Prestige 662HW Series

802.11g Wireless ADSL2+ 4-Port Security Gateway

User's Guide

Version 3.40
August 2004

ZyXEL
Unleash Networking Power

Copyright

Disclaimer

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.

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.

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

If this equipment does cause harmful interference to radio/television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

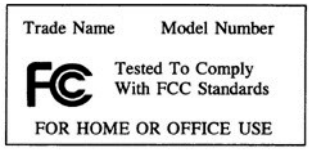
Notice 1

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This product has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

Certifications

1. Go to www.zyxel.com
2. Select your product from the drop-down list box 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 value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product is 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 of character to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Safety Warnings

1. To reduce the risk of fire, use only No. 26 AWG or larger telephone wire.
2. Do not use this product near water, for example, in a wet basement or near a swimming pool.
3. Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightening.

Customer Support

Please have the following information ready when you contact customer support.

- 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.

METHOD LOCATION	SUPPORT E-MAIL SALES E-MAIL	TELEPHONE[A] FAX	WEB SITE FTP SITE	REGULAR MAIL
WORLDWIDE	support@zyxel.com.tw sales@zyxel.com.tw	+886-3-578-3942 +886-3-578-2439	www.zyxel.com www.europe.zyxel.com ftp.zyxel.com ftp.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
NORTH AMERICA	support@zyxel.com sales@zyxel.com	+1-800-255-4101 +1-714-632-0882 +1-714-632-0858	www.us.zyxel.com ftp.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
GERMANY	support@zyxel.de sales@zyxel.de	+49-2405-6909-0 +49-2405-6909-99	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
FRANCE	info@zyxel.fr	+33 (0)4 72 52 97 97 +33 (0)4 72 52 19 20	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
SPAIN	support@zyxel.es sales@zyxel.es	+34 902 195 420 +34 913 005 345	www.zyxel.es	ZyXEL Communications Alejandro Villegas 33 1º, 28043 Madrid Spain
DENMARK	support@zyxel.dk sales@zyxel.dk	+45 39 55 07 00 +45 39 55 07 07	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 5 2860 Soeborg Denmark
NORWAY	support@zyxel.no sales@zyxel.no	+47 22 80 61 80 +47 22 80 61 81	www.zyxel.no	ZyXEL Communications A/S Nils Hansens vei 13 0667 Oslo Norway
SWEDEN	support@zyxel.se sales@zyxel.se	+46 31 744 7700 +46 31 744 7701	www.zyxel.se	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden
FINLAND	support@zyxel.fi sales@zyxel.fi	+358-9-4780-8411 +358-9-4780 8448	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland

a. "+" is the (prefix) number you enter to make an international telephone call.

Table of Contents

Copyright **2**

Federal Communications Commission (FCC) Interference Statement **3**

ZyXEL Limited Warranty **4**

Customer Support **5**

Table of Contents **8**

List of Figures **26**

List of Tables **34**

Preface **40**

Introduction to DSL **42**

Chapter 1
Getting To Know Your Prestige **44**

1.1 Introducing the Prestige 44
1.1.1 Features of the Prestige 45
1.1.2 Applications for the Prestige 50
1.1.2.1 Internet Access 51
1.1.3 Firewall for Secure Broadband Internet Access 51
1.1.3.1 LAN to LAN Application 51
1.1.4 Prestige Hardware Installation and Connection 52

Chapter 2
Introducing the Web Configurator **54**

2.1 Web Configurator Overview 54
2.1.1 Accessing the Prestige Web Configurator 54
2.1.2 Resetting the Prestige 55
2.1.2.1 Using the Reset Button 55
2.1.3 Navigating the Prestige Web Configurator 56

Chapter 3
Wizard Setup for Internet Access **60**

3.1 Introduction 60

3.1.1 Encapsulation 60
3.1.1.1 ENET ENCAP 60
3.1.1.2 PPP over Ethernet 60
3.1.1.3 PPPoA 60
3.1.1.4 RFC 1483 61
3.1.2 Multiplexing 61
3.1.2.1 VC-based Multiplexing 61
3.1.2.2 LLC-based Multiplexing 61
3.1.3 VPI and VCI 61
3.1.4 Internet Access Wizard Setup: First Screen 61
3.2 IP Address and Subnet Mask 62
3.2.1 IP Address Assignment 63
3.2.1.1 IP Assignment with PPPoA or PPPoE Encapsulation 63
3.2.1.2 IP Assignment with RFC 1483 Encapsulation 63
3.2.1.3 IP Assignment with ENET ENCAP Encapsulation 63
3.2.1.4 Private IP Addresses 64
3.2.2 Nailed-Up Connection (PPP) 64
3.2.3 NAT 64
3.2.4 Internet Access Wizard Setup: Second Screen 64
3.2.5 DHCP Setup 69
3.2.5.1 IP Pool Setup 69
3.2.6 Internet Access Wizard Setup: Third Screen 69
3.2.7 Internet Access Wizard Setup: Connection Test 70
3.2.7.1 Test Your Internet Connection 71

Chapter 4
Wizard Setup for Media Bandwidth Management 72

4.1 Introduction 72
4.1.1 Predefined Media Bandwidth Management Services 72
4.2 Media Bandwidth Management Setup 1 73
4.3 Media Bandwidth Mgnt. Wizard Setup: Second Screen 74
4.4 Media Bandwidth Mgnt. Wizard Setup: Finish 75

Chapter 5
Password Setup 76

5.1 Password Overview 76
5.1.1 Configuring Password 76

Chapter 6
LAN Setup 78

6.1 LAN Overview 78
6.1.1 LANs, WANs and the Prestige 78
6.2 DNS Server Address 79

6.3 DNS Server Address Assignment 79
6.4 LAN TCP/IP 80
6.4.1 Factory LAN Defaults 80
6.4.2 IP Address and Subnet Mask 80
6.4.3 RIP Setup 80
6.4.4 Multicast 81
6.5 Any IP 81
6.5.1 How Any IP Works 82
6.6 Configuring LAN 83
6.7 Configuring Static DHCP 84

Chapter 7
DMZ 86

7.1 Introduction 86
7.2 Configuring DMZ 86

Chapter 8
Wireless LAN Setup 90

8.1 Introduction 90
8.1.1 Additional Installation Requirements for Using 802.1x 90
8.1.2 Channel 90
8.1.3 ESS ID 91
8.1.4 RTS/CTS 91
8.1.5 Fragmentation Threshold 92
8.2 Levels of Security 92
8.3 Data Encryption with WEP 93
8.4 Configuring Wireless LAN 93
8.5 Configuring MAC Filter 95
8.6 Network Authentication 97
8.6.1 EAP 97
8.6.1.1 RADIUS 97
8.6.1.2 Types of RADIUS Messages 97
8.6.2 EAP Authentication Overview 98
8.7 Introduction to WPA 99
8.7.1 User Authentication 99
8.7.2 Encryption 99
8.8 WPA-PSK Application Example 100
8.9 WPA with RADIUS Application Example 100
8.10 Security Parameters Summary 101
8.11 Wireless Client WPA Supplicants 102
8.12 Configuring 802.1x and WPA 102
8.12.1 Authentication Required: 802.1x 103
8.12.2 Authentication Required: WPA 105

8.12.3 Authentication Required: WPA-PSK 106
8.13 Configuring Local User Authentication 108
8.14 Configuring RADIUS 109

Chapter 9
WAN Setup 112

9.1 WAN Overview 112
9.2 Metric 112
9.3 PPPoE Encapsulation 113
9.4 Traffic Shaping 113
9.5 Zero Configuration Internet Access 114
9.6 Configuring WAN Setup 114
9.7 Traffic Redirect 117
9.8 Configuring WAN Backup 118
9.9 Configuring Advanced WAN Backup 121
9.10 AT Command Strings 124
9.11 DTR Signal 124
9.12 Response Strings 124
9.13 Configuring Advanced Modem Setup 124

Chapter 10
Network Address Translation (NAT) Screens 128

10.1 NAT Overview 128
10.1.1 NAT Definitions 128
10.1.2 What NAT Does 129
10.1.3 How NAT Works 129
10.1.4 NAT Application 130
10.1.5 NAT Mapping Types 130
10.2 SUA (Single User Account) Versus NAT 131
10.3 SUA Server 132
10.3.1 Default Server IP Address 132
10.3.2 Port Forwarding: Services and Port Numbers 132
10.3.3 Configuring Servers Behind SUA (Example) 133
10.4 Selecting the NAT Mode 133
10.5 Configuring SUA Server 134
10.6 Configuring Address Mapping 136
10.7 Editing an Address Mapping Rule 137

Chapter 11
Dynamic DNS Setup 140

11.1 Dynamic DNS 140
11.1.1 DYNDNS Wildcard 140
11.2 Configuring Dynamic DNS 140

Chapter 12
Time and Date 142

12.1 Configuring Time and Date 142

Chapter 13
Firewalls 144

13.1 Firewall Overview 144
13.2 Types of Firewalls 144
13.2.1 Packet Filtering Firewalls 144
13.2.2 Application-level Firewalls 144
13.2.3 Stateful Inspection Firewalls 145
13.3 Introduction to ZyXEL's Firewall 145
13.3.1 Denial of Service Attacks 146
13.4 Denial of Service 146
13.4.1 Basics 146
13.4.2 Types of DoS Attacks 147
13.4.2.1 ICMP Vulnerability 149
13.4.2.2 Illegal Commands (NetBIOS and SMTP) 149
13.4.2.3 Traceroute 150
13.5 Stateful Inspection 150
13.5.1 Stateful Inspection Process 151
13.5.2 Stateful Inspection and the Prestige 152
13.5.3 TCP Security 152
13.5.4 UDP/ICMP Security 153
13.5.5 Upper Layer Protocols 153
13.6 Guidelines for Enhancing Security with Your Firewall 154
13.6.1 Security In General 154
13.7 Packet Filtering Vs Firewall 155
13.7.1 Packet Filtering: 155
13.7.1.1 When To Use Filtering 155
13.7.2 Firewall 155
13.7.2.1 When To Use The Firewall 156

Chapter 14
Firewall Configuration 158

14.1 Access Methods 158
14.2 Firewall Policies Overview 158
14.3 Rule Logic Overview 159
14.3.1 Rule Checklist 159
14.3.2 Security Ramifications 160
14.3.3 Key Fields For Configuring Rules 160
14.3.3.1 Action 160
14.3.3.2 Service 160

14.3.3.3 Source Address 160
14.3.3.4 Destination Address 161
14.4 Connection Direction Example 161
14.4.1 LAN to WAN Rules 161
14.4.2 WAN to LAN Rules 161
14.4.3 Alerts 162
14.5 Configuring Basic Firewall Settings 162
14.6 Rule Summary 164
14.6.1 Configuring Firewall Rules 165
14.7 Customized Services 168
14.8 Creating/Editing A Customized Service 168
14.9 Example Firewall Rule 169
14.10 Predefined Services 173
14.11 Anti-Probing 175
14.12 Configuring Attack Alert 176
14.12.1 Threshold Values 177
14.12.2 Half-Open Sessions 177
14.12.2.1 TCP Maximum Incomplete and Blocking Time 177

Chapter 15
Content Filtering 180

15.1 Content Filtering Overview 180
15.2 Configuring Keyword Blocking 180
15.3 Configuring the Schedule 181
15.4 Configuring Trusted Computers 182

Chapter 16
Content Access Control 184

16.1 Content Access Control Overview 184
16.1.1 Content Access Control WLAN Application 184
16.1.2 Configuration Steps 184
16.2 Activating CAC and Create User Groups 185
16.2.1 Configuring Time Schedule 186
16.2.2 Configuring Services 188
16.2.2.1 Available Services 189
16.2.3 Configuring Web Site Filters 191
16.2.4 Testing Web Site Access Privileges 197
16.3 User Account Setup 198
16.4 User Online Status 200
16.5 Content Access Control Logins 201
16.5.1 User Login 201
16.5.2 Administrator Login 202

Chapter 17
Anti-Virus Packet Scan 204

17.1 Overview 204
17.1.1 Types of Computer Viruses 204
17.2 Signature-Based Virus Scan 204
17.2.1 Computer Virus Infection and Prevention 205
17.3 Introduction to the Prestige Anti-virus Packet Scan 205
17.3.1 How the Prestige Virus Scan Works 206
17.3.2 Limitations of the Prestige Packet Scan 206
17.4 Anti-virus Packet Scan Configuration 207
17.5 Registration and Online Update 208
17.5.1 Updating the Anti Virus Packet Scan 210

Chapter 18
Introduction to IPSec 212

18.1 VPN Overview 212
18.1.1 IPSec 212
18.1.2 Security Association 212
18.1.3 Other Terminology 212
18.1.3.1 Encryption 212
18.1.3.2 Data Confidentiality 213
18.1.3.3 Data Integrity 213
18.1.3.4 Data Origin Authentication 213
18.1.4 VPN Applications 213
18.2 IPSec Architecture 213
18.2.1 IPSec Algorithms 214
18.2.2 Key Management 214
18.3 Encapsulation 214
18.3.1 Transport Mode 215
18.3.2 Tunnel Mode 215
18.4 IPSec and NAT 215

Chapter 19
VPN Screens 218

19.1 VPN/IPSec Overview 218
19.2 IPSec Algorithms 218
19.2.1 AH (Authentication Header) Protocol 218
19.2.2 ESP (Encapsulating Security Payload) Protocol 218
19.3 My IP Address 219
19.4 Secure Gateway Address 219
19.4.1 Dynamic Secure Gateway Address 220
19.5 VPN Summary Screen 220
19.6 Keep Alive 222

19.7 NAT Traversal 222
19.7.1 NAT Traversal Configuration 223
19.7.2 Remote DNS Server 223
19.8 ID Type and Content 224
19.8.1 ID Type and Content Examples 225
19.9 Pre-Shared Key 226
19.10 Editing VPN Policies 226
19.11 IKE Phases 231
19.11.1 Negotiation Mode 232
19.11.2 Diffie-Hellman (DH) Key Groups 233
19.11.3 Perfect Forward Secrecy (PFS) 233
19.12 Configuring Advanced IKE Settings 233
19.13 Manual Key Setup 236
19.13.1 Security Parameter Index (SPI) 236
19.14 Configuring Manual Key 237
19.15 Viewing SA Monitor 240
19.16 Configuring Global Setting 241
19.17 Telecommuter VPN/IPSec Examples 242
19.17.1 Telecommuters Sharing One VPN Rule Example 242
19.17.2 Telecommuters Using Unique VPN Rules Example 243
19.18 VPN and Remote Management 245

Chapter 20
Remote Management Configuration 246

20.1 Remote Management Overview 246
20.1.1 Remote Management Limitations 246
20.1.2 Remote Management and NAT 247
20.1.3 System Timeout 247
20.2 Telnet 247
20.3 FTP 247
20.4 Web 248
20.5 Configuring Remote Management 248

Chapter 21
Universal Plug-and-Play (UPnP) 250

21.1 Introducing Universal Plug and Play 250
21.1.1 How do I know if I'm using UPnP? 250
21.1.2 NAT Traversal 250
21.1.3 Cautions with UPnP 250
21.2 UPnP and ZyXEL 251
21.2.1 Configuring UPnP 251
21.3 Installing UPnP in Windows Example 252
21.4 Using UPnP in Windows XP Example 256

Chapter 22
Logs Screens 264

22.1 Logs Overview 264
22.1.1 Alerts and Logs 264
22.2 Configuring Log Settings 264
22.3 Displaying the Logs 266
22.4 SMTP Error Messages 267
22.4.1 Example E-mail Log 268

Chapter 23
Media Bandwidth Management Advanced Setup 270

23.1 Bandwidth Management Advanced Setup Overview 270
23.2 Bandwidth Classes and Filters 270
23.3 Proportional Bandwidth Allocation 271
23.4 Bandwidth Management Usage Examples 271
23.4.1 Application-based Bandwidth Management Example 271
23.4.2 Subnet-based Bandwidth Management Example 271
23.4.3 Application and Subnet-based Bandwidth Management Example 272
23.5 Scheduler 272
23.5.1 Priority-based Scheduler 273
23.5.2 Fairness-based Scheduler 273
23.6 Maximize Bandwidth Usage 273
23.6.1 Reserving Bandwidth for Non-Bandwidth Class Traffic 273
23.6.2 Maximize Bandwidth Usage Example 274
23.7 Bandwidth Borrowing 275
23.7.1 Bandwidth Borrowing Example 275
23.7.2 Maximize Bandwidth Usage With Bandwidth Borrowing 277
23.8 Configuring Summary 277
23.9 Configuring Class Setup 278
23.9.1 Media Bandwidth Management Class Configuration 279
23.9.2 Media Bandwidth Management Statistics 282
23.10 Bandwidth Monitor 283

Chapter 24
Maintenance 284

24.1 Maintenance Overview 284
24.2 System Status Screen 284
24.2.1 System Statistics 286
24.3 DHCP Table Screen 288
24.4 Any IP Table Screen 289
24.5 Wireless Screen 289
24.5.1 Association List 289
24.6 Diagnostic Screens 290

24.6.1 Diagnostic General Screen 290
24.6.2 Diagnostic DSL Line Screen 291
24.7 Firmware Screen 293

Chapter 25
Introducing the SMT 296

25.1 SMT Introduction 296
25.1.1 Procedure for SMT Configuration via Telnet 296
25.1.2 Entering Password 296
25.1.3 Prestige SMT Menu Overview 297
25.2 Navigating the SMT Interface 297
25.2.1 System Management Terminal Interface Summary 299
25.3 Changing the System Password 299

Chapter 26
Menu 1 General Setup 302

26.1 General Setup 302
26.2 Procedure To Configure Menu 1 302
26.2.1 Procedure to Configure Dynamic DNS 303

Chapter 27
Menu 2 WAN Backup Setup 306

27.1 Introduction to WAN Backup Setup 306
27.2 Configuring Dial Backup in Menu 2 306
27.2.1 Traffic Redirect Setup 307
27.3 Configuring Dial Backup Setup 308
27.4 Advanced Dial Backup Setup 309

Chapter 28
Menu 3 LAN Setup 312

28.1 LAN Setup 312
28.1.1 General Ethernet Setup 312
28.2 Protocol Dependent Ethernet Setup 313
28.3 CP/IP Ethernet Setup and DHCP 313

Chapter 29
Wireless LAN Setup 316

29.1 Wireless LAN Overview 316
29.2 Wireless LAN Setup 316
29.2.1 Wireless LAN MAC Address Filter 317

Chapter 30
Internet Access 320

30.1 Internet Access Overview 320
30.2 IP Policies 320
30.3 IP Alias 320
30.4 IP Alias Setup 321
30.5 Route IP Setup 322
30.6 Internet Access Configuration 323

Chapter 31
Remote Node Configuration 326

31.1 Remote Node Setup Overview 326
31.2 Remote Node Setup 326
31.2.1 Remote Node Profile 326
31.2.2 Encapsulation and Multiplexing Scenarios 327
31.2.2.1 Scenario 1: One VC, Multiple Protocols 327
31.2.2.2 Scenario 2: One VC, One Protocol (IP) 327
31.2.2.3 Scenario 3: Multiple VCs 327
31.2.3 Outgoing Authentication Protocol 329
31.3 Remote Node Network Layer Options 330
31.3.1 My WAN Addr Sample IP Addresses 331
31.4 Remote Node Filter 332
31.5 Editing ATM Layer Options 333
31.5.1 VC-based Multiplexing (non-PPP Encapsulation) 333
31.5.2 LLC-based Multiplexing or PPP Encapsulation 334
31.5.3 Advance Setup Options 334

Chapter 32
Static Route Setup 336

32.1 IP Static Route Overview 336
32.2 Configuration 336

Chapter 33
Bridging Setup 340

33.1 Bridging in General 340
33.2 Bridge Ethernet Setup 340
33.2.1 Remote Node Bridging Setup 340
33.2.2 Bridge Static Route Setup 342

Chapter 34
Network Address Translation (NAT) 344

34.1 Using NAT 344
34.1.1 SUA (Single User Account) Versus NAT 344

34.2 Applying NAT 344
34.3 NAT Setup 346
34.3.1 Address Mapping Sets 346
34.3.1.1 SUA Address Mapping Set 347
34.3.1.2 User-Defined Address Mapping Sets 348
34.3.1.3 Ordering Your Rules 349
34.4 Configuring a Server behind NAT 350
34.5 General NAT Examples 352
34.5.1 Example 1: Internet Access Only 352
34.5.2 Example 2: Internet Access with an Inside Server 353
34.5.3 Example 3: Multiple Public IP Addresses With Inside Servers 354
34.5.4 Example 4: NAT Unfriendly Application Programs 358

Chapter 35
Enabling the Firewall 360

35.1 Remote Management and the Firewall 360
35.2 Access Methods 360
35.3 Enabling the Firewall 360

Chapter 36
Filter Configuration 362

36.1 About Filtering 362
36.1.1 The Filter Structure of the Prestige 363
36.2 Configuring a Filter Set for the Prestige 364
36.3 Filter Rules Summary Menus 365
36.4 Configuring a Filter Rule 366
36.4.1 TCP/IP Filter Rule 367
36.4.2 Generic Filter Rule 369
36.5 Filter Types and NAT 371
36.6 Example Filter 371
36.7 Applying Filters and Factory Defaults 373
36.7.1 Ethernet Traffic 374
36.7.2 Remote Node Filters 374

Chapter 37
SNMP Configuration 376

37.1 About SNMP 376
37.2 Supported MIBs 377
37.3 SNMP Configuration 377
37.4 SNMP Traps 378

Chapter 38
System Security 380

38.1 System Security 380
38.1.1 System Password 380
38.1.2 Configuring External RADIUS Server 380
38.1.3 IEEE802.1x 382
38.2 Creating User Accounts on the Prestige 384

Chapter 39
System Information and Diagnosis 386

39.1 Overview 386
39.2 System Status 386
39.3 System Information 388
39.3.1 System Information 388
39.3.2 Console Port Speed 389
39.4 Log and Trace 390
39.4.1 Viewing Error Log 390
39.4.2 Syslog and Accounting 391
39.5 Diagnostic 393

Chapter 40
Firmware and Configuration File Maintenance 396

40.1 Filename Conventions 396
40.2 Backup Configuration 397
40.2.1 Backup Configuration 397
40.2.2 Using the FTP Command from the Command Line 398
40.2.3 Example of FTP Commands from the Command Line 398
40.2.4 GUI-based FTP Clients 399
40.2.5 TFTP and FTP over WAN Management Limitations 399
40.2.6 Backup Configuration Using TFTP 400
40.2.7 TFTP Command Example 400
40.2.8 GUI-based TFTP Clients 400
40.2.9 Backup Via Console Port 401
40.3 Restore Configuration 402
40.3.1 Restore Using FTP 402
40.3.2 Restore Using FTP Session Example 403
40.3.3 Restore Via Console Port 404
40.4 Uploading Firmware and Configuration Files 405
40.4.1 Firmware File Upload 405
40.4.2 Configuration File Upload 405
40.4.3 FTP File Upload Command from the DOS Prompt Example 406
40.4.4 FTP Session Example of Firmware File Upload 407
40.4.5 TFTP File Upload 407

40.4.6 TFTP Upload Command Example 408
40.4.7 Uploading Via Console Port 408
40.4.8 Uploading Firmware File Via Console Port 408
40.4.9 Example Xmodem Firmware Upload Using HyperTerminal 409
40.4.10 Uploading Configuration File Via Console Port 409
40.4.11 Example Xmodem Configuration Upload Using HyperTerminal 410

Chapter 41
System Maintenance 412

41.1 Command Interpreter Mode 412
41.2 Call Control Support 413
41.2.1 Budget Management 413
41.3 Time and Date Setting 414
41.3.1 Resetting the Time 416

Chapter 42
Remote Management 418

42.1 Remote Management Overview 418
42.2 Remote Management 418
42.2.1 Remote Management Setup 418
42.2.2 Remote Management Limitations 419
42.3 Remote Management and NAT 420
42.4 System Timeout 420

Chapter 43
IP Policy Routing 422

43.1 IP Policy Routing Overview 422
43.2 Benefits of IP Policy Routing 422
43.3 Routing Policy 422
43.4 IP Routing Policy Setup 423
43.5 Applying an IP Policy 426
43.5.1 Ethernet IP Policies 426
43.6 IP Policy Routing Example 427

Chapter 44
Call Scheduling 430

44.1 Introduction 430

Chapter 45
VPN/IPSec Setup 434

45.1 VPN/IPSec Overview 434
45.2 IPSec Summary Screen 435
45.3 IPSec Setup 437

45.4 IKE Setup 441
45.5 Manual Setup 443
45.5.1 Active Protocol 443
45.5.2 Security Parameter Index (SPI) 443

Chapter 46
SA Monitor 446

46.1 SA Monitor Overview 446
46.2 Using SA Monitor 446

Chapter 47
Internal SPTGEN 450

47.1 Internal SPTGEN Overview 450
47.2 The Configuration Text File Format 450
47.2.1 Internal SPTGEN File Modification - Important Points to Remember ...451
47.3 Internal SPTGEN FTP Download Example 451
47.4 Internal SPTGEN FTP Upload Example 452

Chapter 48
Troubleshooting 454

48.1 Problems Starting Up the Prestige 454
48.2 Problems with the LAN LED 454
48.3 Problems with the DSL LED 455
48.4 Problems with the LAN Interface 455
48.5 Problems with the WAN Interface 455
48.6 Problems with Internet Access 456
48.7 Problems with the Password 456
48.8 Problems with the Web Configurator 457
48.9 Problems with Remote Management 457

Appendix A
Pin Assignments 458

Appendix B
Setting up Your Computer's IP Address 460

Windows 95/98/Me..... 460
Configuring 462
Verifying Settings..... 463
Windows 2000/NT/XP 463
Verifying Settings..... 467
Macintosh OS 8/9..... 468
Verifying Settings..... 469
Macintosh OS X 469

Verifying Settings 471

Appendix C
IP Subnetting 472

IP Addressing 472
IP Classes 472
Subnet Masks 473
Subnetting 473
Example: Two Subnets 474
Example: Four Subnets 476
Example Eight Subnets 477
Subnetting With Class A and Class B Networks. 478

Appendix D
PPPoE 480

PPPoE in Action 480
Benefits of PPPoE 480
Traditional Dial-up Scenario 480
How PPPoE Works 481
Prestige as a PPPoE Client 481

Appendix E
Wireless LAN and IEEE 802.11 482

Benefits of a Wireless LAN 482
IEEE 802.11 482
Ad-hoc Wireless LAN Configuration 483
Infrastructure Wireless LAN Configuration 483

Appendix F
Wireless LAN With IEEE 802.1x 486

Security Flaws with IEEE 802.11 486
Deployment Issues with IEEE 802.11 486
IEEE 802.1x 486
Advantages of the IEEE 802.1x 486
RADIUS Server Authentication Sequence 487

Appendix G
Types of EAP Authentication 488

EAP-MD5 (Message-Digest Algorithm 5) 488
EAP-TLS (Transport Layer Security) 488
EAP-TTLS (Tunneled Transport Layer Service) 488
LEAP 489

Appendix H
Triangle Route 490

The Ideal Setup 490
The "Triangle Route" Problem 490
The "Triangle Route" Solutions 491
IP Aliasing 491
Gateways on the WAN Side 491

Appendix I
myZyXEL.com 494

Introduction 494
A Note on myZyXEL.com Numbers 494
myZyXEL.com Account Login 494
Registering Your ZyXEL Device 495
Activating a Service 498

Appendix J
Windows 98/Me Requirements for Anti-Virus Packet Scan Message Display 500

Appendix K
Example Internal SPTGEN Screens 504

Command Examples 524

Appendix L
Command Interpreter 526

Command Syntax 526
Command Usage 526

Appendix M
Firewall Commands 528

Appendix M Sys Firewall Commands 528

Appendix N
NetBIOS Filter Commands 530

Introduction 530
Display NetBIOS Filter Settings 530
NetBIOS Filter Configuration 531

Appendix O
Brute-Force Password Guessing Protection 534

Example 534

Appendix P
Boot Commands 536

Appendix Q
Log Descriptions 538

Log Commands 550
Configuring What You Want the Prestige to Log 550
Displaying Logs 551
Log Command Example 551

Index 552

List of Figures

Figure 1 Prestige Internet Access Application 51
Figure 2 Firewall Application 51
Figure 3 Prestige LAN-to-LAN Application 52
Figure 4 Password Screen 55
Figure 5 Change Password at Login 55
Figure 6 Web Configurator SITE MAP Screen 56
Figure 7 Internet Access Wizard Setup: First Screen 62
Figure 8 Internet Connection with PPPoE 65
Figure 9 Internet Connection with RFC 1483 66
Figure 10 Internet Connection with ENET ENCAP 67
Figure 11 Internet Connection with PPPoA 68
Figure 12 Internet Access Wizard Setup: Third Screen 69
Figure 13 Internet Access Wizard Setup: LAN Configuration 70
Figure 14 Internet Access Wizard Setup: Connection Tests 71
Figure 15 Media Bandwidth Mgnt. Wizard Setup: First Screen 74
Figure 16 Media Bandwidth Mgnt. Wizard Setup: Second Screen 75
Figure 17 Media Bandwidth Mgnt. Wizard Setup: Finish 75
Figure 18 Password 76
Figure 19 LAN and WAN IP Addresses 78
Figure 20 Any IP Example 82
Figure 21 LAN Setup 83
Figure 22 LAN: Static DHCP 85
Figure 23 DMZ 87
Figure 24 RTS/CTS 91
Figure 25 Prestige Wireless Security Levels 93
Figure 26 Wireless LAN 94
Figure 27 MAC Address Filter 96
Figure 28 EAP Authentication 98
Figure 29 WPA - PSK Authentication 100
Figure 30 WPA with RADIUS Application Example 101
Figure 31 Wireless LAN: 802.1x/WPA 102
Figure 32 Wireless LAN: 802.1x/WPA for 802.1x Protocol 103
Figure 33 Wireless LAN: 802.1x/WPA for WPA Protocol 105
Figure 34 Wireless LAN: 802.1x/WPA for WPA-PSK Protocol 107
Figure 35 Local User Database 108
Figure 36 RADIUS 109

Figure 37 Example of Traffic Shaping 114
Figure 38 WAN Setup (PPPoE) 115
Figure 39 Traffic Redirect Example 118
Figure 40 Traffic Redirect LAN Setup 118
Figure 41 WAN Backup 119
Figure 42 Advanced WAN Backup 121
Figure 43 Advanced Modem Setup 125
Figure 44 How NAT Works 130
Figure 45 NAT Application With IP Alias 130
Figure 46 Multiple Servers Behind NAT Example 133
Figure 47 NAT Mode 134
Figure 48 Edit SUA/NAT Server Set 135
Figure 49 Address Mapping Rules 136
Figure 50 Address Mapping Rule Edit 137
Figure 51 Dynamic DNS 141
Figure 52 Time and Date 142
Figure 53 Prestige Firewall Application 146
Figure 54 Three-Way Handshake 148
Figure 55 SYN Flood 148
Figure 56 Smurf Attack 149
Figure 57 Stateful Inspection 151
Figure 58 LAN to WAN Traffic 161
Figure 59 WAN to LAN Traffic 162
Figure 60 Firewall: Default Policy 163
Figure 61 Firewall: Rule Summary 164
Figure 62 Firewall: Edit Rule 166
Figure 63 Firewall: Customized Services 168
Figure 64 Firewall: Configure Customized Services 169
Figure 65 Firewall Example: Rule Summary 170
Figure 66 Firewall Example: Edit Rule: Destination Address 171
Figure 67 Edit Custom Port Example 171
Figure 68 Firewall Example: Edit Rule: Select Customized Services 172
Figure 69 Firewall Example: Rule Summary: My Service 173
Figure 70 Firewall: Anti Probing 176
Figure 71 Firewall: Threshold 178
Figure 72 Content Filter: Keyword 181
Figure 73 Content Filter: Schedule 182
Figure 74 Content Filter: Trusted 183
Figure 75 Content Access Control with WLAN Application 184
Figure 76 Content Access Control: General 185
Figure 77 Control Access Control: General: Time Scheduling 187
Figure 78 Content Access Control: General: Services 188
Figure 79 Content Access Control: General: Web Site Filter 192

Figure 80 Content Access Control: General: Diagnose 198
Figure 81 Content Access Control: User Profiles 199
Figure 82 Content Access Control: Online Status 200
Figure 83 Content Access Control: User Login Screen 201
Figure 84 Content Access Control: User Logout Screen 201
Figure 85 Prestige Anti-virus Application 205
Figure 86 Anti Virus: Packet Scan 207
Figure 87 Anti Virus: Registration and Virus Information Update 209
Figure 88 Virus Scan Update in Progress 210
Figure 89 Virus Scan Update Successful 210
Figure 90 Encryption and Decryption 213
Figure 91 IPSec Architecture 214
Figure 92 Transport and Tunnel Mode IPSec Encapsulation 215
Figure 93 IPSec Summary Fields 220
Figure 94 VPN Summary 221
Figure 95 NAT Router Between IPSec Routers 223
Figure 96 VPN Host using Intranet DNS Server Example 224
Figure 97 VPN IKE 227
Figure 98 Two Phases to Set Up the IPSec SA 232
Figure 99 VPN IKE: Advanced Setup 234
Figure 100 VPN: Manual Key 237
Figure 101 VPN: SA Monitor 240
Figure 102 VPN: Global Setting 241
Figure 103 Telecommuters Sharing One VPN Rule Example 242
Figure 104 Telecommuters Using Unique VPN Rules Example 244
Figure 105 Telnet Configuration on a TCP/IP Network 247
Figure 106 Remote Management 248
Figure 107 Configuring UPnP 251
Figure 108 Add/Remove Programs: Windows Setup: Communication 253
Figure 109 Add/Remove Programs: Windows Setup: Communication: Components 253
Figure 110 Network Connections 254
Figure 111 Windows Optional Networking Components Wizard 255
Figure 112 Networking Services 256
Figure 113 Network Connections 257
Figure 114 Internet Connection Properties 258
Figure 115 Internet Connection Properties: Advanced Settings 259
Figure 116 Internet Connection Properties: Advanced Settings: Add 259
Figure 117 System Tray Icon 260
Figure 118 Internet Connection Status 260
Figure 119 Network Connections 261
Figure 120 Network Connections: My Network Places 262
Figure 121 Network Connections: My Network Places: Properties: Example 262
Figure 122 Log Settings 265

Figure 123 View Logs 267
Figure 124 E-mail Log Example 268
Figure 125 Application-based Bandwidth Management Example 271
Figure 126 Subnet-based Bandwidth Management Example 272
Figure 127 Application and Subnet-based Bandwidth Management Example 272
Figure 128 Bandwidth Allotment Example 274
Figure 129 Maximize Bandwidth Usage Example 275
Figure 130 Bandwidth Borrowing Example 276
Figure 131 Media Bandwidth Management: Summary 277
Figure 132 Media Bandwidth Management: Class Setup 279
Figure 133 Media Bandwidth Management: Class Configuration 280
Figure 134 Media Bandwidth Management Statistics 282
Figure 135 Media Bandwidth Management: Monitor 283
Figure 136 System Status 285
Figure 137 System Status: Show Statistics 287
Figure 138 DHCP Table 288
Figure 139 Any IP Table 289
Figure 140 Association List 290
Figure 141 Diagnostic: General 291
Figure 142 Diagnostic: DSL Line 292
Figure 143 Firmware Upgrade 293
Figure 144 Network Temporarily Disconnected 294
Figure 145 Error Message 294
Figure 146 Login Screen 297
Figure 147 Prestige SMT Menu Overview 297
Figure 148 Menu 23.1 Change Password 300
Figure 149 Menu 1 General Setup 303
Figure 150 Menu 1.1 Configure Dynamic DNS 304
Figure 151 Menu 2 WAN Backup Setup 306
Figure 152 Menu 2.1Traffic Redirect Setup 307
Figure 153 Menu 2.2 Dial Backup Setup 308
Figure 154 Menu 2.2.1 Advanced Dial Backup Setup 310
Figure 155 Menu 3 LAN Setup 312
Figure 156 Menu 3.1 LAN Port Filter Setup 312
Figure 157 Menu 3.2 TCP/IP and DHCP Ethernet Setup 314
Figure 158 Menu 3.5 - Wireless LAN Setup 316
Figure 159 Menu 3.5.1 WLAN MAC Address Filtering 318
Figure 160 IP Alias Network Example 321
Figure 161 Menu 3.2 TCP/IP and DHCP Setup 321
Figure 162 Menu 3.2.1 IP Alias Setup 322
Figure 163 Menu 1 General Setup 323
Figure 164 Menu 4 Internet Access Setup 323
Figure 165 Menu 11 Remote Node Setup 327

Figure 166 Menu 11.1 Remote Node Profile 328
Figure 167 Menu 11.3 Remote Node Network Layer Options 330
Figure 168 Sample IP Addresses for a TCP/IP LAN-to-LAN Connection 332
Figure 169 Menu 11.5 Remote Node Filter (RFC 1483 or ENET Encapsulation) 333
Figure 170 Menu 11.5 Remote Node Filter (PPPoA or PPPoE Encapsulation) 333
Figure 171 Menu 11.6 for VC-based Multiplexing 334
Figure 172 Menu 11.6 for LLC-based Multiplexing or PPP Encapsulation 334
Figure 173 Menu 11.1 Remote Node Profile 335
Figure 174 Menu 11.8 Advance Setup Options 335
Figure 175 Sample Static Routing Topology 336
Figure 176 Menu 12 Static Route Setup 337
Figure 177 Menu 12.1 IP Static Route Setup 337
Figure 178 Menu12.1.1 Edit IP Static Route 337
Figure 179 Menu 11.1 Remote Node Profile 341
Figure 180 Menu 11.3 Remote Node Network Layer Options 341
Figure 181 Menu 12.3.1 Edit Bridge Static Route 342
Figure 182 Menu 4 Applying NAT for Internet Access 345
Figure 183 Applying NAT in Menus 4 & 11.3 345
Figure 184 Menu 15 NAT Setup 346
Figure 185 Menu 15.1 Address Mapping Sets 347
Figure 186 Menu 15.1.255 SUA Address Mapping Rules 347
Figure 187 Menu 15.1.1 First Set 348
Figure 188 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set 350
Figure 189 Menu 15.2 NAT Server Setup 351
Figure 190 Menu 15.2.1 NAT Server Setup 351
Figure 191 Multiple Servers Behind NAT Example 352
Figure 192 NAT Example 1 353
Figure 193 Menu 4 Internet Access & NAT Example 353
Figure 194 NAT Example 2 354
Figure 195 Menu 15.2.1 Specifying an Inside Server 354
Figure 196 NAT Example 3 355
Figure 197 Example 3: Menu 11.3 356
Figure 198 Example 3: Menu 15.1.1.1 356
Figure 199 Example 3: Final Menu 15.1.1 357
Figure 200 Example 3: Menu 15.2.1 358
Figure 201 NAT Example 4 358
Figure 202 Example 4: Menu 15.1.1.1 Address Mapping Rule 359
Figure 203 Example 4: Menu 15.1.1 Address Mapping Rules 359
Figure 204 Menu 21.2 Firewall Setup 361
Figure 205 Outgoing Packet Filtering Process 362
Figure 206 Filter Rule Process 363
Figure 207 Menu 21 Filter Set Configuration 364
Figure 208 NetBIOS_WAN Filter Rules Summary 364

Figure 209 NetBIOS_LAN Filter Rules Summary 365
Figure 210 IGMP Filter Rules Summary 365
Figure 211 Menu 21.1.x.1 TCP/IP Filter Rule 367
Figure 212 Executing an IP Filter 369
Figure 213 Menu 21.1.5.1 Generic Filter Rule 370
Figure 214 Protocol and Device Filter Sets 371
Figure 215 Sample Telnet Filter 372
Figure 216 Menu 21.1.6.1 Sample Filter 372
Figure 217 Menu 21.1.6.1 Sample Filter Rules Summary 373
Figure 218 Filtering Ethernet Traffic 374
Figure 219 Filtering Remote Node Traffic 374
Figure 220 SNMP Management Model 376
Figure 221 Menu 22 SNMP Configuration 378
Figure 222 Menu 23 – System Security 380
Figure 223 Menu 23 Systm Security 380
Figure 224 Menu 23.2 System Security: RADIUS Server 381
Figure 225 Menu 23 System Security 382
Figure 226 Menu 23.4 System Security: IEEE802.1x 382
Figure 227 Menu 14 Dial-in User Setup 385
Figure 228 Menu 14.1 Edit Dial-in User 385
Figure 229 Menu 24 System Maintenance 386
Figure 230 Menu 24.1 System Maintenance : Status 387
Figure 231 Menu 24.2 System Information and Console Port Speed 388
Figure 232 Menu 24.2.1 System Maintenance: Information 389
Figure 233 Menu 24.2.2 System Maintenance : Change Console Port Speed 390
Figure 234 Menu 24.3 System Maintenance: Log and Trace 390
Figure 235 Sample Error and Information Messages 391
Figure 236 Menu 24.3.2 System Maintenance: Syslog and Accounting 391
Figure 237 Syslog Example 392
Figure 238 Menu 24.4 System Maintenance : Diagnostic 393
Figure 239 Telnet in Menu 24.5 398
Figure 240 FTP Session Example 399
Figure 241 System Maintenance: Backup Configuration 401
Figure 242 System Maintenance: Starting Xmodem Download Screen 401
Figure 243 Backup Configuration Example 402
Figure 244 Successful Backup Confirmation Screen 402
Figure 245 Telnet into Menu 24.6 403
Figure 246 Restore Using FTP Session Example 403
Figure 247 System Maintenance: Restore Configuration 404
Figure 248 System Maintenance: Starting Xmodem Download Screen 404
Figure 249 Restore Configuration Example 404
Figure 250 Successful Restoration Confirmation Screen 405
Figure 251 Telnet Into Menu 24.7.1 Upload System Firmware 405

Figure 252 Telnet Into Menu 24.7.2 System Maintenance 406
Figure 253 FTP Session Example of Firmware File Upload 407
Figure 254 Menu 24.7.1 As Seen Using the Console Port 408
Figure 255 Example Xmodem Upload 409
Figure 256 Menu 24.7.2 As Seen Using the Console Port 409
Figure 257 Example Xmodem Upload 410
Figure 258 Command Mode in Menu 24 412
Figure 259 Valid Commands 412
Figure 260 Menu 24.9 System Maintenance: Call Control 413
Figure 261 Menu 24.9.1 System Maintenance: Budget Management 414
Figure 262 Menu 24 System Maintenance 415
Figure 263 Menu 24.10 System Maintenance: Time and Date Setting 415
Figure 264 Menu 24.11 Remote Management Control 419
Figure 265 Menu 25 IP Routing Policy Setup 423
Figure 266 Menu 25.1 IP Routing Policy Setup 424
Figure 267 Menu 25.1.1 IP Routing Policy 425
Figure 268 Menu 3.2 TCP/IP and DHCP Ethernet Setup 427
Figure 269 Menu 11.3 Remote Node Network Layer Options 427
Figure 270 Example of IP Policy Routing 428
Figure 271 IP Routing Policy Example 428
Figure 272 IP Routing Policy Example 429
Figure 273 Applying IP Policies Example 429
Figure 274 Menu 26 Schedule Setup 430
Figure 275 Menu 26.1 Schedule Set Setup 431
Figure 276 Applying Schedule Set(s) to a Remote Node (PPPoE) 432
Figure 277 VPN SMT Menu Tree 434
Figure 278 Menu 27 VPN/IPSec Setup 435
Figure 279 Menu 27.1 IPSec Summary 435
Figure 280 Menu 27.1.1 IPSec Setup 438
Figure 281 Menu 27.1.1.1KE Setup 442
Figure 282 Menu 27.1.1.2 Manual Setup 444
Figure 283 Menu 27.2 SA Monitor 447
Figure 284 Configuration Text File Format: Column Descriptions 450
Figure 285 Invalid Parameter Entered: Command Line Example 451
Figure 286 Valid Parameter Entered: Command Line Example 451
Figure 287 Internal SPTGEN FTP Download Example 452
Figure 288 Internal SPTGEN FTP Upload Example 452
Figure 289 Console/Dial Backup Port Pin Layouts 458
Figure 290 Ethernet Cable Pin Assignments 459
Figure 291 WIndows 95/98/Me: Network: Configuration 461
Figure 292 Windows 95/98/Me: TCP/IP Properties: IP Address 462
Figure 293 Windows 95/98/Me: TCP/IP Properties: DNS Configuration 463
Figure 294 Windows XP: Start Menu 464

Figure 295 Windows XP: Control Panel 464
Figure 296 Windows XP: Control Panel: Network Connections: Properties 465
Figure 297 Windows XP: Local Area Connection Properties 465
Figure 298 Windows XP: Advanced TCP/IP Settings 466
Figure 299 Windows XP: Internet Protocol (TCP/IP) Properties 467
Figure 300 Macintosh OS 8/9: Apple Menu 468
Figure 301 Macintosh OS 8/9: TCP/IP 469
Figure 302 Macintosh OS X: Apple Menu 470
Figure 303 Macintosh OS X: Network 470
Figure 304 Single-Computer per Router Hardware Configuration 481
Figure 305 Prestige as a PPPoE Client 481
Figure 306 Peer-to-Peer Communication in an Ad-hoc Network 483
Figure 307 ESS Provides Campus-Wide Coverage 484
Figure 308 Sequences for EAP MD5–Challenge Authentication 487
Figure 309 Ideal Setup 490
Figure 310 "Triangle Route" Problem 490
Figure 311 IP Alias 491
Figure 312 Gateways on the WAN Side 491
Figure 313 myZyXEL.com Login Screen 495
Figure 314 Logged Into myZyXEL.com 496
Figure 315 Product Registration 496
Figure 316 Add New Product 497
Figure 317 Product Survey 497
Figure 318 Service Management 498
Figure 319 Service Activation: Entering Licence Key 498
Figure 320 Windows 98: WinPopup 500
Figure 321 WIndows 98: Program Task Bar 500
Figure 322 Windows 98: Task Bar Properties 501
Figure 323 Windows 98: StartUp 501
Figure 324 Windows 98: Startup: Create Shortcut 502
Figure 325 Windows 98: Startup: Select a Title for the Program 502
Figure 326 Windows 98: Startup: Shortcut 503
Figure 327 Option to Enter Debug Mode 536
Figure 328 Boot Module Commands 537
Figure 329 Displaying Log Categories Example 550
Figure 330 Displaying Log Parameters Example 550
Figure 331 Log Command Example 551

