port's two wires, this is the default. 4wire = a 4-wire group (two DSL ports grouped together). mpair4 = an 8-wire group (four DSL ports grouped together).

lp_off	=	Disable line probe. The DSL line card and subscriber modem use line probes to determine the best possible transmission rate. This is used in rate adaptation. This is the default line probe mode. If you disable line probe, the system skips the rate adaptation phase to shorten connection set up time.
lp_on_cur	=	Enable line probe with current target Signal to Noise Ratio margin.
lp_on_wc	=	Enable line probe with worst case target Signal to Noise Ratio margin.
<curr-margin>	=	The current condition target Signal to Noise Ratio margin, -10 ~ 21 in dB.
<worst-margin>	=	The worst case Signal to Noise Ratio margin, -10 ~ 21 in dB.

The profile contains information on SHDSL line configuration. Each entry in this table reflects a parameter defined by a manager, which can be used to configure the DSL line. After you create a DSL profile, assign it to DSL ports.

You must specify at least the profile's name and minimum and maximum rates. The default value will be used for any of the other fields that you omit.

The minimum transmission rate must be less than or equal to the maximum transmission rate.

When using 4 or 8-wire groups, you must apply the profile to every port in a specific set of ports. For example, a profile for a 4-wire group can be used with ports 1,2 or 3,4 but not with ports 2,3 or 4,5. A profile for an 8-wire group can be used with ports 1,2,3,4 or 5,6,7,8 but not with ports 2,3,4,5 or 4,5,6,7.

The following example creates a premium profile (named gold) for providing subscribers with very high connection speeds. The minimum transmission rate is 2112 Kbps and the maximum transmission rate is 4096. It sets two ports to function as a 4-wire group. It uses G.992.1 Annex A (DSL over POTS). It turns on line probes and has them use the current condition target signal to noise ratio margin which it sets to 5 db.

Figure 222 DSL Port Profile Set Command Example

```
ras> shdsl profile set gold 2112 4096 annexa 4wire lp_on_cur 5
```

59.1.6 DSL Port Profile Delete Command

Syntax:

```
ras> shdsl 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 SAM1316-22. 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 223 DSL Port Profile Delete Command Example

```
ras> shdsl profile delete gold
```

59.1.7 DSL Port Profile Map Command

Syntax:

```
ras> shdsl profile 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 <1,5,6~8>.
<profile>       =   The profile that will define the settings of this port.
```

This command assigns a specific DSL profile one or more ports.

59.1.8 DSL Port Name Command

Syntax:

```
ras> shdsl 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 <1,5,6~8>.
```

<name>	=	A descriptive name for the port. You can use up to 31 alphanumeric ASCII characters, hyphens (-), or underscores (_).

This command sets the name of one or more DSL port(s).

The following example sets DSL port 5 to have the name super.

Figure 224 DSL Port Name Command Example

```
ras> shdsl name 5 super
```

59.1.9 DSL Port Tel Command

Syntax:

```
ras> shdsl 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 <1,5,6~8>.
<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's telephone number.

The following example records the telephone number 12345678 for DSL port 5.

Figure 225 DSL Port Tel Command Example

```
ras> shdsl tel 5 12345678
```

59.1.10 DSL Port Loopback Command

Syntax:

```
ras> shdsl 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 <1,5,6~8>.

<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 SAM1316-22 perform an OAMF5 loopback test on the specified DSL port(s).

The following example has the SAM1316-22 perform an OAMF5 loopback test on DSL port 1's PVC at VPI 0 and VCI 33.

Figure 226 DSL Port Loopback Command Example

```
ras> shdsl loopback 1 f5 0 33
port[1] OAM F5 loopback test: failed
```

59.2 Statistics DSL Commands

Use these commands to display DSL port statistics.

59.2.1 DSL Statistics Show Command

Syntax:

```
ras> statistics shdsl 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 <1,5,6~8>.

This command displays DSL port connection statistics including the wire pair, status (V for enabled, - for disabled), actual rate, up time and the number of errored seconds.

The following example displays connection statistics for port 1.

Figure 227 DSL Statistics Show Command Example

```
ras> statistics shdsl show 1
                      actual rate
port wire pair status    (kbps)   up time        error second(15M/24H)
---- --------- ------ ----------- -------------- --------------------
   1         -   -              -              -        -/-
```

59.2.2 DSL Port Lineinfo Command

Syntax:

```
ras> statistics shdsl 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 <1,5,6~8>.

This command shows the line operating values of a DSL port. If a port is down, it shows the connection status.

An example is shown next.

Figure 228 DSL Port Lineinfo Command Example

```
ras> statistics shdsl lineinfo 1~4
[port 1]
link is down
[port 2]
link is down
[port 3]
link is down
[port 4]
link is down
```

The following table explains these counters.

Table 107 DSL Port Lineinfo Command Counters

LABEL	DESCRIPTION
Link	This displays the connection status of the DSL link.
Min Rate(kbps)	This is the minimum rate (in Kbps) of the DSL line.
Max Rate(kbps)	This is the maximum rate (in Kbps) of the DSL line.
Actual Rate(kbps)	This is the rate (in Kbps) at which the port has been sending and receiving data.

Table 107 DSL Port Lineinfo Command Counters (continued)

LABEL	DESCRIPTION
Noise Margin(dB)	This is the DSL line's noise margin measured in decibels (dB).
Attenuation(dB)	This is the reduction in amplitude of the DSL signals, measured in decibels (dB).

Information obtained prior to training to steady state transition will not be valid or will be old information.

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).

59.2.3 DSL Port Lineperf Command

Syntax:

```
ras> statistics shdsl 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 <1,5,6~8>.

This command shows the line performance counters of a DSL port.

An example is shown next.

Figure 229 DSL Port Lineperf Command Example

```
ras> statistics shdsl lineperf 1
[Port 1]
Performance since boot up
                     STUC     STUR
es               :       0        0 seconds
ses              :       0        0 seconds
crc              :       0        0
losws            :       8        0 seconds
uas              :       0        0 seconds
segment anomaly :       0        0
segment defect  :       0        0

Performance since link up
es               :       0 seconds
ses              :       0 seconds
crc              :       0
losws            :       8 seconds
uas              :       0 seconds
segment anomaly :       0
segment defect  :       0
```

These counters display line performance data that has been accumulated since the system started and since the last connection was established. In the list above, STUC refers to errors detected by the STU-C, and STUR refers to errors detected by the STU-R.

The following table explains these counters.