List of Tables

Table 1 ADSL Standards 44
Table 2 IEEE802.11g 46
Table 3 Web Configurator Screens Summary 56
Table 4 Internet Access Wizard Setup: First Screen 62
Table 5 Internet Connection with PPPoE 65
Table 6 Internet Connection with RFC 1483 66
Table 7 Internet Connection with ENET ENCAP 67
Table 8 Internet Connection with PPPoA 68
Table 9 Internet Access Wizard Setup: LAN Configuration 70
Table 10 Media Bandwidth Mgnt. Wizard Setup: Services 72
Table 11 Media Bandwidth Mgnt. Wizard Setup: First Screen 74
Table 12 Media Bandwidth Mgnt. Wizard Setup: Second Screen 75
Table 13 Password 76
Table 14 LAN Setup 84
Table 15 LAN: Static DHCP 85
Table 16 DMZ 87
Table 17 Wireless LAN 94
Table 18 MAC Address Filter 96
Table 19 Wireless Security Relational Matrix 101
Table 20 Wireless LAN: 802.1x/WPA 103
Table 21 Wireless LAN: 802.1x/WPA for 802.1x Protocol 104
Table 22 Wireless LAN: 802.1x/WPA for WPA Protocol 106
Table 23 Wireless LAN: 802.1x/WPA for WPA-PSK Protocol 107
Table 24 Local User Database 109
Table 25 RADIUS 110
Table 26 WAN Setup 115
Table 27 WAN Backup 119
Table 28 Advanced WAN Backup 122
Table 29 Advanced Modem Setup 125
Table 30 NAT Definitions 128
Table 31 NAT Mapping Types 131
Table 32 Services and Port Numbers 132
Table 33 NAT Mode 134
Table 34 Edit SUA/NAT Server Set 135
Table 35 Address Mapping Rules 136
Table 36 Address Mapping Rule Edit 138

Table 37 Dynamic DNS 141
Table 38 Time and Date 143
Table 39 Common IP Ports 147
Table 40 ICMP Commands That Trigger Alerts 149
Table 41 Legal NetBIOS Commands 149
Table 42 Legal SMTP Commands 150
Table 43 Firewall: Default Policy 163
Table 44 Rule Summary 164
Table 45 Firewall: Edit Rule 167
Table 46 Customized Services 168
Table 47 Firewall: Configure Customized Services 169
Table 48 Predefined Services 173
Table 49 Firewall: Anti Probing 176
Table 50 Firewall: Threshold 178
Table 51 Content Filter: Keyword 181
Table 52 Content Filter: Schedule 182
Table 53 Content Filter: Trusted 183
Table 54 Content Access Control: General 185
Table 55 Control Access Control: General: Time Scheduling 187
Table 56 Content Access Control: General: Services 188
Table 57 Available Services 189
Table 58 Content Access Control: General: Web Site Filter 193
Table 59 Content Access Control: General: Diagnose 198
Table 60 Content Access Control: User Profiles 199
Table 61 Content Access Control: Online Status 200
Table 62 Common Computer Virus Types 204
Table 63 Anti Virus: Packet Scan 207
Table 64 Anti Virus: Registration and Virus Information Update 209
Table 65 VPN and NAT 216
Table 66 AH and ESP 219
Table 67 VPN Summary 221
Table 68 Local ID Type and Content Fields 225
Table 69 Peer ID Type and Content Fields 225
Table 70 Matching ID Type and Content Configuration Example 225
Table 71 Mismatching ID Type and Content Configuration Example 226
Table 72 VPN IKE 228
Table 73 VPN IKE: Advanced Setup 234
Table 74 VPN: Manual Key 238
Table 75 241
Table 76 VPN: Global Setting 241
Table 77 Telecommuters Sharing One VPN Rule Example 243
Table 78 Telecommuters Using Unique VPN Rules Example 244
Table 79 Remote Management 248

Table 80 Configuring UPnP 252
Table 81 Log Settings 265
Table 82 View Logs 267
Table 83 SMTP Error Messages 267
Table 84 Application and Subnet-based Bandwidth Management Example 272
Table 85 Media Bandwidth Management: Summary 278
Table 86 Media Bandwidth Management: Class Setup 279
Table 87 Media Bandwidth Management: Class Configuration 280
Table 88 Services and Port Numbers 281
Table 89 Media Bandwidth Management Statistics 282
Table 90 Media Bandwidth Management: Monitor 283
Table 91 System Status 285
Table 92 System Status: Show Statistics 287
Table 93 DHCP Table 288
Table 94 Any IP Table 289
Table 95 Association List 290
Table 96 Diagnostic: General 291
Table 97 Diagnostic: DSL Line 292
Table 98 Firmware Upgrade 293
Table 99 Navigating the SMT Interface 298
Table 100 SMT Main Menu 298
Table 101 Main Menu Summary 299
Table 102 Menu 1 General Setup 303
Table 103 Menu 1.1 Configure Dynamic DNS 304
Table 104 Menu 2 WAN Backup Setup 306
Table 105 Menu 2.1Traffic Redirect Setup 307
Table 106 Menu 2.2 Dial Backup Setup 308
Table 107 Menu 2.2.1 Advanced Dial Backup Setup: AT Commands Fields 310
Table 108 Menu 2.2.1 Advanced Dial Backup Setup: Call Control Parameters 310
Table 109 DHCP Ethernet Setup 314
Table 110 TCP/IP Ethernet Setup 314
Table 111 Menu 3.5 - Wireless LAN Setup 316
Table 112 Menu 3.5.1 WLAN MAC Address Filtering 318
Table 113 Menu 3.2.1 IP Alias Setup 322
Table 114 Menu 4 Internet Access Setup 324
Table 115 Menu 11.1 Remote Node Profile 328
Table 116 Menu 11.3 Remote Node Network Layer Options 330
Table 117 Menu 11.8 Advance Setup Options 335
Table 118 Menu12.1.1 Edit IP Static Route 338
Table 119 Remote Node Network Layer Options: Bridge Fields 341
Table 120 Menu 12.3.1 Edit Bridge Static Route 342
Table 121 Applying NAT in Menus 4 & 11.3 346
Table 122 SUA Address Mapping Rules 347

Table 123 Menu 15.1.1 First Set 349
Table 124 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set 350
Table 125 Abbreviations Used in the Filter Rules Summary Menu 365
Table 126 Rule Abbreviations Used 366
Table 127 Menu 21.1.x.1 TCP/IP Filter Rule 367
Table 128 Menu 21.1.5.1 Generic Filter Rule 370
Table 129 Filter Sets Table 373
Table 130 Menu 22 SNMP Configuration 378
Table 131 SNMP Traps 378
Table 132 Ports and Permanent Virtual Circuits 379
Table 133 Menu 23.2 System Security: RADIUS Server 381
Table 134 Menu 23.4 System Security : IEEE802.1x 383
Table 135 Menu 14.1 Edit Dial-in User 385
Table 136 Menu 24.1 System Maintenance : Status 387
Table 137 Menu 24.2.1 System Maintenance: Information 389
Table 138 Menu 24.3.2 System Maintenance : Syslog and Accounting 391
Table 139 Menu 24.4 System Maintenance Menu: Diagnostic 394
Table 140 Filename Conventions 397
Table 141 General Commands for GUI-based FTP Clients 399
Table 142 General Commands for GUI-based TFTP Clients 401
Table 143 Menu 24.9.1 System Maintenance : Budget Management 414
Table 144 Menu 24.10 System Maintenance: Time and Date Setting 415
Table 145 Menu 24.11 Remote Management Control 419
Table 146 Menu 25.1 IP Routing Policy Setup 424
Table 147 Menu 25.1.1 IP Routing Policy 425
Table 148 Menu 26.1 Schedule Set Setup 431
Table 149 Menu 27.1 IPSec Summary 435
Table 150 Menu 27.1.1 IPSec Setup 438
Table 151 Menu 27.1.1.1 IKE Setup 442
Table 152 Active Protocol: Encapsulation and Security Protocol 443
Table 153 Menu 27.1.1.2 Manual Setup 444
Table 154 Menu 27.2 SA Monitor 447
Table 155 Troubleshooting the Start-Up of Your Prestige 454
Table 156 Troubleshooting the LAN LED 454
Table 157 Troubleshooting the DSL LED 455
Table 158 Troubleshooting the LAN Interface 455
Table 159 Troubleshooting the WAN Interface 455
Table 160 Troubleshooting Internet Access 456
Table 161 Troubleshooting the Password 456
Table 162 Troubleshooting the Web Configurator 457
Table 163 Troubleshooting Remote Management 457
Table 164 Console/Dial Backup Port Pin Assignments 458
Table 165 Classes of IP Addresses 472

Table 166 Allowed IP Address Range By Class 473
Table 167 "Natural" Masks 473
Table 168 Alternative Subnet Mask Notation 474
Table 169 Two Subnets Example 474
Table 170 Subnet 1 475
Table 171 Subnet 2 475
Table 172 Subnet 1 476
Table 173 Subnet 2 476
Table 174 Subnet 3 476
Table 175 Subnet 4 477
Table 176 Eight Subnets 477
Table 177 Class C Subnet Planning 477
Table 178 Class B Subnet Planning 478
Table 179 Comparison of EAP Authentication Types 489
Table 180 myZyXEL.com Numbers 494
Table 181 Abbreviations Used in the Example Internal SPTGEN Screens Table 504
Table 182 Menu 1 General Setup (SMT Menu 1) 504
Table 183 Menu 3 (SMT Menu 1) 504
Table 184 Menu 4 Internet Access Setup (SMT Menu 4) 508
Table 185 Menu 12(SMT Menu 12) 509
Table 186 Menu 15 SUA Server Setup (SMT Menu 15) 513
Table 187 Menu 21.1 Filter Set #1 (SMT Menu 21.1) 515
Table 188 Menu 21.1 Filer Set #2, (SMT Menu 21.1) 519
Table 189 ci command (for annex a): wan adsl opencmd 524
Table 190 Sys Firewall Commands 528
Table 191 NetBIOS Filter Default Settings 531
Table 192 Brute-Force Password Guessing Protection Commands 534
Table 193 System Maintenance Logs 538
Table 194 System Error Logs 539
Table 195 Access Control Logs 539
Table 196 TCP Reset Logs 540
Table 197 Packet Filter Logs 540
Table 198 ICMP Logs 540
Table 199 CDR Logs 541
Table 200 PPP Logs 541
Table 201 UPnP Logs 542
Table 202 Content Filtering Logs 542
Table 203 Attack Logs 543
Table 204 IPSec Logs 544
Table 205 IKE Logs 544
Table 206 802.1X Logs 547
Table 207 ACL Setting Notes 548
Table 208 ICMP Notes 548

Table 209 Syslog Logs 549
Table 210 RFC-2408 ISAKMP Payload Types 549

Preface

Congratulations on your purchase of the Prestige 662HW Series.

> **Note:** Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Your Prestige is easy to install and configure.

About This User's Guide

This manual is designed to guide you through the configuration of your Prestige for its various applications. The web configurator parts of this guide contain background information on features configurable by web configurator. The SMT parts of this guide contain background information solely on features not configurable by web configurator.

> **Note:** Use the web configurator, System Management Terminal (SMT) or command interpreter interface to configure your Prestige. Not all features can be configured through all interfaces.

Related Documentation

- Supporting Disk

  Refer to the included CD for support documents.

- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. They contain connection information and instructions on getting started.

- Web Configurator Online Help

  Embedded web help for descriptions of individual screens and supplementary information.

- ZyXEL Glossary and Web Site

  Please refer to www.zyxel.com for an online glossary of networking terms and additional support documentation.

User Guide Feedback

Help us help you! E-mail all User Guide-related comments, questions or suggestions for improvement to techwriters@zyxel.com.tw or send regular mail to The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Thank you!

Syntax Conventions

- "Enter" means for you to type one or more characters. "Select" or "Choose" means for you to use one predefined choices.
- The SMT menu titles and labels are in **Bold Times New Roman** font. Predefined field choices are in **Bold Arial** font. Command and arrow keys are enclosed in square brackets. [ENTER] means the Enter, or carriage return key; [ESC] means the Escape key and [SPACE BAR] means the Space Bar.
- Mouse action sequences are denoted using a comma. For example, "click the Apple icon, **Control Panels** and then **Modem**" means first click the Apple icon, then point your mouse pointer to **Control Panels** and then click **Modem**.
- For brevity's sake, we will use "e.g.," as a shorthand for "for instance", and "i.e.," for "that is" or "in other words" throughout this manual.
- The Prestige 662HW series may be referred to as the Prestige in this user's guide. This refers to both models (ADSL over POTS and ADSL over ISDN) unless specifically identified.

Graphics Icons Key

Prestige 	Computer 	Notebook computer 
Server 	DSLAM 	Firewall 
Telephone 	Switch 	Router 
Wireless Signal 		

Note: The following section offers some background information on DSL. Skip to *Chapter 1* if you wish to begin working with your router right away.

Introduction to DSL

DSL (Digital Subscriber Line) technology enhances the data capacity of the existing twisted-pair wire that runs between the local telephone company switching offices and most homes and offices. While the wire itself can handle higher frequencies, the telephone switching equipment is designed to cut off signals above 4,000 Hz to filter noise off the voice line, but now everybody is searching for ways to get more bandwidth to improve access to the Web - hence DSL technologies.

There are actually seven types of DSL service, ranging in speeds from 16 Kbits/sec to 52 Mbits/sec. The services are either symmetrical (traffic flows at the same speed in both directions), or asymmetrical (the downstream capacity is higher than the upstream capacity). Asymmetrical services (ADSL) are suitable for Internet users because more information is usually downloaded than uploaded. For example, a simple button click in a web browser can start an extended download that includes graphics and text.

As data rates increase, the carrying distance decreases. That means that users who are beyond a certain distance from the telephone company's central office may not be able to obtain the higher speeds.

A DSL connection is a point-to-point dedicated circuit, meaning that the link is always up and there is no dialing required.

Introduction to ADSL

It is an asymmetrical technology, meaning that the downstream data rate is much higher than the upstream data rate. As mentioned, this works well for a typical Internet session in which more information is downloaded, for example, from Web servers, than is uploaded. ADSL operates in a frequency range that is above the frequency range of voice services, so the two systems can operate over the same cable.

CHAPTER 1
Getting To Know Your Prestige

This chapter describes the key features and applications of your Prestige.

1.1 Introducing the Prestige

Your Prestige integrates high-speed 10/100Mbps auto-negotiating LAN interface(s) and a high-speed ADSL port into a single package. The Prestige is ideal for high-speed Internet browsing and making LAN-to-LAN connections to remote networks. The Prestige is an ADSL router compatible with the ADSL/ADSL2/ADSL2+ standards. Maximum data rates attainable by the Prestige for each standard are shown in the next table.

Table 1 ADSL Standards

DATA RATE STANDARD	UPSTREAM	DOWNSTREAM
ADSL	832 kbps	8Mbps
ADSL2	3.5Mbps	12Mbps
ADSL2+	3.5Mbps	24Mbps

Note: The standard your ISP supports determines the maximum upstream and downstream speeds attainable. Actual speeds attained also depend on the distance from your ISP, line quality, etc.

By integrating DSL and NAT, the Prestige provides ease of installation and Internet access. The Prestige is also a complete security solution with a robust firewall and content filtering.

Three Prestige models are included in this user's guide at the time of writing. In the Prestige product name, "H" denotes an integrated 4-port switch (hub) and "W" denotes an included wireless card. The Prestige 662HW provide 802.11g wireless LAN connectivity allowing users to enjoy the convenience and mobility of working anywhere within the coverage area.

Models ending in "1", for example Prestige 662HW-61, denote a device that works over the analog telephone system, POTS (Plain Old Telephone Service). Models ending in "3" denote a device that works over ISDN (Integrated Synchronous Digital System). Models ending in "7" denote a device that works over T-ISDN (UR-2).

Note: Only use firmware for your Prestige's specific model. Refer to the label on the bottom of your Prestige.

The web browser-based Graphical User Interface (GUI) provides easy management.

1.1.1 Features of the Prestige

The following sections describe the features of the Prestige.

High Speed Internet Access

Your Prestige ADSL/ADSL2/ADSL2+ router can support downstream transmission rates of up to 24Mbps and upstream transmission rates of 3.5Mbps. Actual speeds attained depend on ISP DSLAM environment.

Zero Configuration Internet Access

Once you connect and turn on the Prestige, it automatically detects the Internet connection settings (such as the VCI/VPI numbers and the encapsulation method) from the ISP and makes the necessary configuration changes. In cases where additional account information (such as an Internet account user name and password) is required or the Prestige cannot connect to the ISP, you will be redirected to web screen(s) for information input or troubleshooting.

Any IP

The Any IP feature allows a computer to access the Internet and the Prestige without changing the network settings (such as IP address and subnet mask) of the computer, when the IP addresses of the computer and the Prestige are not in the same subnet.

Firewall

The Prestige is a stateful inspection firewall with DoS (Denial of Service) protection. By default, when the firewall is activated, all incoming traffic from the WAN to the LAN is blocked unless it is initiated from the LAN. The Prestige firewall supports TCP/UDP inspection, DoS detection and prevention, real time alerts, reports and logs.

Note: You can configure most features of the Prestige via SMT but we recommend you configure the firewall and content filters using the web configurator.

Content Filtering

Content filtering allows you to block access to forbidden Internet web sites, schedule when the Prestige should perform the filtering and give trusted LAN IP addresses unfiltered Internet access.

Content Access Control

The Prestige can control access privileges to website and services through Content Access Control (CAC). Content Access Control can be defined as the ability for a LAN administrator to control a LAN user's Internet access privileges. The administrator can create a login name and password for each user on the network. Each user must log into the system before they can gain access to the Internet. Each account will have specific access restrictions.

Anti-Virus Packet Scan[1]

With the anti-virus packet scan, your Prestige detects and removes viruses in network packets (SMTP, POP3, HTTP and FTP). This prevents viruses from infecting computer(s) on the network. You can set the Prestige to log and warn you of any viruses detected. You can also perform online update of the packet scan on the Prestige.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b radio card can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 2 IEEE802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

Note: The Prestige may be prone to RF (Radio Frequency) interference from other 2.4 GHz devices such as microwave ovens, wireless phones, Bluetooth enabled devices, and other wireless LANs.

External Antenna

The Prestige is equipped with an antenna connector and comes with a detachable 5dBi antenna to provide clear radio signal between the wireless stations and the access points.

Note: Under the CE regulations, when using a 5dBi or higher gain antenna with the Prestige, the maximum antenna power output must be less or equal to 20dBm. Refer to the support note for more information.

1. This feature is not available at the time of writing.

Wireless LAN MAC Address Filtering

Your Prestige can check the MAC addresses of wireless stations against a list of allowed or denied MAC addresses.

WEP Encryption

WEP (Wired Equivalent Privacy) encrypts data frames before transmitting over the wireless network to help keep network communications private.

Wi-Fi Protected Access

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i security specification draft. Key differences between WPA and WEP are user authentication and improved data encryption.

Traffic Redirect

Traffic redirect forwards WAN traffic to a backup gateway when the Prestige cannot connect to the Internet, thus acting as an auxiliary if your regular WAN connection fails.

Media Bandwidth Management

ZyXEL's Media Bandwidth Management allows you to specify bandwidth classes based on an application and/or subnet. You can allocate specific amounts of bandwidth capacity (bandwidth budgets) to different bandwidth classes.

Universal Plug and Play (UPnP)

Using the standard TCP/IP protocol, the Prestige and other UPnP enabled devices can dynamically join a network, obtain an IP address and convey its capabilities to other devices on the network.

PPPoE Support (RFC2516)

PPPoE (Point-to-Point Protocol over Ethernet) emulates a dial-up connection. It allows your ISP to use their existing network configuration with newer broadband technologies such as ADSL. The PPPoE driver on the Prestige is transparent to the computers on the LAN, which see only Ethernet and are not aware of PPPoE thus saving you from having to manage PPPoE clients on individual computers.

Network Address Translation (NAT)

Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).

LAN/DMZ Interface

The Prestige provides a LAN port that can function as a virtual DeMilitarized Zone (DMZ) port. Public servers (Web, FTP, etc.) attached to the DMZ port are visible to the outside world (while still being protected from DoS (Denial of Service) attacks such as SYN flooding and Ping of Death) and can also be accessed from the secure LAN.

10/100M Auto-negotiating Ethernet/Fast Ethernet Interface(s)

This auto-negotiation feature allows the Prestige to detect the speed of incoming transmissions and adjust appropriately without manual intervention. It allows data transfer of either 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode depending on your Ethernet network.

Auto-Crossover (MDI/MDI-X) 10/100 Mbps Ethernet Interface(s)

These interfaces automatically adjust to either a crossover or straight-through Ethernet cable.

Dynamic DNS Support

With Dynamic DNS support, you can have a static hostname alias for a dynamic IP address, allowing the host to be more easily accessible from various locations on the Internet. You must register for this service with a Dynamic DNS service provider.

Multiple PVC (Permanent Virtual Circuits) Support

Your Prestige supports up to 8 PVC's.

ADSL Standards

- Full-Rate (ANSI T1.413, Issue 2; G.dmt (G.992.1) with line rate support of up to 8 Mbps downstream and 832 Kbps upstream.
- G.lite (G.992.2) with line rate support of up to 1.5Mbps downstream and 512Kbps upstream.
- Supports Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt (G.992.1); G.lite (G992.2)).
- TCP/IP (Transmission Control Protocol/Internet Protocol) network layer protocol.
- ATM Forum UNI 3.1/4.0 PVC.
- Supports up to 8 PVCs (UBR, CBR, VBR).
- Multiple Protocol over AAL5 (RFC 1483).
- PPP over AAL5 (RFC 2364).
- PPP over Ethernet over AAL5 (RFC 2516).
- RFC 1661.
- PPP over PAP (RFC 1334).
- PPP over CHAP (RFC 1994).

Protocol Support

- DHCP Support

DHCP (Dynamic Host Configuration Protocol) allows the individual clients (computers) to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The Prestige has built-in DHCP server capability enabled by default. It can assign IP addresses, an IP default gateway and DNS servers to DHCP clients. The Prestige can now also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the clients.

- IP Alias

  IP Alias allows you to partition a physical network into logical networks over the same Ethernet interface. The Prestige supports three logical LAN interfaces via its single physical Ethernet interface with the Prestige itself as the gateway for each LAN network.

- IP Policy Routing (IPPR)

  Traditionally, routing is based on the destination address only and the router takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator.

- PPP (Point-to-Point Protocol) link layer protocol.
- Transparent bridging for unsupported network layer protocols.
- RIP I/RIP II
- IGMP Proxy
- ICMP support
- ATM QoS support
- MIB II support (RFC 1213)

Networking Compatibility

Your Prestige is compatible with the major ADSL DSLAM (Digital Subscriber Line Access Multiplexer) providers, making configuration as simple as possible for you.

Multiplexing

The Prestige supports VC-based and LLC-based multiplexing.

Encapsulation

The Prestige supports PPPoA (RFC 2364 - PPP over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM, MAC encapsulated routing (ENET encapsulation) as well as PPP over Ethernet (RFC 2516).

Network Management

- Menu driven SMT (System Management Terminal) management
- Embedded web configurator
- CLI (Command Line Interpreter)
- Remote Management via Telnet or Web
- SNMP manageable

- DHCP Server/Client/Relay
- Built-in Diagnostic Tools
- Syslog
- Telnet Support (Password-protected telnet access to internal configuration manager)
- TFTP/FTP server, firmware upgrade and configuration backup/support supported
- Supports OAM F4/F5 loop-back, AIS and RDI OAM cells

Other PPPoE Features

- PPPoE idle time out
- PPPoE Dial on Demand

Diagnostics Capabilities

The Prestige can perform self-diagnostic tests. These tests check the integrity of the following circuitry:

- FLASH memory
- ADSL circuitry
- RAM
- LAN port

Packet Filters

The Prestige's packet filtering functions allows added network security and management.

Ease of Installation

Your Prestige is designed for quick, intuitive and easy installation.

Housing

Your Prestige's compact and ventilated housing minimizes space requirements making it easy to position anywhere in your busy office.

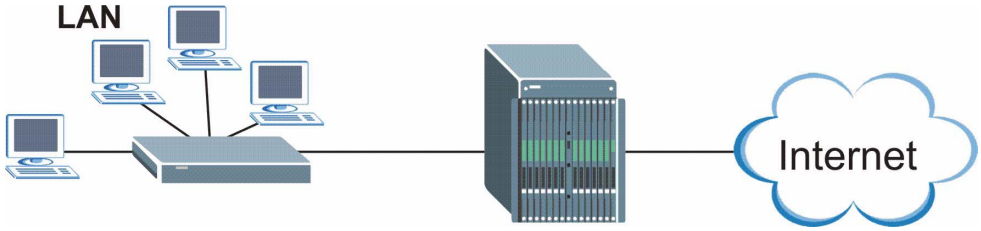
1.1.2 Applications for the Prestige

Here are some example uses for which the Prestige is well suited.

1.1.2.1 Internet Access

The Prestige is the ideal high-speed Internet access solution. Your Prestige supports the TCP/IP protocol, which the Internet uses exclusively. It is compatible with all major ADSL DSLAM (Digital Subscriber Line Access Multiplexer) providers. A DSLAM is a rack of ADSL line cards with data multiplexed into a backbone network interface/connection (for example, T1, OC3, DS3, ATM or Frame Relay). Think of it as the equivalent of a modem rack for ADSL. In addition, the Prestige allows wireless clients access to your network resources. A typical Internet access application is shown below.

Figure 1 Prestige Internet Access Application



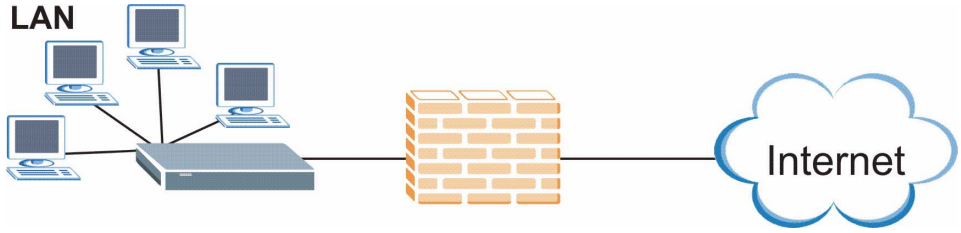
Internet Single User Account

For a SOHO (Small Office/Home Office) environment, your Prestige offers the Single User Account (SUA) feature that allows multiple users on the LAN (Local Area Network) to access the Internet concurrently for the cost of a single IP address.

1.1.3 Firewall for Secure Broadband Internet Access

The Prestige provides protection from attacks by Internet hackers. By default, the firewall blocks all incoming traffic from the WAN. The firewall supports TCP/UDP inspection and DoS (Denial of Services) detection and prevention, as well as real time alerts, reports and logs.

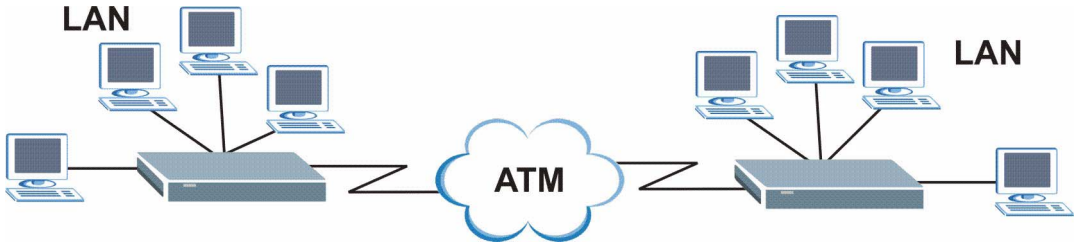
Figure 2 Firewall Application



1.1.3.1 LAN to LAN Application

You can use the Prestige to connect two geographically dispersed networks over the ADSL line. A typical LAN-to-LAN application for your Prestige is shown as follows.

Figure 3 Prestige LAN-to-LAN Application



1.1.4 Prestige Hardware Installation and Connection

Refer to the *Quick Start Guide* for information on hardware installation and connection and LED descriptions.

CHAPTER 2
Introducing the Web Configurator

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

2.1 Web Configurator Overview

The web configurator is an HTML-based management interface that allows easy Prestige setup and management via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions with JavaScript enabled. Recommended screen resolution is 1024 by 768 pixels.

2.1.1 Accessing the Prestige Web Configurator

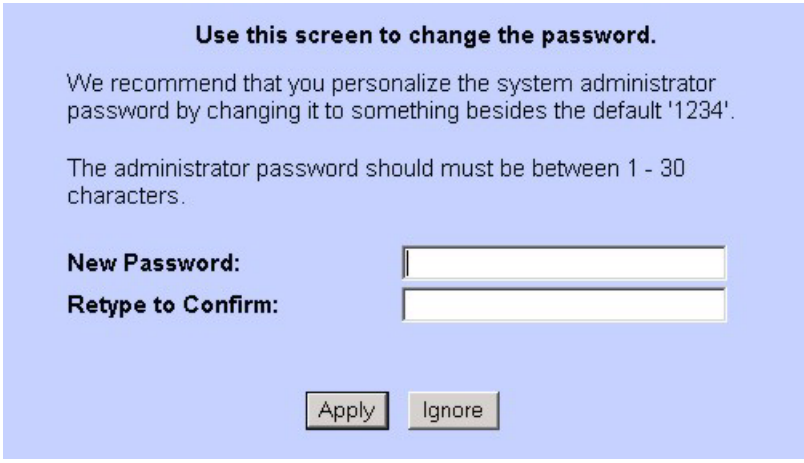
Note: Even though you can connect to the Prestige wirelessly, it is recommended that you connect your computer to a LAN port for initial configuration.

1. Make sure your Prestige hardware is properly connected (refer to the *Quick Start Guide*).
2. Prepare your computer/computer network to connect to the Prestige (refer to the *Quick Start Guide*).
3. Launch your web browser.
4. Type "192.168.1.1" as the URL.
5. An **Enter Network Password** window displays. Enter the user name ("admin" is the default), password ("1234" is the default). Click **Login** to proceed to a screen asking you to change your password. Click **Reset** to revert to the default password in the password field

Figure 4 Password Screen

6 It is highly recommended you change the default password! Enter a new password, retype it to confirm and click **Apply**; alternatively click **Ignore** to proceed to the main menu if you do not want to change the password now.

Figure 5 Change Password at Login



7 You should now see the **SITE MAP** screen.

Note: The Prestige automatically times out after five minutes of inactivity. Simply log back into the Prestige if this happens to you.

2.1.2 Resetting the Prestige

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button at the back of the Prestige to reload the factory-default configuration file. This means that you will lose all configurations that you had previously and the password will be reset to "1234".

2.1.2.1 Using the Reset Button

1 Make sure the **PWR/SYS** LED is on (not blinking).

2 Press the **RESET** button for ten seconds or until the **PWR/SYS** LED begins to blink and then release it. When the **PWR/SYS** LED begins to blink, the defaults have been restored and the Prestige restarts.

2.1.3 Navigating the Prestige Web Configurator

The following summarizes how to navigate the web configurator from the **SITE MAP** screen. We use the Prestige 662HW-61 web screens in this guide as an example. Screens vary slightly for different Prestige models.

- Click **Wizard Setup** to begin a series of screens to configure your Prestige for the first time.
- Click a link under **Advanced Setup** to configure advanced Prestige features.
- Click a link under **Maintenance** to see Prestige performance statistics, upload firmware and back up, restore or upload a configuration file.
- Click **Site Map** to go to the **Site Map** screen.
- Click **Logout** in the navigation panel when you have finished a Prestige management session.

Figure 6 Web Configurator SITE MAP Screen

Note: Click the HELP icon (located in the top right corner of most screens) to view embedded help.

Table 3 Web Configurator Screens Summary

LINK	SUB-LINK	FUNCTION
Wizard Setup	Wizard Setup	Use these screens for initial configuration including general setup, ISP parameters for Internet Access and WAN IP/DNS Server/MAC address assignment.
Advanced Setup		
Password		Use this screen to change your password.
LAN		Use this screen to configure LAN DHCP and TCP/IP settings.
WAN	WAN Setup	Use this screen to change the Prestige's WAN remote node settings.

Table 3 Web Configurator Screens Summary (continued)

LINK	SUB-LINK	FUNCTION
	WAN Backup	Use this screen to configure your traffic redirect properties and WAN backup settings.
NAT	SUA Only	Use this screen to configure servers behind the Prestige.
	Full Feature	Use this screen to configure network address translation mapping rules.
Dynamic DNS		Use this screen to set up dynamic DNS.
Time and Date		Use this screen to change your Prestige's time and date.
Firewall	Default Policy	Use this screen to activate/deactivate the firewall and the direction of network traffic to which to apply the rule.
	Rule Summary	This screen shows a summary of the firewall rules, and allows you to edit/add a firewall rule.
	Anti Probing	Use this screen to change your anti-probing settings.
	Threshold	Use this screen to configure the threshold for DoS attacks.
Content Filter	Keyword	Use this screen to block sites containing certain keywords in the URL.
	Schedule	Use this screen to set the days and times for the Prestige to perform content filtering.
	Trusted	Use this screen to exclude a range of users on the LAN from content filtering on your Prestige.
Content Access Control	General	Use the screens to configure general settings and set up content access classes.
	User Profiles	Use the screens to set up user profiles.
	Online Status	Use this to view the access status of each user.
VPN	Setup	Use the screens to set up VPN tunnels.
	Monitor	Use this screen to view Security Association (SA) connections.
	Global Setting	Use this screen to configure global settings for the VPN tunnels.
Remote Management		Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet/FTP/Web to manage the Prestige.
UPnP		Use this screen to enable UPnP on the Prestige.
Logs	Log Settings	Use this screen to change your Prestige's log settings.
	View Log	Use this screen to view the logs for the categories that you selected.
Media Bandwidth Management	Summary	Use this screen to allocate an interface's outgoing capacity to specific types of traffic.
	Class Setup	Use this screen to define a bandwidth class.
	Monitor	Use this screen to view bandwidth class statistics.
Maintenance		
System Status		This screen contains administrative and system-related information.
DHCP Table		This screen displays DHCP (Dynamic Host Configuration Protocol) related information and is READ-ONLY.

Table 3 Web Configurator Screens Summary (continued)

LINK	SUB-LINK	FUNCTION
Diagnostic	General	These screens display information to help you identify problems with the Prestige general connection.
	DSL Line	These screens display information to help you identify problems with the DSL line.
Firmware		Use this screen to upload firmware to your Prestige
LOGOUT		Click this label to exit the web configurator.

CHAPTER 3
Wizard Setup for Internet Access

This chapter provides information on the Wizard Setup screens for Internet access in the web configurator.

3.1 Introduction

Use the Wizard Setup screens to configure your system for Internet access with the information (provided by your ISP) that you fill in the *Internet Account Information* table in the *Quick Start Guide*. Your ISP may have already configured some of the fields in the wizard screens for you.

3.1.1 Encapsulation

Be sure to use the encapsulation method required by your ISP. The Prestige supports the following methods.

3.1.1.1 ENET ENCAP

The MAC Encapsulated Routing Link Protocol (ENET ENCAP) is only implemented with the IP network protocol. IP packets are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment. For instance, it encapsulates routed Ethernet frames into bridged ATM cells. ENET ENCAP requires that you specify a gateway IP address in the **ENET ENCAP Gateway** field in the second wizard screen. You can get this information from your ISP.

3.1.1.2 PPP over Ethernet

PPPoE provides access control and billing functionality in a manner similar to dial-up services using PPP. The Prestige bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your computer to an ATM PVC (Permanent Virtual Circuit) which connects to ADSL Access Concentrator where the PPP session terminates. One PVC can support any number of PPP sessions from your LAN. For more information on PPPoE, see the appendices.

3.1.1.3 PPPoA

PPPoA stands for Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). A PPPoA connection functions like a dial-up Internet connection. The Prestige encapsulates the PPP session based on RFC1483 and sends it through an ATM PVC (Permanent Virtual Circuit) to the Internet Service Provider's (ISP) DSLAM (digital access multiplexer). Please refer to RFC 2364 for more information on PPPoA. Refer to RFC 1661 for more information on PPP.

3.1.1.4 RFC 1483

RFC 1483 describes two methods for Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5). The first method allows multiplexing of multiple protocols over a single ATM virtual circuit (LLC-based multiplexing) and the second method assumes that each protocol is carried over a separate ATM virtual circuit (VC-based multiplexing). Please refer to the RFC for more detailed information.

3.1.2 Multiplexing

There are two conventions to identify what protocols the virtual circuit (VC) is carrying. Be sure to use the multiplexing method required by your ISP.

3.1.2.1 VC-based Multiplexing

In this case, by prior mutual agreement, each protocol is assigned to a specific virtual circuit; for example, VC1 carries IP, etc. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

3.1.2.2 LLC-based Multiplexing

In this case one VC carries multiple protocols with protocol identifying information being contained in each packet header. 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.

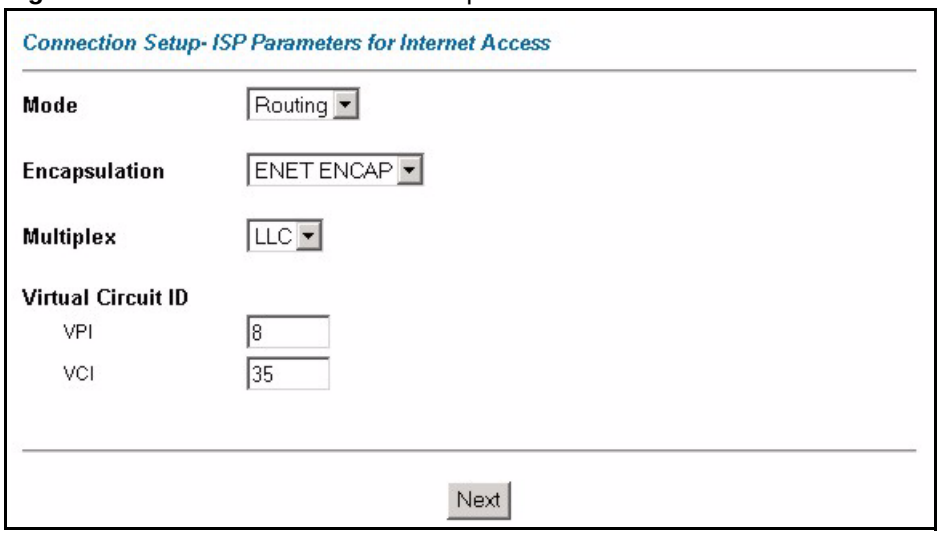
3.1.3 VPI and VCI

Be sure to use the correct Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) numbers assigned to you. The valid range for the VPI is 0 to 255 and for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Please see the appendix for more information.

3.1.4 Internet Access Wizard Setup: First Screen

In the **SITE MAP** screen click **Wizard Setup** to display the first wizard screen.

Figure 7 Internet Access Wizard Setup: First Screen



The following table describes the fields in this screen.

Table 4 Internet Access Wizard Setup: First Screen

LABEL	DESCRIPTION
Mode	From the **Mode** drop-down list box, select **Routing** (default) if your ISP allows multiple computers to share an Internet account. Otherwise select **Bridge**.
Encapsulation	Select the encapsulation type your ISP uses from the **Encapsulation** drop-down list box. Choices vary depending on what you select in the **Mode** field. If you select **Bridge** in the Mode field, select either **PPPoA** or **RFC 1483**. If you select **Routing** in the Mode field, select **PPPoA**, **RFC 1483**, **ENET ENCAP** or **PPPoE**.
Multiplex	Select the multiplexing method used by your ISP from the **Multiplex** drop-down list box either VC-based or LLC-based.
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information.
VPI	Enter the VPI assigned to you. This field may already be configured.
VCI	Enter the VCI assigned to you. This field may already be configured.
Next	Click this button to go to the next wizard screen. The next wizard screen you see depends on what protocol you chose above. Click on the protocol link to see the next wizard screen for that protocol.

3.2 IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the Prestige. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your Prestige, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your Prestige will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the Prestige unless you are instructed to do otherwise.

3.2.1 IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However the encapsulation method assigned influences your choices for IP address and ENET ENCAP gateway.

3.2.1.1 IP Assignment with PPPoA or PPPoE Encapsulation

If you have a dynamic IP, then the **IP Address** and **ENET ENCAP Gateway** fields are not applicable (N/A). If you have a static IP, then you *only* need to fill in the **IP Address** field and *not* the **ENET ENCAP Gateway** field.

3.2.1.2 IP Assignment with RFC 1483 Encapsulation

In this case the IP Address Assignment *must* be static with the same requirements for the **IP Address** and **ENET ENCAP Gateway** fields as stated above.

3.2.1.3 IP Assignment with ENET ENCAP Encapsulation

In this case you can have either a static or dynamic IP. For a static IP you must fill in all the **IP Address** and **ENET ENCAP Gateway** fields as supplied by your ISP. However for a dynamic IP, the Prestige acts as a DHCP client on the WAN port and so the **IP Address** and **ENET ENCAP Gateway** fields are not applicable (N/A) as the DHCP server assigns them to the Prestige.

3.2.1.4 Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Note: Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space.*

3.2.2 Nailed-Up Connection (PPP)

A nailed-up connection is a dial-up line where the connection is always up regardless of traffic demand. The Prestige does two things when you specify a nailed-up connection. The first is that idle timeout is disabled. The second is that the Prestige will try to bring up the connection when turned on and whenever the connection is down. A nailed-up connection can be very expensive for obvious reasons.

Do not specify a nailed-up connection unless your telephone company offers flat-rate service or you need a constant connection and the cost is of no concern

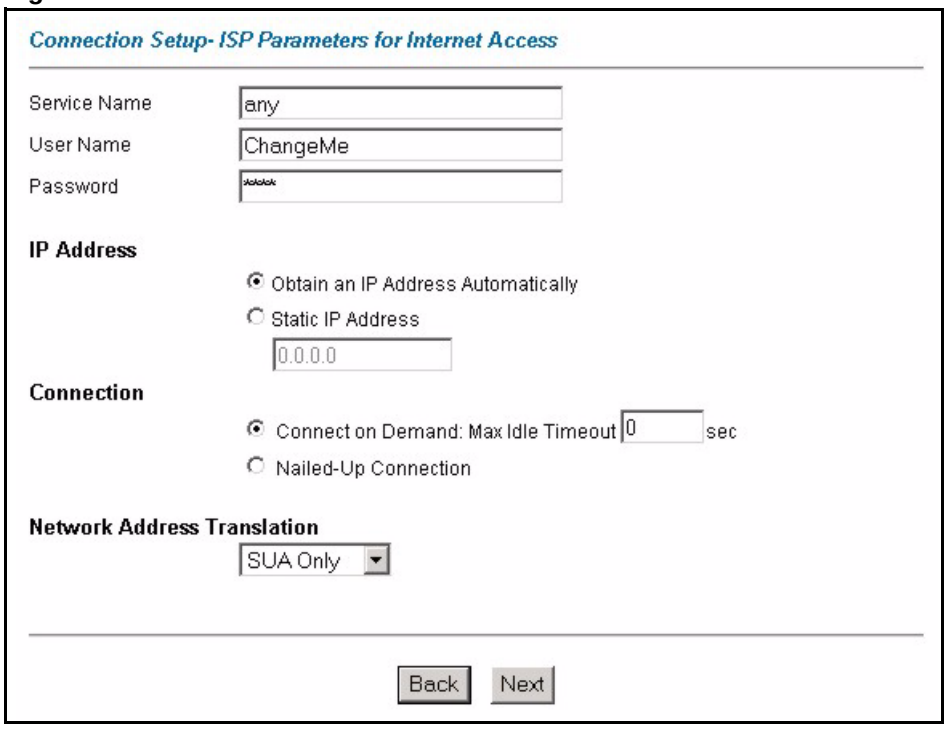
3.2.3 NAT

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

3.2.4 Internet Access Wizard Setup: Second Screen

The second wizard screen varies depending on what mode and encapsulation type you use. All screens shown are with routing mode. Configure the fields and click **Next** to continue.

Figure 8 Internet Connection with PPPoE

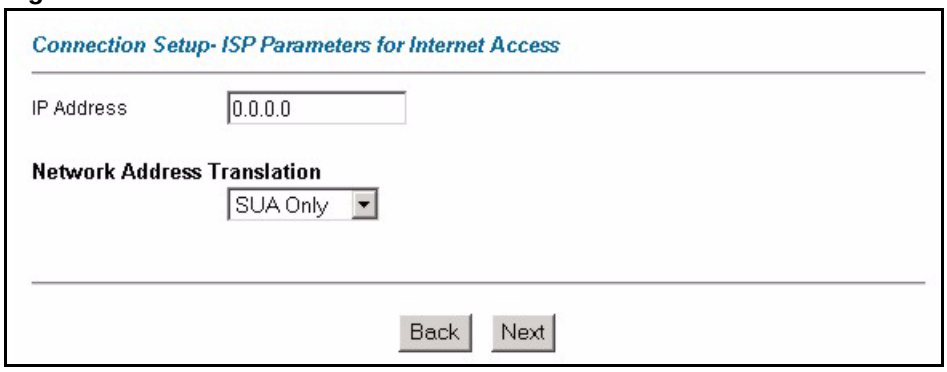


The following table describes the fields in this screen.

Table 5 Internet Connection with PPPoE

LABEL	DESCRIPTION
Service Name	Type the name of your PPPoE service here.
User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the user name above.
IP Address	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select **Obtain an IP Address Automatically** if you have a dynamic IP address; otherwise select **Static IP Address** and type your ISP assigned IP address in the text box below.
Connection	Select **Connect on Demand** when you don't want the connection up all the time and specify an idle time-out (in seconds) in the **Max. Idle Timeout** field. The default setting selects **Connection on Demand** with 0 as the idle time-out, which means the Internet session will not timeout. Select **Nailed-Up Connection** when you want your connection up all the time. The Prestige will try to bring up the connection automatically if it is disconnected. The schedule rule(s) in SMT menu 26 has priority over your **Connection** settings.
Network Address Translation	Select **None**, **SUA Only** or **Full Feature** from the drop-sown list box. Refer to the NAT chapter for more details.
Back	Click **Back** to go back to the first wizard screen.
Next	Click **Next** to continue to the next wizard screen.

Figure 9 Internet Connection with RFC 1483

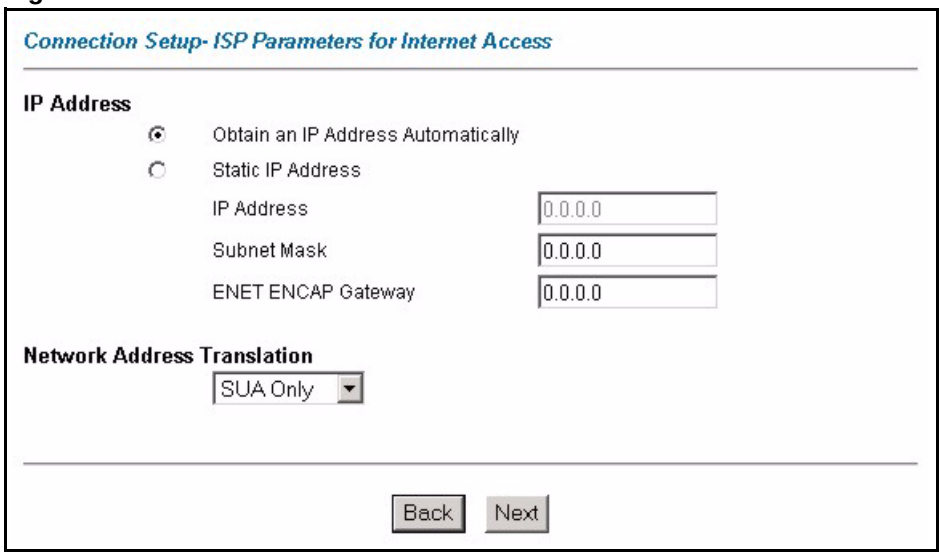


The following table describes the fields in this screen.

Table 6 Internet Connection with RFC 1483

LABEL	DESCRIPTION
IP Address	This field is available if you select **Routing** in the **Mode** field. Type your ISP assigned IP address in this field.
Network Address Translation	Select **None**, **SUA Only** or **Full Feature** from the drop-sown list box. Refer to the Network Address Translation (NAT) Screens chapter for more details.
Back	Click **Back** to go back to the first wizard screen.
Next	Click **Next** to continue to the next wizard screen.

Figure 10 Internet Connection with ENET ENCAP

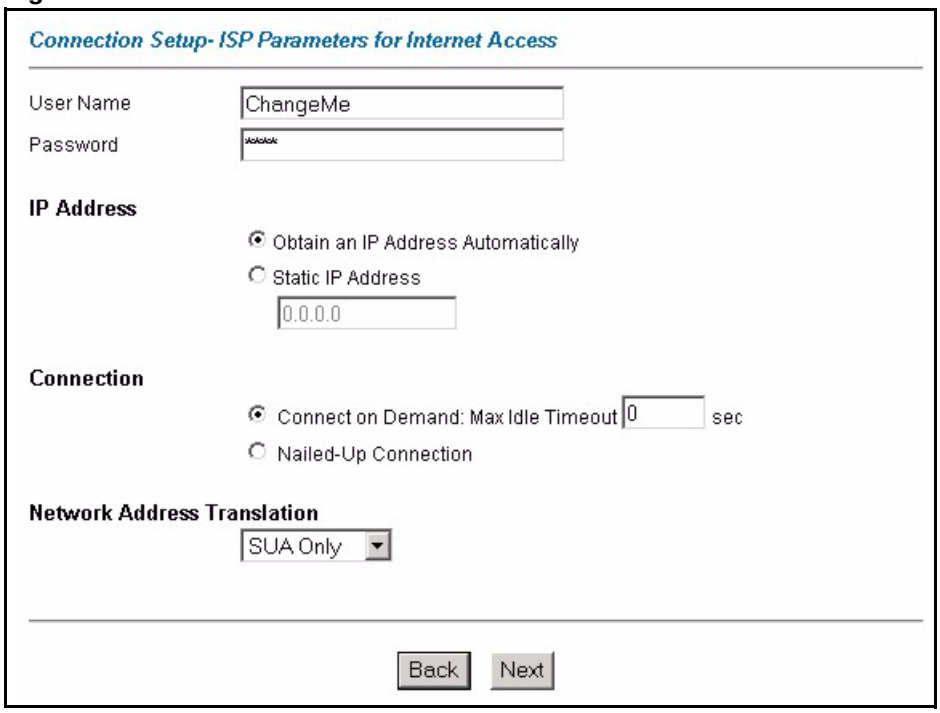


The following table describes the fields in this screen.

Table 7 Internet Connection with ENET ENCAP

LABEL	DESCRIPTION
IP Address	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. . Select **Obtain an IP Address Automatically** if you have a dynamic IP address; otherwise select **Static IP Address** and type your ISP assigned IP address in the IP Address text box below.
Subnet Mask	Enter a subnet mask in dotted decimal notation. Refer to the IP Subnetting appendix to calculate a subnet mask If you are implementing subnetting.
ENET ENCAP Gateway	You must specify a gateway IP address (supplied by your ISP) when you use **ENET ENCAP** in the **Encapsulation** field in the previous screen.
Network Address Translation	Select **None**, **SUA Only** or **Full Feature** from the drop-sown list box. Refer to the NAT chapter for more details.
Back	Click **Back** to go back to the first wizard screen.
Next	Click **Next** to continue to the next wizard screen.

Figure 11 Internet Connection with PPPoA



The following table describes the fields in this screen.

Table 8 Internet Connection with PPPoA

LABEL	DESCRIPTION
User Name	Enter the login name that your ISP gives you.
Password	Enter the password associated with the user name above.
IP Address	This option is available if you select **Routing** in the **Mode** field. A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Click **Obtain an IP Address Automatically** if you have a dynamic IP address; otherwise click **Static IP Address** and type your ISP assigned IP address in the IP Address text box below.
Connection	Select **Connect on Demand** when you don't want the connection up all the time and specify an idle time-out (in seconds) in the **Max. Idle Timeout** field. The default setting selects **Connection on Demand** with 0 as the idle time-out, which means the Internet session will not timeout. Select **Nailed-Up Connection** when you want your connection up all the time. The Prestige will try to bring up the connection automatically if it is disconnected. The schedule rule(s) in SMT menu 26 has priority over your **Connection** settings.
Network Address Translation	This option is available if you select **Routing** in the **Mode** field. Select **None**, **SUA Only** or **Full Feature** from the drop-sown list box. Refer to the Network Address Translation (NAT) Screens chapter for more details.
Back	Click **Back** to go back to the first wizard screen.
Next	Click **Next** to continue to the next wizard screen.

3.2.5 DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the Prestige as a DHCP server or disable it. When configured as a server, the Prestige provides the TCP/IP configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured.

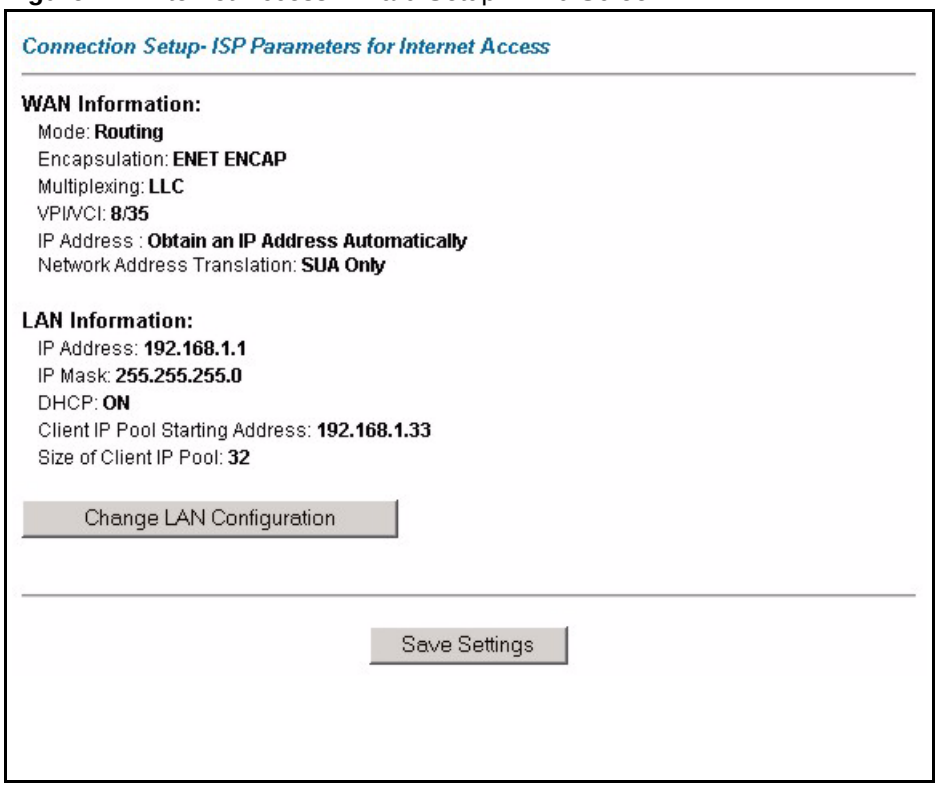
3.2.5.1 IP Pool Setup

The Prestige is pre-configured with a pool of 32 IP addresses starting from 192.168.1.33 to 192.168.1.64 for the client machines. This leaves 31 IP addresses, 192.168.1.2 to 192.168.1.32 (excluding the Prestige itself which has a default IP of 192.168.1.1) for other server machines, for example, server for mail, FTP, telnet, web, etc., that you may have.

3.2.6 Internet Access Wizard Setup: Third Screen

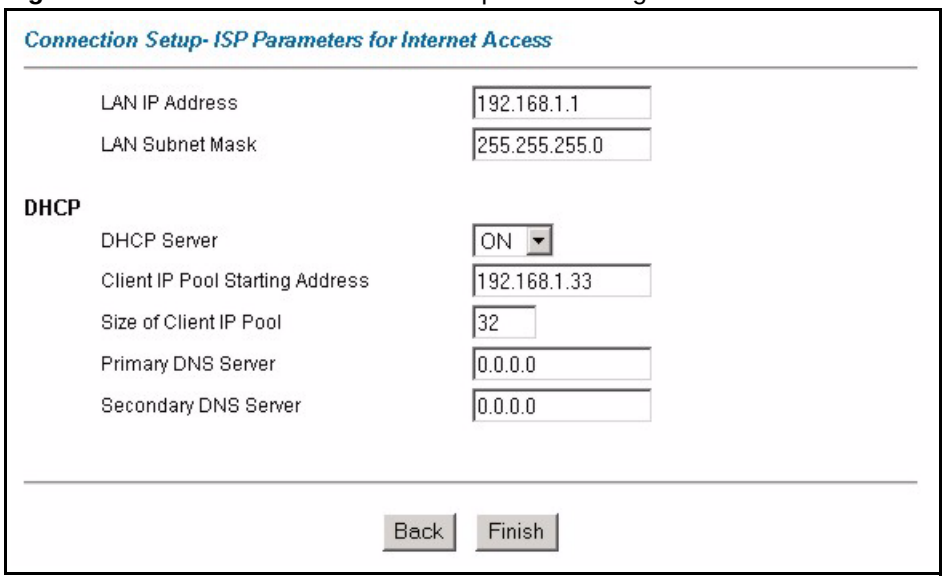
Verify the settings in the screen shown next. To change the LAN information on the Prestige, click **Change LAN Configurations**. Otherwise click **Save Settings** to save the configuration and skip to the section 3.13.

Figure 12 Internet Access Wizard Setup: Third Screen



If you want to change your Prestige LAN settings, click **Change LAN Configuration** to display the screen as shown next.

Figure 13 Internet Access Wizard Setup: LAN Configuration



The following table describes the fields in this screen.

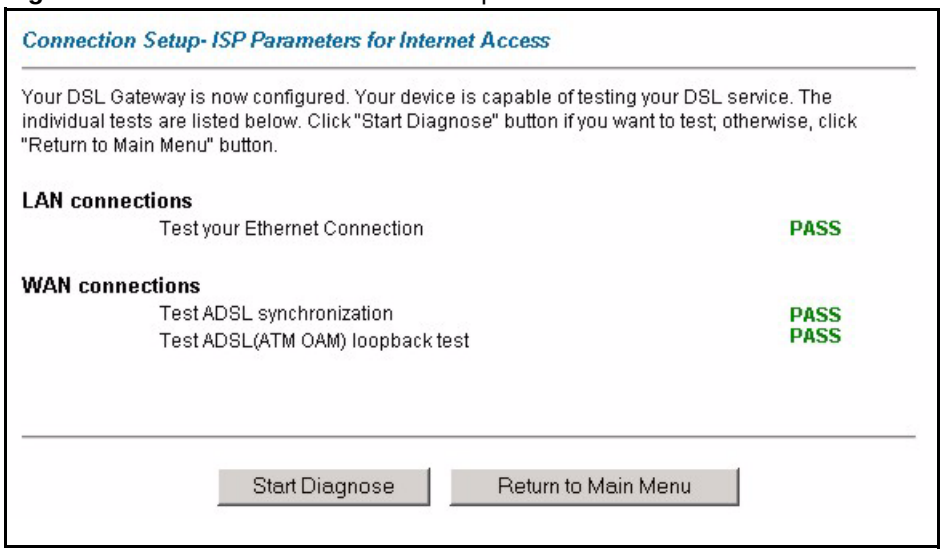
Table 9 Internet Access Wizard Setup: LAN Configuration

LABEL	DESCRIPTION
LAN IP Address	Enter the IP address of your Prestige in dotted decimal notation, for example, 192.168.1.1 (factory default). If you changed the Prestige's LAN IP address, you must use the new IP address if you want to access the web configurator again.
LAN Subnet Mask	Enter a subnet mask in dotted decimal notation.
DHCP	
DHCP Server	From the **DHCP Server** drop-down list box, select **On** to allow your Prestige to assign IP addresses, an IP default gateway and DNS servers to computer systems that support the DHCP client. Select **Off** to disable DHCP server. When DHCP server is used, set the following items:
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Size of Client IP Pool	This field specifies the size or count of the IP address pool.
Primary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Secondary DNS Server	As above.
Back	Click **Back** to go back to the previous screen.
Finish	Click **Finish** to save the settings and proceed to the next wizard screen.

3.2.7 Internet Access Wizard Setup: Connection Test

The Prestige automatically tests the connection to the computer(s) connected to the LAN ports. To test the connection from the Prestige to the ISP, click **Start Diagnose**. Otherwise click **Return to Main Menu** to go back to the **Site Map** screen.

Figure 14 Internet Access Wizard Setup: Connection Tests



3.2.7.1 Test Your Internet Connection

Launch your web browser and navigate to www.zyxel.com. Internet access is just the beginning. Refer to the rest of this *User's Guide* for more detailed information on the complete range of Prestige features. If you cannot access the Internet, open the web configurator again to confirm that the Internet settings you configured in the Wizard Setup are correct.

CHAPTER 4
Wizard Setup for Media Bandwidth Management

This chapter shows you how to configure basic bandwidth management using the wizard screens.

4.1 Introduction

The web configurator's **Media Bandwidth Magnt.** screens under **Wizard Setup** allows you to specify bandwidth classes based on an application (or service). You can allocate specific amounts of bandwidth capacity (bandwidth budgets) to different bandwidth classes.

The Prestige applies bandwidth management to traffic that it forwards out through an interface. The Prestige does not control the bandwidth of traffic that comes into an interface.

Bandwidth management applies to all traffic flowing out of the Prestige through the interface, regardless of the traffic's source.

Traffic redirect or IP alias may cause LAN-to-LAN traffic to pass through the Prestige and be managed by bandwidth management.

Refer to Chapter 23, "Media Bandwidth Management Advanced Setup for more information and advanced configuration.

4.1.1 Predefined Media Bandwidth Management Services

The following is a description of the services that you can select and to which you can apply media bandwidth management using the Wizard Setup screens.

Table 10 Media Bandwidth Mgnt. Wizard Setup: Services

SERVICE	DESCRIPTION
Xbox Live	This is Microsoft's online gaming service that lets you play multiplayer Xbox games on the Internet via broadband technology. Xbox Live uses port 3074.
VoIP (SIP)	Sending voice signals over the Internet is called Voice over IP or VoIP. Session Initiated Protocol (SIP) is an internationally recognized standard for implementing VoIP. SIP is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP is transported primarily over UDP but can also be transported over TCP, using the default port number 5060.

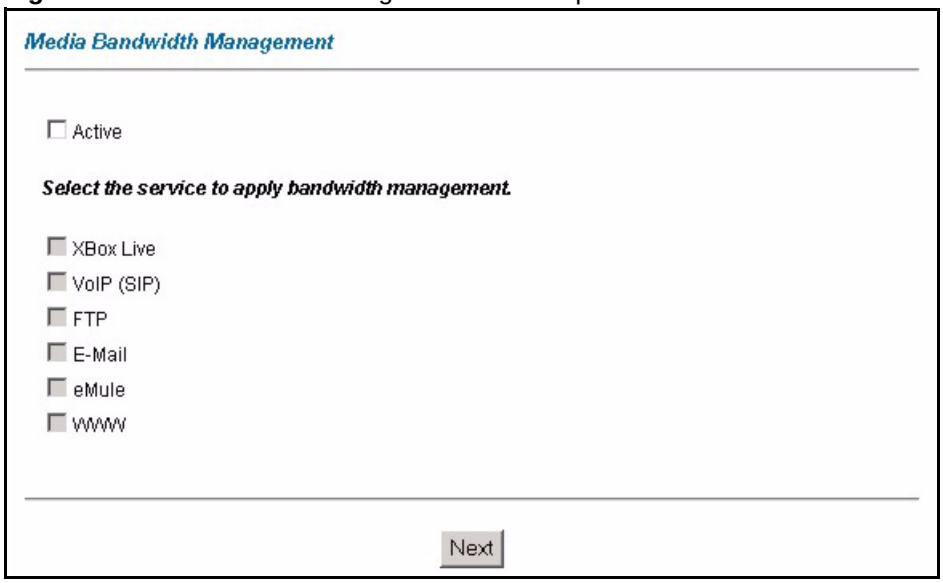
Table 10 Media Bandwidth Mgnt. Wizard Setup: Services (continued)

SERVICE	DESCRIPTION
FTP	File Transfer Program enables fast transfer of files, including large files that may not be possible by e-mail. FTP uses port number 21.
E-Mail	Electronic mail consists of messages sent through a computer network to specific groups or individuals. Here are some default ports for e-mail: POP3 - port 110 IMAP - port 143 SMTP - port 25 HTTP - port 80
eMule	These programs use advanced file sharing applications relying on central servers to search for files. They use default port 4662.
WWW	The World Wide Web (WWW) is an Internet system to distribute graphical, hyper-linked information, based on Hyper Text Transfer Protocol (HTTP) - a client/server protocol for the World Wide Web. The Web is not synonymous with the Internet; rather, it is just one service on the Internet. Other services on the Internet include Internet Relay Chat and Newsgroups. The Web is accessed through use of a browser.

4.2 Media Bandwidth Management Setup 1

Click **Media Bandwidth Mgnt.** under **Wizard Setup** in the **SITE MAP** screen.

Figure 15 Media Bandwidth Mgnt. Wizard Setup: First Screen



The following table describes the labels in this screen.

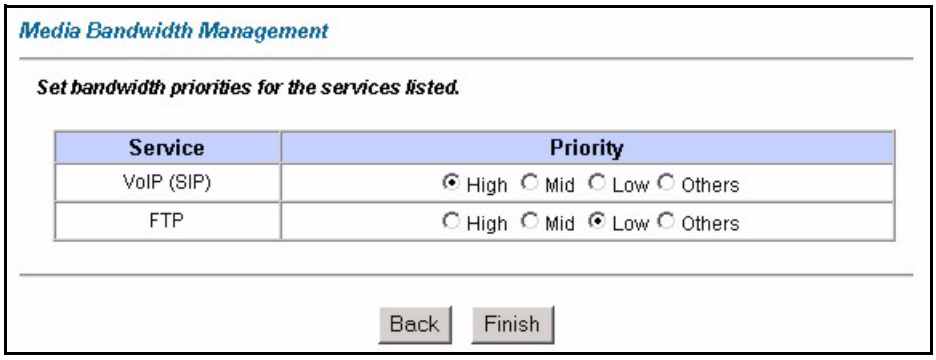
Table 11 Media Bandwidth Mgnt. Wizard Setup: First Screen

LABEL	DESCRIPTION
Active	Select the **Active** check box to have the Prestige apply bandwidth management to traffic going out through the Prestige's WAN, LAN or WLAN port.
Select the service to apply bandwidth management.	These checkboxes are applicable when you select the **Active** checkbox above. Create bandwidth management classes by selecting services from the list provided. • XBox Live • VoIP (SIP) • FTP • E-Mail • eMule • WWW Refer to Table 12 for more information.
Next	Click **Next** to continue.

4.3 Media Bandwidth Mgnt. Wizard Setup: Second Screen

The Prestige automatically creates the bandwidth class for each service you select. You may set the priority for each bandwidth class in the second wizard screen.

Figure 16 Media Bandwidth Mgnt. Wizard Setup: Second Screen



The following table describes the fields in this screen.

Table 12 Media Bandwidth Mgnt. Wizard Setup: Second Screen

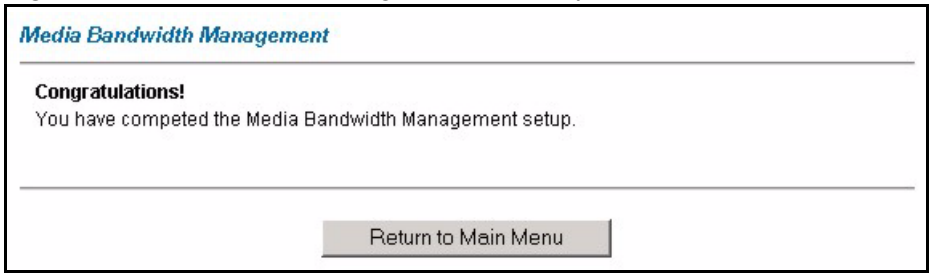
LABEL	DESCRIPTION
Service	These fields display the service(s) selected in the previous screen.
Priority	Select **High**, **Mid** or **Low** priority for each service to have your Prestige use a priority for traffic that matches that service. If the rules set up in this wizard are changed in **ADVANCED - Media Bandwidth Mgnt. - Class Setup**, then the service priority radio button will be set to **Others**. The **Class Configuration** screen allow you to edit these rule configurations (see the Media Bandwidth Management Class Configuration section for more information).
Back	Click **Back** to return to the previous screen.
Finish	Click **Finish** to complete and save the bandwidth management setup.

4.4 Media Bandwidth Mgnt. Wizard Setup: Finish

Well done! You have finished configuration of Media Bandwidth Management. You may now continue configuring your device.

Click **Return to Main Menu** to return to the **Site Map** screen.

Figure 17 Media Bandwidth Mgnt. Wizard Setup: Finish



CHAPTER 5
Password Setup

*This chapter provides information on the **Password** screen.*

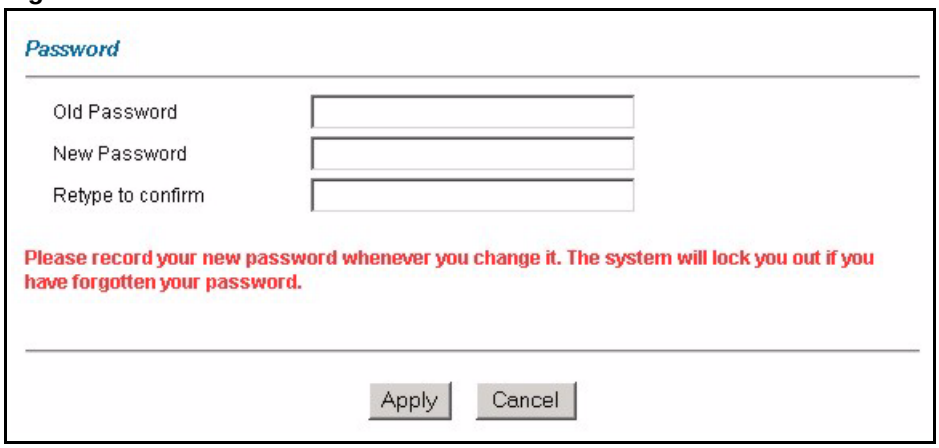
5.1 Password Overview

It is highly recommended that you change the password for accessing the Prestige.

5.1.1 Configuring Password

To change your Prestige's password (recommended), click **Password** in the **Site Map** screen.

Figure 18 Password



The following table describes the fields in this screen.

Table 13 Password

LABEL	DESCRIPTION
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type the new password in this field.
Retype to Confirm	Type the new password again in this field.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to begin configuring this screen afresh.

CHAPTER 6
LAN Setup

This chapter describes how to configure LAN settings.

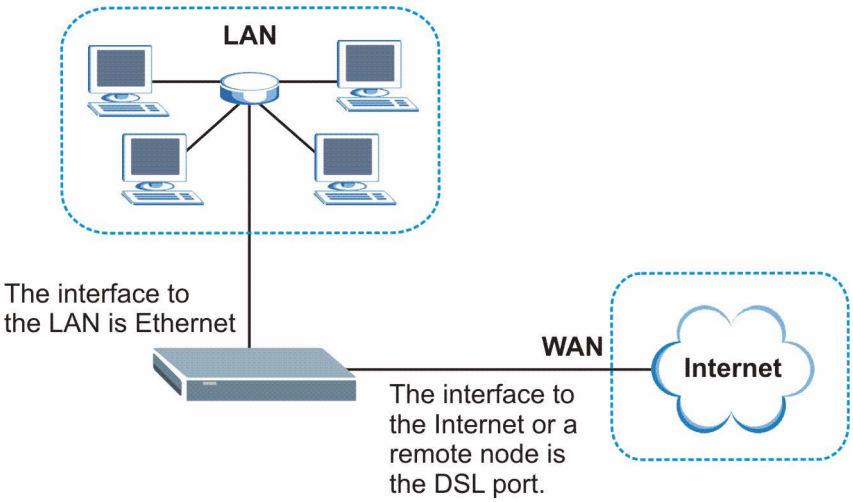
6.1 LAN Overview

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building. The LAN screens can help you configure a LAN DHCP server and manage IP addresses.

6.1.1 LANs, WANs and the Prestige

The actual physical connection determines whether the Prestige ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 19 LAN and WAN IP Addresses



6.2 DNS Server Address

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. The DNS server addresses that you enter in the DHCP setup are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses. The first is for an ISP to tell a customer the DNS server addresses, usually in the form of an information sheet, when s/he signs up. If your ISP gives you the DNS server addresses, enter them in the **DNS Server** fields in **DHCP Setup**, otherwise, leave them blank.

Some ISP's choose to pass the DNS servers using the DNS server extensions of PPP IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation. The Prestige supports the IPCP DNS server extensions through the DNS proxy feature.

If the **Primary** and **Secondary DNS Server** fields in the **LAN Setup** screen are not specified, for instance, left as 0.0.0.0, the Prestige tells the DHCP clients that it itself is the DNS server. When a computer sends a DNS query to the Prestige, the Prestige forwards the query to the real DNS server learned through IPCP and relays the response back to the computer.

Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you enter their IP addresses in the **LAN Setup** screen. This way, the Prestige can pass the DNS servers to the computers and the computers can query the DNS server directly without the Prestige's intervention.

6.3 DNS Server Address Assignment

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

There are two ways that an ISP disseminates the DNS server addresses.

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the DNS Server fields in DHCP Setup.
- The Prestige acts as a DNS proxy when the **Primary** and **Secondary DNS Server** fields are left blank in the **LAN Setup** screen.

6.4 LAN TCP/IP

The Prestige has built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

6.4.1 Factory LAN Defaults

The LAN parameters of the Prestige are preset in the factory with the following values:

- IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled with 32 client IP addresses starting from 192.168.1.33.

These parameters should work for the majority of installations. If your ISP gives you explicit DNS server address(es), read the embedded web configurator help regarding what fields need to be configured.

6.4.2 IP Address and Subnet Mask

Refer to the *IP Address and Subnet Mask* section in the **Wizard Setup** chapter for this information.

6.4.3 RIP Setup

RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. When set to:

- **Both** - the Prestige will broadcast its routing table periodically and incorporate the RIP information that it receives.
- **In Only** - the Prestige will not send any RIP packets but will accept all RIP packets received.
- **Out Only** - the Prestige will send out RIP packets but will not accept any RIP packets received.
- **None** - the Prestige will not send any RIP packets and will ignore any RIP packets received.

The **Version** field controls the format and the broadcasting method of the RIP packets that the Prestige sends (it recognizes both formats when receiving). **RIP-1** is universally supported; but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology.

Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting.

6.4.4 Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

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. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236. The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The Prestige supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the Prestige queries all directly connected networks to gather group membership. After that, the Prestige periodically updates this information. IP multicasting can be enabled/ disabled on the Prestige LAN and/or WAN interfaces in the web configurator (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

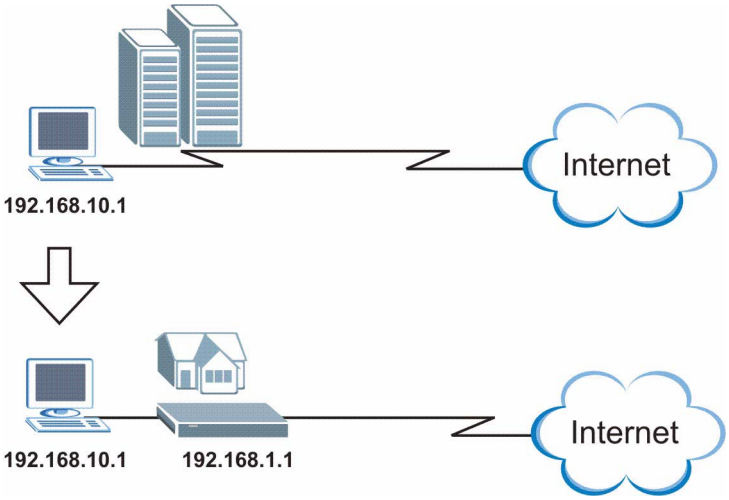
6.5 Any IP

Traditionally, you must set the IP addresses and the subnet masks of a computer and the Prestige to be in the same subnet to allow the computer to access the Internet (through the Prestige). In cases where your computer is required to use a static IP address in another network, you may need to manually configure the network settings of the computer every time you want to access the Internet via the Prestige.

With the Any IP feature and NAT enabled, the Prestige allows a computer to access the Internet without changing the network settings (such as IP address and subnet mask) of the computer, when the IP addresses of the computer and the Prestige are not in the same subnet. Whether a computer is set to use a dynamic or static (fixed) IP address, you can simply connect the computer to the Prestige and access the Internet.

The following figure depicts a scenario where a computer is set to use a static private IP address in the corporate environment. In a residential house where a Prestige is installed, you can still use the computer to access the Internet without changing the network settings, even when the IP addresses of the computer and the Prestige are not in the same subnet.

Figure 20 Any IP Example



The Any IP feature does not apply to a computer using either a dynamic IP address or a static IP address that is in the same subnet as the Prestige's IP address.

Note: You *must* enable NAT/SUA to use the Any IP feature on the Prestige.

6.5.1 How Any IP Works

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. IP routing table is defined on IP Ethernet devices (the Prestige) to decide which hop to use, to help forward data along to its specified destination.

The following lists out the steps taken, when a computer tries to access the Internet for the first time through the Prestige.

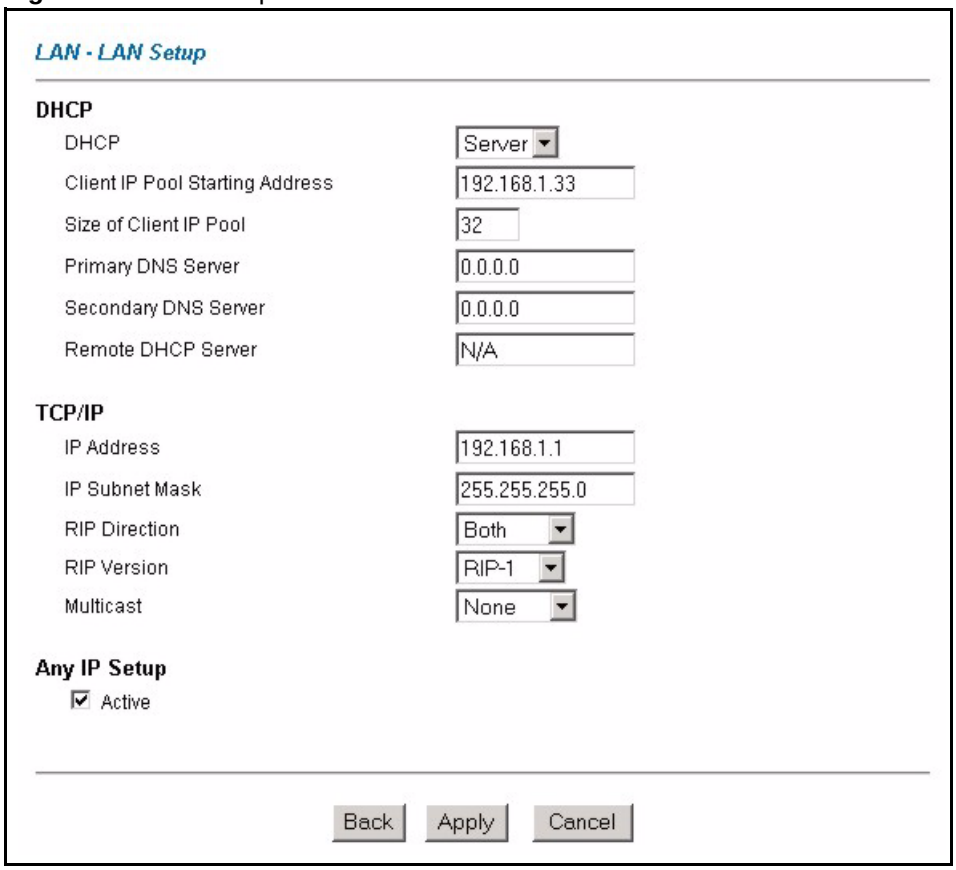
1. When a computer (which is in a different subnet) first attempts to access the Internet, it sends packets to its default gateway (which is not the Prestige) by looking at the MAC address in its ARP table.
2. When the computer cannot locate the default gateway, an ARP request is broadcast on the LAN.
3. The Prestige receives the ARP request and replies to the computer with its own MAC address.
4. The computer updates the MAC address for the default gateway to the ARP table. Once the ARP table is updated, the computer is able to access the Internet through the Prestige.
5. When the Prestige receives packets from the computer, it creates an entry in the IP routing table so it can properly forward packets intended for the computer.

After all the routing information is updated, the computer can access the Prestige and the Internet as if it is in the same subnet as the Prestige.

6.6 Configuring LAN

Click **LAN** and **LAN Setup** to open the following screen.

Figure 21 LAN Setup



The following table describes the fields in this screen.

Table 14 LAN Setup

LABEL	DESCRIPTION
DHCP	
DHCP	If set to **Server**, your Prestige can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client. If set to **None**, the DHCP server will be disabled. If set to **Relay**, the Prestige acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the **Remote DHCP Server** field in this case. When DHCP is used, the following items need to be set:
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Size of Client IP Pool	This field specifies the size or count of the IP address pool.
Primary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Secondary DNS Server	As above.
Remote DHCP Server	If **Relay** is selected in the **DHCP** field above then enter the IP address of the actual remote DHCP server here.
TCP/IP	
IP Address	Enter the IP address of your Prestige in dotted decimal notation, for example, 192.168.1.1 (factory default).
IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
RIP Direction	Select the RIP direction from **None**, **Both**, **In Only** and **Out Only**.
RIP Version	Select the RIP version from **RIP-1**, **RIP-2B** and **RIP-2M**.
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group. The Prestige supports both IGMP version 1 (**IGMP-v1**) and **IGMP-v2**. Select **None** to disable it.
Any IP Setup	Select the **Active** checkbox to enable the Any IP feature. This allows a computer to access the Internet without changing the network settings (such as IP address and subnet mask) of the computer, even when the IP addresses of the computer and the Prestige are not in the same subnet. When you disable the Any IP feature, only computers with dynamic IP addresses or static IP addresses in the same subnet as the Prestige's LAN IP address can connect to the Prestige or access the Internet through the Prestige.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to begin configuring this screen afresh.

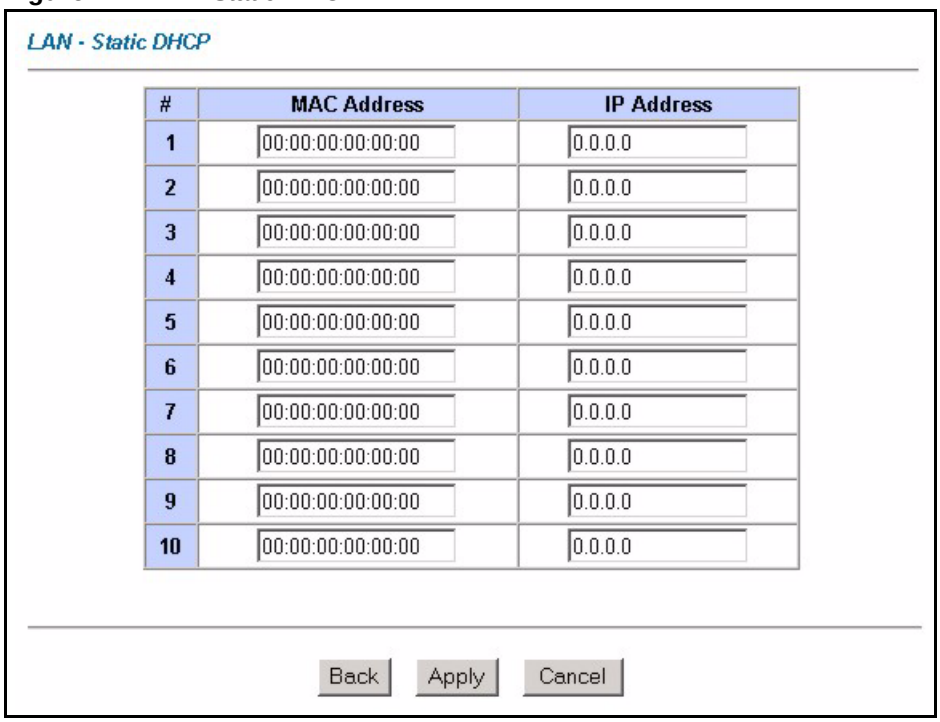
6.7 Configuring Static DHCP

This table allows you to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

To change your Prestige's static DHCP settings, click **LAN**, then the **Static DHCP** tab. The screen appears as shown.

Figure 22 LAN: Static DHCP



The following table describes the labels in this screen.

Table 15 LAN: Static DHCP

LABEL	DESCRIPTION
#	This is the index number of the Static IP table entry (row).
MAC Address	Type the MAC address (with colons) of a computer on your LAN.
IP Address	This field specifies the size, or count of the IP address pool.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

CHAPTER 7
DMZ

This chapter describes how to configure the Prestige's DMZ.

7.1 Introduction

The DeMilitarized Zone (DMZ) auto-negotiating 10/100 Mbps Ethernet port provides a way for public servers (Web, e-mail, FTP, etc.) to be visible to the outside world (while still being protected from DoS (Denial of Service) attacks such as SYN flooding and Ping of Death). These public servers can also still be accessed from the secure LAN.

By default the firewall allows traffic between the WAN and the DMZ, traffic from the DMZ to the LAN is denied, and traffic from the LAN to the DMZ is allowed. Internet users can have access to host servers on the DMZ but no access to the LAN, unless special filter rules allowing access were configured by the administrator or the user is an authorized remote user.

It is highly recommended that you connect all of your public servers to the DMZ port. If you have more than one public server, connect a hub to the DMZ port.

It is also highly recommended that you keep all sensitive information off of the public servers connected to the DMZ port. Store sensitive information on LAN computers.

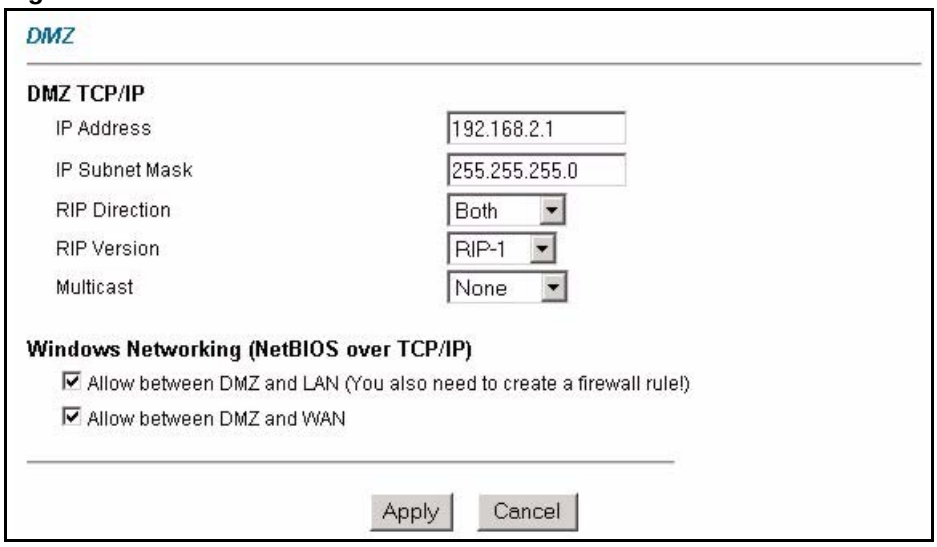
7.2 Configuring DMZ

You can assign public or private IP addresses to computers connected to the DMZ port.

With public IP addresses, the WAN and DMZ ports must use public IP addresses that are on separate subnets. See the appendix for information on IP subnetting.

From the main menu, click **DMZ**. The screen appears as shown next.

Figure 23 DMZ



The following table describes the labels in this screen..

Table 16 DMZ

LABEL	DESCRIPTION
DMZ TCP/IP	
IP Address	Type the IP address of your Prestige's DMZ port in dotted decimal notation. Make sure the IP address is on a separate subnet from the LAN port.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your Prestige will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Prestige 255.255.255.0.
RIP Direction	RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Select the RIP direction from **Both**/**In Only**/**Out Only**/**None**. When set to **Both** or **Out Only**, the Prestige will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to None, it will not send any RIP packets and will ignore any RIP packets received. **Both** is the default.
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the Prestige sends (it recognizes both formats when receiving). RIP-1 is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both RIP-2B and RIP-2M sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to **Both** and the **Version** set to **RIP-1**.
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group. The Prestige supports both IGMP version 1 (**IGMP-v1**) and **IGMP-v2**. Select **None** to disable it.
Windows Networking (NetBIOS over TCP/IP)	

Table 16 DMZ (continued)

LABEL	DESCRIPTION
Allow between DMZ and LAN	Select this check box to forward NetBIOS packets from the LAN to the DMZ and from the DMZ to the LAN. If your firewall is enabled with the default policy set to block DMZ to LAN traffic, you also need to enable the default DMZ to LAN firewall rule that forwards NetBIOS traffic.Clear this check box to block all NetBIOS packets going from the LAN to the DMZ and from the DMZ to the LAN.
Allow between DMZ and WAN	Select this check box to forward NetBIOS packets from the WAN to the DMZ and from the DMZ to the WAN. Clear this check box to block all NetBIOS packets going from the WAN to the DMZ and from the DMZ to the WAN.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to begin configuring this screen afresh.

CHAPTER 8
Wireless LAN Setup

This chapter discusses how to configure Wireless LAN on the Prestige.

8.1 Introduction

This section introduces the wireless LAN and some basic configurations. Wireless LANs can be as simple as two computers with wireless LAN cards communicating in a peer-to-peer network or as complex as a number of computers with wireless LAN cards communicating through access points which bridge network traffic to the wired LAN.

Note: The WLAN screens are only available when a WLAN card is installed.

8.1.1 Additional Installation Requirements for Using 802.1x

- A computer with an IEEE 802.11b/g wireless LAN card and equipped with a web browser (with JavaScript enabled) and/or Telnet.
- A wireless station computer must be running IEEE 802.1x-compliant software. Not all Windows operating systems support IEEE 802.1X (see the Microsoft web site for details). For other operating systems, see its documentation. If your operating system does not support IEEE 802.1X, then you may need to install IEEE 802.1X client software.
- An optional network RADIUS server for remote user authentication and accounting.

8.1.2 Channel

A channel is the radio frequency(ies) used by IEEE 802.11b/g wireless devices. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel than an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

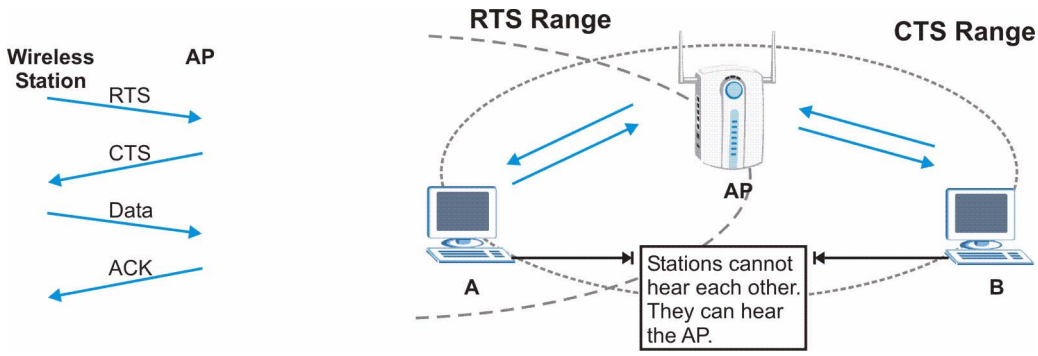
8.1.3 ESS ID

An Extended Service Set (ESS) is a group of access points or wireless gateways connected to a wired LAN on the same subnet. An ESS ID uniquely identifies each set. All access points or wireless gateways and their associated wireless stations in the same set must have the same ESSID.

8.1.4 RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 24 RTS/CTS



When station A sends data to the Prestige, it might not know that the station B is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

8.1.5 Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the Prestige will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

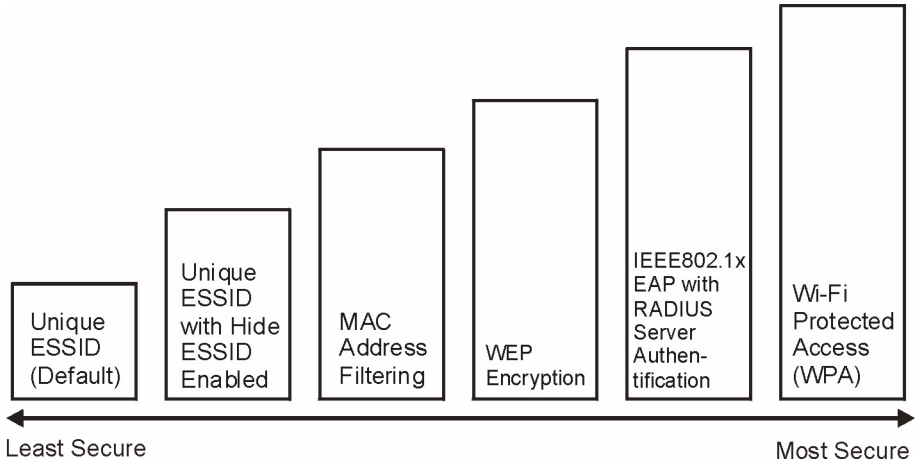
If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

8.2 Levels of Security

Wireless security is vital to your network to protect wireless communication between wireless stations, access points and the wired network.