Table 108 DSL Port Lineperf Command Counters

LABEL	DESCRIPTION
es	The number of Errored Seconds that have occurred on this DSL port. An Errored Second is defined as a count of 1-second intervals during which one or more CRC anomalies are declared and/or one or more LOSW defects are declared.
ses	The number of Severely Errored Seconds that have occurred on this DSL port. A Severely Errored Second is defined as a count of 1-second intervals during which at least 50 CRC anomalies are declared or one or more LOSW defects are declared. (50 CRC anomalies during a 1-second interval is equivalent to a 30% errored frame rate for a nominal frame length.)
crc	The number of CRC anomalies that have occurred on this DSL port.
losws	The number of Loss of Sync Word Seconds that have occurred on this DSL port.
uas	The number of UnAvailable Seconds.that have occurred on this DSL port. An Unavailable Second is a count of 1-second entrails for which the SHDSL line is unavailable. The SHDSL line becomes unavailable at the onset of 10 contiguous SESs. The 10 SESs are included in the unavailable time. Once unavailable, the SHDSL line becomes available at the onset of 10 contiguous seconds with no SESs. The 10 s with no SESs are excluded from unavailable time.
segment anomaly	The number of Segment Anomalies that have occurred on this DSL port. A segment anomaly indicates that a regenerator operating on a segment has received corrupted data and therefore the regenerated data is unreliable.
segment defect	The number of Segment Defects that have occurred on this DSL port. A segment defect indicates that a regenerator has lost SHDSL synchronization and therefore the regenerated data is unavailable.

59.2.4 DSL Port 15 Minute Performance Command

Syntax:

```
ras> statistics shdsl 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 <1,5,6~8>.

[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 specified number of previous 15-minute periods.

An example is shown next.

Figure 230 DSL Port 15 Minute Performance Command Example

```
ras> statistics shdsl 15mperf 1 3
Port 1 Current 15 Min elapsed time: 187 secs (Link Down)
   Current 15 Min PM:      STUC      STUR
                   ES:         0         0
                  SES:         0         0
                  CRC:         0         0
                LOSWS:         0         0
                  UAS:         0         0
  History 15 Min PM-1:      STUC      STUR
                   ES:         0         0
                  SES:         0         0
                  CRC:         0         0
                LOSWS:         0         0
                  UAS:         0         0
  History 15 Min PM-2:      STUC      STUR
                   ES:         0         0
                  SES:         0         0
                  CRC:         0         0
                LOSWS:         0         0
                  UAS:         0         0
```

In the list above, STUC refers to data detected by the STU-C, and STUR refers to data detected by the STU-R. See Table 108 on page 394 for an explanation of these counters.

These counters are also used in the alarm profiles (see Section 59.3 on page 397).

59.2.5 DSL Port 1 Day Performance Command

Syntax:

```
ras> statistics shdsl 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 <1,5,6~8>.

This command displays line performance statistics for the current and previous four days.

An example is shown next.

Figure 231 DSL Port 1Day Performance Command Example

```
ras> statistics shdsl 1dayperf 1
Port 1 the current day elapsed time: 74278 secs (Link Down)
          1 Day Perf       STUC       STUR
                   ES:          0          0
                  SES:          0          0
                  CRC:          0          0
                LOSWS:          0          0
                  UAS:          0          0
Port 1 the previous 0 day
          1 Day Perf       STUC       STUR
                   ES:          0          0
                  SES:          0          0
                  CRC:          0          0
                LOSWS:          0          0
                  UAS:          0          0
Port 1 the previous 1 day
          1 Day Perf       STUC       STUR
                   ES:          0          0
                  SES:          0          0
                  CRC:          0          0
                LOSWS:          8          0
                  UAS:          0          0
Port 1 the previous 2 day
          1 Day Perf       STUC       STUR
                   ES:          0          0
                  SES:          0          0
                  CRC:          0          0
                LOSWS:          0          0
                  UAS:          0          0
Port 1 the previous 3 day
          1 Day Perf       STUC       STUR
                   ES:          0          0
                  SES:          0          0
                  CRC:          0          0
                LOSWS:          0          0
                  UAS:          0          0
Port 1 the previous 4 day
          1 Day Perf       STUC       STUR
                   ES:          0          0
                  SES:          0          0
                  CRC:          0          0
                LOSWS:          0          0
                  UAS:          0          0
```

In the list above, STUC refers to data detected by the STU-C, and STUR refers to data detected by the STU-R. See Table 108 on page 394 for an explanation of these counters.

59.3 Alarm Profile Commands

Configure alarm profiles to set alarm settings and thresholds for the DSL ports.

59.3.1 Alarm Profile Show Command

Syntax:

```
ras> shdsl 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 232 Alarm Profile Show Command Example

```
ras> shdsl alarmprofile show DEFVAL
01. DEFVAL
ThreshLoopAttenuation: 0
ThreshSNRMargin      : 0
ThreshES             : 0
ThreshSES            : 0
ThreshCRCanomalies   : 0
ThreshLOSWS          : 0
ThreshUAS            : 0
```

See Section 59.3.2 on page 397 for a description of each attribute.

59.3.2 Alarm Profile Set Command

Syntax:

```
ras> shdsl alarmprofile set <profile> [atten <atten>] [snrmgn <snrmgn>] [es
<es>] [ses <ses>][crc <crc>] [losws <losws>] [uas <uas>]
```

where

<profile>	=	A name for the alarm profile (up to 31 ASCII characters).
<atten>	=	The permitted loop attenuation of a port, 0~127
<snrmgn>	=	The permitted signal to noise ratio margin, 0~15.

<es>	=	The number of Errored SecondS (0~900) that are permitted to occur within 15 minutes.
<ses>	=	The number of Severely Errored Seconds (0~900) that are permitted to occur within 15 minutes.
<crc>		The number of Cyclic Redundancy Checking anomalies that are permitted to occur within 15 minutes.
<losws>		The number of Loss Of Sync Word Seconds (0~900) that are permitted to occur within 15 minutes.
<uas>	=	The number of UnAvailable Seconds (0~900) that are permitted to occur within 15 minutes.

This command configures DSL port alarm thresholds. The SAM1316-22 sends an alarm trap and generates a syslog entry when the thresholds of the alarm profile are exceeded.

Configure alarm profiles first and then use the `shdsl alarmprofile map` command to use them with specific DSL ports.

The following example sets an alarm profile named SESalarm that has the SAM1316-22 send an alarm trap and generate a syslog whenever the connection's number of severely errored seconds exceeds three within a 15 minute period.

```
ras> shdsl alarmprofile set SESalarm ses 3
```

59.3.3 Alarm Profile Delete Command

Syntax:

```
ras> shdsl 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 233 Alarm Profile Delete Command Example

```
ras> shdsl alarm profile delete SESalarm
```

59.3.4 Alarm Profile Map Command

Syntax:

```
ras> shdsl alarmprofile map <portlist> <profile> <span|stuc|stur|*>
```

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 <1,5,6~8>.
`<profile>`	=	The name of an alarm profile.
`<span|stuc|stur|*>`	=	The type of alarm profile the specified alarm profile is for the specified ports. The alarm profile can apply for the whole span (span), the STU-C end point (stuc), the STU-R end point (stur), or all STU-C and STU-R end points (*).