The figure below shows the possible wireless security levels on your Prestige. EAP (Extensible Authentication Protocol) is used for authentication and utilizes dynamic WEP key exchange. It requires interaction with a RADIUS (Remote Authentication Dial-In User Service) server either on the WAN or your LAN to provide authentication service for wireless stations.

Figure 25 Prestige Wireless Security Levels



If you do not enable any wireless security on your Prestige, your network is accessible to any wireless networking device that is within range.

Use the Prestige web configurator to configurator to set up your wireless LAN security settings. Refer to the chapter on using the Prestige web configurator to see how to access the web configurator.

8.3 Data Encryption with WEP

WEP encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private. It encrypts unicast and multicast communications in a network. Both the wireless stations and the access points must use the same WEP key for data encryption and decryption.

Your Prestige allows you to configure up to four 64-bit, 128-bit or 256-bit WEP keys but only one key can be enabled at any one time.

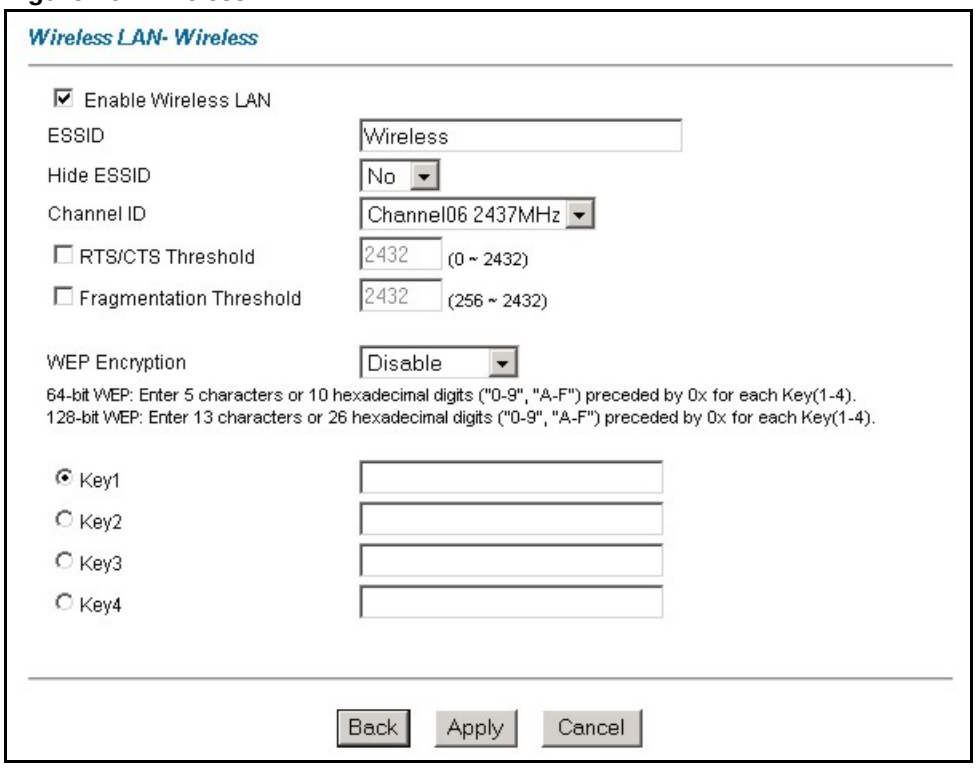
In order to configure and enable WEP encryption; click **Wireless LAN** and **Wireless** to the display the **Wireless** screen.

8.4 Configuring Wireless LAN

Note: If you are configuring the Prestige from a computer connected to the wireless LAN and you change the Prestige's ESSID or WEP settings, you will lose your wireless connection when you press Apply to confirm. You must then change the wireless settings of your computer to match the Prestige's new settings.

Click **Wireless LAN**, **Wireless** to open the **Wireless** screen.

Figure 26 Wireless LAN



The following table describes the fields in this screen.

Table 17 Wireless LAN

LABEL	DESCRIPTION
Enable Wireless LAN	The wireless LAN is turned off by default, before you enable the wireless LAN you should configure some security by setting MAC filters and/or 802.1x security; otherwise your wireless LAN will be vulnerable upon enabling it. Select the check box to enable the wireless LAN.
ESSID	The ESSID (Extended Service Set Identification) is a unique name to identify the Prestige in the wireless LAN. Wireless stations associating to the Prestige must have the same ESSID. Enter a descriptive name (up to 32 characters).
Hide ESSID	Select **Yes** to hide the ESSID in so a station cannot obtain the ESSID through passive scanning. Select **No** to make the ESSID visible so a station can obtain the ESSID through passive scanning.
Channel ID	The radio frequency used by IEEE 802.11b wireless devices is called a channel. Select a channel from the drop-down list box.
RTS/CTS Threshold	The RTS (Request To Send) threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between 0 and 2432.

Table 17 Wireless LAN (continued)

LABEL	DESCRIPTION
Fragmentation Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between 256 and 2432.
WEP Encryption	WEP (Wired Equivalent Privacy) encrypts data frames before transmitting over the wireless network. Select **Disable** to allow all wireless computers to communicate with the access points without any data encryption. Select **64-bit WEP**, **128-bit WEP** or **256-bit WEP** to use data encryption.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the Prestige and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit WEP**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). If you chose **256-bit WEP**, then enter 29 ASCII characters or 58 hexadecimal characters ("0-9", "A-F"). The values for the WEP keys must be set up exactly the same on all wireless devices in the same wireless LAN. You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.
Back	Click **Back** to go to the main wireless LAN setup screen.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to begin configuring this screen afresh.

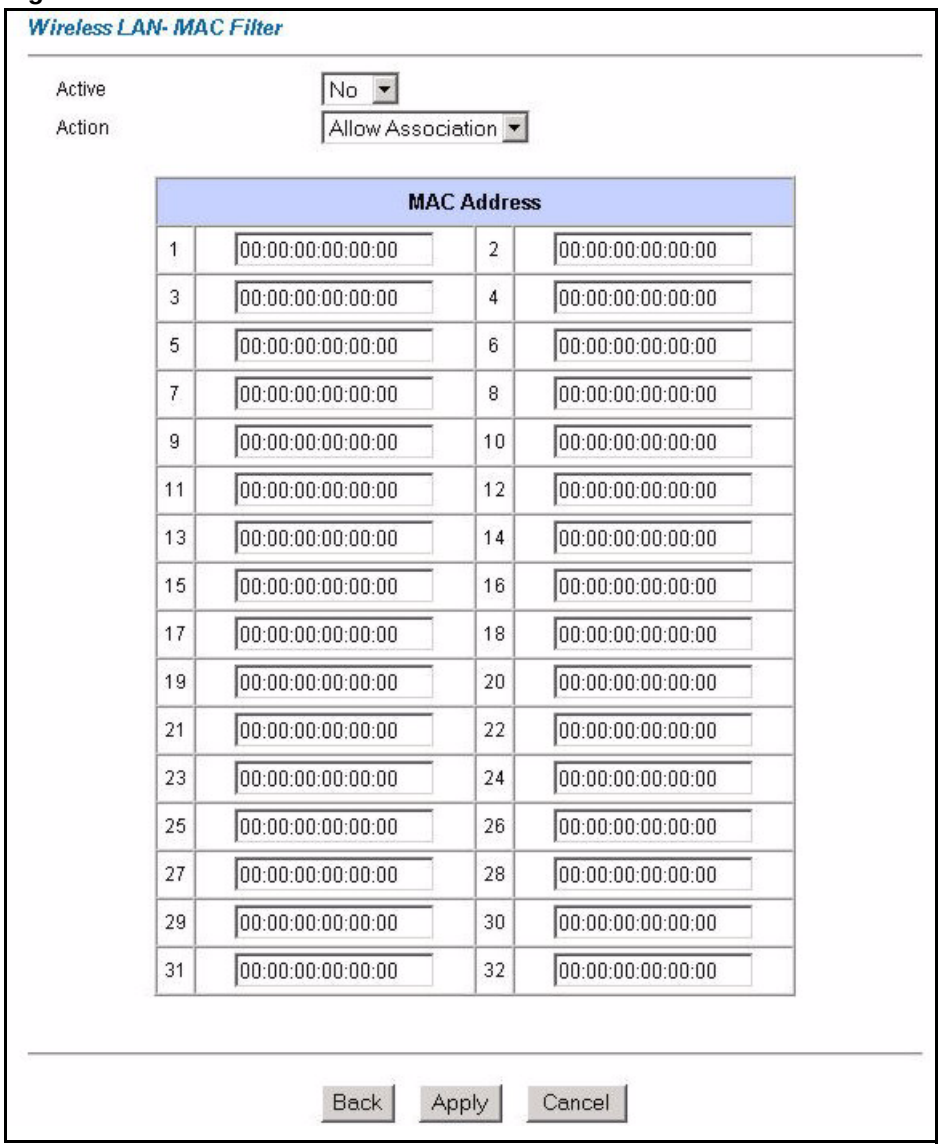
8.5 Configuring MAC Filter

The MAC filter screen allows you to configure the Prestige to give exclusive access to up to 32 devices (Allow Association) or exclude up to 32 devices from accessing the Prestige (Deny Association). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the devices to configure this screen.

To change your Prestige's MAC filter settings, click **Wireless LAN**, **MAC Filter** to open the **MAC Filter** screen. The screen appears as shown.

Note: Be careful not to list your computer's MAC address and set the **Action** field to **Deny Association** when managing the Prestige via a wireless connection. This would lock you out.

Figure 27 MAC Address Filter



The following table describes the fields in this menu.

Table 18 MAC Address Filter

LABEL	DESCRIPTION
Active	Select **Yes** from the drop down list box to enable MAC address filtering.
Action	Define the filter action for the list of MAC addresses in the **MAC Address** table. Select **Deny Association** to block access to the router, MAC addresses not listed will be allowed to access the Prestige. Select **Allow Association** to permit access to the router, MAC addresses not listed will be denied access to the Prestige.
MAC Address	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless station that are allowed or denied access to the Prestige in these address fields.
Back	Click **Back** to go to the main wireless LAN setup screen.

Table 18 MAC Address Filter (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to begin configuring this screen afresh.

8.6 Network Authentication

You can set the Prestige and your network to authenticate a wireless station before the wireless station can communicate with the Prestige and the wired network to which the Prestige is connected.

8.6.1 EAP

EAP is an authentication protocol designed originally to run over PPP (Point-to-Point Protocol) frame in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, the access point helps a wireless station and a RADIUS server to perform mutual authentication.

8.6.1.1 RADIUS

RADIUS is based on a client-sever model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication

  Determines the identity of the users.

- Authorization

  Determines the network services available to authenticated users once they are connected to the network.

- Accounting

  Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your Prestige acts as a message relay between the wireless station and the network RADIUS server.

8.6.1.2 Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request

  Sent by an access point requesting authentication.

- Access-Reject

  Sent by a RADIUS server rejecting access.

- Access-Accept

  Sent by a RADIUS server allowing access.

- Access-Challenge

  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request

  Sent by the access point requesting accounting.

- Accounting-Response

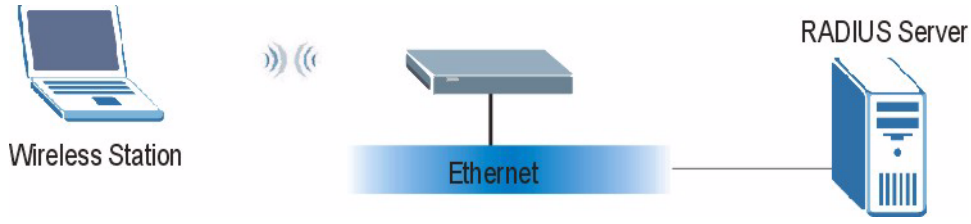
  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

8.6.2 EAP Authentication Overview

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, the access point helps a wireless station and a RADIUS server perform authentication.

Figure 28 EAP Authentication



The details below provide a general description of how IEEE 802.1x EAP authentication works. For an example list of EAP-MD5 authentication steps, see the appendix about IEEE 802.1x.

1. The wireless station sends a "start" message to the Prestige.
2. The Prestige sends a "request identity" message to the wireless station for identity information.

3 The wireless station replies with identity information, including username and password.

4 The RADIUS server checks the user information against its user profile database and determines whether or not to authenticate the wireless station.

8.7 Introduction to WPA

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i security specification draft. Key differences between WPA and WEP are user authentication and improved data encryption.

8.7.1 User Authentication

WPA applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. You can't use the Prestige's Local User Database for WPA authentication purposes since the Local User Database uses EAP-MD5 which cannot be used to generate keys. See later in this chapter and the appendices for more information on IEEE 802.1x, RADIUS and EAP.

Therefore, if you don't have an external RADIUS server you should use WPA-PSK (WPA - Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a client will be granted access to a WLAN.

8.7.2 Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x.

Temporal Key Integrity Protocol (TKIP) uses 128-bit keys that are dynamically generated and distributed by the authentication server. It includes a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

TKIP regularly changes and rotates the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), TKIP makes it much more difficult to decode data on a Wi-Fi network than WEP, making it difficult for an intruder to break into the network.

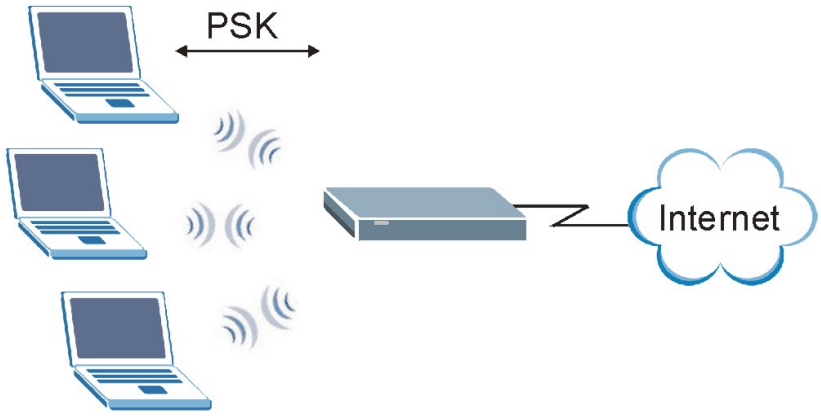
The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs an easier-to-use, consistent, single, alphanumeric password.

8.8 WPA-PSK Application Example

A WPA-PSK application looks as follows.

1. First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters (including spaces and symbols).
2. The AP checks each client's password and (only) allows it to join the network if it matches its password.
3. The AP derives and distributes keys to the wireless clients.
4. The AP and wireless clients use the TKIP encryption process to encrypt data exchanged between them.

Figure 29 WPA - PSK Authentication



8.9 WPA with RADIUS Application Example

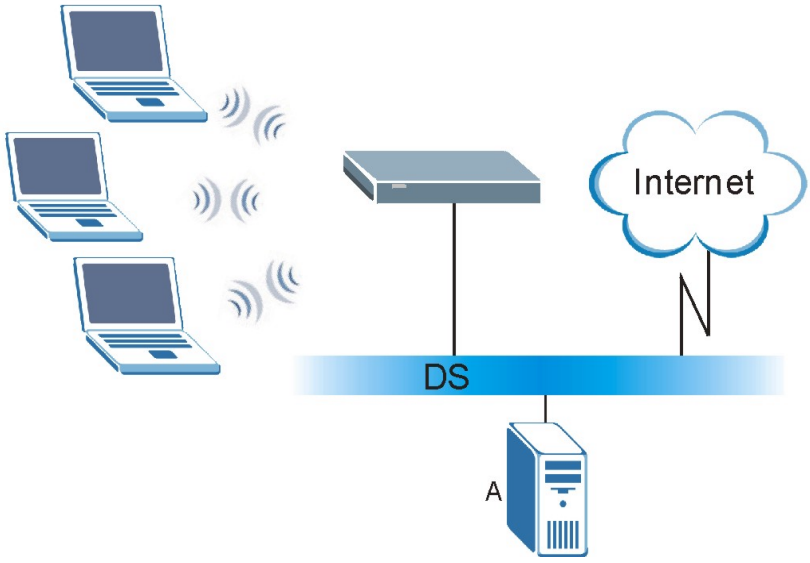
You need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1. The AP passes the wireless client's authentication request to the RADIUS server.

2 The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.

3 The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients

Figure 30 WPA with RADIUS Application Example



8.10 Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each Authentication Method/ key management protocol type. You enter manual keys by first selecting **64-bit WEP** or **128-bit WEP** from the **WEP Encryption** field and then typing the keys (in ASCII or hexadecimal format) in the key text boxes. MAC address filters are not dependent on how you configure these security features.

Table 19 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	ENABLE IEEE 802.1X
Open	None	No	No
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable

Table 19 Wireless Security Relational Matrix (continued)

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	ENABLE IEEE 802.1X
WPA	WEP	No	Yes
WPA	TKIP	No	Yes
WPA-PSK	WEP	Yes	Yes
WPA-PSK	TKIP	Yes	Yes

8.11 Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicants are the WPA patch for Windows XP, Funk Software's Odyssey client, and Meetinghouse Data Communications' AEGIS client.

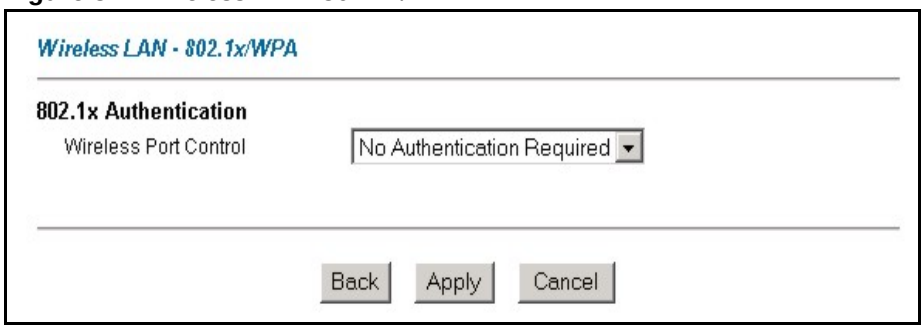
The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

8.12 Configuring 802.1x and WPA

To change your Prestige's authentication settings, click the **Wireless LAN** link under **Advanced Setup** and then the **802.1x/WPA** tab. The screen varies by the key management protocol you select.

You see the next screen when you select **No Access Allowed** or **No Authentication Required** in the **Wireless Port Control** field.

Figure 31 Wireless LAN: 802.1x/WPA



The following table describes the label in this screen.

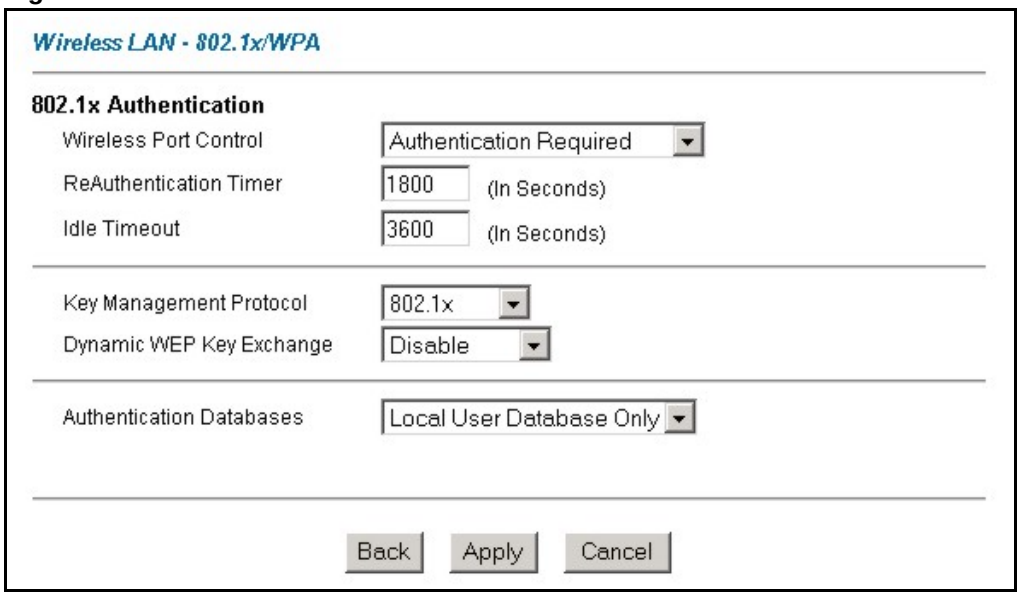
Table 20 Wireless LAN: 802.1x/WPA

LABEL	DESCRIPTION
Wireless Port Control	To control wireless stations access to the wired network, select a control method from the drop-down list box. Choose from **No Access Allowed**, **No Authentication Required** and **Authentication Required**. **No Access Allowed** blocks all wireless stations access to the wired network. **No Authentication Required** allows all wireless stations access to the wired network without entering usernames and passwords. This is the default setting. **Authentication Required** means that all wireless stations have to enter usernames and passwords before access to the wired network is allowed. Select **Authentication Required** to configure **Key Management Protocol** and other related fields.
Back	Click **Back** to go to the main wireless LAN setup screen.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to begin configuring this screen afresh.

8.12.1 Authentication Required: 802.1x

Select **Authentication Required** in the **Wireless Port Control** field and **802.1x** in the **Key Management Protocol** field to display the next screen.

Figure 32 Wireless LAN: 802.1x/WPA for 802.1x Protocol



The following table describes the labels in this screen.

Table 21 Wireless LAN: 802.1x/WPA for 802.1x Protocol

LABEL	DESCRIPTION
Wireless Port Control	To control wireless stations access to the wired network, select a control method from the drop-down list box. Choose from **No Authentication Required**, **Authentication Required** and **No Access Allowed**. The following fields are only available when you select **Authentication Required**.
ReAuthentication Timer (in Seconds)	Specify how often wireless stations have to reenter usernames and passwords in order to stay connected. This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. Enter a time interval between 10 and 9999 seconds. The default time interval is **1800** seconds (30 minutes). **Note:** If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Idle Timeout (in Seconds)	The Prestige automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed. This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. The default time interval is **3600** seconds (or 1 hour).
Key Management Protocol	Choose **802.1x** from the drop-down list.
Dynamic WEP Key Exchange	This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. Also set the **Authentication Databases** field to **RADIUS Only**. Local user database may not be used. Select **Disable** to allow wireless stations to communicate with the access points without using dynamic WEP key exchange. Select **64-bit WEP** or **128-bit WEP** to enable data encryption. Up to 32 stations can access the Prestige when you configure dynamic WEP key exchange. This field is not available when you set **Key Management Protocol** to **WPA** or **WPA-PSK**.
Authentication Databases	The authentication database contains wireless station login information. The local user database is the built-in database on the Prestige. The RADIUS is an external server. Use this drop-down list box to select which database the Prestige should use (first) to authenticate a wireless station. Before you specify the priority, make sure you have set up the corresponding database correctly first. Select **Local User Database Only** to have the Prestige just check the built-in user database on the Prestige for a wireless station's username and password. Select **RADIUS Only** to have the Prestige just check the user database on the specified RADIUS server for a wireless station's username and password. Select **Local first, then RADIUS** to have the Prestige first check the user database on the Prestige for a wireless station's username and password. If the user name is not found, the Prestige then checks the user database on the specified RADIUS server. Select **RADIUS first, then Local** to have the Prestige first check the user database on the specified RADIUS server for a wireless station's username and password. If the Prestige cannot reach the RADIUS server, the Prestige then checks the local user database on the Prestige. When the user name is not found or password does not match in the RADIUS server, the Prestige will not check the local user database and the authentication fails.

Table 21 Wireless LAN: 802.1x/WPA for 802.1x Protocol (continued)

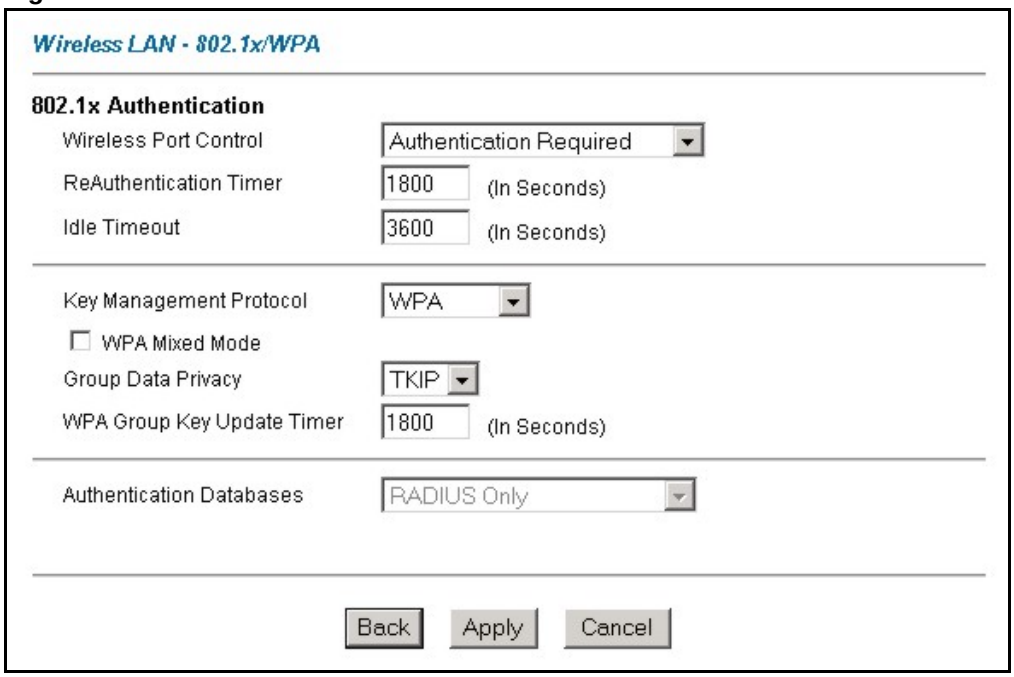
LABEL	DESCRIPTION
Back	Click **Back** to go to the main wireless LAN setup screen.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Note: Once you enable user authentication, you need to specify an external RADIUS server or create local user accounts on the Prestige for authentication.

8.12.2 Authentication Required: WPA

Select **Authentication Required** in the **Wireless Port Control** field and **WPA** in the **Key Management Protocol** field to display the next screen.

Figure 33 Wireless LAN: 802.1x/WPA for WPA Protocol



The following table describes the labels not previously discussed

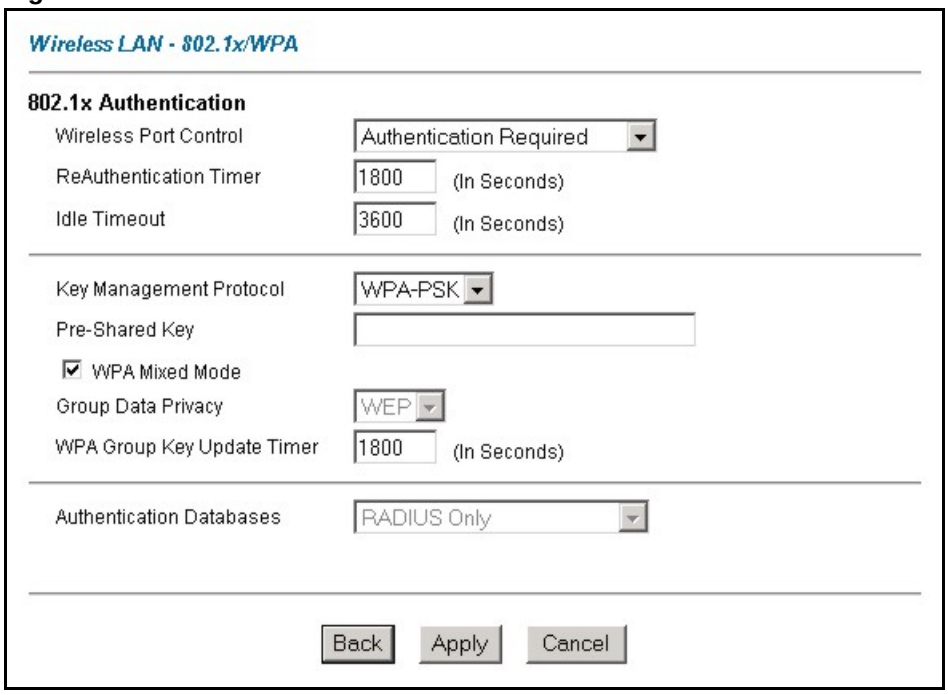
Table 22 Wireless LAN: 802.1x/WPA for WPA Protocol

LABEL	DESCRIPTION
Key Management Protocol	Choose **WPA** in this field.
WPA Mixed Mode	The Prestige can operate in **WPA Mixed Mode**, which supports both clients running WPA and clients running dynamic WEP key exchange with 802.1x in the same Wi-Fi network. Select the check box to activate WPA mixed mode. Otherwise, clear the check box and configure the **Group Data Privacy** field.
Group Data Privacy	**Group Data Privacy** allows you to choose **TKIP** (recommended) or **WEP** for broadcast and multicast ("group") traffic if the **Key Management Protocol** is **WPA** and **WPA Mixed Mode** is disabled. **WEP** is used automatically if you have enabled **WPA Mixed Mode**. All unicast traffic is automatically encrypted by **TKIP** when **WPA** or **WPA-PSK Key Management Protocol** is selected.
WPA Group Key Update Timer	The **WPA Group Key Update Timer** is the rate at which the AP (if using **WPA-PSK** key management) or RADIUS server (if using **WPA** key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **WPA Group Key Update Timer** is also supported in WPA-PSK mode. The Prestige default is 1800 seconds (30 minutes).
Authentication Databases	When you configure **Key Management Protocol** to **WPA**, the **Authentication Databases** must be **RADIUS Only**. You can only use the **Local User Database Only** with **802.1x Key Management Protocol**.

8.12.3 Authentication Required: WPA-PSK

Select **Authentication Required** in the **Wireless Port Control** field and **WPA-PSK** in the **Key Management Protocol** field to display the next screen.

Figure 34 Wireless LAN: 802.1x/WPA for WPA-PSK Protocol



The following table describes the labels not previously discussed.

Table 23 Wireless LAN: 802.1x/WPA for WPA-PSK Protocol

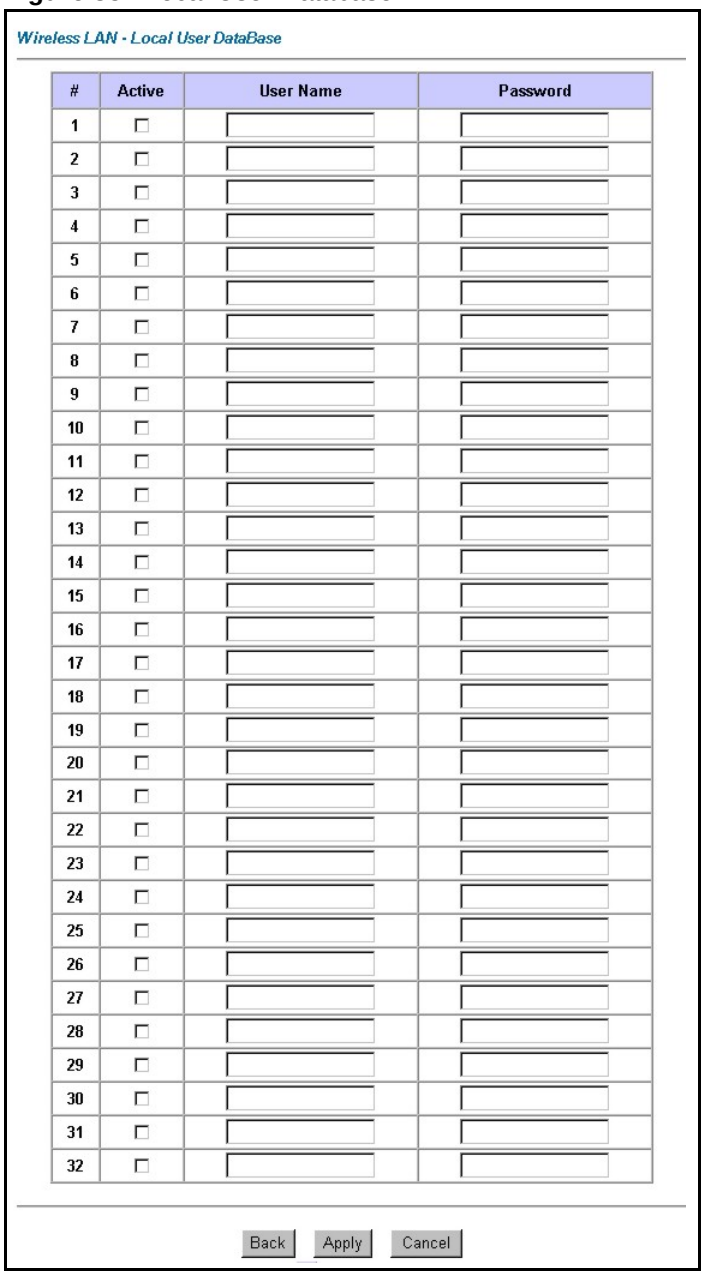
LABEL	DESCRIPTION
Key Management Protocol	Choose **WPA-PSK** in this field.
Pre-Shared Key	The encryption mechanisms used for **WPA** and **WPA-PSK** are the same. The only difference between the two is that **WPA-PSK** uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
WPA Mixed Mode	The Prestige can operate in **WPA Mixed Mode**, which supports both clients running WPA and clients running dynamic WEP key exchange with 802.1x in the same Wi-Fi network. Select the check box to activate WPA mixed mode. Otherwise, clear the check box and configure the **Group Data Privacy** field.
Group Data Privacy	**Group Data Privacy** allows you to choose **TKIP** (recommended) or **WEP** for broadcast and multicast ("group") traffic if the **Key Management Protocol** is **WPA** and **WPA Mixed Mode** is disabled. **WEP** is used automatically if you have enabled **WPA Mixed Mode**. All unicast traffic is automatically encrypted by **TKIP** when **WPA** or **WPA-PSK Key Management Protocol** is selected.
Authentication Databases	This field is only visible when **WPA Mixed Mode** is enabled.

8.13 Configuring Local User Authentication

By storing user profiles locally, your Prestige is able to authenticate wireless users without interacting with a network RADIUS server. However, there is a limit on the number of users you may authenticate in this way.

To change your Prestige's local user database, click **Wireless LAN**, **Local User Database**. The screen appears as shown.

Figure 35 Local User Database



The following table describes the fields in this screen.

Table 24 Local User Database

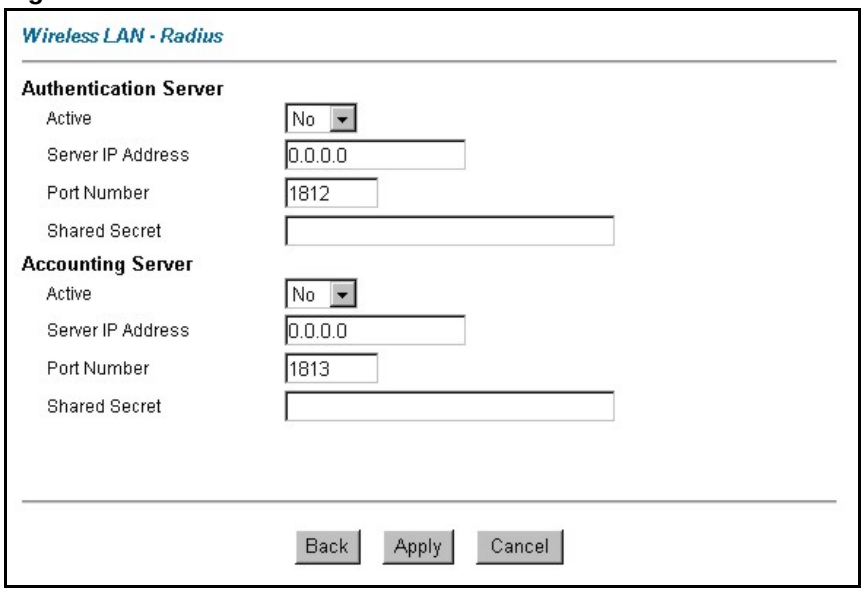
LABEL	DESCRIPTION
#	This is the index number of a local user account.
Active	Select this check box to enable the user profile.
User Name	Enter the user name of the user profile.
Password	Enter a password up to 31 characters long for this user profile.
Back	Click **Back** to go to the main wireless LAN setup screen.
Apply	Click **Apply** to save these settings back to the Prestige.
Cancel	Click **Cancel** to begin configuring this screen again.

8.14 Configuring RADIUS

Once you enable the EAP authentication, you need to specify the external sever for remote user authentication and accounting.

To set up your Prestige's RADIUS server settings, click **WIRELESS LAN**, **RADIUS**. The screen appears as shown.

Figure 36 RADIUS



The following table describes the fields in this screen.

Table 25 RADIUS

LABEL	DESCRIPTION
Authentication Server	
Active	Select **Yes** from the drop-down list box to enable user authentication through an external authentication server.
Server IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	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 with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the access points. The key is not sent over the network. This key must be the same on the external authentication server and Prestige.
Accounting Server	
Active	Select **Yes** from the drop-down list box to enable user authentication through an external accounting server.
Server IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port Number	The default port of the RADIUS server for accounting is **1813**. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the access points. The key is not sent over the network. This key must be the same on the external accounting server and the Prestige.
Back	Click **Back** to go to the main wireless LAN setup screen.
Apply	Click **Apply** to save these settings back to the Prestige.
Cancel	Click **Cancel** to begin configuring this screen again.

CHAPTER 9
WAN Setup

This chapter describes how to configure WAN settings.

9.1 WAN Overview

A WAN (Wide Area Network) is an outside connection to another network or the Internet.

See Chapter 3 Wizard Setup for Internet Access for more information on the fields in the WAN screens.

9.2 Metric

The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".

The metric sets the priority for the Prestige's routes to the Internet. If any two of the default routes have the same metric, the Prestige uses the following pre-defined priorities:

- Normal route: designated by the ISP (see the Configuring WAN Setup section)
- Traffic-redirect route (see the Traffic Redirect section)
- WAN-backup route, also called dial-backup (see the Configuring WAN Backup section)

For example, if the normal route has a metric of "1" and the traffic-redirect route has a metric of "2" and dial-backup route has a metric of "3", then the normal route acts as the primary default route. If the normal route fails to connect to the Internet, the Prestige tries the traffic-redirect route next. In the same manner, the Prestige uses the dial-backup route if the traffic-redirect route also fails.

If you want the dial-backup route to take first priority over the traffic-redirect route or even the normal route, all you need to do is set the dial-backup route's metric to "1" and the others to "2" (or greater).

IP Policy Routing overrides the default routing behavior and takes priority over all of the routes mentioned above (see Chapter 43 IP Policy Routing).

9.3 PPPoE Encapsulation

The Prestige supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPPoE** option is for a dial-up connection using PPPoE.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example Radius). PPPoE provides a login and authentication method that the existing Microsoft Dial-Up Networking software can activate, and therefore requires no new learning or procedures for Windows users.

One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the Prestige (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the Prestige does that part of the task. Furthermore, with NAT, all of the LANs' computers will have access.

9.4 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.

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.

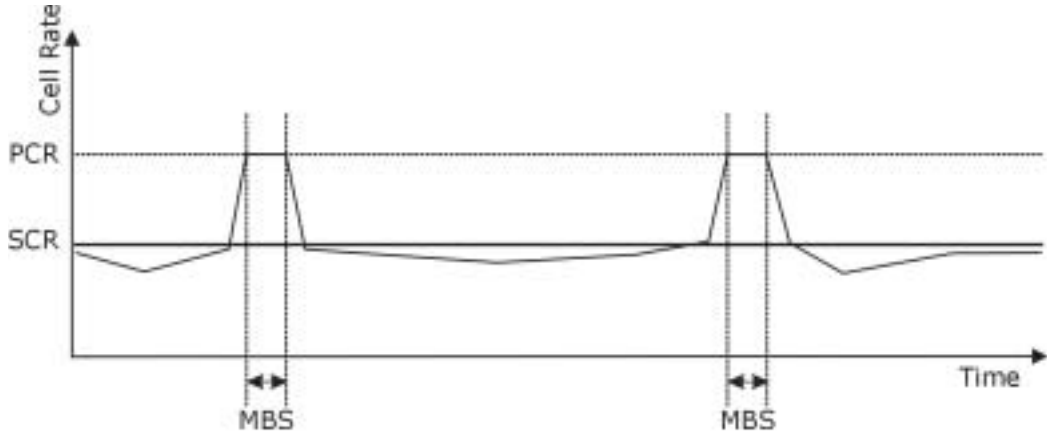
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

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.

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 37 Example of Traffic Shaping



9.5 Zero Configuration Internet Access

Once you turn on and connect the Prestige to a telephone jack, it automatically detects the Internet connection settings (such as the VCI/VPI numbers and the encapsulation method) from the ISP and makes the necessary configuration changes. In cases where additional account information (such as an Internet account user name and password) is required or the Prestige cannot connect to the ISP, you will be redirected to web screen(s) for information input or troubleshooting.

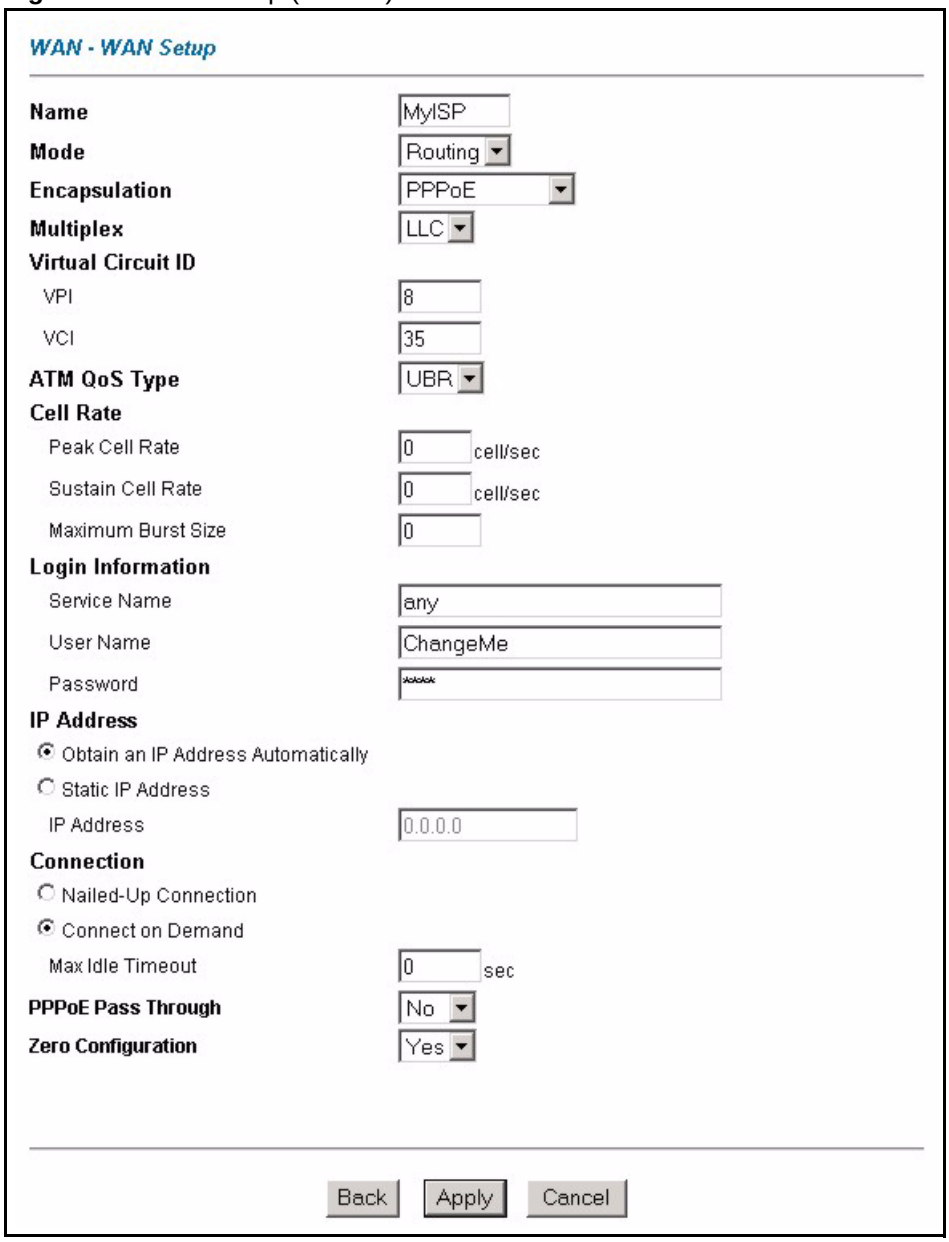
Zero configuration for Internet access is disable when

- the Prestige is in bridge mode
- you set the Prestige to use a static (fixed) WAN IP address.

9.6 Configuring WAN Setup

To change your Prestige's WAN remote node settings, click **WAN** and **WAN Setup**. The screen differs by the encapsulation.

Figure 38 WAN Setup (PPPoE)



The following table describes the fields in this screen.

Table 26 WAN Setup

LABEL	DESCRIPTION
Name	Enter the name of your Internet Service Provider, e.g., MyISP. This information is for identification purposes only.
Mode	Select **Routing** (default) from the drop-down list box if your ISP allows multiple computers to share an Internet account. Otherwise select **Bridge**.

Table 26 WAN Setup (continued)

LABEL	DESCRIPTION
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. Choices vary depending on the mode you select in the **Mode** field. If you select **Bridge** in the **Mode** field, select either **PPPoA** or **RFC 1483**. If you select **Routing** in the **Mode** field, select **PPPoA**, **RFC 1483**, **ENET ENCAP** or **PPPoE**.
Multiplex	Select the method of multiplexing used by your ISP from the drop-down list. Choices are **VC** or **LLC**.
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information.
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
ATM QoS Type	Select **CBR** (Continuous 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** (Variable Bit Rate) for bursty traffic and bandwidth sharing with other applications.
Cell Rate	Cell rate configuration often helps eliminate traffic congestion that slows transmission of real time data such as audio and video connections.
Peak Cell Rate	Divide the DSL line rate (bps) by 424 (the size of an ATM cell) to find the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells. Type the PCR here.
Sustain Cell Rate	The Sustain Cell Rate (SCR) sets the average cell rate (long-term) that can be transmitted. Type the SCR, which must be less than the PCR. Note that system default is 0 cells/sec.
Maximum Burst Size	Maximum Burst Size (MBS) refers to the maximum number of cells that can be sent at the peak rate. Type the MBS, which is less than 65535.
Login Information	(PPPoA and PPPoE encapsulation only)
Service Name	(PPPoE only) Type the name of your PPPoE service here.
User Name	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the user name above.
IP Address	This option is available if you select **Routing** in the **Mode** field. A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select **Obtain an IP Address Automatically** if you have a dynamic IP address; otherwise select **Static IP Address** and type your ISP assigned IP address in the **IP Address** field below.
Connection (PPPoA and PPPoE encapsulation only)	The schedule rule(s) in SMT menu 26 have priority over your **Connection** settings.
Nailed-Up Connection	Select **Nailed-Up Connection** when you want your connection up all the time. The Prestige will try to bring up the connection automatically if it is disconnected.