Sets the SAM1316-22 to use an (already-configured) alarm profile with the specified DSL ports.

The following example sets the SAM1316-22 to use the SESalarm alarm profile for the STU-C end point with DSL port 5.

Figure 234 Alarm Profile Map Command Example

```
ras> shdsl alarmprofile map 5 SESalarm stuc
```

59.3.5 Alarm Profile Showmap Command

Syntax:

```
ras> shdsl alarmprofile showmap <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 <1,5,6~8>.

Displays which alarm profiles the SAM1316-22 is set to use for specific (or all) DSL ports.

The following example displays which alarm profile the SAM1316-22 is set to use for DSL ports 1-3.

Figure 235 Alarm Profile Showmap Command Example

```
ras> shdsl alarmprofile showmap 1~3

port span/endpoint alarm profile name
---- ------------ ------------------------------
   1          span DEFVAL
   1          stuc
   1          stur
   2          span DEFVAL
   2          stuc
   2          stur
   3          span DEFVAL
   3          stuc
   3          stur
```

60

Virtual Channel Management

This chapter shows you how to use commands to configure virtual channels.

60.1 Virtual Channel Management Overview

See Chapter 13 on page 91 for background information on virtual channels and ATM QoS.

60.2 Virtual Channel Profile Commands

Use the following commands to configure virtual channel profiles.

60.2.1 Show Virtual Channel Profile Command

Syntax:

```
ras> shdsl 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).

60.2.2 Set Virtual Channel Profile Command

Syntax:

```
ras> shdsl vcprofile set <vcprofile> <vc|llc> <ubr|cbr> <pcr> <cdvt>
ras> shdsl 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 name of 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 in the SAM1316-22.

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 236 Set Virtual Channel Profile Command Example 1

```
ras> shdsl 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 237 Set Virtual Channel Profile Command Example 2

```
ras> shdsl 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 238 Set Virtual Channel Profile Command Example 3

```
ras> shdsl vcprofile set gold llc cbr 50000 100
```

60.2.3 Delete Virtual Channel Profile Command

Syntax:

```
ras> shdsl 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 239 Delete Virtual Channel Profile Command Example

```
ras> shdsl vcprofile delete silver
```

60.3 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.

60.3.1 PVC Show Command

Syntax:

```
ras> shdsl 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 <1,5,6~8>.
[<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.

60.3.2 PVC Set Command

Syntax:

```
ras> shdsl 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 <1,5,6~8>.
<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 SAM1316-22 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 SAM1316-22 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 SAM1316-22 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 SAM1316-22 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 240 PVC Set Command Example

```
ras> shdsl pvc set 1 1 34 100 3 platinum,plus
```

60.3.3 PVC Delete Command

Syntax:

```
ras> shdsl 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 <1,5,6~8>.
[<vpi> <vci>]	=	The VPI and VCI of an individual PVC.

This command deletes the specified PVC channel.

60.4 Priority-based PVCs

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

The SAM1316-22 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 13 on page 91 for the factory default mapping.

Use these commands to configure PPVCs and add and remove member PVCs.

60.4.1 PPVC Set Command

Syntax:

```
ras> shdsl 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 <1,5,6~8>.
<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 SAM1316-22 uses this PVC channel internally. This PVC is not needed on the subscriber's device.

Figure 241 PPVC Set Command Example

```
ras> shdsl ppvc set 5 8 35 llc 25 3
```

60.4.2 PPVC Member Set Command

Syntax:

```
  ras> shdsl 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 <1,5,6~8>.
`<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 SAM1316-22 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 242 PPVC Member Set Command Example

```
ras> shdsl ppvc member set 5 8 35 8 36 DEFVAL,DEFVAL 2
```

60.5 PPVC Member Delete Command

Syntax:

```
  ras> shdsl 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 <1,5,6~8>.
<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 243 PPVC Member Delete Command Example

```
ras> shdsl ppvc member delete 5 8 35 8 36
```

60.6 PPVC Member Show Command

Syntax:

```
ras> shdsl 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 <1,5,6~8>.
<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 244 PPVC Member Show Command Example

```
ras> shdsl ppvc member show 5
port vpi   vci mvpi  mvci  level DS/US vcprofile
---- --- ----- ---- ----- ------ --------------------
   5   8    35    8    36      2 DEFVAL/DEFVAL
```

60.6.1 PPVC Show Command

Syntax:

```
ras> shdsl 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 <1,5,6~8>.
<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 245 PPVC Show Command Example

```
ras> shdsl ppvc show 5
port  vpi    vci  encap pvid pri
================================
  5     8     35   llc    25  6
```

60.6.2 PPVC Delete Command

Syntax:

```
ras> shdsl 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 <1,5,6~8>.
`<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 246 PPVC Delete Command Example

```
ras> shdsl ppvc delete 5 8 35
```

60.7 2684 Routed Mode Commands

Use the 2684 routed mode to have the SAM1316-22 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 SAM1316-22 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 `shdsl rpvc gateway` commands to configure gateway settings.

2 Use the `shdsl rpvc set` command to configure RPVCs (2684 routed mode PVCs) for 2684 routed mode traffic.

3 Use the `shdsl 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 `shdsl 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 SAM1316-22 reassembles the Ethernet packets from the AAL5 ATM cells, the SAM1316-22 will append the routed mode gateway's MAC address and the SAM1316-22's MAC address as the destination/source MAC address.

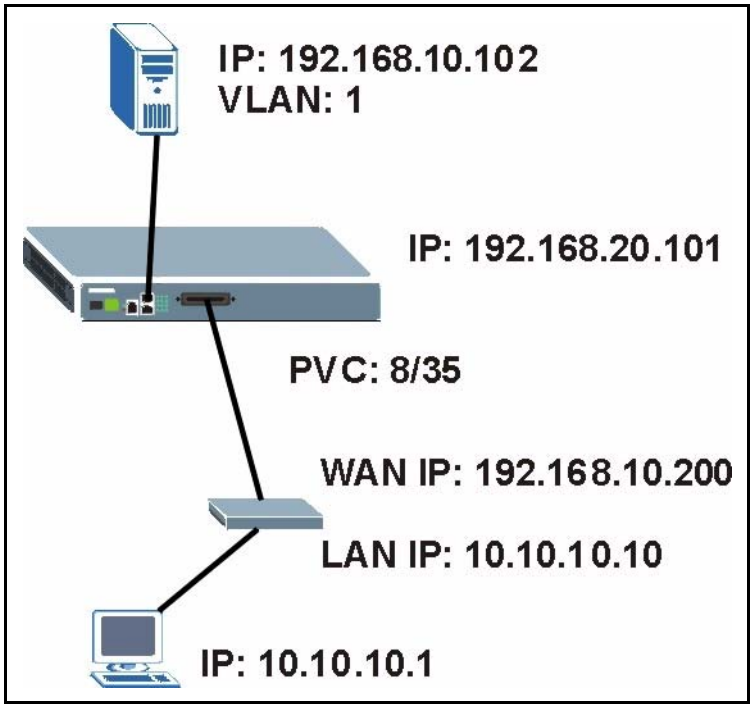
6 For downstream traffic: When the SAM1316-22 sees the destination IP address is specified in the RPVC (or RPVC domain), the SAM1316-22 will strip out the MAC header and send them to the corresponding RPVC.

60.7.1 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 SAM1316-22 uses IP address 192.168.20.101. The subscriber's device (the CPE) is connected to DSL port 1 on the SAM1316-22 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 247 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 SAM1316-22'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 SAM1316-22'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 SAM1316-22's management IP address should not be in the same subnet range of any RPVC and RPVC domain. It will make the SAM1316-22 confused if the SAM1316-22 receives a packet with this IP as destination IP.
- The SAM1316-22'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 SAM1316-22 for this example set up.

Figure 248 2684 Routed Mode Commands Example

```
ras> shdsl rpvc gateway set 192.168.10.102 1
ras> shdsl rpvc set 1 8 35 DEFVAL 192.168.10.200/32 192.168.10.102
ras> shdsl rpvc route set 1 8 35 10.10.10.1/24
```

60.7.2 RPVC Gateway Set Command

Syntax:

```
ras> shdsl 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 249 RPVC Gateway Set Command Example

```
ras> shdsl rpvc gateway set 192.168.10.102 1 3
```

60.7.3 RPVC Gateway Show Command

Syntax:

```
ras> shdsl 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 250 RPVC Gateway Show Command Example

```
ras> shdsl rpvc gateway show
gateway ip      vid  priority
--------------- ---- --------
192.168.10.102  1    3
```

60.7.4 RPVC Gateway Delete Command

Syntax:

```
ras> shdsl 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 251 RPVC Gateway Delete Command Example

```
ras> shdsl rpvc gateway delete 192.168.10.102
```

60.7.5 RPVC Set Command

Syntax:

```
ras> shdsl 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 <1,5,6~8>.
<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 SAM1316-22 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 SAM1316-22'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 252 RPVC Set Command Example

```
ras> shdsl rpvc set 1 8 35 DEFVAL,DEFVAL 192.168.10.200/32 192.168.10.102
```

60.7.6 RPVC Show Command

Syntax:

```
ras> shdsl 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 <1,5,6~8>.

This command lists the PVCs for handling 2684 routed mode traffic (RPVCs).

The following example displays the RPVCs for DSL port 1.

Figure 253 RPVC Show Command Example

```
ras> shdsl 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
```

60.7.7 RPVC Delete Command

Syntax:

```
ras> shdsl 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 <1,5,6~8>.
<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 254 RPVC Delete Command Example

```
ras> shdsl rpvc delete 1 8 35
```

60.7.8 RPVC Route Set Command

Syntax:

```
ras> shdsl 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 SAM1316-22 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 255 RPVC Route Set Command Example

```
ras> shdsl rpvc route set 1 8 35 10.10.10.1/24
```

60.7.9 RPVC Route Show Command

Syntax:

```
ras> shdsl 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 <1,5,6~8>.

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 256 RPVC Route Show Command Example

```
ras> shdsl 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
```

60.7.10 RPVC Route Delete Command

Syntax:

```
ras> shdsl 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 SAM1316-22 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 257 RPVC Route Delete Command Example

```
ras> shdsl rpvc route delete 1 8 35 10.10.10.1/24
```

60.7.11 RPVC ARP Agingtime Set Command

Syntax:

```
ras> shdsl 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 258 RPVC ARP Agingtime Command Example

```
ras> shdsl rpvc arp agingtime set 500
```

60.7.12 RPVC ARP Agingtime Show Command

Syntax:

```
ras> shdsl 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 259 RPVC ARP Agingtime Show Command Example

```
ras> shdsl rpvc arp agingtime show
rpvc aging time (sec): 600
```

60.7.13 RPVC ARP Show Command

Syntax:

```
ras> shdsl 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 260 RPVC ARP Agingtime Show Command Example

```
ras> shdsl rpvc arp show
gateway ip       vid  mac
---------------  ---- -----------------
192.168.10.102      1 00:0d:9d:d9:43:3b
```

60.7.14 RPVC ARP Flush Command

Syntax:

```
ras> shdsl rpvc arp flush
```

This command clears the IP addresses of 2684 routed mode gateways from the Address Resolution Protocol table.

60.8 PPPoA to PPPoE (PAE) Commands

You can use these commands to create PVCs for PAE translation.

60.8.1 PAE PVC Delete Command

Syntax:

```
ras> shdsl 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 <1,5,6~8>.
<vpi>	=	The VPI of the PAE PVC.
<vci>	=	The VCI of the PAE PVC.

This command removes a PAE PVC.

60.8.2 PAE PVC Set Command

Syntax:

```
  ras> shdsl 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 <1,5,6~8>.
<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 SAM1316-22 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 261 PAE PVC Set Command Example

```
ras> shdsl paepvc set 1 1 33 DEFVAL 1 0 acname vom srvcname video hellotime
10
```

60.8.3 PAE PVC Show Command

Syntax:

```
ras> shdsl 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 <1,5,6~8>.
<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 262 PAE PVC Show Command Example

```
ras> shdsl 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
```

60.8.4 PAE PVC Session Command

Syntax:

```
ras> shdsl 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 <1,5,6~8>.
<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 263 PAE PVC Session Command Example

```
ras> shdsl paepvc session 1
pvc 1-1/33
session state : down
session id    : 0
session uptime: 0 secs
acname        :
srvcname      :
```

60.8.5 PAE PVC Counter Command

Syntax:

```
ras> shdsl 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 <1,5,6~8>.
<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 264 PAE PVC Counter Command Example

```
ras> shdsl 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 SAM1316-22.
ppp lcp config-request	=	The number of config-request PDUs received by the SAM1316-22 from the CPE (client) device.
ppp lcp echo-request	=	The number of echo-request PDUs received by the SAM1316-22 from the CPE (client) device.
ppp lcp echo-reply	=	The number of echo-reply PDUs received by the SAM1316-22 from the CPE (client) device.
pppoe padi	=	The number of padi PDUs sent by the SAM1316-22 to the BRAS.
pppoe pado	=	The number of pado PDUs sent by the BRAS to the SAM1316-22.
pppoe padr	=	The number of padr PDUs sent by the SAM1316-22 to the BRAS.
pppoe pads	=	The number of pads PDUs sent by the BRAS to the SAM1316-22.
pppoe padt	=	The number of padt PDUs sent and received by the SAM1316-22.
pppoe srvcname error	=	The number of service name errors; for example, the SAM1316-22'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 SAM1316-22 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 SAM1316-22 and the BRAS.

60.9 Transparent LAN Service (TLS) Commands

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

60.9.1 TLS PVC Delete Command

Syntax:

```
ras> shdsl 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 <1,5,6~8>.
<vpi>	=	The VPI of the TLS PVC.
<vci>	=	The VCI of the TLS PVC.