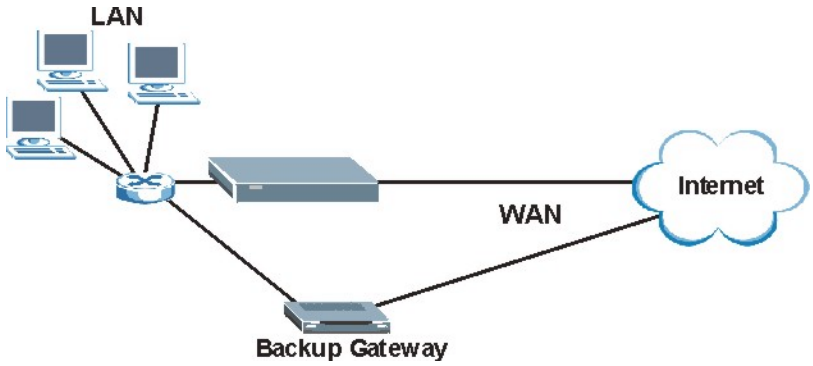
Table 26 WAN Setup (continued)

LABEL	DESCRIPTION
Connect on Demand	Select **Connect on Demand** when you don't want the connection up all the time and specify an idle time-out in the **Max Idle Timeout** field.
Max Idle Timeout	Specify an idle time-out in the **Max Idle Timeout** field when you select **Connect on Demand**. The default setting is 0, which means the Internet session will not timeout.
PPPoE Passthrough (PPPoE encapsulation only)	This field is available when you select **PPPoE** encapsulation. In addition to the Prestige's built-in PPPoE client, you can enable PPPoE pass through to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the Prestige. Each host can have a separate account and a public WAN IP address. PPPoE pass through is an alternative to NAT for application where NAT is not appropriate. Disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.
Subnet Mask (ENET ENCAP encapsulation only)	Enter a subnet mask in dotted decimal notation. Refer to the IP Subnetting appendix in the to calculate a subnet mask If you are implementing subnetting.
ENET ENCAP Gateway (ENET ENCAP encapsulation only)	You must specify a gateway IP address (supplied by your ISP) when you select **ENET ENCAP** in the **Encapsulation** field
Zero Configuration	This feature is not applicable/available when you configure the Prestige to use a static WAN IP address or in bridge mode. Select **Yes** to set the Prestige to automatically detect the Internet connection settings (such as the VCI/VPI numbers and the encapsulation method) from the ISP and make the necessary configuration changes. Select **No** to disable this feature. You must manually configure the Prestige for Internet access.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

9.7 Traffic Redirect

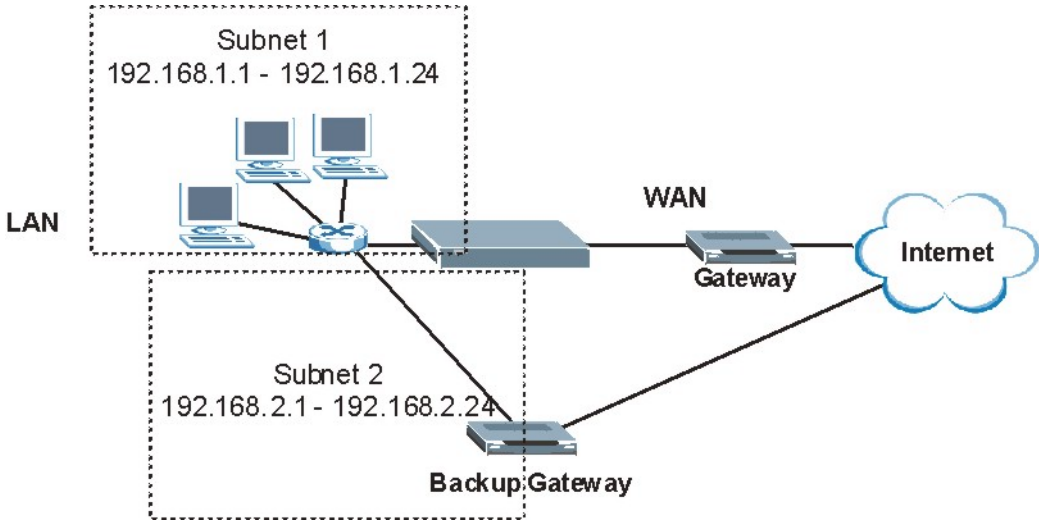
Traffic redirect forwards traffic to a backup gateway when the Prestige cannot connect to the Internet. An example is shown in the figure below.

Figure 39 Traffic Redirect Example



The following network topology allows you to avoid triangle route security issues when the backup gateway is connected to the LAN. Use IP alias to configure the LAN into two or three logical networks with the Prestige itself as the gateway for each LAN network. Put the protected LAN in one subnet (Subnet 1 in the following figure) and the backup gateway in another subnet (Subnet 2). Configure filters that allow packets from the protected LAN (Subnet 1) to the backup gateway (Subnet 2).

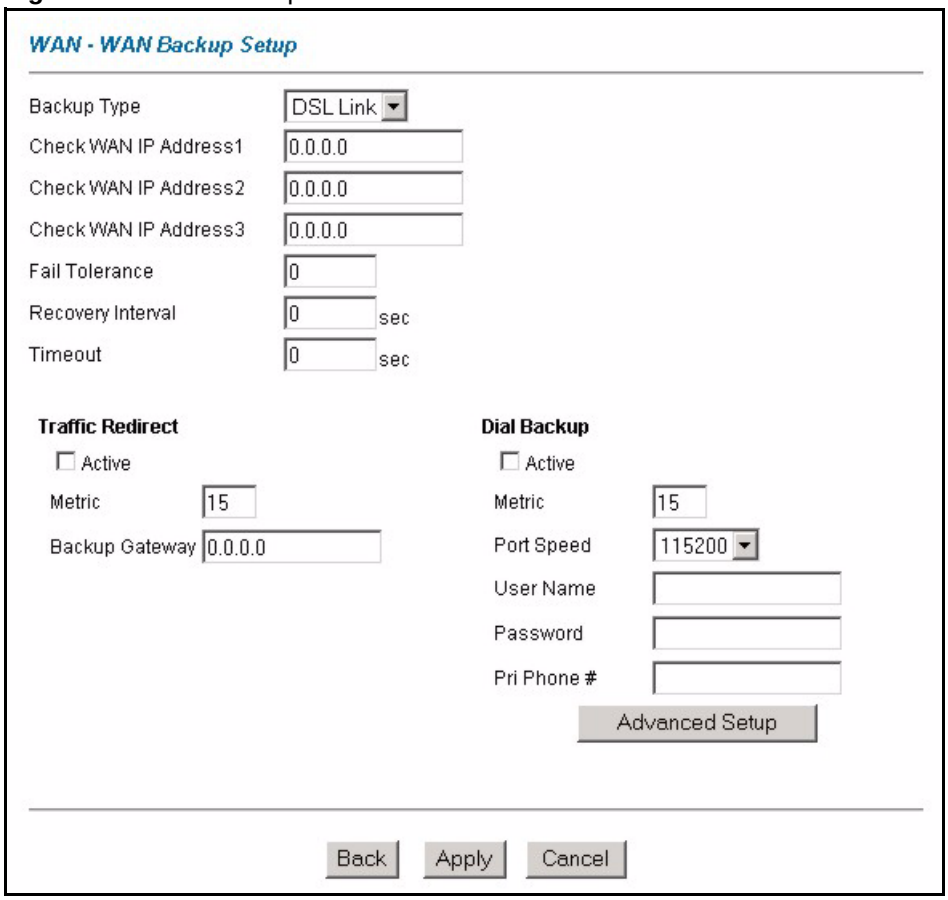
Figure 40 Traffic Redirect LAN Setup



9.8 Configuring WAN Backup

To change your Prestige's WAN backup settings, click **WAN**, then **WAN Backup**. The screen appears as shown.

Figure 41 WAN Backup



The following table describes the fields in this screen.

Table 27 WAN Backup

LABEL	DESCRIPTION
Backup Type	Select the method that the Prestige uses to check the DSL connection. Select **DSL Link** to have the Prestige check if the connection to the DSLAM is up. Select **ICMP** to have the Prestige periodically ping the IP addresses configured in the **Check WAN IP Address** fields.
Check WAN IP Address1-3	Configure this field to test your Prestige's WAN accessibility. Type the IP address of a reliable nearby computer (for example, your ISP's DNS server address). **Note:** If you activate either traffic redirect or dial backup, you must configure at least one IP address here. When using a WAN backup connection, the Prestige periodically pings the addresses configured here and uses the other WAN backup connection (if configured) if there is no response.
Fail Tolerance	Type the number of times (2 recommended) that your Prestige may ping the IP addresses configured in the **Check WAN IP Address** field without getting a response before switching to a WAN backup connection (or a different WAN backup connection).

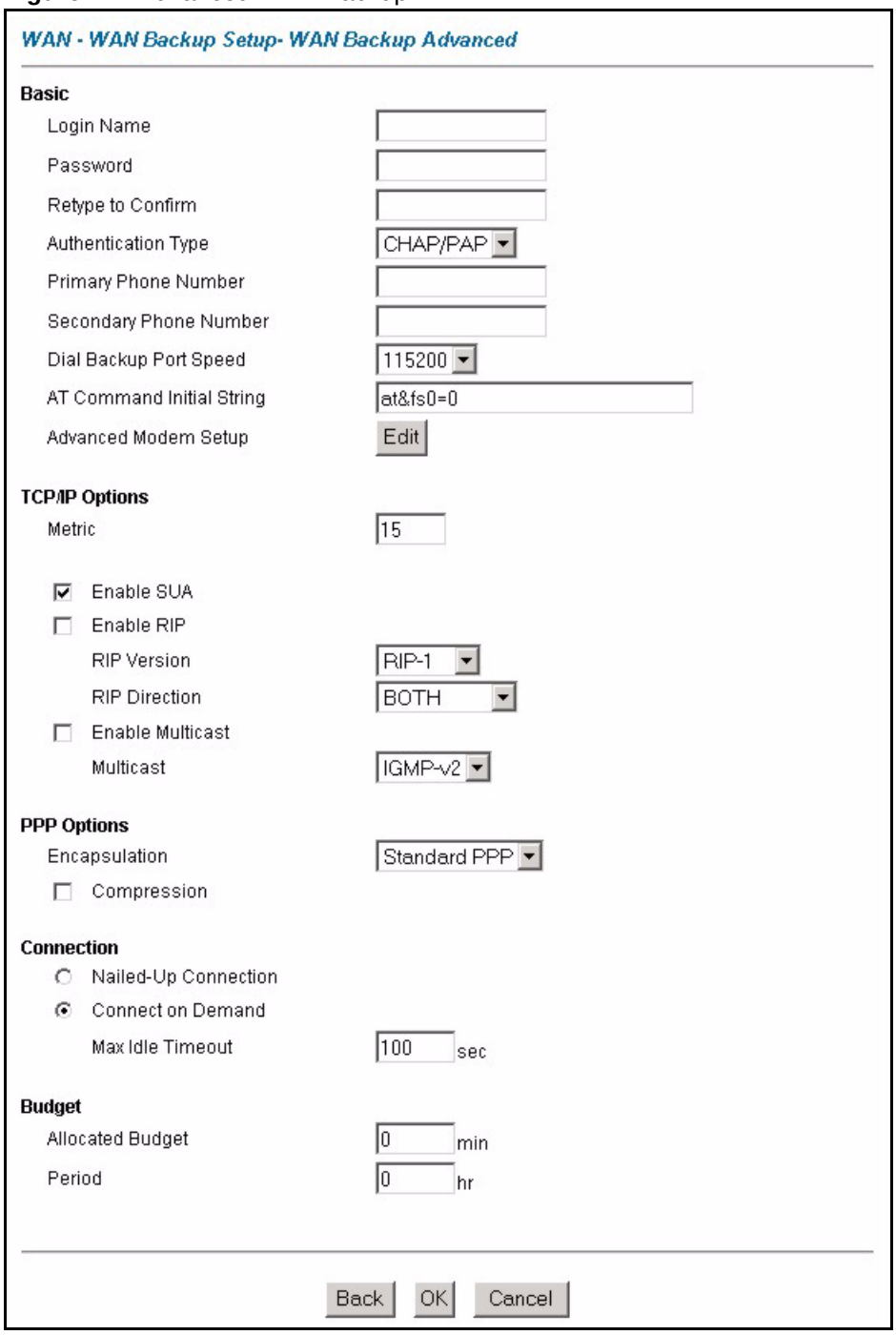
Table 27 WAN Backup (continued)

LABEL	DESCRIPTION
Recovery Interval	When the Prestige is using a lower priority connection (usually a WAN backup connection), it periodically checks to whether or not it can use a higher priority connection. Type the number of seconds (30 recommended) for the Prestige to wait between checks. Allow more time if your destination IP address handles lots of traffic.
Timeout	Type the number of seconds (3 recommended) for your Prestige to wait for a ping response from one of the IP addresses in the **Check WAN IP Address** field before timing out the request. The WAN connection is considered "down" after the Prestige times out the number of times specified in the **Fail Tolerance** field. Use a higher value in this field if your network is busy or congested.
Traffic Redirect	
Active	Select this check box to have the Prestige use traffic redirect if the normal WAN connection goes down. **Note:** If you activate traffic redirect, you must configure at least one Check WAN IP Address.
Metric	This field sets this route's priority among the routes the Prestige uses. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".
Backup Gateway	Type the IP address of your backup gateway in dotted decimal notation. The Prestige automatically forwards traffic to this IP address if the Prestige's Internet connection terminates.
Dial Backup	
Active	Select this check box to turn on dial backup. **Note:** If you activate traffic redirect, you must configure at least one Check WAN IP Address.
Metric	This field sets this route's priority among the three routes the Prestige uses (normal, traffic redirect and dial backup). Type a number (1 to 15) to set the priority of the dial backup route for data transmission. The smaller the number, the higher the priority. If the three routes have the same metrics, the priority of the routes is as follows: **WAN**, **Traffic Redirect**, **Dial Backup**.
Port Speed	Use the drop-down list box to select the speed of the connection between the dial backup port and the external device. Available speeds are: **9600**, **19200**, **38400**, **57600**, **115200** or **230400** bps.
User Name	Type the login name assigned by your ISP.
Password	Type the password assigned by your ISP.
Pri Phone #	Type the first (primary) phone number from the ISP for this remote node. Some areas require dialing the pound sign # before the phone number for local calls. Include a # symbol at the beginning of the phone numbers as required.
Advanced Setup	Click this button to display the **Advanced Setup** screen and edit more details of your WAN backup setup.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

9.9 Configuring Advanced WAN Backup

To edit your Prestige's advanced WAN backup settings, click **WAN**, **WAN Backup** and then the **Advanced Setup** button. The screen appears as shown.

Figure 42 Advanced WAN Backup



The following table describes the fields in this screen.

Table 28 Advanced WAN Backup

LABEL	DESCRIPTION
Basic	
Login Name	Type the login name assigned by your ISP.
Password	Type the password assigned by your ISP.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Authentication Type	Use the drop-down list box to select an authentication protocol for outgoing calls. Options are: **CHAP/PAP** - Your Prestige accepts either CHAP or PAP when requested by this remote node. **CHAP** - Your Prestige accepts CHAP only. **PAP** - Your Prestige accept PAP only.
Primary/ Secondary Phone Number	Type the first (primary) phone number from the ISP for this remote node. If the primary phone number is busy or does not answer, your Prestige dials the secondary phone number if available. Some areas require dialing the pound sign # before the phone number for local calls. Include a # symbol at the beginning of the phone numbers as required.
Dial Backup Port Speed	Use the drop-down list box to select the speed of the connection between the dial backup port and the external device. Available speeds are: **9600**, **19200**, **38400**, **57600**, **115200** or **230400** bps.
AT Command Initial String	Type the AT command string to initialize the WAN device. Consult the manual of your WAN device connected to your dial backup port for specific AT commands.
Advanced Modem Setup	Click the **Edit** button to display the **Advanced Modem Setup** screen and edit the details of your dial backup setup.
TCP/IP Options	
Metric	This field sets this route's priority among the three routes the Prestige uses (normal, traffic redirect and dial backup). Type a number (1 to 15) to set the priority of the dial backup route for data transmission. The smaller the number, the higher the priority. If the three routes have the same metrics, the priority of the routes is as follows: **WAN**, **Traffic Redirect**, **Dial Backup**.
Enable SUA	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network to a different IP address known within another network. SUA (Single User Account) is a subset of NAT that supports two types of mapping: Many-to-One and Server. When you select this option the Prestige will use Address Mapping Set 255 in the SMT (see Figure 185).
Enable RIP	Select this check box to turn on RIP (Routing Information Protocol), which allows a router to exchange routing information with other routers.

Table 28 Advanced WAN Backup (continued)

LABEL	DESCRIPTION
RIP Version	The **RIP Version** field controls the format and the broadcasting method of the RIP packets that the Prestige sends (it recognizes both formats when receiving). Choose **RIP-1**, **RIP-2B** or **RIP-2M**. **RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.
RIP Direction	RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. Choose **Both**, **In Only** or **Out Only**. When set to **Both** or **Out Only**, the Prestige will broadcast its routing table periodically. When set to **Both** or **In Only**, the Prestige will incorporate RIP information that it receives.
Enable Multicast	Select this check box to turn on IGMP (Internet Group Multicast Protocol). IGMP is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data.
Multicast	Select **IGMP-v1** or **IGMP-v2**. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see *sections 4* and *5* of *RFC 2236*.
PPP Options	
Encapsulation	Select **CISCO PPP** from the drop-down list box if your backup WAN device uses **Cisco PPP** encapsulation; otherwise select **Standard PPP**.
Compression	Select this check box to enable compression.
Connection	
Nailed-Up Connection	Select **Nailed-Up Connection** when you want your connection up all the time. The Prestige will try to bring up the connection automatically if it is disconnected.
Connect on Demand	Select **Connect on Demand** when you don't want the connection up all the time and specify an idle time-out in the **Max Idle Timeout** field.
Max Idle Timeout	Specify an idle time-out in the **Max Idle Timeout** field when you select **Connect on Demand**. The default setting is 0, which means the Internet session will not timeout.
Budget	The configuration in the **Budget** fields has priority over your **Connection** settings.
Allocate Budget	Type the amount of time (in minutes) that the dial backup connection can be used during the time configured in the **Period** field. Set an amount that is less than the time period configured in the **Period** field. If you set the **Allocated Budget** to 0, you will not be able to use the dial backup connection.
Period	Type the time period (in hours) for how often the budget should be reset. For example, to allow calls to this remote node for a maximum of 10 minutes every hour, set the **Allocated Budget** to 10 (minutes) and the **Period** to 1 (hour). If you set the **Period** to 0, there is no budget control and the Prestige uses the **Connection** settings.

Table 28 Advanced WAN Backup (continued)

LABEL	DESCRIPTION
Back	Click **Back** to return to the previous screen.
OK	Click **OK** to return to the previous screen, then click **Apply** to save the changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

9.10 AT Command Strings

For regular telephone lines, the default "Dial" string tells the modem that the line uses tone dialing. "ATDT" is the command for a switch that requires tone dialing. If your switch requires pulse dialing, change the string to "ATDP".

For ISDN lines, there are many more protocols and operational modes. Please consult the documentation of your TA. You may need additional commands in both "Dial" and "Init" strings.

9.11 DTR Signal

The majority of WAN devices default to hanging up the current call when the DTR (Data Terminal Ready) signal is dropped by the DTE. When the "Drop DTR When Hang Up" check box is selected, the Prestige uses this hardware signal to force the WAN device to hang up, in addition to issuing the drop command "ATH".

9.12 Response Strings

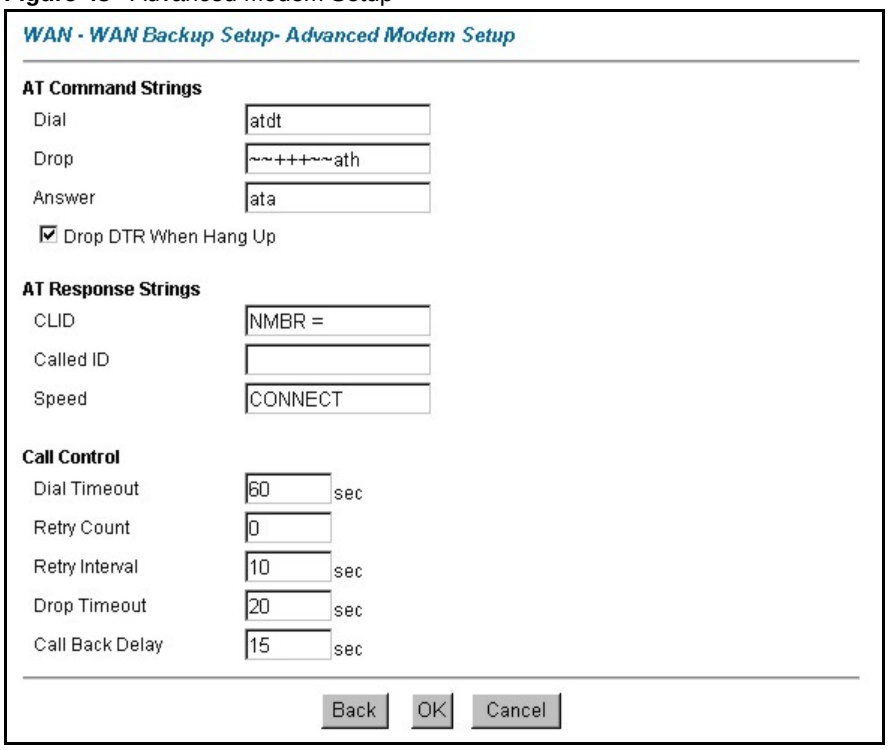
The response strings tell the Prestige the tags, or labels, immediately preceding the various call parameters sent from the WAN device. The response strings have not been standardized; please consult the documentation of your WAN device to find the correct tags.

9.13 Configuring Advanced Modem Setup

To configure settings for your backup WAN modem, click **WAN**, **WAN Backup** and then the **Advanced Setup** button. The **Advanced Setup** screen displays, click the **Edit** button to open the **Advanced Modem Setup** screen as shown next.

Note: Consult the manual of your WAN device connected to your dial backup port for specific AT commands.

Figure 43 Advanced Modem Setup



The following table describes the fields in this screen.

Table 29 Advanced Modem Setup

LABEL	DESCRIPTION
AT Command Strings	
Dial	Type the AT Command string to make a call. Example: atdt
Drop	Type the AT Command string to drop a call. "~" represents a one second wait, for example, "~~+++~~ath" can be used if your modem has a slow response time.
Answer	Type the AT Command string to answer a call. Example: ata
Drop DTR When Hang Up	Select this check box to have the Prestige drop the DTR (Data Terminal Ready) signal after the "AT Command String: Drop" is sent out.
AT Response Strings	
CLID	Type the keyword that precedes the CLID (Calling Line Identification) in the AT response string. This lets the Prestige capture the CLID in the AT response string that comes from the WAN device. CLID is required for CLID authentication. Example: NMBR
Called ID	Type the keyword preceding the dialed number.
Speed	Type the keyword preceding the connection speed. Example: CONNECT
Call Control	
Dial Timeout	Type a number of seconds for the Prestige to try to set up an outgoing call before timing out (stopping). Example: 60
Retry Count	Type a number of times for the Prestige to retry a busy or no-answer phone number before blacklisting the number. Example: 0

Table 29 Advanced Modem Setup (continued)

LABEL	DESCRIPTION
Retry Interval	Type a number of seconds for the Prestige to wait before trying another call after a call has failed. This applies before a phone number is blacklisted. Example: 10
Drop Timeout	Type the number of seconds for the Prestige to wait before dropping the DTR signal if it does not receive a positive disconnect confirmation. Example: 20
Call Back Delay	Type a number of seconds for the Prestige to wait between dropping a callback request call and dialing the corresponding callback call. Example: 15
Back	Click **Back** to return to the previous screen.
OK	Click **OK** to return to the previous screen, then click **OK** to return to the next previous screen and click **Apply** to save the changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

CHAPTER 10
Network Address Translation (NAT) Screens

This chapter discusses how to configure NAT on the Prestige.

10.1 NAT Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network.

10.1.1 NAT Definitions

Inside/outside denotes where a host is located relative to the Prestige, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 30 NAT Definitions

ITEM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

NAT never changes the IP address (either local or global) of an outside host.

10.1.2 What NAT Does

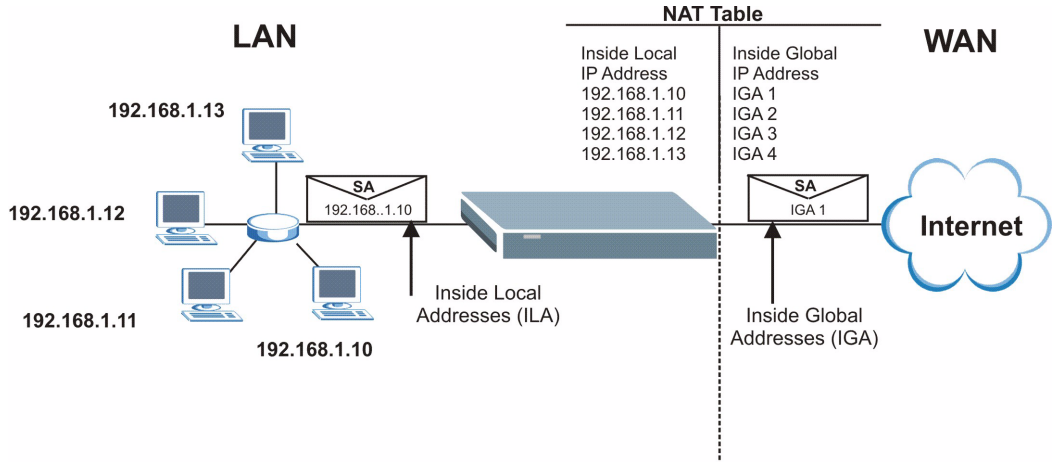
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping – see *Table 31*), NAT offers the additional benefit of firewall protection. With no servers defined, your Prestige filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631, The IP Network Address Translator (NAT)*.

10.1.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The Prestige keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored. The following figure illustrates this.

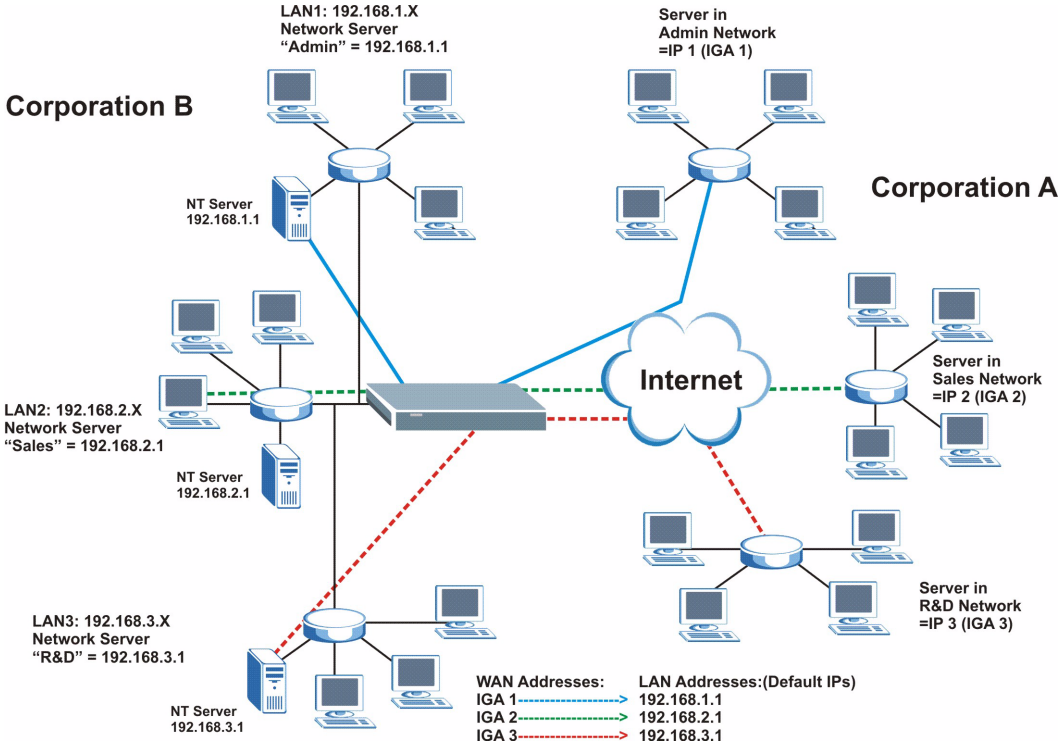
Figure 44 How NAT Works



10.1.4 NAT Application

The following figure illustrates a possible NAT application, where three inside LANs (logical LANs using IP Alias) behind the Prestige can communicate with three distinct WAN networks. More examples follow at the end of this chapter.

Figure 45 NAT Application With IP Alias



10.1.5 NAT Mapping Types

NAT supports five types of IP/port mapping. They are:

- **One to One**: In One-to-One mode, the Prestige maps one local IP address to one global IP address.
- **Many to One**: In Many-to-One mode, the Prestige maps multiple local IP addresses to one global IP address. This is equivalent to SUA (for instance, PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported (the **SUA Only** option in today's routers).
- **Many to Many Overload**: In Many-to-Many Overload mode, the Prestige maps the multiple local IP addresses to shared global IP addresses.
- **Many-to-Many No Overload**: In Many-to-Many No Overload mode, the Prestige maps each local IP address to a unique global IP address.
- **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.

Port numbers do **not** change for **One-to-One** and **Many-to-Many No Overload** NAT mapping types.

The following table summarizes these types.

Table 31 NAT Mapping Types

TYPE	IP MAPPING	SMT ABBREVIATION
One-to-One	ILA1←→ IGA1	1:1
Many-to-One (SUA/PAT)	ILA1←→ IGA1 ILA2←→ IGA1 …	M:1
Many-to-Many Overload	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA1 ILA4←→ IGA2 …	M:M Ov
Many-to-Many No Overload	ILA1←→ IGA1 ILA2←→ IGA2 ILA3←→ IGA3 …	M:M No OV
Server	Server 1 IP←→ IGA1 Server 2 IP←→ IGA1 Server 3 IP←→ IGA1	Server

10.2 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. The Prestige also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types as outlined in *Table 31* .

- Choose **SUA Only** if you have just one public WAN IP address for your Prestige.

- Choose **Full Feature** if you have multiple public WAN IP addresses for your Prestige.

10.3 SUA Server

A SUA server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though SUA makes your whole inside network appear as a single computer to the outside world.

You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

10.3.1 Default Server IP Address

In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in this screen.

If you do not assign an IP address in **Server Set 1** (default server) the Prestige discards all packets received for ports that are not specified here or in the remote management setup.

10.3.2 Port Forwarding: Services and Port Numbers

The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers.

Table 32 Services and Port Numbers

SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161

Table 32 Services and Port Numbers (continued)

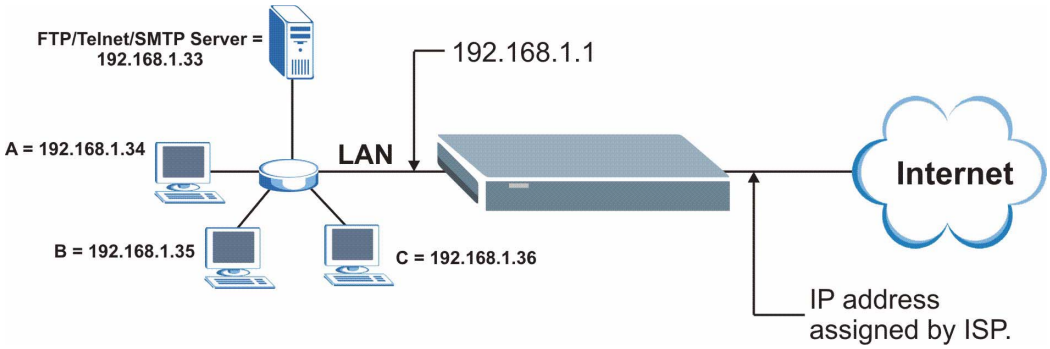
SERVICES	PORT NUMBER
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

10.3.3 Configuring Servers Behind SUA (Example)

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (A in the example), port 80 to another (B in the example) and assign a default server IP address of 192.168.1.35 to a third (C in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

IP address assigned by ISP.

Figure 46 Multiple Servers Behind NAT Example

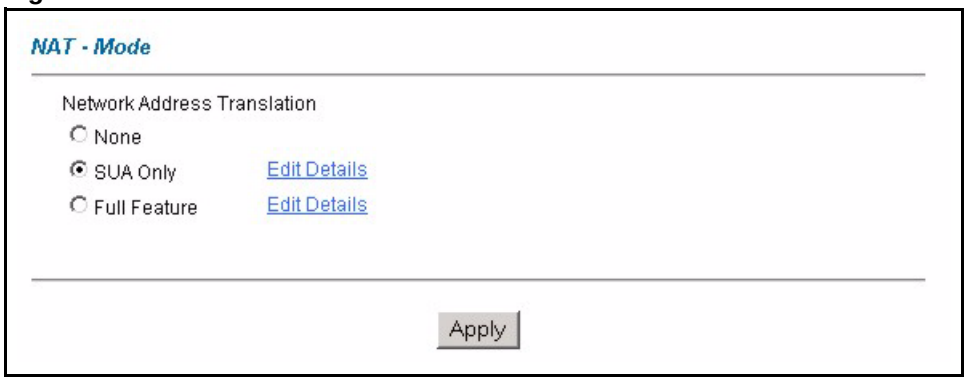


10.4 Selecting the NAT Mode

You must create a firewall rule in addition to setting up SUA/NAT, to allow traffic from the WAN to be forwarded through the Prestige.

Click **NAT** to open the following screen.

Figure 47 NAT Mode



The following table describes the labels in this screen.

Table 33 NAT Mode

LABEL	DESCRIPTION
None	Select this radio button to disable NAT.
SUA Only	Select this radio button if you have just one public WAN IP address for your Prestige. The Prestige uses Address Mapping Set 1 in the **NAT - Edit SUA/NAT Server Set** screen.
Edit Details	Click this link to go to the **NAT - Edit SUA/NAT Server Set** screen.
Full Feature	Select this radio button if you have multiple public WAN IP addresses for your Prestige.
Edit Details	Click this link to go to the **NAT - Address Mapping Rules** screen.
Apply	Click **Apply** to save your configuration.

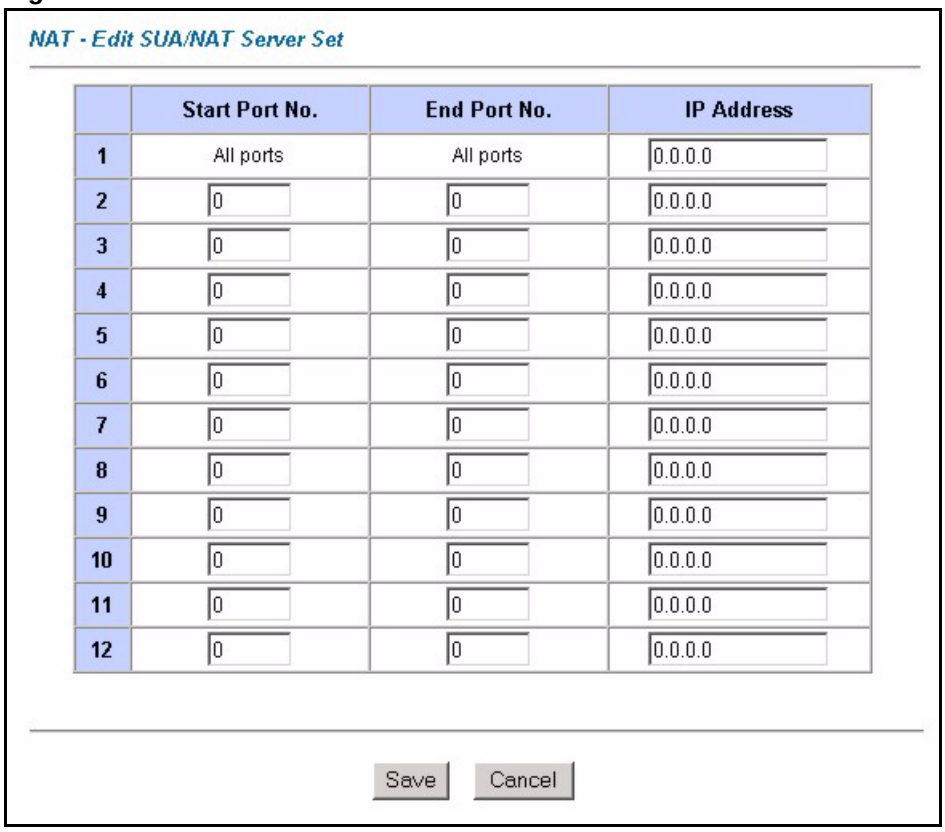
10.5 Configuring SUA Server

If you do not assign an IP address in **Server Set 1** (default server) the Prestige discards all packets received for ports that are not specified here or in the remote management setup.

Click **NAT**, select **SUA Only** and click **Edit Details** to open the following screen.

Refer to Table 32 for port numbers commonly used for particular services.

Figure 48 Edit SUA/NAT Server Set



The following table describes the fields in this screen.

Table 34 Edit SUA/NAT Server Set

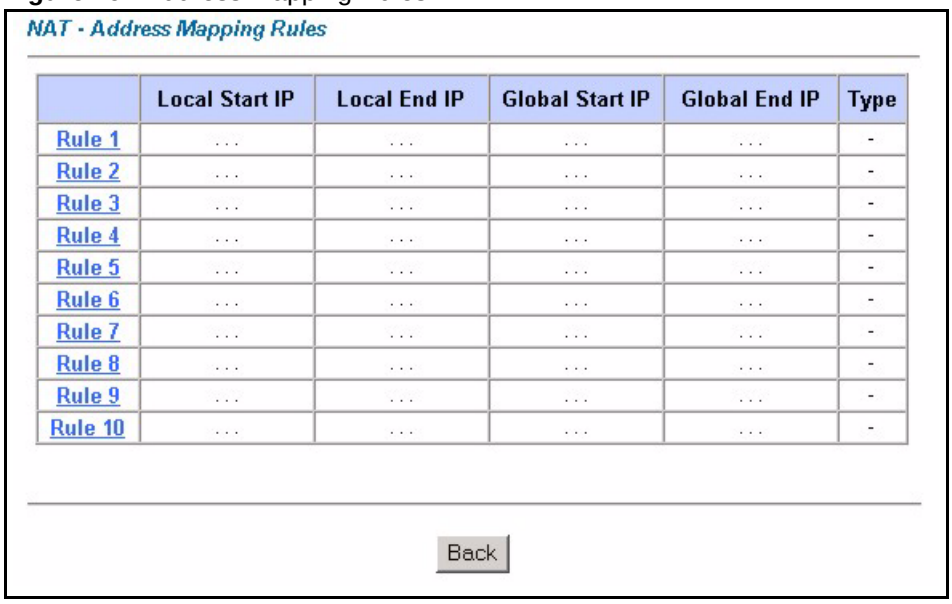
LABEL	DESCRIPTION
Start Port No.	Enter a port number in this field. To forward only one port, enter the port number again in the **End Port No.** field. To forward a series of ports, enter the start port number here and the end port number in the **End Port No.** field.
End Port No.	Enter a port number in this field. To forward only one port, enter the port number again in the **Start Port No.** field above and then enter it again in this field. To forward a series of ports, enter the last port number in a series that begins with the port number in the **Start Port No.** field above.
Server IP Address	Enter your server IP address in this field.
Save	Click **Save** to save your changes back to the Prestige.
Cancel	Click **Cancel** to return to the previous configuration.

10.6 Configuring Address Mapping

Ordering your rules is important because the Prestige applies the rules in the order that you specify. When a rule matches the current packet, the Prestige takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9. Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so old rules 5, 6 and 7 become new rules 4, 5 and 6.

To change your Prestige's address mapping settings, click **NAT**, Select **Full Feature** and click **Edit Details** to open the following screen.

Figure 49 Address Mapping Rules



The following table describes the fields in this screen.

Table 35 Address Mapping Rules

LABEL	DESCRIPTION
Local Start IP	This is the starting Inside Local IP Address (ILA). Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the **Local Start IP** address and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-one** and **Server** mapping types.
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP. You can only do this for **Many-to-One** and **Server** mapping types.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is **N/A** for **One-to-one**, **Many-to-One** and **Server** mapping types.

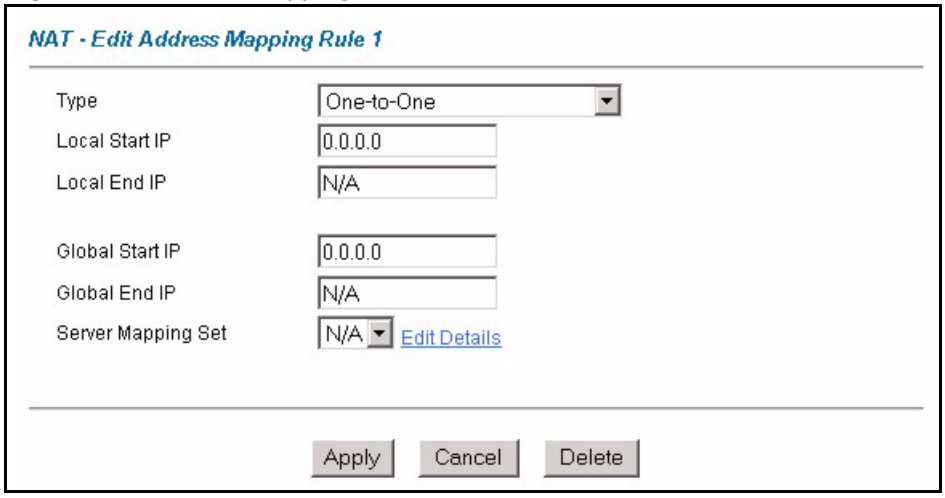
Table 35 Address Mapping Rules (continued)

LABEL	DESCRIPTION
Type	**1-1**: One-to-one mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type. **M-1**: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only. **M-M Ov** (Overload): Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. **MM No** (No Overload): Many-to-Many No Overload mode maps each local IP address to unique global IP addresses. **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Back	Click **Back** to return to the **NAT Mode** screen.

10.7 Editing an Address Mapping Rule

To edit an address mapping rule, click the rule's link in the **NAT Address Mapping Rules** screen to display the screen shown next.

Figure 50 Address Mapping Rule Edit



The following table describes the fields in this screen.

Table 36 Address Mapping Rule Edit

LABEL	DESCRIPTION
Type	Choose the port mapping type from one of the following. • **One-to-One**: One-to-One mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-one NAT mapping type. • **Many-to-One**: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only. • **Many-to-Many Overload**: Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. • **Many-to-Many No Overload**: Many-to-Many No Overload mode maps each local IP address to unique global IP addresses. • **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Local Start IP	This is the starting local IP address (ILA). Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end local IP address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the **Local Start IP** address and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-One** and **Server** mapping types.
Global Start IP	This is the starting global IP address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP.
Global End IP	This is the ending global IP address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types.
Server Mapping Set	Only available when **Type** is set to **Server**. Select a number from the drop-down menu to choose a server set from the **NAT - Address Mapping Rules** screen.
Edit Details	Click this link to go to the **NAT - Edit SUA/NAT Server Set** screen to edit a server set that you have selected in the **Server Mapping Set** field.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to return to the previously saved settings.
Delete	Click **Delete** to exit this screen without saving.

CHAPTER 11
Dynamic DNS Setup

This chapter discusses how to configure your Prestige to use Dynamic DNS.

11.1 Dynamic DNS

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a domain name. The Dynamic DNS service provider will give you a password or key.

11.1.1 DYNDNS Wildcard

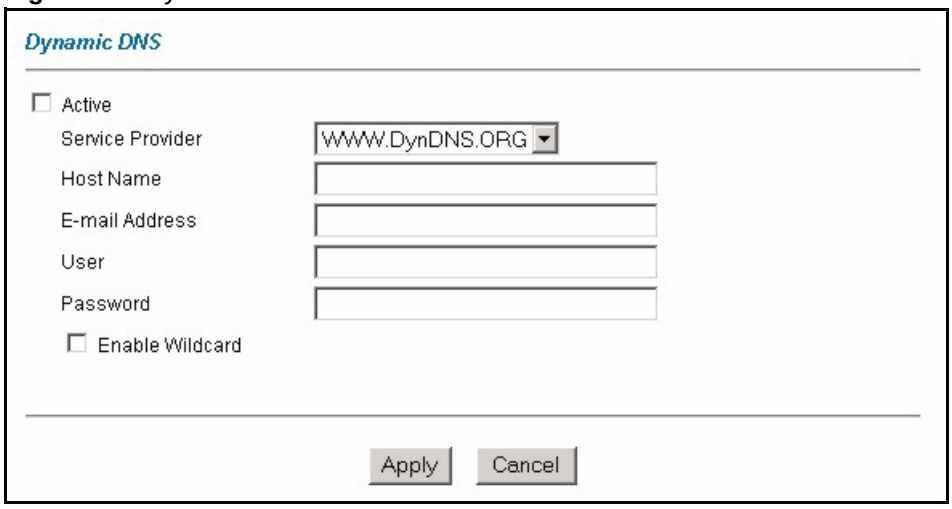
Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

If you have a private WAN IP address, then you cannot use Dynamic DNS.

11.2 Configuring Dynamic DNS

To change your Prestige's DDNS, click **Dynamic DNS**. The screen appears as shown.

Figure 51 Dynamic DNS



The following table describes the fields in this screen.

Table 37 Dynamic DNS

LABEL	DESCRIPTION
Active	Select this check box to use dynamic DNS.
Service Provider	This is the name of your Dynamic DNS service provider.
Host Names	Type the domain name assigned to your Prestige by your Dynamic DNS provider.
E-mail Address	Type your e-mail address.
User	Type your user name.
Password	Type the password assigned to you.
Enable Wildcard	Select the check box to enable DYNDNS Wildcard.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to begin configuring this screen afresh.

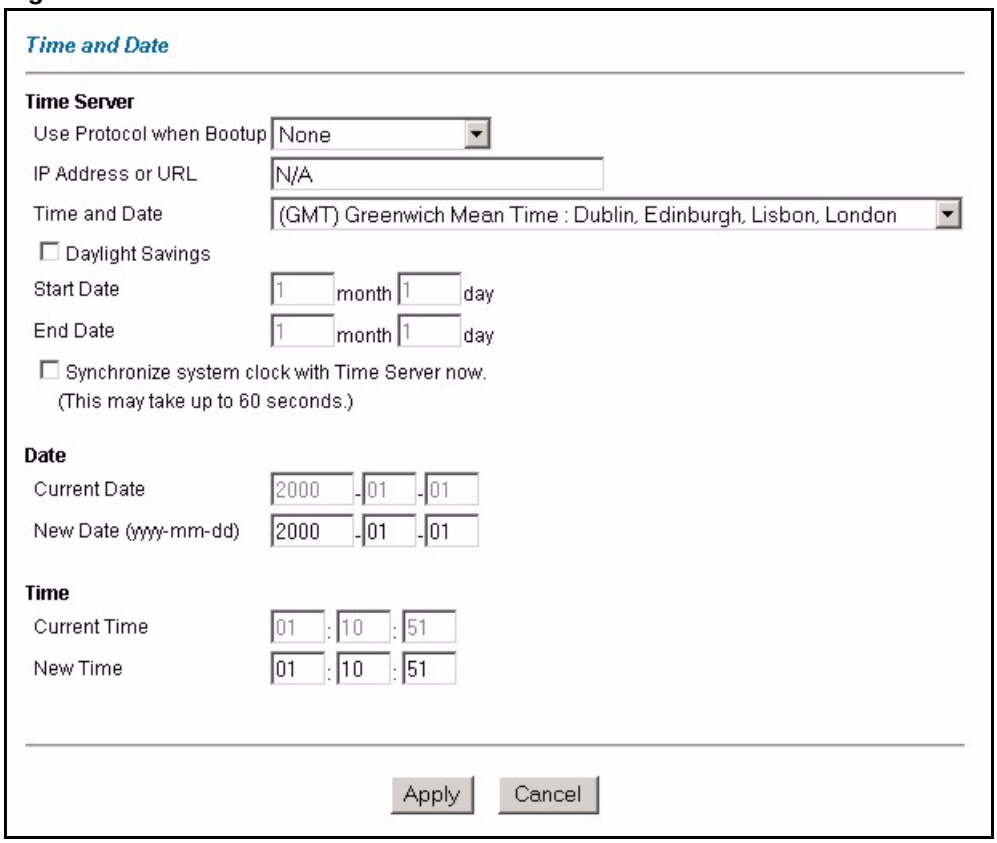
CHAPTER 12
Time and Date

This screen is not available on all models. Use this screen to configure the Prestige's time and date settings.

12.1 Configuring Time and Date

To change your Prestige's time and date, click **Time And Date**. The screen appears as shown. Use this screen to configure the Prestige's time based on your local time zone.

Figure 52 Time and Date



The following table describes the fields in this screen.

Table 38 Time and Date

LABEL	DESCRIPTION
Time Server	
Use Protocol when Bootup	Select the time service protocol that your time server sends when you turn on the Prestige. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main difference between them is the format. **Daytime (RFC 867)** format is day/month/year/time zone of the server. **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)**. Select **None** to enter the time and date manually.
IP Address or URL	Enter the IP address or URL of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time and Date	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Select this option if you use daylight savings time. Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
Start Date	Enter the month and day that your daylight-savings time starts on if you selected **Daylight Savings**.
End Date	Enter the month and day that your daylight-savings time ends on if you selected **Daylight Savings**.
Synchronize system clock with Time Server now.	Select this option to have your Prestige use the time server (that you configured above) to set its internal system clock. Please wait for up to 60 seconds while the Prestige locates the time server. If the Prestige cannot find the time server, please check the time server protocol and its IP address. If the IP address was entered correctly, try pinging it for example to test the connection.
Date	
Current Date	This field displays the date of your Prestige. Each time you reload this page, the Prestige synchronizes the time with the time server.
New Date (yyyy-mm-dd)	This field displays the last updated date from the time server. When you select **None** in the **Use Protocol when Bootup** field, enter the new date in this field and then click **Apply**.
Time	
Current Time	This field displays the time of your Prestige. Each time you reload this page, the Prestige synchronizes the time with the time server.
New Time	This field displays the last updated time from the time server. When you select **None** in the **Use Protocol when Bootup** field, enter the new time in this field and then click **Apply**.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to begin configuring this screen afresh.

CHAPTER 13
Firewalls

This chapter gives some background information on firewalls and introduces the Prestige firewall.

13.1 Firewall Overview

Originally, the term *firewall* referred to a construction technique designed to prevent the spread of fire from one room to another. The networking term "firewall" is a system or group of systems that enforces an access-control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from an untrusted network. Of course, firewalls cannot solve every security problem. A firewall is *one* of the mechanisms used to establish a network security perimeter in support of a network security policy. It should never be the *only* mechanism or method employed. For a firewall to guard effectively, you must design and deploy it appropriately. This requires integrating the firewall into a broad information-security policy. In addition, specific policies must be implemented within the firewall itself.

13.2 Types of Firewalls

There are three main types of firewalls:

- Packet Filtering Firewalls
- Application-level Firewalls
- Stateful Inspection Firewalls

13.2.1 Packet Filtering Firewalls

Packet filtering firewalls restrict access based on the source/destination computer network address of a packet and the type of application.

13.2.2 Application-level Firewalls

Application-level firewalls restrict access by serving as proxies for external servers. Since they use programs written for specific Internet services, such as HTTP, FTP and telnet, they can evaluate network packets for valid application-specific data. Application-level gateways have a number of general advantages over the default mode of permitting application traffic directly to internal hosts:

Information hiding prevents the names of internal systems from being made known via DNS to outside systems, since the application gateway is the only host whose name must be made known to outside systems.

Robust authentication and logging pre-authenticates application traffic before it reaches internal hosts and causes it to be logged more effectively than if it were logged with standard host logging. Filtering rules at the packet filtering router can be less complex than they would be if the router needed to filter application traffic and direct it to a number of specific systems. The router need only allow application traffic destined for the application gateway and reject the rest.

13.2.3 Stateful Inspection Firewalls

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also "inspect" the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency, however, they may lack the granular application level access control or caching that some proxies support. See theStateful Inspection section for more information on Stateful Inspection.

Firewalls, of one type or another, have become an integral part of standard security solutions for enterprises.

13.3 Introduction to ZyXEL's Firewall

The Prestige firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated (in SMT menu 21.2 or in the web configurator). The Prestige's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The Prestige can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network. The Prestige also has packet filtering capabilities.

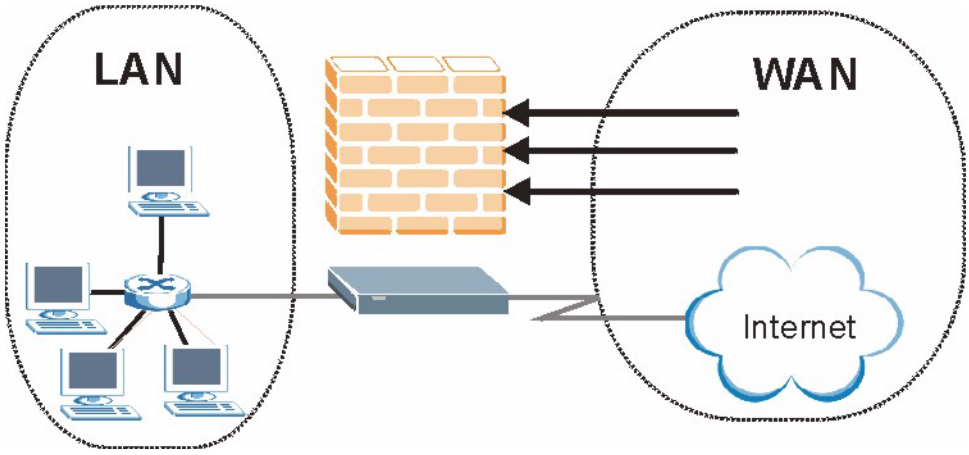
The Prestige is installed between the LAN and the Internet. This allows it to act as a secure gateway for all data passing between the Internet and the LAN.

The Prestige has one DSL/ISDN port and one Ethernet LAN port, which physically separate the network into two areas.

- The DSL/ISDN port connects to the Internet.
- The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP, and the World Wide Web. However, "inbound access" will not be allowed unless you configure remote management or create a firewall rule to allow a remote host to use a specific service.

13.3.1 Denial of Service Attacks

Figure 53 Prestige Firewall Application



13.4 Denial of Service

Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. The Prestige is pre-configured to automatically detect and thwart all known DoS attacks.

13.4.1 Basics

Computers share information over the Internet using a common language called TCP/IP. TCP/IP, in turn, is a set of application protocols that perform specific functions. An “extension number”, called the "TCP port" or "UDP port" identifies these protocols, such as HTTP (Web), FTP (File Transfer Protocol), POP3 (E-mail), etc. For example, Web traffic by default uses TCP port 80.

When computers communicate on the Internet, they are using the client/server model, where the server "listens" on a specific TCP/UDP port for information requests from remote client computers on the network. For example, a Web server typically listens on port 80. Please note that while a computer may be intended for use over a single port, such as Web on port 80, other ports are also active. If the person configuring or managing the computer is not careful, a hacker could attack it over an unprotected port.

Some of the most common IP ports are:

Table 39 Common IP Ports

21	FTP	53	DNS
23	Telnet	80	HTTP
25	SMTP	110	POP3

13.4.2 Types of DoS Attacks

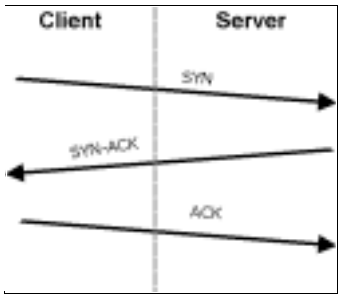
There are four types of DoS attacks:

1. Those that exploit bugs in a TCP/IP implementation.
2. Those that exploit weaknesses in the TCP/IP specification.
3. Brute-force attacks that flood a network with useless data.
4. IP Spoofing.
5. "**Ping of Death**" and "**Teardrop**" attacks exploit bugs in the TCP/IP implementations of various computer and host systems.

- Ping of Death uses a "ping" utility to create an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. The oversize packet is then sent to an unsuspecting system. Systems may crash, hang or reboot.
- Teardrop attack exploits weaknesses in the re-assembly of IP packet fragments. As data is transmitted through a network, IP packets are often broken up into smaller chunks. Each fragment looks like the original IP packet except that it contains an offset field that says, for instance, "This fragment is carrying bytes 200 through 400 of the original (non fragmented) IP packet." The Teardrop program creates a series of IP fragments with overlapping offset fields. When these fragments are reassembled at the destination, some systems will crash, hang, or reboot.

6. Weaknesses in the TCP/IP specification leave it open to "**SYN Flood**" and "**LAND**" attacks. These attacks are executed during the handshake that initiates a communication session between two applications.

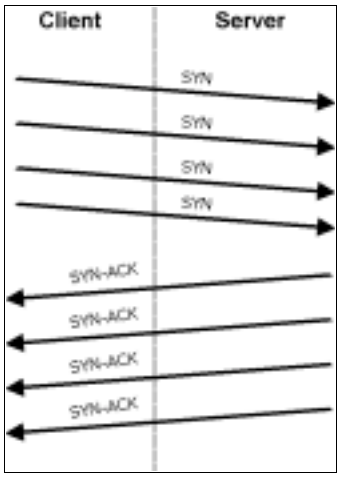
Figure 54 Three-Way Handshake



Under normal circumstances, the application that initiates a session sends a SYN (synchronize) packet to the receiving server. The receiver sends back an ACK (acknowledgment) packet and its own SYN, and then the initiator responds with an ACK (acknowledgment). After this handshake, a connection is established.

- **SYN Attack** floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on what is known as a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer (which is set at relatively long intervals) terminates the three-way handshake. Once the queue is full, the system will ignore all incoming SYN requests, making the system unavailable for legitimate users.

Figure 55 SYN Flood

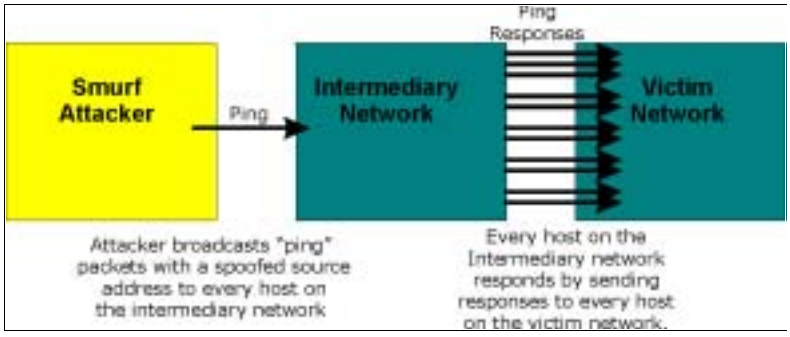


- In a **LAND Attack**, hackers flood SYN packets into the network with a spoofed source IP address of the targeted system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

7 A **brute-force** attack, such as a "Smurf" attack, targets a feature in the IP specification known as directed or subnet broadcasting, to quickly flood the target network with useless data. A Smurf hacker floods a router with Internet Control Message Protocol (ICMP) echo request packets (pings). Since the destination IP address of each packet is the broadcast address of the network, the router will broadcast the ICMP echo request packet to all hosts on the network. If there are numerous hosts, this will create a large

amount of ICMP echo request and response traffic. If a hacker chooses to spoof the source IP address of the ICMP echo request packet, the resulting ICMP traffic will not only clog up the "intermediary" network, but will also congest the network of the spoofed source IP address, known as the "victim" network. This flood of broadcast traffic consumes all available bandwidth, making communications impossible.

Figure 56 Smurf Attack



13.4.2.1 ICMP Vulnerability

ICMP is an error-reporting protocol that works in concert with IP. The following ICMP types trigger an alert:

Table 40 ICMP Commands That Trigger Alerts

5	REDIRECT
13	TIMESTAMP_REQUEST
14	TIMESTAMP_REPLY
17	ADDRESS_MASK_REQUEST
18	ADDRESS_MASK_REPLY

13.4.2.2 Illegal Commands (NetBIOS and SMTP)

The only legal NetBIOS commands are the following - all others are illegal.

Table 41 Legal NetBIOS Commands

MESSAGE:
REQUEST:
POSITIVE:
VE:
RETARGET:
KEEPALIVE:

All SMTP commands are illegal except for those displayed in the following tables.

Table 42 Legal SMTP Commands

AUTH	DATA	EHLO	ETRN	EXPN	HELO	HELP	MAIL	NOOP
QUIT	RCPT	RSET	SAML	SEND	SOML	TURN	VRFY	

13.4.2.3 Traceroute

Traceroute is a utility used to determine the path a packet takes between two endpoints. Sometimes when a packet filter firewall is configured incorrectly an attacker can traceroute the firewall gaining knowledge of the network topology inside the firewall.

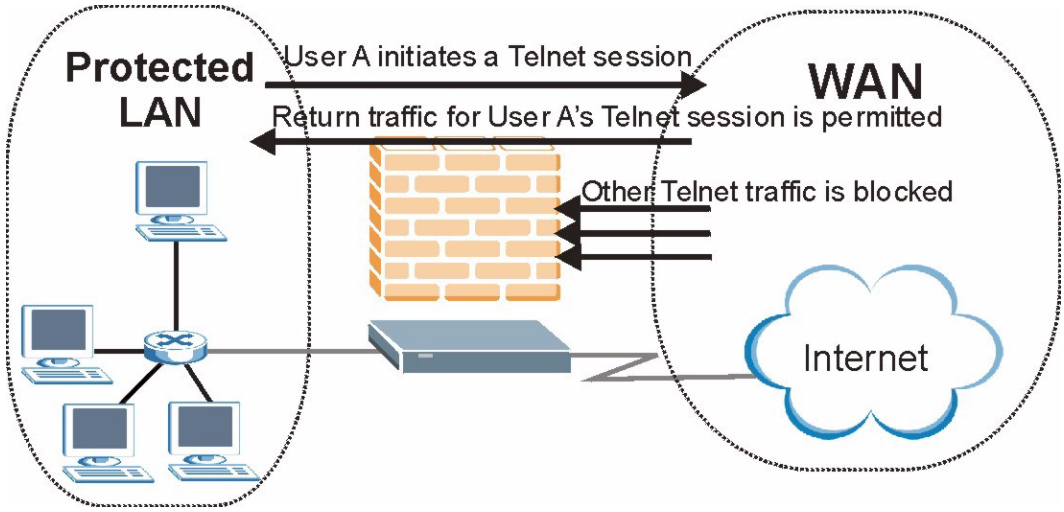
Often, many DoS attacks also employ a technique known as "**IP Spoofing**" as part of their attack. IP Spoofing may be used to break into systems, to hide the hacker's identity, or to magnify the effect of the DoS attack. IP Spoofing is a technique used to gain unauthorized access to computers by tricking a router or firewall into thinking that the communications are coming from within the trusted network. To engage in IP spoofing, a hacker must modify the packet headers so that it appears that the packets originate from a trusted host and should be allowed through the router or firewall. The Prestige blocks all IP Spoofing attempts.

13.5 Stateful Inspection

With stateful inspection, fields of the packets are compared to packets that are already known to be trusted. For example, if you access some outside service, the proxy server remembers things about your original request, like the port number and source and destination addresses. This "remembering" is called *saving the state*. When the outside system responds to your request, the firewall compares the received packets with the saved state to determine if they are allowed in. The Prestige uses stateful packet inspection to protect the private LAN from hackers and vandals on the Internet. By default, the Prestige's stateful inspection allows all communications to the Internet that originate from the LAN, and blocks all traffic to the LAN that originates from the Internet. In summary, stateful inspection:

- Allows all sessions originating from the LAN (local network) to the WAN (Internet).
- Denies all sessions originating from the WAN to the LAN.

Figure 57 Stateful Inspection



The previous figure shows the Prestige's default firewall rules in action as well as demonstrates how stateful inspection works. User A can initiate a Telnet session from within the LAN and responses to this request are allowed. However other Telnet traffic initiated from the WAN is blocked.

13.5.1 Stateful Inspection Process

In this example, the following sequence of events occurs when a TCP packet leaves the LAN network through the firewall's WAN interface. The TCP packet is the first in a session, and the packet's application layer protocol is configured for a firewall rule inspection:

1. The packet travels from the firewall's LAN to the WAN.
2. The packet is evaluated against the interface's existing outbound access list, and the packet is permitted (a denied packet would simply be dropped at this point).
3. The packet is inspected by a firewall rule to determine and record information about the state of the packet's connection. This information is recorded in a new state table entry created for the new connection. If there is not a firewall rule for this packet and it is not an attack, then the settings in the **Default Policy** screen determine the action for this packet.
4. Based on the obtained state information, a firewall rule creates a temporary access list entry that is inserted at the beginning of the WAN interface's inbound extended access list. This temporary access list entry is designed to permit inbound packets of the same connection as the outbound packet just inspected.
5. The outbound packet is forwarded out through the interface.
6. Later, an inbound packet reaches the interface. This packet is part of the connection previously established with the outbound packet. The inbound packet is evaluated against the inbound access list, and is permitted because of the temporary access list entry previously created.
7. The packet is inspected by a firewall rule, and the connection's state table entry is updated as necessary. Based on the updated state information, the inbound extended access list

temporary entries might be modified, in order to permit only packets that are valid for the current state of the connection.

8 Any additional inbound or outbound packets that belong to the connection are inspected to update the state table entry and to modify the temporary inbound access list entries as required, and are forwarded through the interface.

9 When the connection terminates or times out, the connection's state table entry is deleted and the connection's temporary inbound access list entries are deleted.

13.5.2 Stateful Inspection and the Prestige

Additional rules may be defined to extend or override the default rules. For example, a rule may be created which will:

- Block all traffic of a certain type, such as IRC (Internet Relay Chat), from the LAN to the Internet.
- Allow certain types of traffic from the Internet to specific hosts on the LAN.
- Allow access to a Web server to everyone but competitors.
- Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by evaluating the network traffic's Source IP address, Destination IP address, IP protocol type, and comparing these to rules set by the administrator.

Note: The ability to define firewall rules is a very powerful tool. Using custom rules, it is possible to disable all firewall protection or block all access to the Internet. Use extreme caution when creating or deleting firewall rules. Test changes after creating them to make sure they work correctly.

Below is a brief technical description of how these connections are tracked. Connections may either be defined by the upper protocols (for instance, TCP), or by the Prestige itself (as with the "virtual connections" created for UDP and ICMP).

13.5.3 TCP Security

The Prestige uses state information embedded in TCP packets. The first packet of any new connection has its SYN flag set and its ACK flag cleared; these are "initiation" packets. All packets that do not have this flag structure are called "subsequent" packets, since they represent data that occurs later in the TCP stream.

If an initiation packet originates on the WAN, this means that someone is trying to make a connection from the Internet into the LAN. Except in a few special cases (see "Upper Layer Protocols" shown next), these packets are dropped and logged.

If an initiation packet originates on the LAN, this means that someone is trying to make a connection from the LAN to the Internet. Assuming that this is an acceptable part of the security policy (as is the case with the default policy), the connection will be allowed. A cache entry is added which includes connection information such as IP addresses, TCP ports, sequence numbers, etc.

When the Prestige receives any subsequent packet (from the Internet or from the LAN), its connection information is extracted and checked against the cache. A packet is only allowed to pass through if it corresponds to a valid connection (that is, if it is a response to a connection which originated on the LAN).

13.5.4 UDP/ICMP Security

UDP and ICMP do not themselves contain any connection information (such as sequence numbers). However, at the very minimum, they contain an IP address pair (source and destination). UDP also contains port pairs, and ICMP has type and code information. All of this data can be analyzed in order to build "virtual connections" in the cache.

For instance, any UDP packet that originates on the LAN will create a cache entry. Its IP address and port pairs will be stored. For a short period of time, UDP packets from the WAN that have matching IP and UDP information will be allowed back in through the firewall.

A similar situation exists for ICMP, except that the Prestige is even more restrictive. Specifically, only outgoing echoes will allow incoming echo replies, outgoing address mask requests will allow incoming address mask replies, and outgoing timestamp requests will allow incoming timestamp replies. No other ICMP packets are allowed in through the firewall, simply because they are too dangerous and contain too little tracking information. For instance, ICMP redirect packets are never allowed in, since they could be used to reroute traffic through attacking machines.

13.5.5 Upper Layer Protocols

Some higher layer protocols (such as FTP and RealAudio) utilize multiple network connections simultaneously. In general terms, they usually have a "control connection" which is used for sending commands between endpoints, and then "data connections" which are used for transmitting bulk information.

Consider the FTP protocol. A user on the LAN opens a control connection to a server on the Internet and requests a file. At this point, the remote server will open a data connection from the Internet. For FTP to work properly, this connection must be allowed to pass through even though a connection from the Internet would normally be rejected.

In order to achieve this, the Prestige inspects the application-level FTP data. Specifically, it searches for outgoing "PORT" commands, and when it sees these, it adds a cache entry for the anticipated data connection. This can be done safely, since the PORT command contains address and port information, which can be used to uniquely identify the connection.

Any protocol that operates in this way must be supported on a case-by-case basis. You can use the web configurator's Custom Ports feature to do this.

13.6 Guidelines for Enhancing Security with Your Firewall

- Change the default password via SMT or web configurator.
- Limit who can telnet into your router.
- Don't enable any local service (such as SNMP or NTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.
- For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
- Protect against IP spoofing by making sure the firewall is active.
- Keep the firewall in a secured (locked) room.

13.6.1 Security In General

You can never be too careful! Factors outside your firewall, filtering or NAT can cause security breaches. Below are some generalizations about what you can do to minimize them.

- Encourage your company or organization to develop a comprehensive security plan. Good network administration takes into account what hackers can do and prepares against attacks. The best defense against hackers and crackers is information. Educate all employees about the importance of security and how to minimize risk. Produce lists like this one!
- DSL or cable modem connections are "always-on" connections and are particularly vulnerable because they provide more opportunities for hackers to crack your system. Turn your computer off when not in use.
- Never give out a password or any sensitive information to an unsolicited telephone call or e-mail.
- Never e-mail sensitive information such as passwords, credit card information, etc., without encrypting the information first.
- Never submit sensitive information via a web page unless the web site uses secure connections. You can identify a secure connection by looking for a small "key" icon on the bottom of your browser (Internet Explorer 3.02 or better or Netscape 3.0 or better). If a web site uses a secure connection, it is safe to submit information. Secure web transactions are quite difficult to crack.
- Never reveal your IP address or other system networking information to people outside your company. Be careful of files e-mailed to you from strangers. One common way of getting BackOrifice on a system is to include it as a Trojan horse with other files.
- Change your passwords regularly. Also, use passwords that are not easy to figure out. The most difficult passwords to crack are those with upper and lower case letters, numbers and a symbol such as % or #.

- Upgrade your software regularly. Many older versions of software, especially web browsers, have well known security deficiencies. When you upgrade to the latest versions, you get the latest patches and fixes.
- If you use "chat rooms" or IRC sessions, be careful with any information you reveal to strangers.
- If your system starts exhibiting odd behavior, contact your ISP. Some hackers will set off hacks that cause your system to slowly become unstable or unusable.
- Always shred confidential information, particularly about your computer, before throwing it away. Some hackers dig through the trash of companies or individuals for information that might help them in an attack.

13.7 Packet Filtering Vs Firewall

Below are some comparisons between the Prestige's filtering and firewall functions.

13.7.1 Packet Filtering:

- The router filters packets as they pass through the router's interface according to the filter rules you designed.
- Packet filtering is a powerful tool, yet can be complex to configure and maintain, especially if you need a chain of rules to filter a service.
- Packet filtering only checks the header portion of an IP packet.

13.7.1.1 When To Use Filtering

- To block/allow LAN packets by their MAC addresses.
- To block/allow special IP packets which are neither TCP nor UDP, nor ICMP packets.
- To block/allow both inbound (WAN to LAN) and outbound (LAN to WAN) traffic between the specific inside host/network "A" and outside host/network "B". If the filter blocks the traffic from A to B, it also blocks the traffic from B to A. Filters can not distinguish traffic originating from an inside host or an outside host by IP address.
- To block/allow IP trace route.

13.7.2 Firewall

- The firewall inspects packet contents as well as their source and destination addresses. Firewalls of this type employ an inspection module, applicable to all protocols, that understands data in the packet is intended for other layers, from the network layer (IP headers) up to the application layer.
- The firewall performs stateful inspection. It takes into account the state of connections it handles so that, for example, a legitimate incoming packet can be matched with the outbound request for that packet and allowed in. Conversely, an incoming packet masquerading as a response to a nonexistent outbound request can be blocked.
- The firewall uses session filtering, i.e., smart rules, that enhance the filtering process and control the network session rather than control individual packets in a session.

- The firewall provides e-mail service to notify you of routine reports and when alerts occur.

13.7.2.1 When To Use The Firewall

- To prevent DoS attacks and prevent hackers cracking your network.
- A range of source and destination IP addresses as well as port numbers can be specified within one firewall rule making the firewall a better choice when complex rules are required.
- To selectively block/allow inbound or outbound traffic between inside host/networks and outside host/networks. Remember that filters can not distinguish traffic originating from an inside host or an outside host by IP address.
- The firewall performs better than filtering if you need to check many rules.
- Use the firewall if you need routine e-mail reports about your system or need to be alerted when attacks occur.
- The firewall can block specific URL traffic that might occur in the future. The URL can be saved in an Access Control List (ACL) database.

CHAPTER 14
Firewall Configuration

This chapter shows you how to enable and configure the Prestige firewall.

14.1 Access Methods

The web configurator is, by far, the most comprehensive firewall configuration tool your Prestige has to offer. For this reason, it is recommended that you configure your firewall using the web configurator. SMT screens allow you to activate the firewall. CLI commands provide limited configuration options and are only recommended for advanced users.

14.2 Firewall Policies Overview

Firewall rules are grouped based on the direction of travel of packets to which they apply:

- LAN to LAN/ Router
- LAN to WAN
- LAN to DMZ
- WAN to LAN
- WAN to WAN/ Router
- WAN to DMZ
- DMZ to LAN
- DMZ to WAN
- DMZ to DMZ/ Router

Note: The LAN includes both the LAN port and the WLAN.

By default, the Prestige's stateful packet inspection allows packets traveling in the following directions:

- LAN to LAN/ Router

  This allows computers on the LAN to manage the Prestige and communicate between networks or subnets connected to the LAN interface.
- LAN to WAN
- LAN to DMZ
- WAN to DMZ
- DMZ to WAN

By default, the Prestige's stateful packet inspection blocks packets traveling in the following directions:

- WAN to LAN

- WAN to WAN/ Router

  This prevents computers on the WAN from using the Prestige as a gateway to communicate with other computers on the WAN and/or managing the Prestige.

- DMZ to LAN
- DMZ to DMZ/ Router

  This prevents computers on the DMZ from communicating between networks or subnets connected to the DMZ interface and/or managing the Prestige.

  You may define additional rules and sets or modify existing ones but please exercise extreme caution in doing so.

Note: If you configure firewall rules without a good understanding of how they work, you might inadvertently introduce security risks to the firewall and to the protected network. Make sure you test your rules after you configure them.

For example, you may create rules to:

- Block certain types of traffic, such as IRC (Internet Relay Chat), from the LAN to the Internet.
- Allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN.
- Allow everyone except your competitors to access a Web server.
- Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by comparing the Source IP address, Destination IP address and IP protocol type of network traffic to rules set by the administrator. Your customized rules take precedence and override the Prestige's default rules.

14.3 Rule Logic Overview

Note: Study these points carefully before configuring rules.

14.3.1 Rule Checklist

State the intent of the rule. For example, "This restricts all IRC access from the LAN to the Internet." Or, "This allows a remote Lotus Notes server to synchronize over the Internet to an inside Notes server."

1. Is the intent of the rule to forward or block traffic?

2 What direction of traffic does the rule apply to (refer to the Firewall Policies Overview section)?

3 What IP services will be affected?

4 What computers on the LAN or DMZ are to be affected (if any)?

5 What computers on the Internet will be affected? The more specific, the better. For example, if traffic is being allowed from the Internet to the LAN, it is better to allow only certain machines on the Internet to access the LAN.

14.3.2 Security Ramifications

1 Once the logic of the rule has been defined, it is critical to consider the security ramifications created by the rule:

2 Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?

3 Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?

4 Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.

5 Does this rule conflict with any existing rules?

6 Once these questions have been answered, adding rules is simply a matter of plugging the information into the correct fields in the web configurator screens.

14.3.3 Key Fields For Configuring Rules

14.3.3.1 Action

Should the action be to **Block** or **Forward**?

Note: "Block" means the firewall silently discards the packet.

14.3.3.2 Service

Select the service from the **Service** scrolling list box. If the service is not listed, it is necessary to first define it. See the Predefined Services section for more information on predefined services.

14.3.3.3 Source Address

What is the connection's source address; is it on the LAN, DMZ, WAN? Is it a single IP, a range of IPs or a subnet?

14.3.3.4 Destination Address

What is the connection's destination address; is it on the LAN, DMZ, WAN? Is it a single IP, a range of IPs or a subnet?

14.4 Connection Direction Example

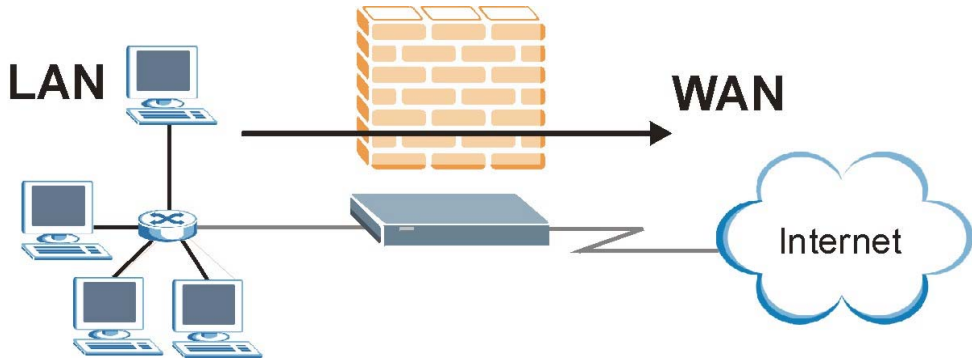
This section describes examples for firewall rules for connections going from LAN to WAN and from WAN to LAN. Rules for the DMZ work in a similar fashion.

LAN to LAN/ Router, WAN to WAN/ Router and DMZ to DMZ/Router rules applies to packets coming in on the associated interface (LAN, WAN, or DMZ respectively). LAN to LAN/ Router means policies for LAN-to-Prestige (the policies for managing the Prestige through the LAN interface) and policies for LAN-to-LAN (the policies that control routing between two subnets on the LAN). Similarly, WAN to WAN/ Router and DMZ to DMZ/ Router polices apply in the same way to the WAN and DMZ ports.

14.4.1 LAN to WAN Rules

The default rule for LAN to WAN traffic is that all users on the LAN are allowed non-restricted access to the WAN. When you configure a LAN to WAN rule, you in essence want to limit some or all users from accessing certain services on the WAN. See the following figure.

Figure 58 LAN to WAN Traffic

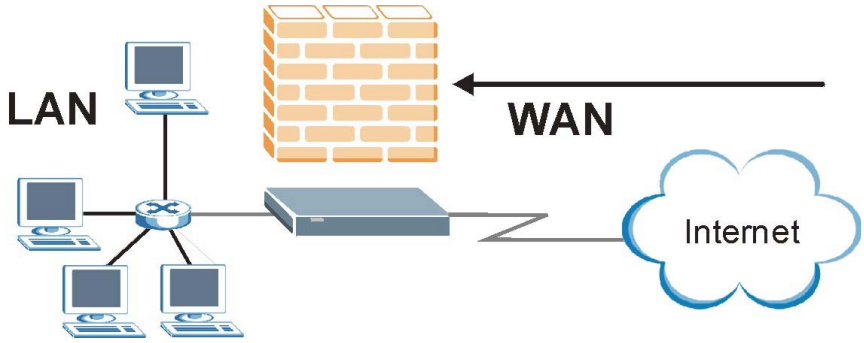


14.4.2 WAN to LAN Rules

The default rule for WAN to LAN traffic blocks all incoming connections (WAN to LAN). If you wish to allow certain WAN users to have access to your LAN, you will need to create custom rules to allow it.

See the following figure.

Figure 59 WAN to LAN Traffic



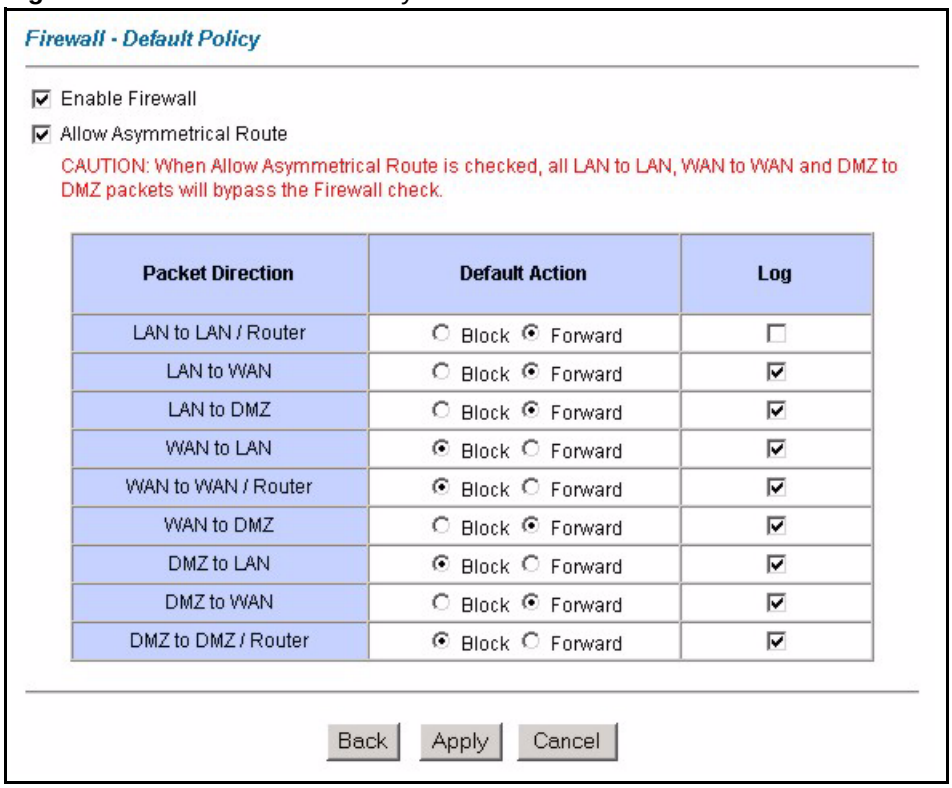
14.4.3 Alerts

Alerts are reports on events, such as attacks, that you may want to know about right away. You can choose to generate an alert when an attack is detected in the **Edit Rule** screen *(*select the **Send Alert Message to Administrator When Matched** checkbox) or when a rule is matched in the **Edit Rule** screen (see the Configuring Firewall Rules section). When an event generates an alert, a message can be immediately sent to an e-mail account that you specify in the **Log Settings** screen (see the chapter on logs).

14.5 Configuring Basic Firewall Settings

Click **Firewall** and then **Default Policy** to display the following screen. Activate the firewall by selecting the **Firewall Enabled** check box as seen in the following screen.

Figure 60 Firewall: Default Policy



The following table describes the labels in this screen.

Table 43 Firewall: Default Policy

LABEL	DESCRIPTION
Firewall Enabled	Select this check box to activate the firewall. The Prestige performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Allow Asymmetrical Route	Select this check box to have the Prestige firewall permit the use of triangle route topology on the network. See the appendix for more on triangle route topology.
Packet Direction	This is the direction of travel of packets (**LAN to LAN/Router, LAN to WAN**, **LAN to DMZ**, **WAN to WAN/Router**, **WAN to LAN**, **WAN to DMZ**, **DMZ to DMZ/ Router**, **DMZ to LAN** or **DMZ to WAN**). Firewall rules are grouped based on the direction of travel of packets to which they apply. For example, **LAN to LAN/Router** means packets traveling from a computer/subnet on the LAN to either another computer/subnet on the LAN interface of the Prestige or the Prestige itself.
Default Action	Use the radio buttons to select whether to **Block** (silently discard) or **Forward** (allow the passage of) packets that are traveling in the selected direction.
Log	Select the check box to create a log (when the above action is taken) for packets that are traveling in the selected direction and do not match any of the rules below.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to begin configuring this screen afresh.

14.6 Rule Summary

Note: The ordering of your rules is very important as rules are applied in turn.

Click on **Firewall**, then **Rule Summary** to bring up the following screen. This screen is a summary of the existing rules. Note the order in which the rules are listed.

Figure 61 Firewall: Rule Summary

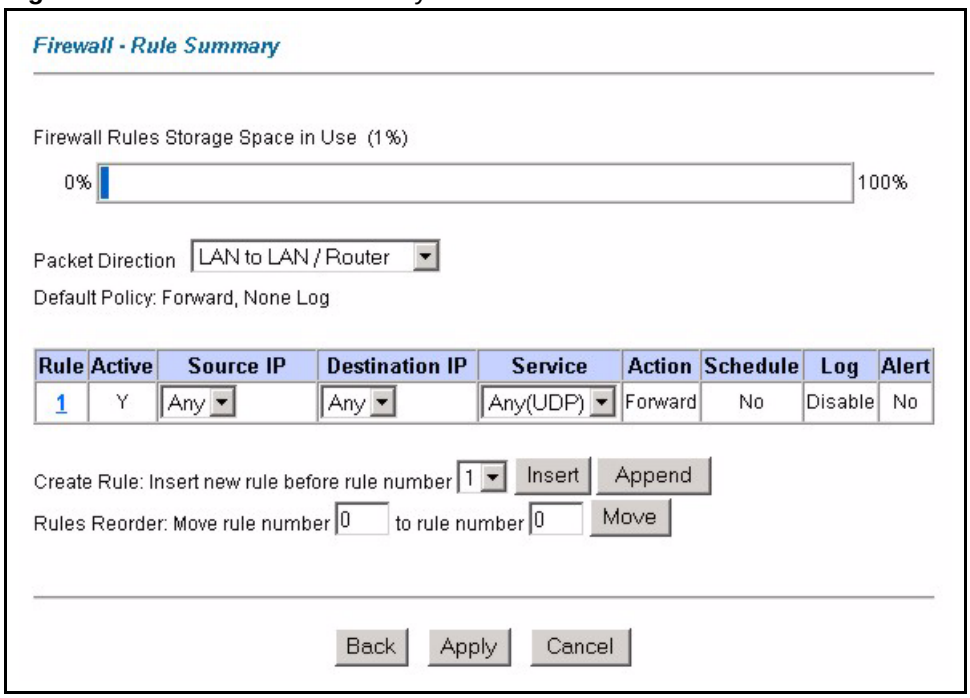


Table 44 Rule Summary

LABEL	DESCRIPTION
Firewall Rules Storage Space in Use	This read-only bar shows how much of the Prestige's memory for recording firewall rules it is currently using. When you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red.
Packet Direction	Use the drop-down list box to select a direction of travel of packets for which you want to configure firewall rules.
Default Policy	This field displays the default action and log policy you selected in the **Default Rule** screen for the packet direction shown in the field above.
	The following read-only fields summarize the rules you have created that apply to traffic traveling in the selected packet direction. The firewall rules that you configure (summarized below) take priority over the general firewall action settings above.
Rule	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn. Click a rule's number to go to the **Firewall Edit Rule** screen to configure or edit a firewall rule.

Table 44 Rule Summary (continued)

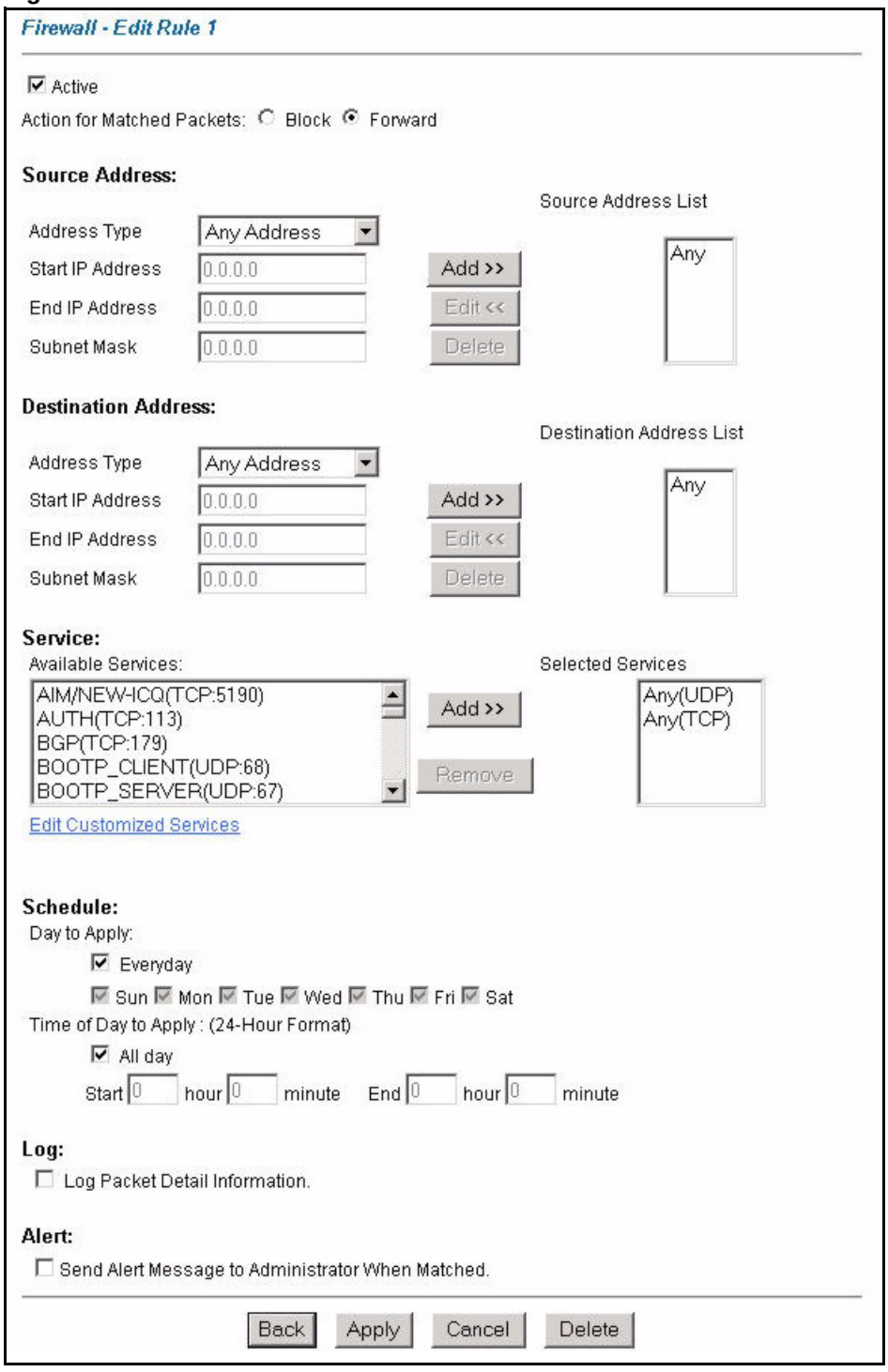
LABEL	DESCRIPTION
Active	This field displays whether a firewall is turned on (**Y**) or not (**N**).
Source IP	This drop-down list box displays the source addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to **Any**.
Destination IP	This drop-down list box displays the destination addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to **Any**.
Service	This drop-down list box displays the services to which this firewall rule applies. Please note that a blank service type is equivalent to **Any**. See for more information.
Action	This is the specified action for that rule, either **Block** or **Forward**. Note that **Block** means the firewall silently discards the packet.
Schedule	This field tells you whether a schedule is specified (**Yes**) or not (**No**).
Log	This field shows you whether a log is created when packets match this rule (**Enabled**) or not (**Disable**).
Alert	This field tells you whether this rule generates an alert (**Yes**) or not (**No**) when the rule is matched.
Insert/Append	Type the index number for where you want to put a rule. For example, if you type "6", your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7. Click **Insert** to add a new firewall rule before the specified index number. Click **Append** to add a new firewall rule after the specified index number.
Move	Type a rule's index number and the number for where you want to put that rule. Click **Move** to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to begin configuring this screen afresh.