This command clears TLS settings for the PVC.

60.9.2 TLS PVC Set Command

Syntax:

```
ras> shdsl 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 <1,5,6~8>.
<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 SAM1316-22 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 265 TLS PVC Set Command Example

```
ras> shdsl tlspvc set 2 1 33 DEFVAL 100 0
```

60.9.3 TLS PVC Show Command

Syntax:

```
ras> shdsl 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 <1,5,6~8>.
<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.

Figure 266 TLS PVC Show Command Example

```
ras> shdsl tlspvc show 2
port vpi   vci  pvid pri DS/US vcprofile
---- --- ----- ----- --- ----------------------------------
   2   1    33   100   0 DEFVAL
```

61

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.

61.1 ACL Profile Commands

Use these commands to set up ACL profiles.

61.1.1 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 267 ACL Profile Set Command Example

```
ras> switch acl profile set test vlan 10 priority 2 rate 1000 rpri 7
```

61.1.2 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.

61.1.3 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 268 ACL Profile Show Map Command Example

```
ras> switch acl profile showmap test
profile: test
port type   vpi   vci
---- ------ --- -----
```

61.1.4 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 269 ACL Profile Show Command Example

```
ras> switch acl profile show test
profile test:
rule:
  vlan   :10
  priority:2

action:
  rpri    :7
  rate    :1000
```

61.2 ACL Assignment Commands

Use these commands to apply ACL profiles to PVCs.

61.2.1 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 <1,5,6~8>.
<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 270 ACL Assignment Set Command Example

```
ras> switch acl set 1 0 33 test
```

61.2.2 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 <1,5,6~8>.
<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.

61.2.3 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 <1,5,6~8>.
<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 271 ACL Assignment Show Command Example

```
ras> switch acl show
port vpi   vci type profile
---- --- ----- ---- --------------------------------
   1   0    33 PVC  test
```

62

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.

62.1 The SYS LED Does Not Turn On

The SYS LED does not turn on.

Table 109 SYS LED Troubleshooting

STEP	CORRECTIVE ACTION
1	Make sure the SAM1316-22 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.

62.2 The ALM LED Is On

The **ALM** (alarm) LED lights when the SAM1316-22 is overheated or the voltage readings are outside the tolerance levels.

Table 110 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 SAM1316-22 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.

62.3 LAN Port LEDs Do Not Turn On

A LAN port's LEDs do not turn on.

Table 111 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.

62.4 LAN Port Data Transmission

The LAN port's LED is on, but data cannot be transmitted.

Table 112 Troubleshooting Data Transmission

STEPS	CORRECTIVE ACTION
1	Make sure that the LAN port has the appropriate mode setting.
2	Make sure that the SAM1316-22's IP settings are properly configured.
3	Check the VLAN configuration.
4	Ping the SAM1316-22 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.

62.5 DSL Data Transmission

The DSL link is up, but data cannot be transmitted.

Table 113 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 SAM1316-22's DSL port's data rates are set high enough.
2	Check the VLAN configuration.
3	Ping the SAM1316-22 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.

62.6 Local Server

The computer behind a DSL modem or router cannot access a local server connected to the SAM1316-22.

Table 114 Troubleshooting a Local Server

STEPS	CORRECTIVE ACTION
1	See Section 62.5 on page 437 to make sure that the subscriber is able to transmit to the SAM1316-22.
2	Make sure the computer behind the DSL device has the correct gateway IP address configured.
3	Check the VLAN configuration (see Chapter 17 on page 133).
4	Check the cable and connections between the SAM1316-22 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.

62.7 Data Rate

The SYNC-rate is not the same as the configured rate.

Table 115 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.

62.8 Configured Settings

The configured settings do not take effect.

Table 116 Troubleshooting the SAM1316-22's Configured Settings

CORRECTIVE ACTION
Use the "config save" command after you finish configuring to save the SAM1316-22's settings.

62.9 Password

If you forget your password, you will need to use the console port to reload the factory-default configuration file (see Section 62.13 on page 440).

62.10 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 62.13 on page 440.

62.11 SNMP

The SNMP manager server cannot get information from the SAM1316-22.

Table 117 Troubleshooting the SNMP Server

STEPS	CORRECTIVE ACTION
1	Ping the SAM1316-22 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 SAM1316-22 matches the SNMP server's community.
3	Make sure that your computer's IP address matches a configured trusted host IP address or secured client IP address.
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.

62.12 Telnet

I cannot telnet into the SAM1316-22.

Table 118 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 SAM1316-22 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 SAM1316-22 uses for Telnet.

Table 118 Troubleshooting Telnet (continued)

STEPS	CORRECTIVE ACTION
4	Ping the SAM1316-22 from your computer. If you are able to ping the SAM1316-22 but are still unable to telnet, contact the distributor. If you cannot ping the SAM1316-22, 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.

62.13 Resetting the Defaults

If you lock yourself (and others) from the SAM1316-22, 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.

62.13.1 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 3.2.1 on page 38 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 SAM1316-22 restarts.

Figure 272 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 SAM1316-22 is now reinitialized with a default configuration file including the default user name of “admin” and the default password of “1234”.

62.13.2 Uploading the Default Configuration File

If you forget your password or cannot access the SAM1316-22, 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.

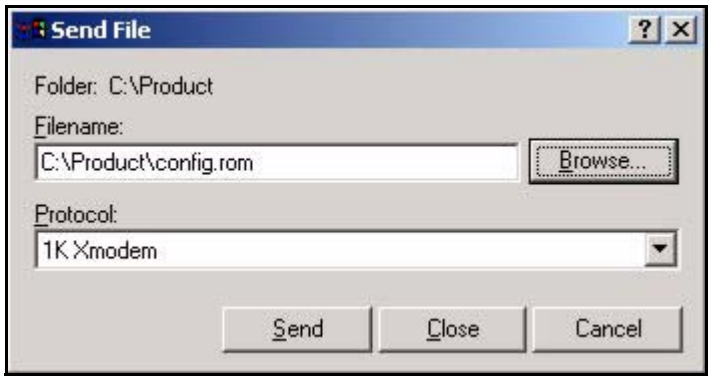
Note: Uploading the factory default configuration file erases the SAM1316-22’s entire configuration.

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 SAM1316-22’s console port. Turn the SAM1316-22 off and then on to begin a session. When you turn on the SAM1316-22 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 273 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 SAM1316-22.

The SAM1316-22 is now reinitialized with a default configuration file including the default password of “1234”.

62.14 Recovering the Firmware

Usually you should use FTP or the web configurator to upload the SAM1316-22’s firmware. If the SAM1316-22 will not start up, the firmware may be lost or corrupted. Use the following procedure to upload firmware to the SAM1316-22 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 SAM1316-22 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 SAM1316-22.

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 274 Example Xmodem Upload

Type the firmware file's location, or click **Browse** to search for it. Choose the **1K Xmodem** protocol. Then click **Send**.

10 After a successful firmware upload, type atgo to restart the SAM1316-22. The console port speed automatically changes back to 9600 bps when the SAM1316-22 restarts.

63

Specifications

This chapter provides the specifications for the SAM1316-22.

Table 119 Default Settings

VLAN Default Settings	One VLAN is created (this is also the management VLAN).
VID:	1
Registration:	Fixed for the Ethernet and DSL ports
Tagging:	Untagged for all ports
SHDSL Default Settings	
Enable/Disable State:	Enabled
Port Profile Default Settings	
Name:	DEFVAL
Profile Status:	Active
Max Rate	2304 Kbps
Min Rate	192 Kbps
Annex Mode	Annex B
Wire Pair	2-wire
Line Probe	Off
Current Condition SNR Margin	0 dB
Worst Case SNR Margin	0 dB
Virtual Channel Default Settings[A].	
Super channel:	Enabled
VPI:	0
VCI:	33
VC Profile:	DEFVAL (factory default)
Default VC Profile Settings	
DEFVAL Profile Settings	
Multiplexing:	LLC-based
Traffic Class:	UBR
PCR:	300000 cells/second
CDVT:	0
VC Profile:	DEFVAL_VC
Multiplexing:	VC-based

Table 119 Default Settings (continued)

Traffic Class:	UBR
PCR:	300000 cells/second
CDVT:	0
Default IGMP Filter Profile Settings	The **DEFVAL** IGMP filter profile is assigned to all of the DSL ports by default. It allows a port to join all multicast IP addresses (224.0.0.0~239.255.255.255).

A. The SAM1316-22 DSL ports' PVCs use ATM Adaptation Layer (AAL) 5.

Table 120 Hardware Specifications

FEATURE	DESCRIPTION
SHDSL	Standard Compliant - ETSI SDSL (ETSI TS 101 524 V 1.2.1) - ITU G.shdsl (ITU-T G.991.2 (2001)) - ITU G.shdls.bis (ITU-T G.991.2 (2004)) Line coding: TC-PAM Transmit power: up to 16.8 dBm Density: 16 ports per chip SHDSL payload format: ATM Rate Adaptation Mode: fixed, line probing 192-5696 Kbps (single pair) 2-wire, 4-wire, and 8-wire bonding Annex A and annex B PSD mask SHDSL line profile SHDSL alarm profile Power backoff
Connections	One Telco 50 connectors for 16-port G.SHDSL.bis One mini RJ11 console port for local management Two 10/100Base-TX for uplink
Power	15 VDC, 25 Watts
Temperature	Operating: 0 ~ 60 Storage: -40 ~ 70
Humidity	Operating 10 ~ 90% (non-condensing) Storage 10 ~ 95% (non-condensing)
Dimensions	166.8 mm (W) x 296 mm (D) x 44.45 mm (H)

The following table shows the specifications for wire gauge.

Note: Make sure you use wires of the specified wire gauge.

Table 121 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.

Table 122 Firmware Specifications

FEATURE	DESCRIPTION
SHDSL	Standard Compliant - ITU-T G.991.2 (2004) - Line probing - Annex F and Annex G (.bis mode) Support Protocols: multiple Protocols over AAL5 (RFC 2684). Support LLC and VC multiplexing modes. Monitor of SHDSL lines quality Multiple PVC support - PVC to VLAN mapping - 802.1p default priority - PVC with traffic class (UBR, CBR, nrt-VBR, rt-VBR) - Full range VPI and VCI OAM F5 end-to-end loopback (ATM mode)
Ethernet	Standalone and daisy chain mode RSTP support
Bridging	IEEE 802.1Q VLAN aware bridging - Accept untagged packets from SHDSL ports - Accept tagged and untagged packets from Ethernet interface - GVRP Port isolation

Table 122 Firmware Specifications (continued)

FEATURE	DESCRIPTION
Packet filtering	MAC count limiting MAC filtering: only selected MACs can pass through PPPoE filtering (pass-through/filter out) IGMP filtering (pass-through/filter out) DHCP filtering (pass-through/filter out) NetBIOS filtering (pass-through/filter out) IEEE 802.1X (EAPOL) filtering (pass-through/filter out) IP filtering (pass-through/filter out) ARP filtering (pass-through/filter out)
QoS	Four output priority queues with packet priority scheduling Packet prioritizing per 802.1p - Static configuration – default priority setting - 4 priority queues per PVC (up to 4 PVCs)
Broadband access support	DHCP snooping DHCP relay agent option 82 IEEE 802.1x port-based authentication with remote radius server
Multicast	IPv4 multicast forwarding (through L2 MAC) Static multicast membership configuration IGMP v1& v2 snooping & IGMP proxy mode support Shared VLAN multicast IGMP filtering profile IGMP count limiting MVLAN DSL port multicast bandwidth control

Table 122 Firmware Specifications (continued)

FEATURE	DESCRIPTION
Management support	CLI-based management from console/Ethernet port SNMPV1,v2 and telnet through in-band Ethernet port Web-based management through in-band Ethernet port Secured Host: configure remote host IP addresses for management UNIX syslog F/W upgrade, configuration backup & restore via FTP and Web Text-based configuration file support SHDSL port configuration Alarm/Status Surveillance – Automatic alarm and status report – LED indication for alarm and system status – Alarm/event history Performance monitoring – Periodical DSL performance counter update Security and Memory Backup – Support login authorization – Provides non-volatile memory to back-up system database – Keep previous system parameters during re-booting Self diagnostics – FLASH memory – DRAM – LAN port – Line interface loop-back test Remote reset

Table 122 Firmware Specifications (continued)