14.6.1 Configuring Firewall Rules

Follow these directions to create a new rule.

1. In the **Rule Summary** screen, type the index number for where you want to put the rule. For example, if you type "6", your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7.
2. Click **Insert** to display this screen and refer to the following table for information on the labels.

Figure 62 Firewall: Edit Rule



The following table describes the labels in this screen.

Table 45 Firewall: Edit Rule

LABEL	DESCRIPTION
Active	Select this option to enable this firewall rule.
Action for Matched Packet	Use the radio button to select whether to discard (**Block**) or allow the passage of (**Forward**) packets that match this rule.
Source/Destination Address	
Address Type	Do you want your rule to apply to packets with a particular (single) IP, a range of IP addresses (e.g., 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop-down list box that includes: **Single Address**, **Range Address**, **Subnet Address** and **Any Address**.
Start IP Address	Enter the single IP address or the starting IP address in a range here.
End IP Address	Enter the ending IP address in a range here.
Subnet Mask	Enter the subnet mask here, if applicable.
Add	Click **Add** to add a new address to the **Source** or **Destination Address** box. You can add multiple addresses, ranges of addresses, and/or subnets.
Edit	To edit an existing source or destination address, select it from the box and click **Edit**.
Delete	Highlight an existing source or destination address from the **Source** or **Destination Address** box above and click **Delete** to remove it.
Services	
Available/ Selected Services	Please see for more information on services available. Highlight a service from the **Available Services** box on the left, then click **Add>>** to add it to the **Selected Services** box on the right. To remove a service, highlight it in the **Selected Services** box on the right, then click **Remove**.
Edit Customized Service	Click the **Edit Customized Services** link to bring up the screen that you use to configure a new custom service that is not in the predefined list of services.
Schedule	
Day to Apply	Select everyday or the day(s) of the week to apply the rule.
Time of Day to Apply (24-Hour Format)	Select **All Day** or enter the start and end times in the hour-minute format to apply the rule.
Log	
Log Packet Detail Information	This field determines if a log for packets that match the rule is created (**Enable**) or not (**Disable**). Go to the **Log Settings** page and select the **Access Control** logs category to have the Prestige record these logs.
Alert	
Send Alert Message to Administrator When Matched	Select the check box to have the Prestige generate an alert when the rule is matched.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to exit this screen without saving.
Delete	Click **Delete** to remove this firewall rule and return to the **Firewall Rule Summary** screen.

14.7 Customized Services

Configure customized services and port numbers not predefined by the Prestige. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. For further information on these services, please read the Predefined Services section. Click the **Customized Services** link while editing a firewall rule to configure a custom service port. This displays the following screen.

Figure 63 Firewall: Customized Services

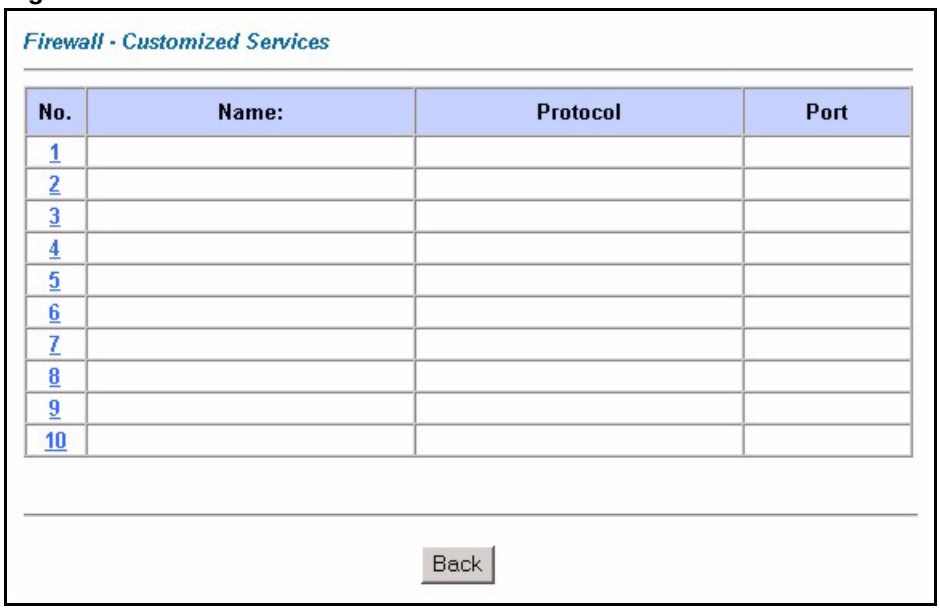


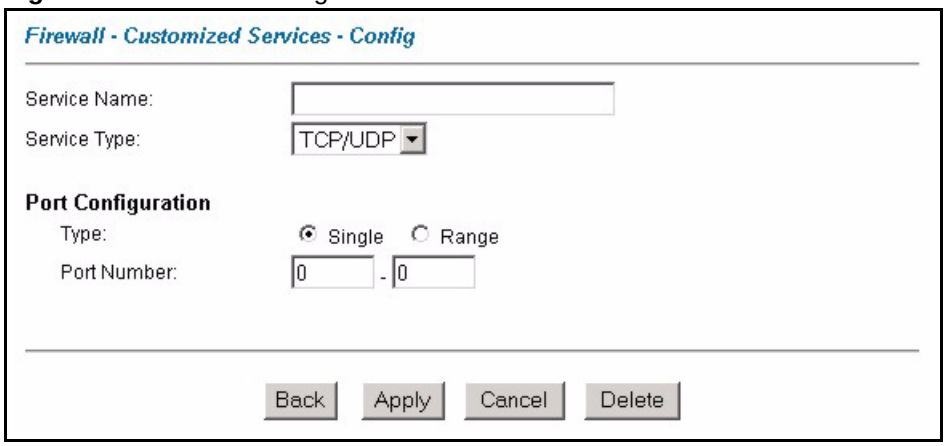
Table 46 Customized Services

LABEL	DESCRIPTION
No.	This is the number of your customized port. Click a rule's number of a service to go to the **Firewall Customized Services Config** screen to configure or edit a customized service.
Name	This is the name of your customized service.
Protocol	This shows the IP protocol (**TCP**, **UDP** or **TCP/UDP**) that defines your customized service.
Port	This is the port number or range that defines your customized service.
Back	Click **Back** to return the **Firewall Edit Rule** screen.

14.8 Creating/Editing A Customized Service

Click a rule number in the **Firewall Customized Services** screen to create a new custom port or edit an existing one. This action displays the following screen.

Figure 64 Firewall: Configure Customized Services



The following table describes the labels in this screen.

Table 47 Firewall: Configure Customized Services

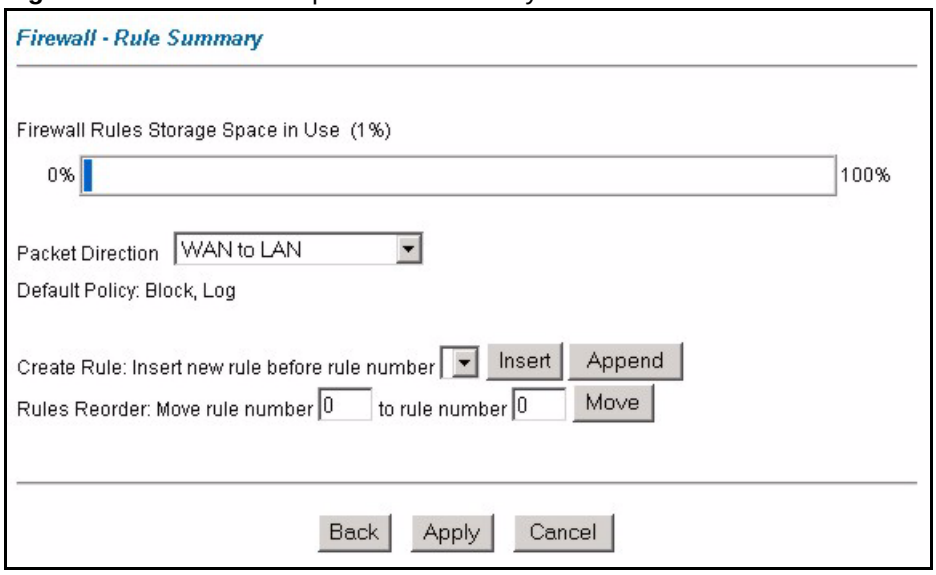
LABEL	DESCRIPTION
Service Name	Type a unique name for your custom port.
Service Type	Choose the IP port (**TCP**, **UDP** or **TCP/UDP**) that defines your customized port from the drop down list box.
Port Configuration	
Type	Click **Single** to specify one port only or **Range** to specify a span of ports that define your customized service.
Port Number	Type a single port number or the range of port numbers that define your customized service.
Back	Click **Back** to return to the **Firewall Customized Services** screen.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to return to the previously saved settings.
Delete	Click **Delete** to delete the current rule.

14.9 Example Firewall Rule

The following Internet firewall rule example allows a hypothetical "My Service" connection from the Internet.

1. Click **Firewall** in the navigation panel and click **Rule Summary**.
2. Select **WAN to LAN** in the **Packet Direction** field.

Figure 65 Firewall Example: Rule Summary



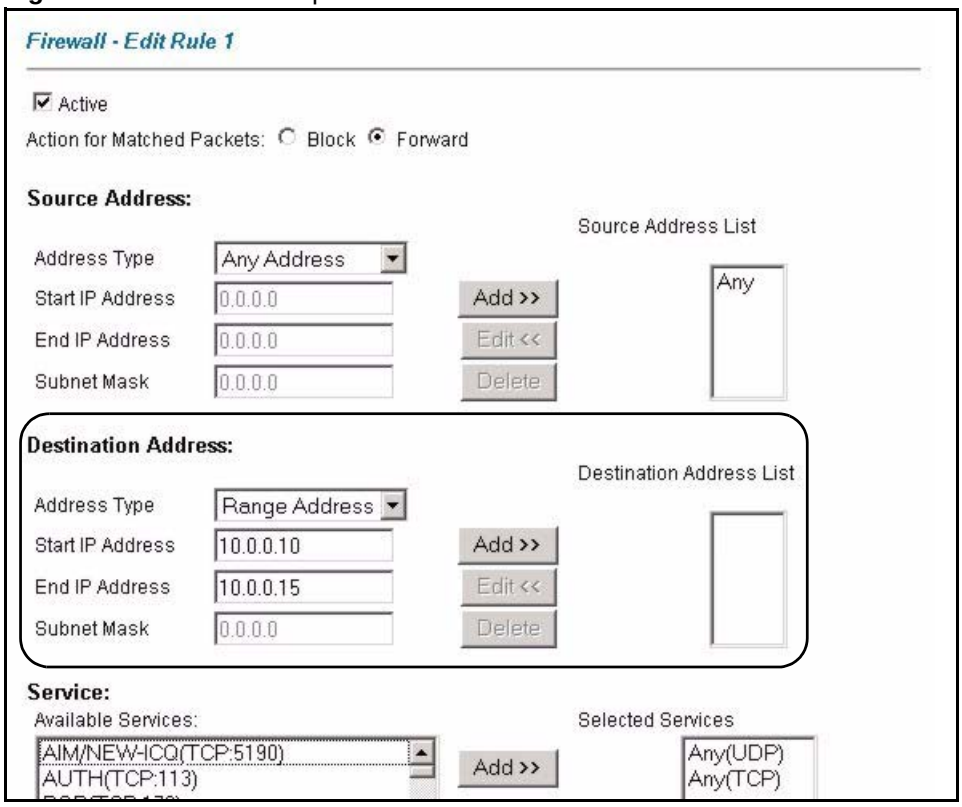
3 In the **Rule Summary** screen, type the index number for where you want to put the rule. For example, if you type "6", your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7.

4 Click **Insert** to display the firewall rule configuration screen.

5 Select **Any** in the **Destination Address** box and then click **Delete**.

6 Configure the destination address screen as follows and click **Add**.

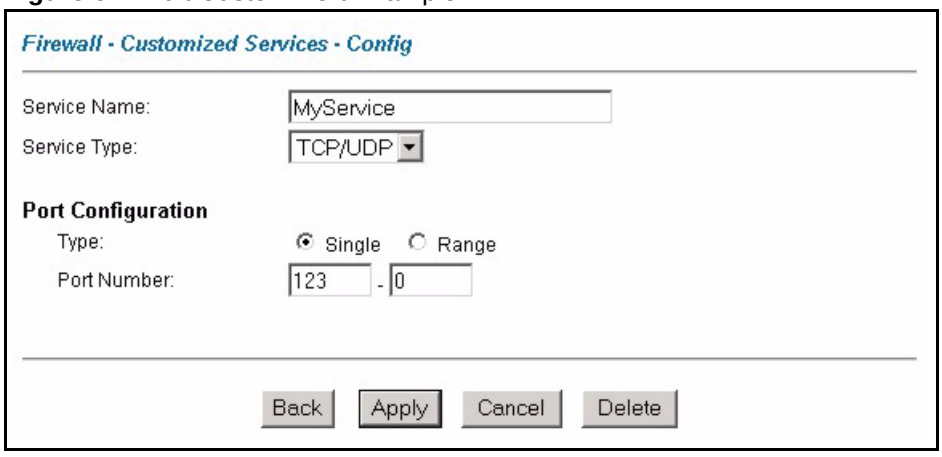
Figure 66 Firewall Example: Edit Rule: Destination Address



7 In the **Edit Rule** screen, click the **Customized Services** link to open the **Customized Service** screen.

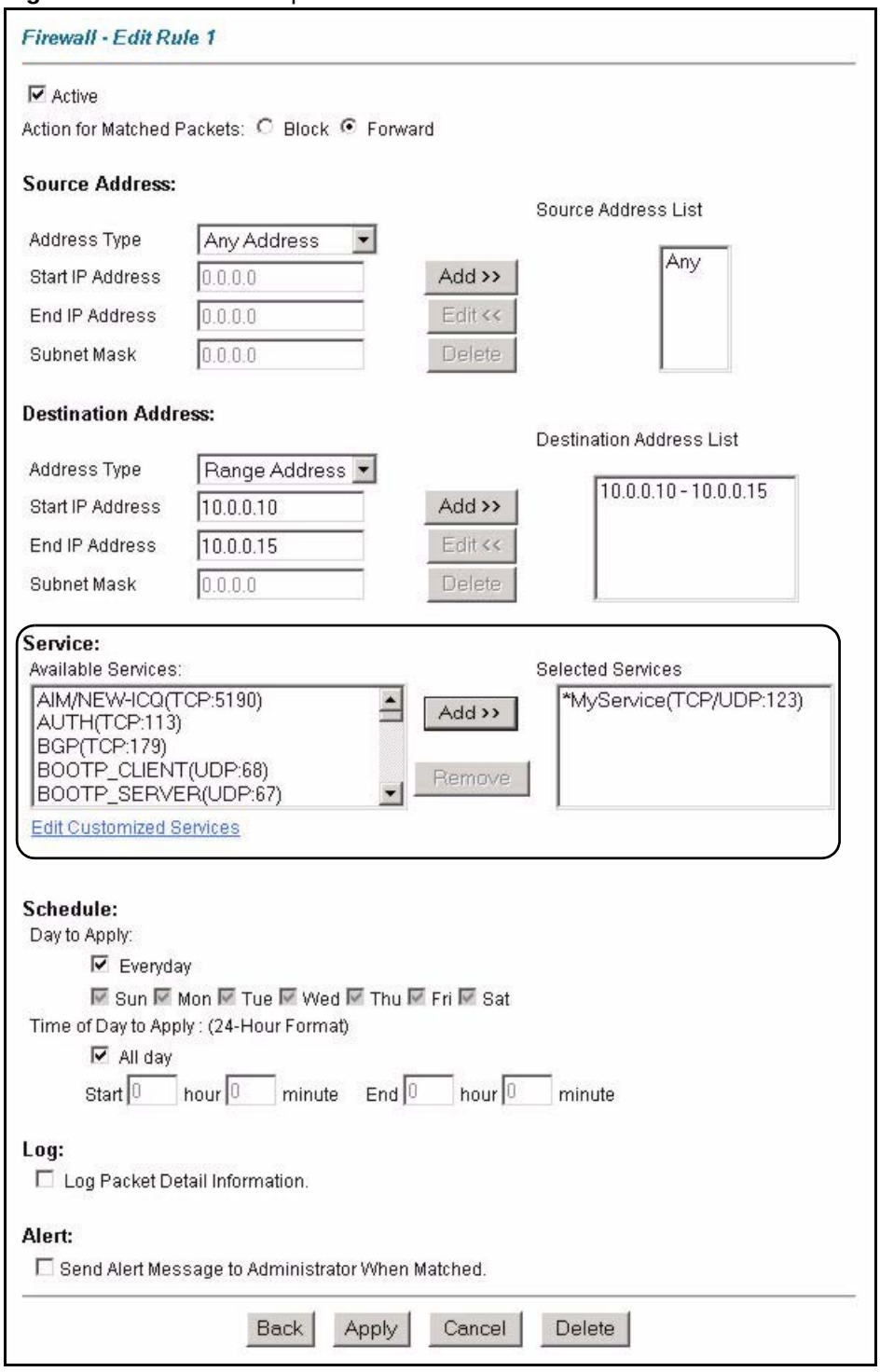
8 Click an index number to display the **Customized Services -Config** screen and configure the screen as follows and click **Apply**.

Figure 67 Edit Custom Port Example



9 In the **Edit Rule** screen, use the **Add**>> and **Remove** buttons between **Available Services** and **Selected Services** list boxes to configure it as follows. Click **Apply** when you are done.

Figure 68 Firewall Example: Edit Rule: Select Customized Services



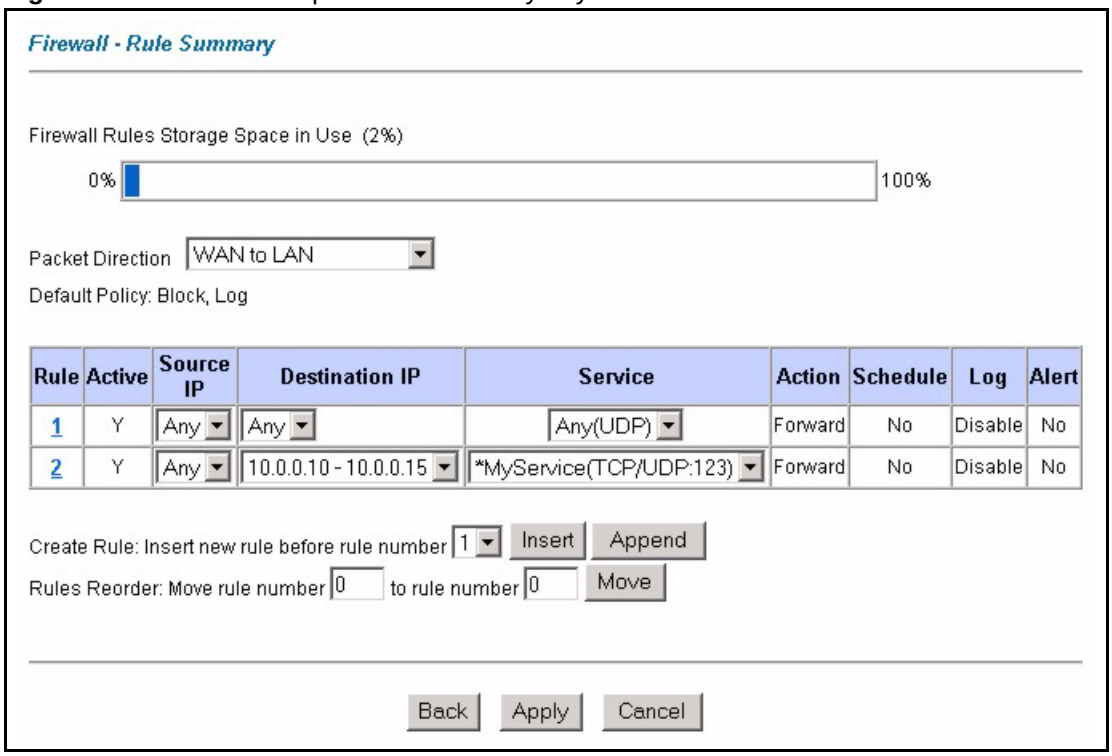
Note: Custom ports show up with an "*" before their names in the Services list box and the **Rule Summary** list box. Click **Apply** after you've created your custom port.

On completing the configuration procedure for this Internet firewall rule, the **Rule Summary**

screen should look like the following.

Rule 2 allows a "My Service" connection from the WAN to IP addresses 10.0.0.10 through 10.0.0.15 on the LAN.

Figure 69 Firewall Example: Rule Summary: My Service



14.10 Predefined Services

The **Available Services** list box in the **Edit Rule** screen (see the Configuring Firewall Rules section) displays all predefined services that the Prestige already supports. Next to the name of the service, two fields appear in brackets. The first field indicates the IP protocol type (TCP, UDP, or ICMP). The second field indicates the IP port number that defines the service. (Note that there may be more than one IP protocol type. For example, look at the default configuration labeled "(**DNS**)". **(UDP/TCP:53)** means UDP port 53 and TCP port 53. Up to 128 entries are supported. Custom service ports may also be configured using the **Edit Customized Services** function discussed previously.

Table 48 Predefined Services

SERVICE	DESCRIPTION
AIM/NEW_ICQ(TCP:5190)	AOL's Internet Messenger service, used as a listening port by ICQ.
AUTH(TCP:113)	Authentication protocol used by some servers.
BGP(TCP:179)	Border Gateway Protocol.
BOOTP_CLIENT(UDP:68)	DHCP Client.

Table 48 Predefined Services (continued)

SERVICE	DESCRIPTION
BOOTP_SERVER(UDP:67)	DHCP Server.
CU-SEEME(TCP/UDP:7648, 24032)	A popular videoconferencing solution from White Pines Software.
DNS(UDP/TCP:53)	Domain Name Server, a service that matches web names (e.g. www.zyxel.com) to IP numbers.
FINGER(TCP:79)	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP(TCP:20.21)	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323(TCP:1720)	Net Meeting uses this protocol.
HTTP(TCP:80)	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	HTTPS is a secured http session often used in e-commerce.
ICQ(UDP:4000)	This is a popular Internet chat program.
IPSEC_TRANSPORT/ TUNNEL(AH:0)	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
IPSEC_TUNNEL(ESP:0)	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
IRC(TCP/UDP:6667)	This is another popular Internet chat program.
MSN Messenger(TCP:1863)	Microsoft Networks' messenger service uses this protocol.
MULTICAST(IGMP:0)	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
NEWS(TCP:144)	A protocol for news groups.
NFS(UDP:2049)	Network File System - NFS is a client/server distributed file service that provides transparent file-sharing for network environments.
NNTP(TCP:119)	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING(ICMP:0)	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3(TCP:110)	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP(TCP:1723)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL(GRE:0)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the data channel.
RCMD(TCP:512)	Remote Command Service.
REAL_AUDIO(TCP:7070)	A streaming audio service that enables real time sound over the web.
REXEC(TCP:514)	Remote Execution Daemon.
RLOGIN(TCP:513)	Remote Login.
RTELNET(TCP:107)	Remote Telnet.
RTSP(TCP/UDP:554)	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP(TCP:115)	Simple File Transfer Protocol.

Table 48 Predefined Services (continued)

SERVICE	DESCRIPTION
SMTP(TCP:25)	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP(TCP/UDP:161)	Simple Network Management Program.
SNMP-TRAPS (TCP/ UDP:162)	Traps for use with the SNMP (RFC:1215).
SQL-NET(TCP:1521)	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSDP(UDP:1900)	Simole Service Discovery Protocol (SSDP) is a discovery service searching for Universal Plug and Play devices on your home network or upstream Internet gateways using DUDP port 1900.
SSH(TCP/UDP:22)	Secure Shell Remote Login Program.
STRMWORKS(UDP:1558)	Stream Works Protocol.
SYSLOG(UDP:514)	Syslog allows you to send system logs to a UNIX server.
TACACS(UDP:49)	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET(TCP:23)	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP(UDP:69)	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE(TCP:7000)	Another videoconferencing solution.

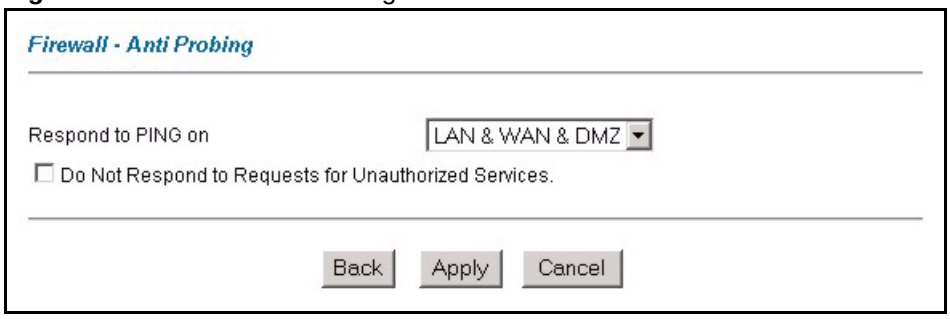
14.11 Anti-Probing

If an outside user attempts to probe an unsupported port on your Prestige, an ICMP response packet is automatically returned. This allows the outside user to know the Prestige exists. The Prestige supports anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your Prestige when unsupported ports are probed.

Internet Control Message Protocol (ICMP) is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.

Click **Firewall** in the navigation panel and click **Anti Probing** to display the screen as shown.

Figure 70 Firewall: Anti Probing



The following table describes the labels in this screen.

Table 49 Firewall: Anti Probing

LABEL	DESCRIPTION
Respond to PING on	The Prestige does not respond to any incoming Ping requests when **Disable** is selected. Select **LAN** to reply to incoming LAN Ping requests. Select **WAN** to reply to incoming WAN Ping requests. Select **DMZ** to reply to incoming DMZ Ping requests. Otherwise select **LAN & WAN & DMZ** to reply to both incoming LAN and WAN and DMZ Ping requests.
Do not respond to requests for unauthorized services.	Select this option to prevent hackers from finding the Prestige by probing for unused ports. If you select this option, the Prestige will not respond to port request(s) for unused ports, thus leaving the unused ports and the Prestige unseen. By default this option is not selected and the Prestige will reply with an ICMP Port Unreachable packet for a port probe on its unused UDP ports, and a TCP Reset packet for a port probe on its unused TCP ports. Note that the probing packets must first traverse the Prestige 's firewall mechanism before reaching this anti-probing mechanism. Therefore if the firewall mechanism blocks a probing packet, the Prestige reacts based on the firewall policy, which by default, is to send a TCP reset packet for a blocked TCP packet. You can use the command "sys firewall tcprst rst [on|off]" to change this policy. When the firewall mechanism blocks a UDP packet, it drops the packet without sending a response packet.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the Prestige.
Reset	Click **Reset** to begin configuring this screen afresh.

14.12 Configuring Attack Alert

Attack alerts are the first defense against DOS attacks. In the **Threshold** screen, shown later, you may choose to generate an alert whenever an attack is detected. For DoS attacks, the Prestige uses thresholds to determine when to drop sessions that do not become fully established. These thresholds apply globally to all sessions.

You can use the default threshold values, or you can change them to values more suitable to your security requirements.

14.12.1 Threshold Values

Tune these parameters when something is not working and after you have checked the firewall counters. These default values should work fine for most small offices. Factors influencing choices for threshold values are:

- The maximum number of opened sessions.
- The minimum capacity of server backlog in your LAN network.
- The CPU power of servers in your LAN network.
- Network bandwidth.
- Type of traffic for certain servers.

If your network is slower than average for any of these factors (especially if you have servers that are slow or handle many tasks and are often busy), then the default values should be reduced.

You should make any changes to the threshold values before you continue configuring firewall rules.

14.12.2 Half-Open Sessions

An unusually high number of half-open sessions (either an absolute number or measured as the arrival rate) could indicate that a Denial of Service attack is occurring. For TCP, "half-open" means that the session has not reached the established state-the TCP three-way handshake has not yet been completed (see Figure 54). For UDP, "half-open" means that the firewall has detected no return traffic.

The Prestige measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.

When the number of existing half-open sessions rises above a threshold (**max-incomplete high**), the Prestige starts deleting half-open sessions as required to accommodate new connection requests. The Prestige continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below another threshold (**max-incomplete low**).

When the rate of new connection attempts rises above a threshold (**one-minute high**), the Prestige starts deleting half-open sessions as required to accommodate new connection requests. The Prestige continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below another threshold (**one-minute low**). The rate is the number of new attempts detected in the last one-minute sample period.

14.12.2.1 TCP Maximum Incomplete and Blocking Time

An unusually high number of half-open sessions with the same destination host address could indicate that a Denial of Service attack is being launched against the host.

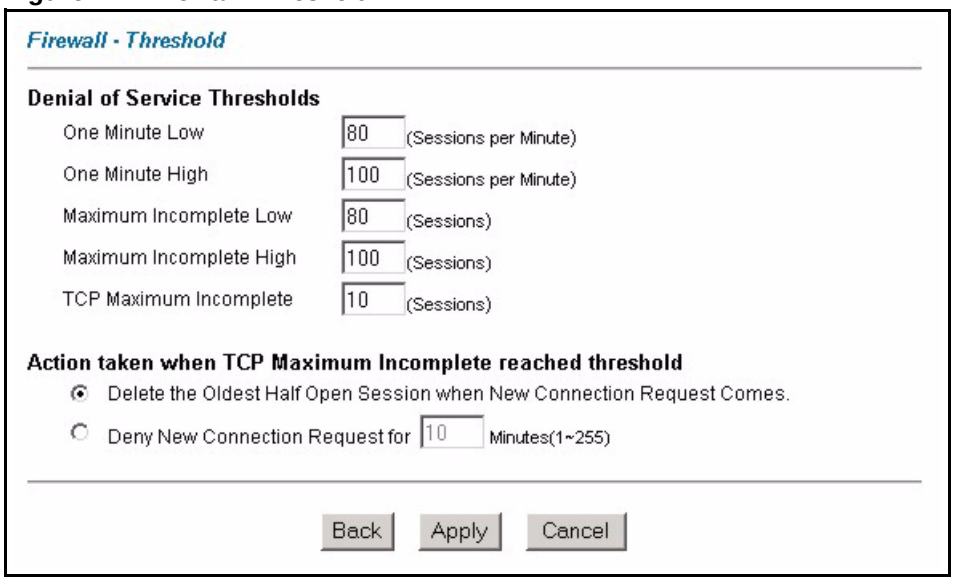
Whenever the number of half-open sessions with the same destination host address rises above a threshold (**TCP Maximum Incomplete**), the Prestige starts deleting half-open sessions according to one of the following methods:

- If the **Blocking Time** timeout is 0 (the default), then the Prestige deletes the oldest existing half-open session for the host for every new connection request to the host. This ensures that the number of half-open sessions to a given host will never exceed the threshold.
- If the **Blocking Time** timeout is greater than 0, then the Prestige blocks all new connection requests to the host giving the server time to handle the present connections. The Prestige continues to block all new connection requests until the **Blocking Time** expires.

The Prestige also sends alerts whenever **TCP Maximum Incomplete** is exceeded. The global values specified for the threshold and timeout apply to all TCP connections.

Click **Firewall**, and **Threshold** to bring up the next screen.

Figure 71 Firewall: Threshold



The following table describes the labels in this screen.

Table 50 Firewall: Threshold

LABEL	DESCRIPTION	DEFAULT VALUES
Denial of Service Thresholds		
One Minute Low	This is the rate of new half-open sessions that causes the firewall to stop deleting half-open sessions. The Prestige continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below this number.	80 existing half-open sessions.

Table 50 Firewall: Threshold (continued)

LABEL	DESCRIPTION	DEFAULT VALUES
One Minute High	This is the rate of new half-open sessions that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the Prestige deletes half-open sessions as required to accommodate new connection attempts.	100 half-open sessions per minute. The above numbers cause the Prestige to start deleting half-open sessions when more than 100 session establishment attempts have been detected in the last minute, and to stop deleting half-open sessions when fewer than 80 session establishment attempts have been detected in the last minute.
Maximum Incomplete Low	This is the number of existing half-open sessions that causes the firewall to stop deleting half-open sessions. The Prestige continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below this number.	80 existing half-open sessions.
Maximum Incomplete High	This is the number of existing half-open sessions that causes the firewall to start deleting half-open sessions. When the number of existing half-open sessions rises above this number, the Prestige deletes half-open sessions as required to accommodate new connection requests. Do not set **Maximum Incomplete High** to lower than the current **Maximum** I**ncomplete Low** number.	100 existing half-open sessions. The above values causes the Prestige to start deleting half-open sessions when the number of existing half-open sessions rises above 100, and to stop deleting half-open sessions with the number of existing half-open sessions drops below 80.
TCP Maximum Incomplete	This is the number of existing half-open TCP sessions with the same destination host IP address that causes the firewall to start dropping half-open sessions to that same destination host IP address. Enter a number between 1 and 256. As a general rule, you should choose a smaller number for a smaller network, a slower system or limited bandwidth.	30 existing half-open TCP sessions.
Action taken when the TCP Maximum Incomplete threshold is reached.		
Delete the oldest half open session when new connection request comes	Select this radio button to clear the oldest half open session when a new connection request comes.	
Deny new connection request for	Select this radio button and specify for how long the Prestige should block new connection requests when **TCP Maximum Incomplete** is reached. Enter the length of blocking time in minutes (between 1 and 256).	
Back	Click **Back** to return to the previous screen.	
Apply	Click **Apply** to save your changes back to the Prestige.	
Cancel	Click **Cancel** to begin configuring this screen afresh.	

CHAPTER 15
Content Filtering

This chapter covers how to configure content filtering.

15.1 Content Filtering Overview

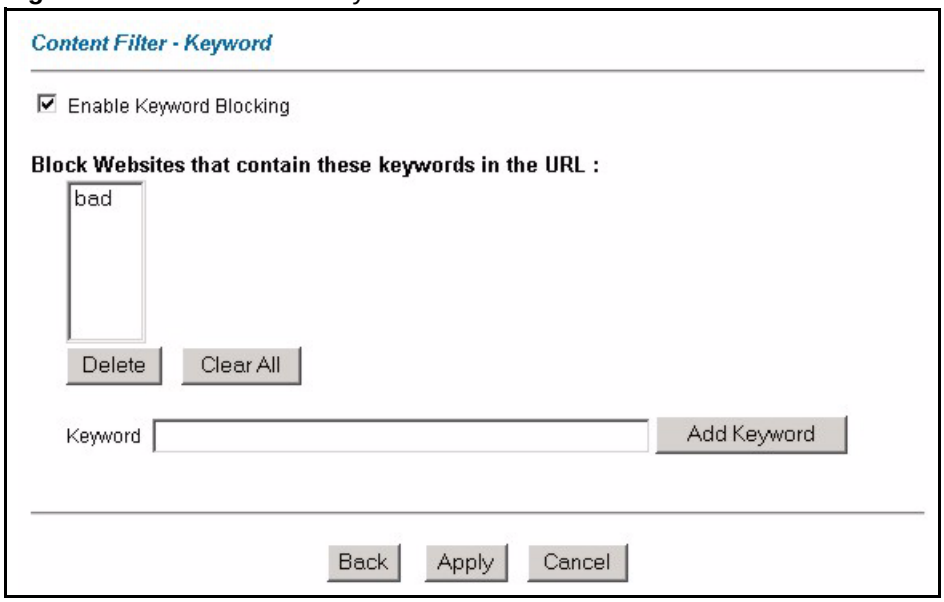
Internet content filtering allows you to create and enforce Internet access policies tailored to your needs. Content filtering gives you the ability to block web sites that contain key words (that you specify) in the URL. You can set a schedule for when the Prestige performs content filtering. You can also specify trusted IP addresses on the LAN for which the Prestige will not perform content filtering.

15.2 Configuring Keyword Blocking

Use this screen to block sites containing certain keywords in the URL. For example, if you enable the keyword "bad", the Prestige blocks all sites containing this keyword including the URL http://www.website.com/bad.html, even if it is not included in the Filter List.

To have your Prestige block Web sites containing keywords in their URLs, click **Content Filter** and **Keyword**. The screen appears as shown.

Figure 72 Content Filter: Keyword



The following table describes the labels in this screen.

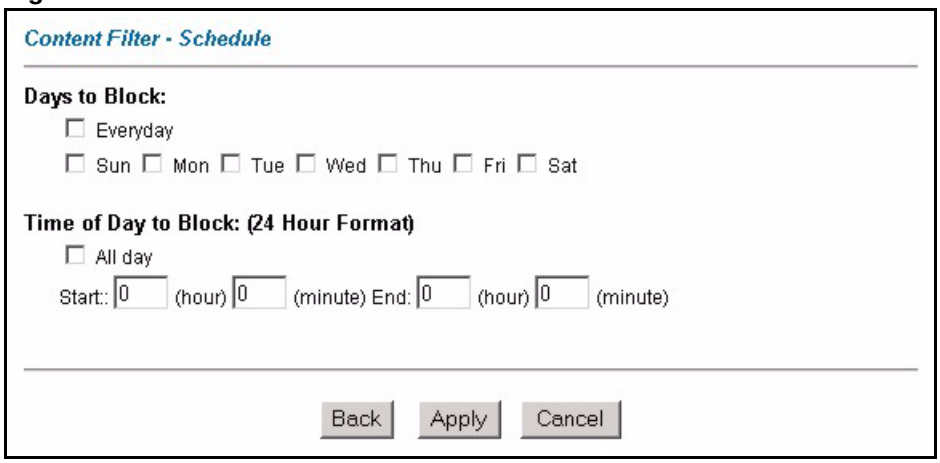
Table 51 Content Filter: Keyword

LABEL	DESCRIPTION
Enable Keyword Blocking	Select this check box to enable this feature.
Block Websites that contain these keywords in the URL:	This box contains the list of all the keywords that you have configured the Prestige to block.
Delete	Highlight a keyword in the box and click **Delete** to remove it.
Clear All	Click **Clear All** to remove all of the keywords from the list.
Keyword	Type a keyword in this field. You may use any character (up to 127 characters). Wildcards are not allowed.
Add Keyword	Click **Add Keyword** after you have typed a keyword. Repeat this procedure to add other keywords. Up to 64 keywords are allowed. When you try to access a web page containing a keyword, you will get a message telling you that the content filter is blocking this request.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to return to the previously saved settings.

15.3 Configuring the Schedule

To set the days and times for the Prestige to perform content filtering, click **Content Filter** and **Schedule**. The screen appears as shown.

Figure 73 Content Filter: Schedule



The following table describes the labels in this screen.

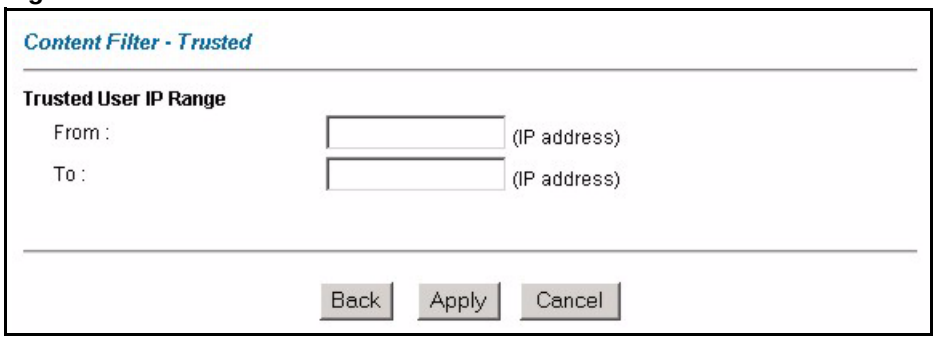
Table 52 Content Filter: Schedule

LABEL	DESCRIPTION
Days to Block:	Select a check box to configure which days of the week (or everyday) you want the content filtering to be active.
Time of Day to Block:	Use the 24 hour format to configure which time of the day (or select the **All day** check box) you want the content filtering to be active.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes.
Cancel	Click **Cancel** to return to the previously saved settings.

15.4 Configuring Trusted Computers

To exclude a range of users on the LAN from content filtering on your Prestige, click **Content Filter** and **Trusted**. The screen appears as shown.

Figure 74 Content Filter: Trusted



The following table describes the labels in this screen.

Table 53 Content Filter: Trusted

LABEL	DESCRIPTION
Trusted User IP Range	
From	Type the IP address of a computer (or the beginning IP address of a specific range of computers) on the LAN that you want to exclude from content filtering.
To	Type the ending IP address of a specific range of users on your LAN that you want to exclude from content filtering. Leave this field blank if you want to exclude an individual computer.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to return to the previously saved settings.

CHAPTER 16
Content Access Control

This chapter gives some background information on Content Access Control and explains how to get started with the Prestige Content Access Control.

16.1 Content Access Control Overview

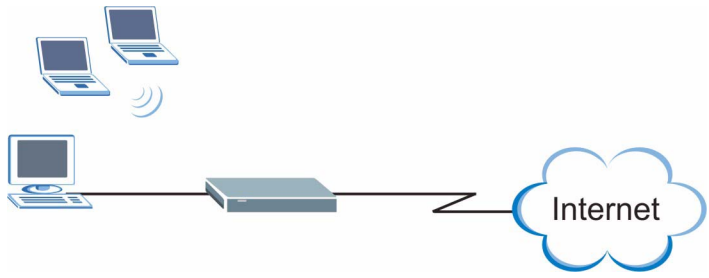
Content Access Control (CAC) lets a LAN administrator control a LAN user's Internet access privileges by blocking services that you specify. The administrator can create user groups with access restrictions and set up user accounts (with a login name and password) for each person (user) on the network. The user accounts are associated to a user group. Each person must log into the system before they can gain access to the Internet.

16.1.1 Content Access Control WLAN Application

You can control LAN user Internet access by having an administrator configure Content Access Control on the Prestige.

The administrator must create user groups and accounts (each person (user) on the network). Each person must log into the system before they can gain access to the Internet. Each user group will hold the details (access rights and privileges and time schedule) for the associated user accounts. The Prestige enforces these access restrictions.

Figure 75 Content Access Control with WLAN Application



16.1.2 Configuration Steps

To activate and set up Content Access Control on the Prestige, you must do the following tasks.

1. Create four user groups with access restrictions and schedule.
2. Create user accounts and associate the user accounts to a user group.

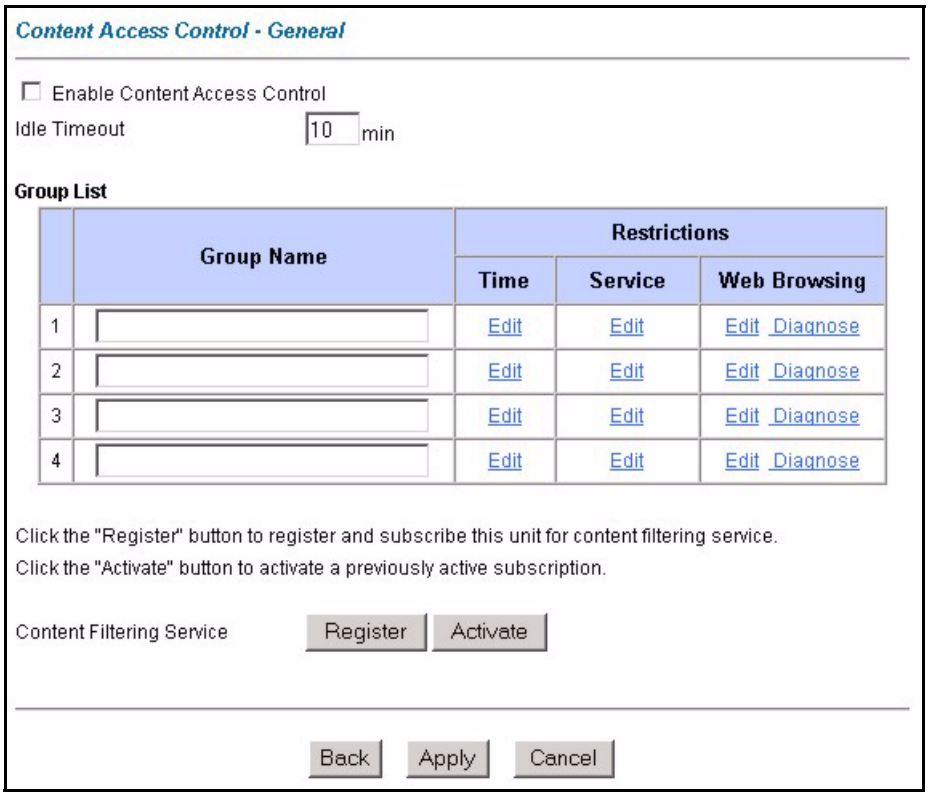
16.2 Activating CAC and Create User Groups

From the **Site Map**, click **Content Access Control** and **General** to open the configuration screen.

Use this screen to activate Content Access Control and set up the four user groups.

Note: You must set up all four user groups.

Figure 76 Content Access Control: General



The following table describes the labels in this screen.

Table 54 Content Access Control: General

LABEL	DESCRIPTION
Enable Content Access Control	Select the check box to allow the LAN administrator to have control over a LAN user's Internet access.
Idle Timeout	Type the time in minutes that elapses before the Prestige automatically terminates the Internet session. The default time is **10** minutes.
Group List	These groups are used in conjunction with content filtering to decide which web pages cannot be accessed by the user. You can set up to four user groups.