FEATURE	DESCRIPTION
Supported MIB	RFC1213 SNMP MIB II RFC1493 Bridge MIB RFC1643 Ethernet MIB RFC1757 RMON MIB, group 1,2,3,9 RFC2674 Q MIB RFC4319 SHDSL Line MIB ZyXEL proprietary MIB: AESCommon.mib, AS.mib, AS-ATM.mib, IESCommon.mib, ies1000.mib
Additional	Downstream Broadcast control per DSL port per VLAN RFC 2684 routed mode PPPoA to PPPoE conversion Broadcast storm control DHCP IP, MAC anti-spoofing Alarm severity assignment table Access Control Logic support

Per system limitations:

- Number of VLAN: 256
- SHDSL profile: 24
- ATM profile: 48
- IGMP filter profile: 32
- SHDSL ALARM profile: 24
- Dot1X profile: 64
- DHCP relay server: 32
- IP ROUTE: 128
- Static multicast address: 32
- IGMP groups: 256 groups (18 members per group)
- MAC learning: 10k (128 per SHDSL port, 4k per ENET port)
- RPVC gateway IP address: 96
- RPVC routing entries: 96
- ACL profile: 128

Per DSL port limitations:

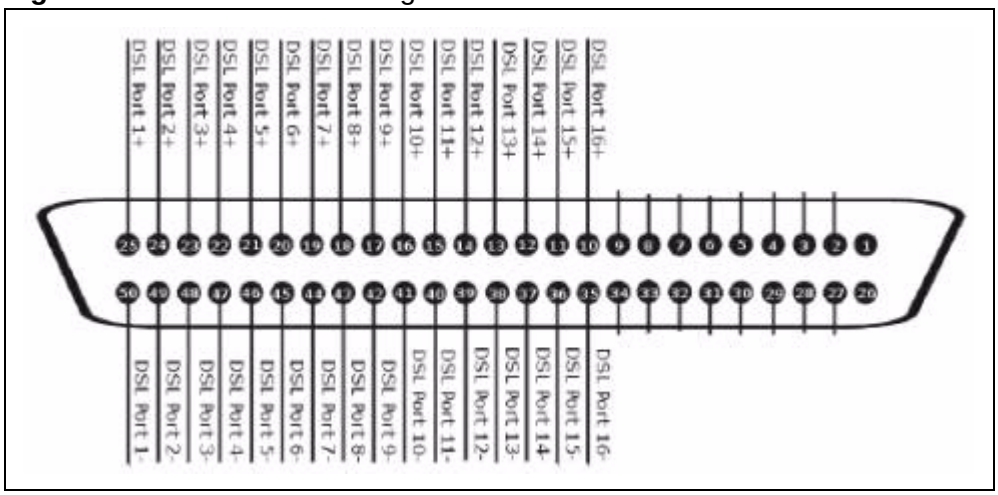
- Number of MAC filter: 10

- 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 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

63.1 Hardware Telco-50 Connector Pin Assignments

The following diagram shows the pin assignments of the Telco-50 connector.

Figure 275 Telco-50 Pin Assignments



This table lists the ports and matching pin numbers for the hardware Telco-50 connectors.

Table 123 Hardware Telco-50 Connector Port and Pin Numbers

PORT NUMBER	PIN NUMBER
1	25, 50
2	24, 49

Table 123 Hardware Telco-50 Connector Port and Pin Numbers (continued)

PORT NUMBER	PIN NUMBER
3	23, 48
4	22, 47
5	21, 46
6	20, 45
7	19, 44
8	18, 43
9	17, 42
10	16, 41
11	15, 40
12	14, 39
13	13, 38
14	12, 37
15	11, 36
16	10, 35

63.2 Console Cable Pin Assignments

The following diagrams and chart show the pin assignments of the console cable.

Figure 276 Console Cable RJ-11 Male Connector

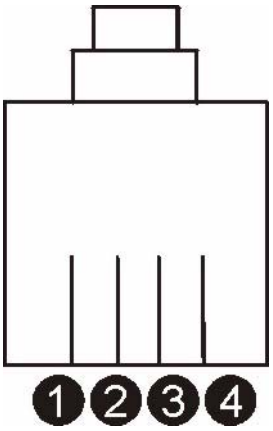


Figure 277 Console Cable DB-9 Female Connector

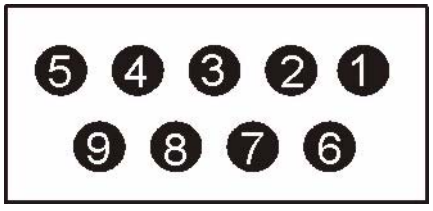


Table 124 Console Cable Connector Pin Assignments

RJ-11 MALE	DB-9 FEMALE
Pin 2: TXD	Pin 2
Pin 3: RXD	Pin 3
Pin 4: GND	Pin 5

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.

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.

Index

Numerics

2684 routed mode 410
4-wire 107
8-wire 107

A

Access Control 229
acl ouifilter commands 361
Address Resolution Protocol. See ARP.
aging time 85
alarm commands 303
Alarm Profile Screen 116, 117
ALM LED
  troubleshooting 435
American Wire Gauge (AWG) 447
Annex A 109
Annex B 109
ARP 162, 271
  table 271
ATM F5 266
ATM Forum Traffic Management 4.0 Specification 110
ATM QoS 110
ATM traffic class 110, 114
authentication 78
  default privilege level for administrators 80
  modes for administrators 79
  user 78
authentication modes
  administrator 79

B

back up configuration 263
Bridge Protocol Data Units (BPDU) 168
Burst Tolerance (BT) 112

C

Canonical Format Indicator (CFI) 134
Cell Delay Variation Tolerance (CDVT) 112
certifications 455
  notices 456
  viewing 456
CI 273
CI commands. See commands.
CLI 273
CLI commands. See commands.
Command Line Interface. See CI or CLI.
commands 273, 274
  abbreviations 273
  acl dhcpsnoop pool delete 321
  acl dhcpsnoop pool set 320
  acl ouifilter disable 361
  acl ouifilter enable 361
  acl ouifilter mode 361
  acl ouifilter set 362
  acl ouifilter show 362
  switch isolation vlan delete 299
  switch isolation vlan set 300
config save 274
configuration
  back up 263, 375
  file names 375
  restore 262, 375
  using FTP 375
console port 38, 442
  pin assignments 453
Constant Bit Rate (CBR) 110
contact person's name 76
copyright 455
CRC anomalies 127
Cyclic Redundancy Checking 398

D

Daytime (RFC 867) 76
default gateway 87
default privilege level 80
DEFVAL 98
DEFVAL profile settings 445
DEFVAL_VC 98
DHCP 162, 183
DHCP relay 183
  option 82 183
Diagnostic 265
disclaimer 455
double-tagged frames 213
downstream (traffic) 91
DSL port statistics 64
DSL profiles 91
  default 92
duplex 89
Dynamic Host Configuration Protocol. See DHCP.

E

EAPoL 162
encapsulation
  LLC 98
  VC Mux 98
EPL 96
Errored Seconds (ES) 126, 127, 394, 398
Estimated Power Loss 96
Ethernet address. See MAC address.
Ethernet port
  default settings 38
  statistics 61
Extensible Authentication Protocol. See EAPoL.

F

factory defaults 263, 440
FCC interference statement 455
filtering databases 324
firmware upgrade 261, 375
  file names 375
  using FTP 375
  when unable to use FTP 442
firmware version 72
front panel 37
  LEDs 37
  ports 38
FTP 264, 375
full duplex 89

G

GARP 81
GARP timer 85
GARP timer setup 81
General Setup 75
Generic Attribute Registration Protocol. See GARP.

H

hardware installation 33
Home screen 46, 59
host name 76

I

IEEE 802.1D. See STP.
IEEE 802.1Q. See VLAN.
IEEE 802.1w. See RSTP.
IEEE 802.1x 175, 178
IEEE 802.1x. See also RADIUS.
IGMP 162
  leave packets 144
  modes 148
  query packets 144
  report packets 144
IGMP Filter Profile Screen 119
IGMP snooping 141, 142
initial configuration 53

Internet Explorer 45, 53
Internet Group Multicast Protocol. See IGMP.
Internet Protocol. See IP.
IP 162
ip commands 369
IP Setup 87
ISDN 109

L

LEDs 37
line operating values 123
Line Performance 125
LLC 98
location 76
log format 307
logging out 51
Login screen 46
loopback test 266
Loss Of Sync Word Seconds (LOSWS) 398
Loss of Sync Word Seconds (LOSWS) 127

M

MAC address 72
MAC address learning 85
MAC filter 165
Management Information Base (MIB) 230
Maximum Burst Size (MBS) 111
Media Access Control. See MAC address.
metric 250
model 76
mpair4 107
multicast MAC address 154
Multicast VLAN. See MVLAN.
MVLAN 155

N

NetBIOS 162
Network Basic Input/Output System. See NetBIOS.
non real-time Variable Bit Rate (nrt-VBR) 111
NTP (RFC-1305) 76
N-wire Mode 107

O

OAM F5 Loopback 266
option 82 183
Organizationally Unique Identifier, See OUI 247
OUI 247
  filter 247

P

packet filter 161
password 50
Peak Cell Rate (PCR) 111
Permanent Virtual Circuit. See PVC.
ping 266
Point-to-Point Protocol over Ethernet. See PPPoE.
Port Security 181
Port Setup 89
Port VLAN ID. See PVID.
POTS 109
PPPoE 162
PPVC 406
PPVC Setup 103
PPVC Setup Members 104
priority queue assignment 86
product registration 457
PVC 97, 403
PVID 100
  default 134
PWR LED
  troubleshooting 435

Q

Q-in-Q. See TLS.
Quality of Service (QOS) 110

R

RADIUS 175
  shared secret 176
RADIUS Setup 176
Rapid Spanning Tree Protocol. See RSTP.
real-time Variable Bit Rate (rt-VBR) 111
reboot 264
Region Setting 109
registration
  product 457
related documentation 3
Remote Authentication Dial In User Service. See RADIUS.
Remote Management screen 234
restart 264
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 167
  port states 169
  See also STP.

S

safety warnings 7
save configuration 51
Secured Client Setup screen 234
Service Access Control 234
Service Provider's Network (SPN) 213
Severely Errored Seconds (SES) 126, 127, 394, 398
shared secret 80
shdsl alarmprofile commands 397
shdsl commands 385
shdsl paepvc commands 420
shdsl ppvc commands 406
shdsl pvc commands 403
SHDSL Rates 107
SHDSL rates 107
shdsl rpvc commands 410
shdsl tlspvc commands 425
shdsl vcprofile commands 401
Simple Network Management Protocol. See SNMP.
slot ID 76
SNMP 229
  commands 231
  Get 231
  GetNext 231
  manager 230
  MIBs 231
  supported versions 230
  Trap 231
  traps 231
SNMP screen 233
Spanning Tree Protocol. See STP.
specifications 445
static multicast filter 153
static route 249
  metric 250
Static VLAN. See SVLAN.
statistics
  DSL port 64
  Ethernet port 61
statistics dhcp commands 319
statistics igmpsnoop commands 349
statistics ip commands 373
statistics monitor command 300
statistics port command 301
statistics shdsl commands 391
stdio Timeout 76
STP 167
  Bridge Protocol Data Units (BPDU) 168
  designated bridge 168
  hello time 168

max age 168
path cost 167
port path cost 173
port priority 173
port states 169
root bridge 167
root port 167
super channel 97
Sustained Cell Rate (SCR) 111
SVLAN 324
switch acl commands 432
switch acl profile commands 429
switch dhcprelay commands 311
switch dhcpsnoop commands 317
switch igmpfilter commands 341
switch igmpsnoop bandwidth commands 344
switch igmpsnoop commands 339
switch igmpsnoop igmpcount commands 347
switch igmpsnoop mvlan commands 351
switch isolation commands 298
switch mac count commands 336
switch mac filter commands 333
switch pktfilter commands 365
Switch Setup 84
switch vlan commands 324
syntax conventions 5
sys commands 297
SYS LED
troubleshooting 435
sys snmp commands 381
syslog 227
System Information 71
system log 266
system up time 59

T

Tag Control Information (TCI) 134
Tag Protocol Identifier (TPID) 134
tagged VLAN. See VLAN.
telco-50 connector
pin assignments 451
temperature 72
terminal emulation 442
Theoretical Arrival Time (TAT) 112
Time (RFC-868) 76
time server protocols supported 76
time zone 76
TLS 213
trademarks 455
traffic parameters 111
traffic shaping 110
Transparent LAN Service. See TLS.
troubleshooting 435

U

UnAvailable Seconds (UAS) 126, 127, 394, 398
UNIX syslog 227
Unspecified Bit Rate (UBR) 111
up time 60
upstream (traffic) 91
User Account 77

V

Variable Bit Rate (VBR) 110
VC 98
VC Mux 98
VC Profile Screen 114
VC Setup 98
virtual channel 97
downstream profile 100
profile 98
upstream profile 100
Virtual Circuit. See VC.
Virtual Local Area Network. See VLAN.
VLAN 133
explicit tagging 323
forwarding 134
implicit tagging 323
priority frame 134
registration information 324
VLAN ID 133
VLAN ID, maximum number of 134

when VLAN ID is zero 134
VLAN stacking. See TLS.
voltage 72

W

warranty 457
note 457

X

XMODEM upload 441, 442