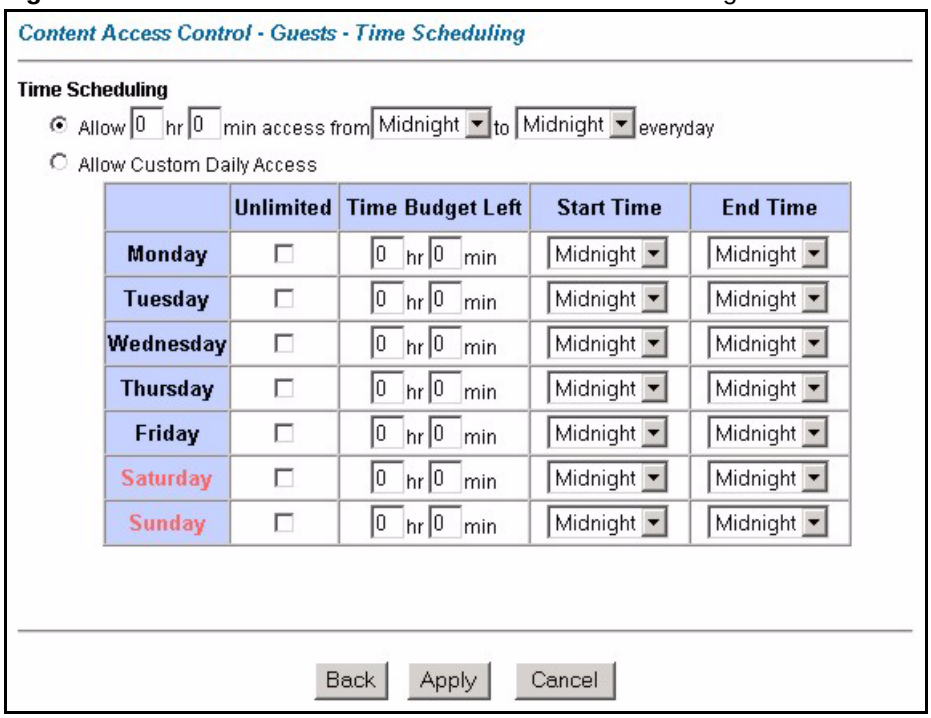
Table 54 Content Access Control: General (continued)

LABEL	DESCRIPTION
Group Name	Enter the name of a user group for identification purposes.
Restrictions	Use the links below to configure the access restrictions for the user group..
Time	Click **Edit** to set up the time allowances, start times and end times of the day(s) when access is allowed.
Service	Click **Edit** to select the services you wish to block access for a user group.
Web Browsing	Click **Edit** to specify the web site category(ies) and/or key words in a web site address you wish to block access for a user group. Click **Diagnose** to test the access privilege on a specified web site address.
Content Filtering Service	Click **Register** to go to a web site where you can register for category-based content filtering (using an external database). You can use a trial application or register your iCard's PIN. Refer to the web site's on-line help for details. **Note:** Refer to the myZyXEL.com appendix on more information on device and service registration. You can also manage your registration status or view content filtering reports after you register this device in the service registration web site. **Note:** The web site displays a registration successful web page. It may take up to another ten minutes for content filtering to be activated. See on how to check the content filtering activation. Click **Activate** to begin the content filtering service now.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to return to the previously saved settings.

16.2.1 Configuring Time Schedule

To set up the time schedule for each user group, click **Edit** under **Time** in the **Control Access Control-General** screen. A screen displays as shown next.

Figure 77 Control Access Control: General: Time Scheduling



The following table describes the labels in this screen.

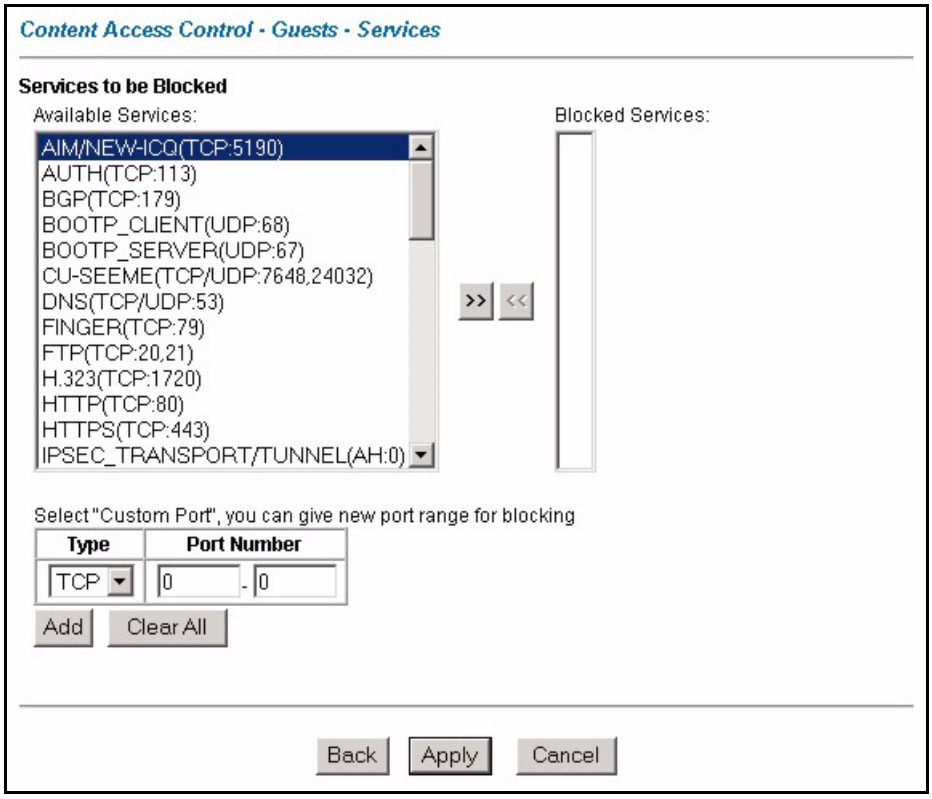
Table 55 Control Access Control: General: Time Scheduling

LABEL	DESCRIPTION
Time Scheduling	Select the first radio button to allow everyday access at the same times to the Internet. Type the interval time allowance (number of hours and minutes). Select the start and end times from the drop-down list boxes to configure the period during the day when access is allowed. Select **Allow Custom Daily Access** to configure time allowances, start times and end times for each day.
Unlimited	Select the check box for the day(s) that you do not want any time restrictions for user Internet access.
Time Budget Left	Type the number of hours (0 to 23) and minutes (0 to 59) to allow Internet access of unblocked sites. **Note:** If you want to allow twenty-four hour access, you should select the **Unlimited** check box.
Start Time	Select from the drop-down list box a time during the day when a user can begin accessing unblocked sites.
End Time	Select from the drop-down list box a time during the day when a user can no longer access unblocked sites. The time allowance must be less than or equal to the period from the start time to the end time. **Note:** User access will be denied after the **End Time** for that day even if the time allowance has not run out.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to return to the previously saved settings.

16.2.2 Configuring Services

To customize services for each user group, click **Edit** under **Services** for that user group in the **Content Access Control: General** screen.

Figure 78 Content Access Control: General: Services



The following table describes the labels in this screen.

Table 56 Content Access Control: General: Services

LABEL	DESCRIPTION
Service to be Blocked	
Available services	Select a service from the list and click the **>>** button to have the service blocked on a weekday (Monday to Friday) or to have the service blocked on a day in the weekend (Saturday or Sunday). These services will be blocked according to the settings you configure in **Time Scheduling** screen.
Blocked Services	This box shows all the services that you want to block during the specified time for the user group. Click the **<<** button to remove a service from the box.
Customized Services	A customized service is a service that is not available in the pre-defined **Available Services** list and you must define using the next two fields.
Type	Services are either **TCP** and/or **UDP**. Select from either **TCP** or **UDP**.
Port Number	Enter a port number or a range of port numbers to define the service. For example, suppose you want to define the Gnutella service. Select **TCP** type and enter a port range from 6345-6349.

Table 56 Content Access Control: General: Services (continued)

LABEL	DESCRIPTION
Add	Click **Add** to add a service to be blocked to the **Blocked Services** box.
Clear All	Click **Clear All** to empty the **Blocked Services** box.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to return to the previously saved settings.

16.2.2.1 Available Services

The **Available Services** list box in the **Services** screen displays some predefined services that the Prestige supports. The following table shows a list of services that can be configured. Next to the name of the service, two fields appear in brackets. The first field indicates the IP protocol type (TCP, UDP, or ICMP). The second field indicates the IP port number that defines the service. (Note that there may be more than one IP protocol type. For example, look at the default configuration labeled "(**DNS**)". **(UDP/TCP:53)** means UDP port 53 and TCP port 53.

Table 57 Available Services

SERVICE	DESCRIPTION
AIM/New-ICQ(TCP:5190)	AOL's Internet Messenger service, used as a listening port by ICQ.
AUTH(TCP:113)	Authentication protocol used by some servers.
BGP(TCP:179)	Border Gateway Protocol.
BOOTP_CLIENT(UDP:68)	DHCP Client.
BOOTP_SERVER(UDP:67)	DHCP Server.
CU-SEEME(TCP/ UDP:7648, 24032)	A popular videoconferencing solution from White Pines Software.
DNS(UDP/TCP:53)	Domain Name Server, a service that matches web names (e.g. www.zyxel.com) to IP numbers.
FINGER(TCP:79)	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP(TCP:20.21)	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323(TCP:1720)	NetMeeting uses this protocol.
HTTP(TCP:80)	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS(TCP:443)	HTTPS is a secured http session often used in e-commerce.
ICQ(UDP:4000)	This is a popular Internet chat program.
IKE(UDP:500)	The Internet Key Exchange algorithm is used for key distribution and management.
IPSEC_TUNNEL(AH:0)	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
IPSEC_TUNNEL(ESP:0)	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
IRC(TCP/UDP:6667)	This is another popular Internet chat program.

Table 57 Available Services (continued)

SERVICE	DESCRIPTION
MSN Messenger(TCP:1863)	Microsoft Networks' messenger service uses this protocol.
MULTICAST(IGMP:0)	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
NEW-ICQ(TCP:5190)	An Internet chat program.
NEWS(TCP:144)	A protocol for news groups.
NFS(UDP:2049)	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP(TCP:119)	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING(ICMP:0)	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
PING(ICMP:0)	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
PPTP(TCP:1723)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL(GRE:0)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the data channel.
RCMD(TCP:512)	Remote Command Service.
REAL_AUDIO(TCP:7070)	A streaming audio service that enables real time sound over the web.
REXEC(TCP:514)	Remote Execution Daemon.
RLOGIN(TCP:513)	Remote Login.
RTELNET(TCP:107)	Remote Telnet.
RTSP(TCP/UDP:554)	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP(TCP:115)	Simple File Transfer Protocol.
SMTP(TCP:25)	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP(TCP/UDP:161)	Simple Network Management Program.
SNMP-TRAPS(TCP/ UDP:162)	Traps for use with the SNMP (RFC:1215).
SQL-NET(TCP:1521)	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH(TCP/UDP:22)	Secure Shell Remote Login Program.
STRM WORKS(UDP:1558)	Stream Works Protocol.
SYSLOG(UDP:514)	Syslog allows you to send system logs to a UNIX server.
TACACS(UDP:49)	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET(TCP:23)	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.

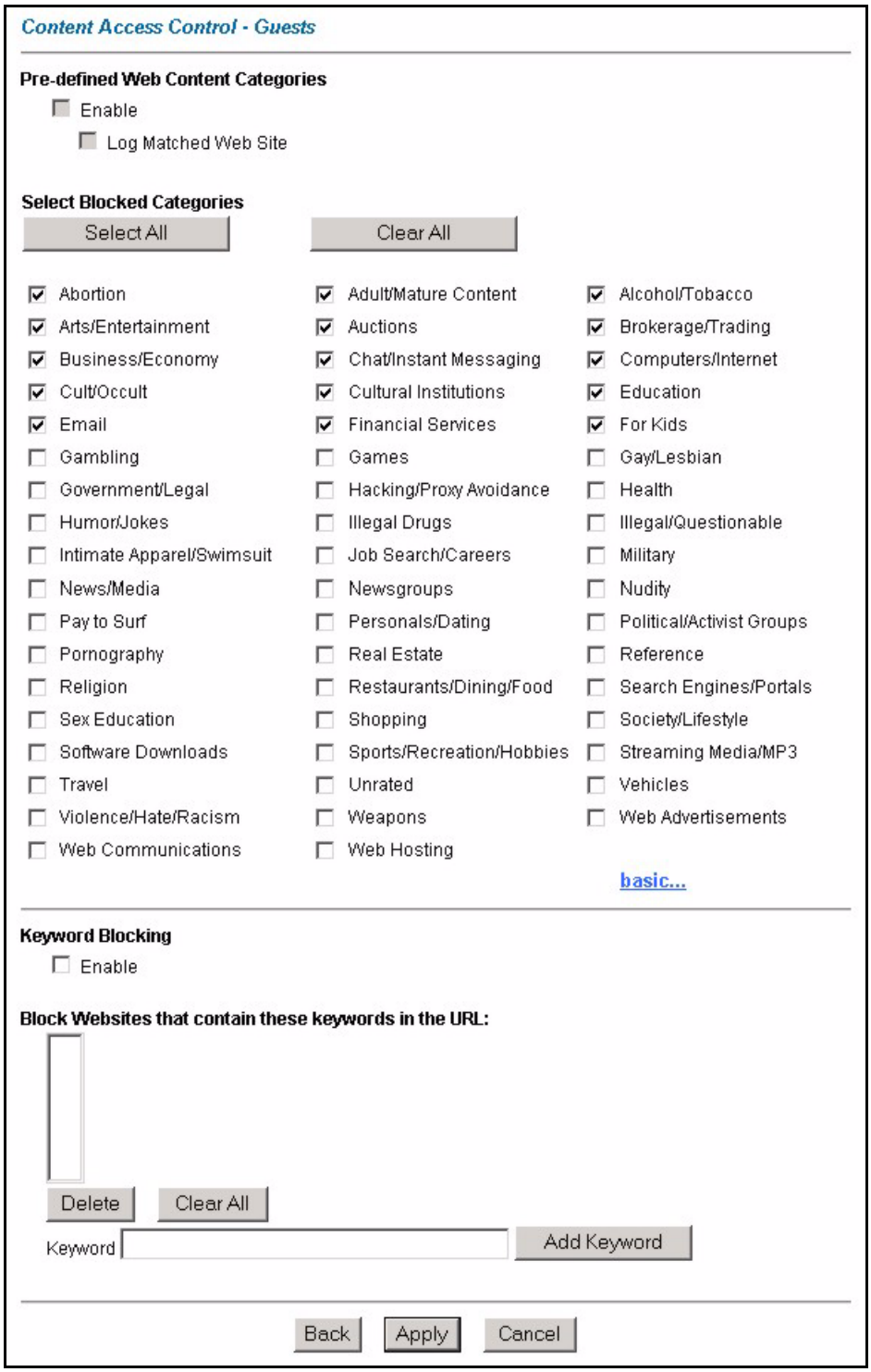
Table 57 Available Services (continued)

SERVICE	DESCRIPTION
TFTP(UDP:69)	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE(TCP:7000)	Another videoconferencing solution.

16.2.3 Configuring Web Site Filters

To enable content filtering and to configure URL keyword blocking for a user group, click **Edit** under **Web Browsing** in the **Content Access Control: General** screen. A screen displays as shown next.

Figure 79 Content Access Control: General: Web Site Filter



The following table describes the labels in this screen.

Table 58 Content Access Control: General: Web Site Filter

LABEL	DESCRIPTION
Pre-defined Web Content Categories	Enable **Pre-defined Web Content Categories** to have the Prestige check an external database to find to which category a requested web page belongs. The Prestige then blocks or forwards access to the web page depending on the configuration of the rest of this page.
Enable	This field is applicable when you have successfully registered for and activated the content filtering services. Refer to the User's Guide for more information. Select this option to start using the external content filtering service on the Prestige.
Log Matched Web Site	Select this option to record attempts to access prohibited web pages.
Select Blocked Categories	Use this section to prevent users from accessing web pages that match the categories that you select below.
Select All	Select this check box to restrict access to all site categories listed below.
Clear All	Select this check box to clear the selected categories below.
Adult/Mature Content	Selecting this category excludes pages that contain material of adult nature that does not necessarily contain excessive violence, sexual content, or nudity. These pages include very profane or vulgar content and pages that are not appropriate for children.
Pornography	Selecting this category excludes pages that contain sexually explicit material for the purpose of arousing a sexual or prurient interest.
Sex Education	Selecting this category excludes pages that provide graphic information (sometimes graphic) on reproduction, sexual development, safe sex practices, sexuality, birth control, and sexual development. It also includes pages that offer tips for better sex as well as products used for sexual enhancement.
Intimate Apparel/ Swimsuit	Selecting this category excludes pages that contain images or offer the sale of swimsuits or intimate apparel or other types of suggestive clothing. It does not include pages selling undergarments as a subsection of other products offered.
Nudity	Selecting this category excludes pages containing nude or seminude depictions of the human body. These depictions are not necessarily sexual in intent or effect, but may include pages containing nude paintings or photo galleries of artistic nature. This category also includes nudist or naturist pages that contain pictures of nude individuals.
Alcohol/Tobacco	Selecting this category excludes pages that promote or offer the sale alcohol/ tobacco products, or provide the means to create them. It also includes pages that glorify, tout, or otherwise encourage the consumption of alcohol/ tobacco. It does not include pages that sell alcohol or tobacco as a subset of other products.
Illegal/Questionable	Selecting this category excludes pages that advocate or give advice on performing illegal acts such as service theft, evading law enforcement, fraud, burglary techniques and plagiarism. It also includes pages that provide or sell questionable educational materials, such as term papers.

Table 58 Content Access Control: General: Web Site Filter (continued)

LABEL	DESCRIPTION
Gambling	Selecting this category excludes pages where a user can place a bet or participate in a betting pool (including lotteries) online. It also includes pages that provide information, assistance, recommendations, or training on placing bets or participating in games of chance. It does not include pages that sell gambling related products or machines. It also does not include pages for offline casinos and hotels (as long as those pages do not meet one of the above requirements).
Violence/Hate/Racism	Selecting this category excludes pages that depict extreme physical harm to people or property, or that advocate or provide instructions on how to cause such harm. It also includes pages that advocate, depict hostility or aggression toward, or denigrate an individual or group on the basis of race, religion, gender, nationality, ethnic origin, or other characteristics.
Weapons	Selecting this category excludes pages that sell, review, or describe weapons such as guns, knives or martial arts devices, or provide information on their use, accessories, or other modifications. It does not include pages that promote collecting weapons, or groups that either support or oppose weapons use.
Abortion	Selecting this category excludes pages that provide information or arguments in favor of or against abortion, describe abortion procedures, offer help in obtaining or avoiding abortion, or provide information on the effects, or lack thereof, of abortion.
Arts/Entertainment	Selecting this category excludes pages that promote and provide information about motion pictures, videos, television, music and programming guides, books, comics, movie theatres, galleries, artists or reviews on entertainment.
Business/Economy	Selecting this category excludes pages devoted to business firms, business information, economics, marketing, business management and entrepreneurship. This does not include pages that perform services that are defined in another category (such as Information Technology companies, or companies that sell travel services).
Cult/Occult	Selecting this category excludes pages that promote or offer methods, means of instruction, or other resources to affect or influence real events through the use of spells, curses, magic powers and satanic or supernatural beings.
Illegal Drugs	Selecting this category excludes pages that promote, offer, sell, supply, encourage or otherwise advocate the illegal use, cultivation, manufacture, or distribution of drugs, pharmaceuticals, intoxicating plants or chemicals and their related paraphernalia.
Education	Selecting this category excludes pages that offer educational information, distance learning and trade school information or programs. It also includes pages that are sponsored by schools, educational facilities, faculty, or alumni groups.
Cultural Institutions	Selecting this category excludes pages sponsored by cultural institutions, or those that provide information about museums, galleries, and theaters (not movie theaters). It includes groups such as 4H and the Boy Scouts of America.
Financial Services	Selecting this category excludes pages that provide or advertise banking services (online or offline) or other types of financial information, such as loans. It does not include pages that offer market information, brokerage or trading services.
Brokerage/Trading	Selecting this category excludes pages that provide or advertise trading of securities and management of investment assets (online or offline). It also includes insurance pages, as well as pages that offer financial investment strategies, quotes, and news.

Table 58 Content Access Control: General: Web Site Filter (continued)

LABEL	DESCRIPTION
Games	Selecting this category excludes pages that provide information and support game playing or downloading, video games, computer games, electronic games, tips, and advice on games or how to obtain cheat codes. It also includes pages dedicated to selling board games as well as journals and magazines dedicated to game playing. It includes pages that support or host online sweepstakes and giveaways.
Government/Legal	Selecting this category excludes pages sponsored by or which provide information on government, government agencies and government services such as taxation and emergency services. It also includes pages that discuss or explain laws of various governmental entities.
Military	Selecting this category excludes pages that promote or provide information on military branches or armed services.
Political/Activist Groups	Selecting this category excludes pages sponsored by or which provide information on political parties, special interest groups, or any organization that promotes change or reform in public policy, public opinion, social practice, or economic activities.
Health	Selecting this category excludes pages that provide advice and information on general health such as fitness and well-being, personal health or medical services, drugs, alternative and complimentary therapies, medical information about ailments, dentistry, optometry, general psychiatry, self-help, and support organizations dedicated to a disease or condition.
Computers/Internet	Selecting this category excludes pages that sponsor or provide information on computers, technology, the Internet and technology-related organizations and companies.
Hacking/Proxy Avoidance	Pages providing information on illegal or questionable access to or the use of communications equipment/software, or provide information on how to bypass proxy server features or gain access to URLs in any way that bypasses the proxy server.
Search Engines/Portals	Selecting this category excludes pages that support searching the Internet, indices, and directories.
Web Communications	Selecting this category excludes pages that allow or offer Web-based communication via e-mail, chat, instant messaging, message boards, etc.
Job Search/Careers	Selecting this category excludes pages that provide assistance in finding employment, and tools for locating prospective employers.
News/Media	Selecting this category excludes pages that primarily report information or comments on current events or contemporary issues of the day. It also includes radio stations and magazines. It does not include pages that can be rated in other categories.
Personals/Dating	Selecting this category excludes pages that promote interpersonal relationships.
Reference	Selecting this category excludes pages containing personal, professional, or educational reference, including online dictionaries, maps, census, almanacs, library catalogues, genealogy-related pages and scientific information.
Chat/Instant Messaging	Selecting this category excludes pages that provide chat or instant messaging capabilities or client downloads.
Email	Selecting this category excludes pages offering web-based email services, such as online email reading, e-cards, and mailing list services.
Newsgroups	Selecting this category excludes pages that offer access to Usenet news groups or other messaging or bulletin board systems.

Table 58 Content Access Control: General: Web Site Filter (continued)

LABEL	DESCRIPTION
Religion	Selecting this category excludes pages that promote and provide information on conventional or unconventional religious or quasi-religious subjects, as well as churches, synagogues, or other houses of worship. It does not include pages containing alternative religions such as Wicca or witchcraft (Cult/Occult) or atheist beliefs (Political/Activist Groups).
Shopping	Selecting this category excludes pages that provide or advertise the means to obtain goods or services. It does not include pages that can be classified in other categories (such as vehicles or weapons).
Auctions	Selecting this category excludes pages that support the offering and purchasing of goods between individuals. This does not include classified advertisements.
Real Estate	Selecting this category excludes pages that provide information on renting, buying, or selling real estate or properties.
Society/Lifestyle	Selecting this category excludes pages providing information on matters of daily life. This does not include pages relating to entertainment, sports, jobs, sex or pages promoting alternative lifestyles such as homosexuality. Personal homepages fall within this category if they cannot be classified in another category.
Gay/Lesbian	Selecting this category excludes pages that provide information, promote, or cater to gay and lesbian lifestyles. This does not include pages that are sexually oriented.
Restaurants/Dining/ Food	Selecting this category excludes pages that list, review, discuss, advertise and promote food, catering, dining services, cooking and recipes.
Sports/Recreation/ Hobbies	Selecting this category excludes pages that promote or provide information about spectator sports, recreational activities, or hobbies. This includes pages that discuss or promote camping, gardening, and collecting.
Travel	Selecting this category excludes pages that promote or provide opportunity for travel planning, including finding and making travel reservations, vehicle rentals, descriptions of travel destinations, or promotions for hotels or casinos.
Vehicles	Selecting this category excludes pages that provide information on or promote vehicles, boats, or aircraft, including pages that support online purchase of vehicles or parts.
Humor/Jokes	Selecting this category excludes pages that primarily focus on comedy, jokes, fun, etc. This may include pages containing jokes of adult or mature nature. Pages containing humorous Adult/Mature content also have an Adult/Mature category rating.
Streaming Media/MP3	Selecting this category excludes pages that sell, deliver, or stream music or video content in any format, including pages that provide downloads for such viewers.
Software Downloads	Selecting this category excludes pages that are dedicated to the electronic download of software packages, whether for payment or at no charge.
Pay to Surf	Selecting this category excludes pages that pay users in the form of cash or prizes, for clicking on or reading specific links, email, or web pages.
For Kids	Selecting this category excludes pages designed specifically for children.
Web Advertisements	Selecting this category excludes pages that provide online advertisements or banners. This does not include advertising servers that serve adult-oriented advertisements.
Web Hosting	Selecting this category excludes pages of organizations that provide top-level domain pages, as well as web communities or hosting services.

Table 58 Content Access Control: General: Web Site Filter (continued)

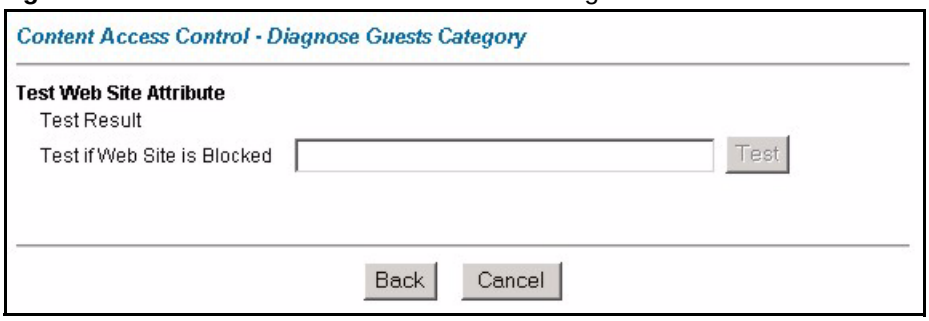
LABEL	DESCRIPTION
More/Basic	Click **more...** to see an expanded list of categories, or click **basic...** to see a smaller list.
Keyword Blocking	Select the **Enable** check box to block the URL containing the keywords in the keyword list.
Block Websites that contain these keywords in the URL	Type a keyword in this field. You may use any character (up to 64 characters). Wildcards are not allowed.
Delete	Select a keyword from the keyword list and then click **Delete** to remove this keyword from the list.
Clear All	Click **Clear All** to empty the keyword list.
Keyword	Type a keyword in the **Keyword** field and click then **Add Keyword** to add a keyword to the list of keywords. The list of keywords that will be inaccessible to computers on your LAN once you enable URL keyword blocking.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to return to the previously saved settings.

16.2.4 Testing Web Site Access Privileges

To check the access restrictions of a web site, click **Diagnose** under **Web Browsing** in the **Content Access Control: General** screen. A screen displays as shown next.

The Prestige first checks the web site address for the specified keyword(s) to block. If the web site address does not contain any blocking keywords, the Prestige then checks the rating information on the remote content filtering database (provided that you have successfully registered for and activated this service) and block or allow access depending on the rating information of the web site.

Figure 80 Content Access Control: General: Diagnose



The following table describes the labels in this screen.

Table 59 Content Access Control: General: Diagnose

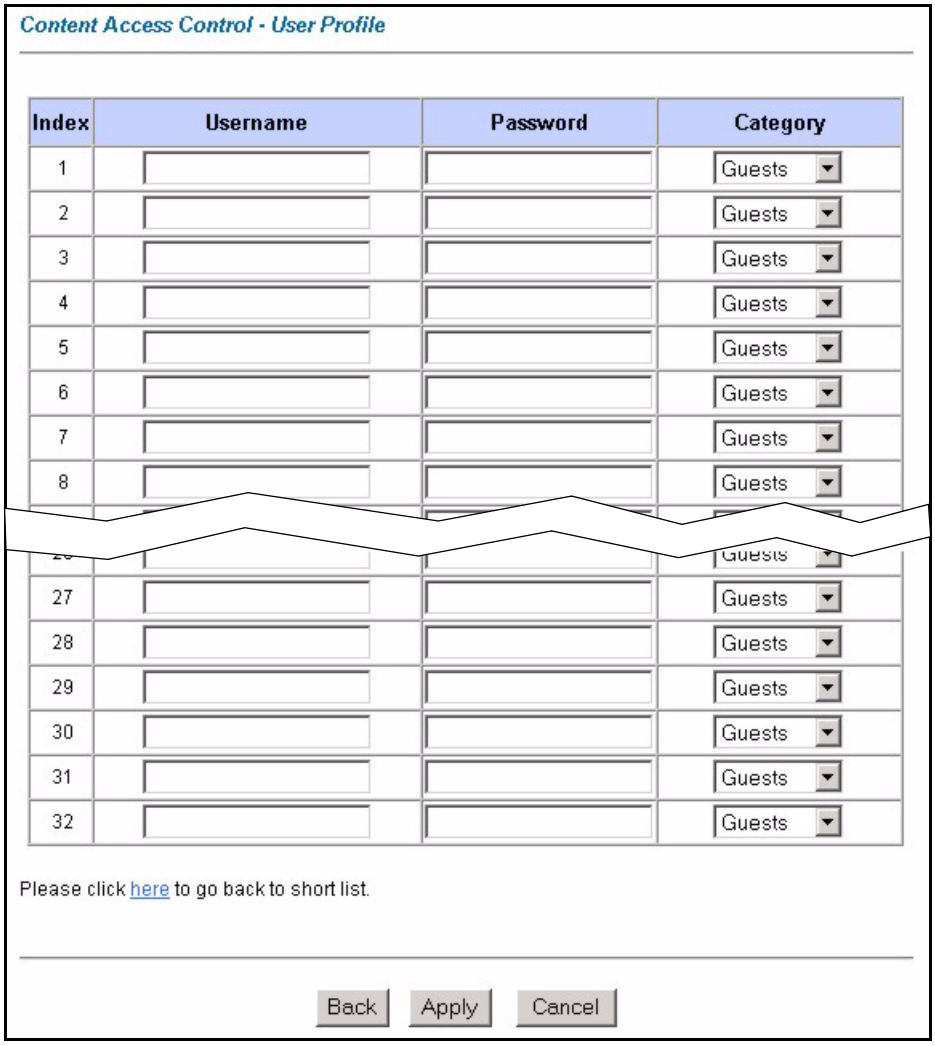
LABEL	DESCRIPTION
Test Web Site Attribute	
Test Result	This field displays the web site address check result.
Test if web site is blocked	Enter the URL or web site address in the field provided and click **Test** to check the access restrictions of the web site.
Test	This button is applicable when you have either activated and/or configured keyword blocking or registered and activated the content filtering service. Click **Test** to check the access privileges of the specified web site address.
Back	Click **Back** to return to the previous screen.
Cancel	Click **Cancel** to return to the previously saved settings.

16.3 User Account Setup

With Content Access Control, the Prestige requires LAN users to login with valid username and password before they are allowed to access the Internet.

Use the **User Profile** screen to set up user accounts. From the **Site Map** screen, click **Content Access Control** and **User Profiles** to display the screen as shown next.

Figure 81 Content Access Control: User Profiles



The following table describes the labels in this screen.

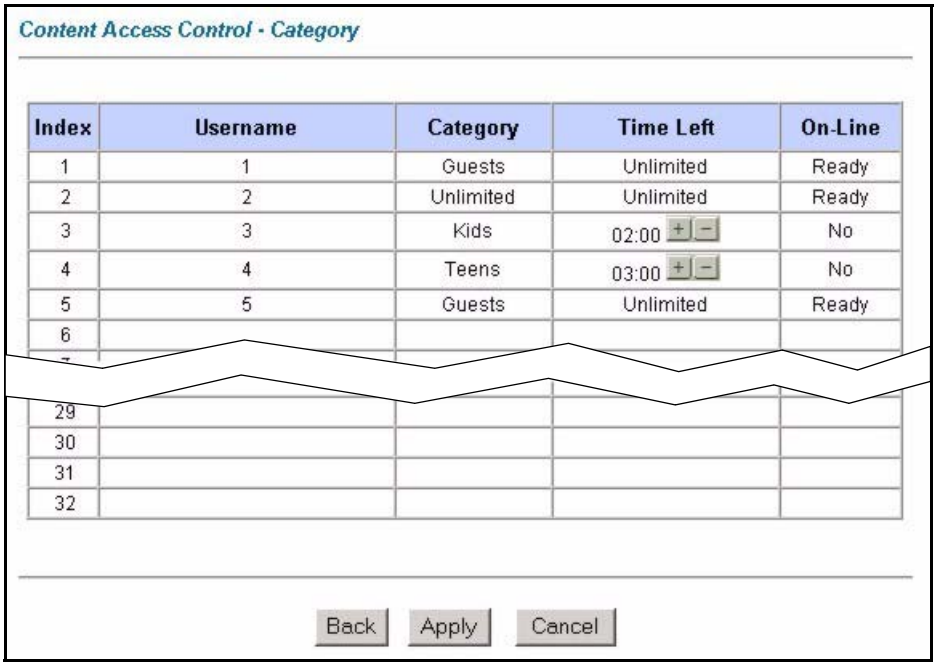
Table 60 Content Access Control: User Profiles

LABEL	DESCRIPTION
Index	This field displays the index number.
Username	Enter the user name for this account.
Password	Enter a password associated to the user name above.
Category	Select a user group from the drop-down list box to associate this user account to the user group. The drop-down list box displays the name of the user group you configure in the **General** screen.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to return to the previously saved settings.

16.4 User Online Status

To view the online status of each user, click **Content Access Control** in the **Site Map** screen and click **Online Status** to display the screen as shown.

Figure 82 Content Access Control: Online Status



The following table describes the labels in this screen.

Table 61 Content Access Control: Online Status

LABEL	DESCRIPTION
Index	This field displays the index number.
Username	This field displays the username (up to 30 characters) for this user profile.
Group	This field displays the name of the associated user group.
Time Left	This field displays the amount of time that you have before the Prestige logs you out and terminates your Internet access. This time depends on the time allowance configured in **Time Scheduling** screen. By using the **+** or – buttons, the administrator can increase or decrease the time left in 15 minute increments without re-configuring the time allowances.
On-Line	This field displays **Yes** if a user is currently on-line. This field displays **Ready** if a user is allowed to access the Internet at the moment and is currently not on-line. This field displays **No** if a user is not allowed to access the Internet at the moment and is currently not on-line.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to return to the previously saved settings.

16.5 Content Access Control Logins

The following sections describe the user and administrator login experience.

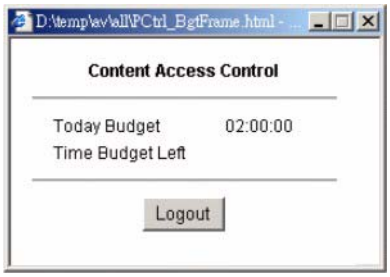
16.5.1 User Login

1. Once the initial configuration is complete, a computer on the network cannot gain Internet access without first logging into the Prestige.
2. When you attempt to access a website, you are directed to the Prestige's user login screen.

Figure 83 Content Access Control: User Login Screen

3. After you enter your login name and password the Prestige checks the access profile and begins enforcing the access control restriction as defined by the administrator.
4. The access privileges remain in force until you log out.
5. After a successful login, the system launches a small pop-up window that displays the remaining budget time and a logout button.

Figure 84 Content Access Control: User Logout Screen



There are four ways to be logged out of the system.

- Click the **Logout** button in the user logout screen.
- The idle timeout triggers the logout (the default is ten minutes).
- The access time allowance budget reaches zero and triggers the logout.
- The system clock reaches the end time for the user's account and triggers the logout.

16.5.2 Administrator Login

The administrator can log into the system.

- The administrator opens their browser and is directed to the Prestige user login page (this is the same as the user login).
- The administrator enters "admin" as the username and the system password.
- The system administrator **Site Map** screen opens.

CHAPTER 17
Anti-Virus Packet Scan

This chapter introduces and shows you how to configure the anti-virus packet scan.

17.1 Overview

A computer virus is a small program designed to corrupt and/or alter the operation of other legitimate programs. A worm is a self-replicating virus that resides in active memory and duplicates itself. The effect of a virus attack varies from doing so little damage that you are unaware your computer is infected to wiping out the entire contents of a hard drive to rendering your computer inoperable.

17.1.1 Types of Computer Viruses

The following table describes some of the common computer viruses.

Table 62 Common Computer Virus Types

TYPE	DESCRIPTION
File Infector	This is a small program that embeds itself in a legitimate program. A file infector is able to copy and attach itself to other programs that are executed on an infected computer.
Boot Sector Virus	This type of virus infects the area of a hard drive that a computer reads and executes during startup. The virus causes computer crashes and to some extend renders the infected computer inoperable.
Macro Virus	Macros are small programs that are created to perform repetitive actions. Macros run automatically when a file to which they are attached is opened. Macro viruses spread more rapidly than other types of viruses as data files are often shared on a network.
E-mail Virus	E-mail viruses are malicious programs that spread through e-mail. These can infect your computer even if you do not read the e-mail messages.

17.2 Signature-Based Virus Scan

The "signature-based" approach is the most common way to detect the presence of viruses. Signature-based anti-virus scanning consists of two key components: a pattern file that contains the signatures for known viruses and a scanning engine.

Signatures are byte patterns that are unique to a particular virus. These signatures are stored in a pattern file. The scanning engine compares the files with the signatures in the pattern file.

For maximum protection, you must keep the pattern file up-to-date.

17.2.1 Computer Virus Infection and Prevention

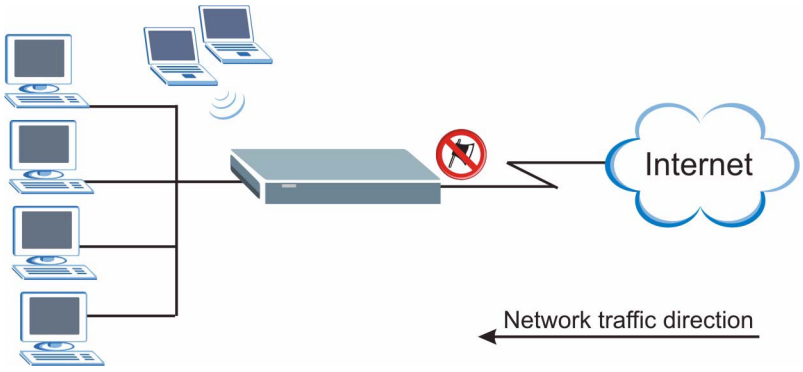
The follow describes a simplistic life cycle of a computer virus.

1. A computer gets a copy of a virus from an unknown source (such as the Internet, e-mail, file sharing or any removable storage media). The virus is harmless until the execution of an infected program.
2. The virus spreads to other files and programs on the computer.
3. The infected files are unintentionally sent to another computer thus starting the spread of the virus.
4. Once the virus is spread through the network, the number of infected networked computers can grow exponentially.
5. To prevent the spread of viruses, you need to install host-based anti-virus software on a computer or buy an anti-virus system.

17.3 Introduction to the Prestige Anti-virus Packet Scan

The Prestige has an integrated signature-based anti-virus packet scan. Set up the Prestige between your local network and the Internet. This way the Prestige can scan incoming traffic to your local network from the Internet. Thus the Prestige helps stop threats at the network edge before they reach the local host computers.

Figure 85 Prestige Anti-virus Application



Your Prestige is able to scan the following network traffic types for viruses:

- HTTP (Hyper Text Transfer Protocol)

  This is the most common protocol used on the Internet. HTTP is the primary protocol used for web sites and web browsers.
- Mail messages (SMPT, POP3)
- FTP (File Transfer Protocol)

This is an Internet file transfer service that operates on the Internet and over TCP/IP networks. A system running the FTP server accepts commands from a system running an FTP client. The service allows users to send commands to the server for uploading and downloading files.

Note: The anti-virus packet scan on the Prestige offers the first defense against possible virus attacks on your network. It is not a replacement of the anti-virus client software that you may install on network computers.

17.3.1 How the Prestige Virus Scan Works

The following describes the virus scanning process on the Prestige.

1. The Prestige first identifies the packet types (SMTP, POP3, HTTP and FTP) from the network traffic.
2. If the packets are not session connection setup packets (such as SYN, ACK and FIN), the Prestige records the sequence of the packets.
3. The scanning engine scans the content of the packet for virus.
4. If a virus pattern is matched, the Prestige "cleans" the virus by deleting the infected packet and alerts the intended computer user(s).

Note: Since the Prestige "destroys" a file by deleting the infected portion of the file content, you cannot open the file.

17.3.2 Limitations of the Prestige Packet Scan

The Prestige does not scan the following types of file for virus:

- Compressed or zipped files
- Simultaneous file downloads (for example, when you use the FlashGet download program).
- When a virus is detected, an alert message is displayed in Miscrosoft Windows-based operation systems only.[2]

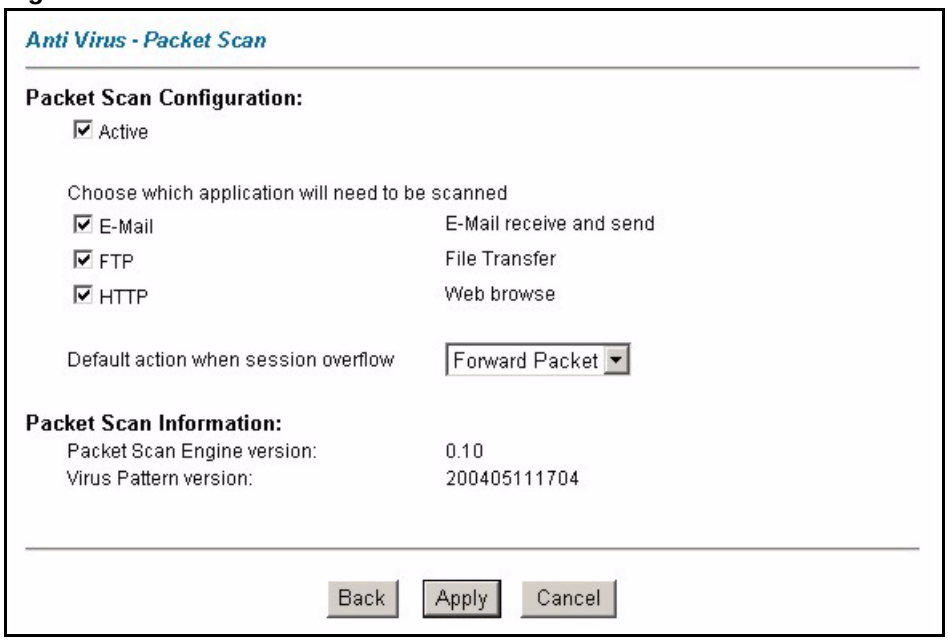
2. For Windows 98/Me, refer to the Windows 98/Me Requirements for Anti-Virus Packet Scan Message Display appendix for requirements.

17.4 Anti-virus Packet Scan Configuration

Note: Before you can use the anti-virus packet scan on the Prestige, you must register for the anti-virus service in the **Registration and Virus Information Update** screen (see the Registration and Online Update section for more information).

Click **Anti Virus** and **Packet Scan** to display the configuration screen as shown next.

Figure 86 Anti Virus: Packet Scan



The following table describes the labels in this screen.

Table 63 Anti Virus: Packet Scan

LABEL	DESCRIPTION
Packet Scan Configuration	
Active	Select this check box to enable the anti virus packet scan on the Prestige. Clear this check box to disable it. Before you activate the anti virus packet scan, register for the service in the **Registration and Virus Information Update** screen (refer to *Section* for more information).
Choose which application to be scanned:	
E-Mail	Select this option to scan incoming/outgoing e-mail content for viruses.
FTP	Select this option to scan FTP traffic for viruses.
HTTP	Select this option to scan HTTP traffic for viruses.

Table 63 Anti Virus: Packet Scan (continued)

LABEL	DESCRIPTION
Default action when session overflow	Select whether to allow passage of (**Forward Packet**) or silently discard (**Block Packet**) the packets of new connections when the maximum number of opened connections is reached (default is 300 connections at a time).
Packet Scan Information	
Packet Scan Engine Version	This read-only field displays the version of the scanning engine on the Prestige.
Virus Pattern Version	This read-only field displays the version number of the virus pattern. It is recommended that you update the pattern file regularly in the **Registration and Virus Information Update** screen (refer to the Registration and Online Update section for more information).
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to return to the previously saved settings.

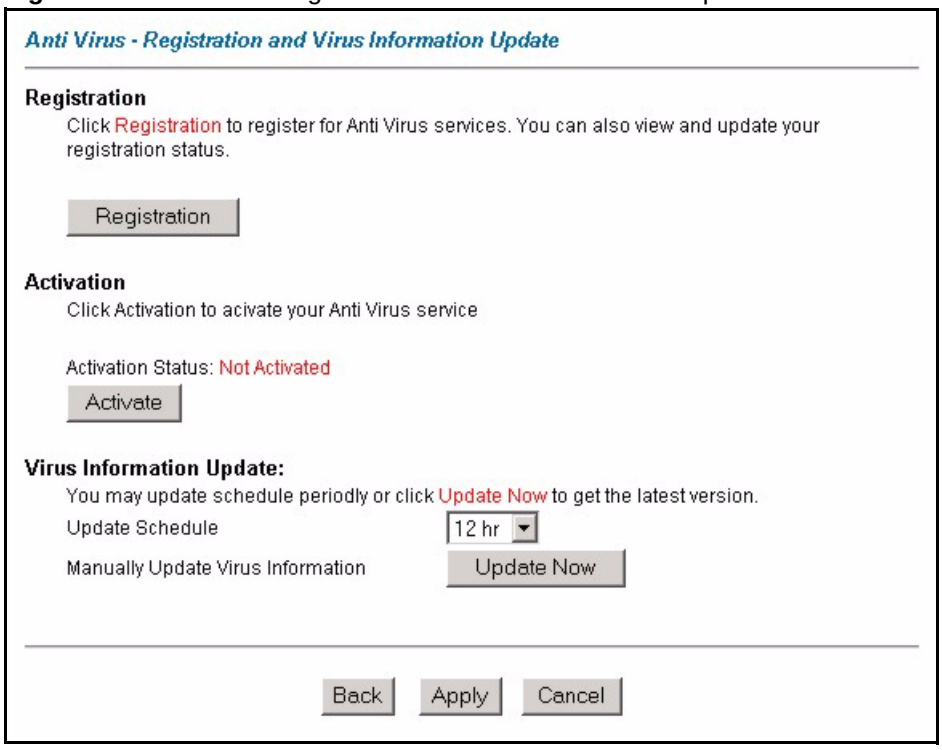
17.5 Registration and Online Update

Use the **Registration and Virus Information Update** screen to register for and activate the anti-virus packet scan feature on the Prestige. You can also configure a schedule for the Prestige to automatically update the virus pattern file in this screen.

Click **Anti Virus** and **Registration and Virus Information Update** to display the screen as shown.

Note: The Prestige automatically restarts after the virus scan update is complete.

Figure 87 Anti Virus: Registration and Virus Information Update



The following table describes the labels in this screen.

Table 64 Anti Virus: Registration and Virus Information Update

LABEL	DESCRIPTION
Registration	You must register for the anti-virus service before you can use the packet scan feature on the Prestige. Registering for the service allows you to activate packet scan and download the virus pattern file. Click **Registration** and follow the online instructions to register. Refer to the myZyXEL.com appendix for more information.
Activation	After you have successfully registered for the anti-virus service, click **Activate** to enable and start using the anti-virus feature.This also sets the Prestige to automatically update the pattern file.
Virus Information Update	Set the fields below to configure the Prestige to automatically update the pattern file.
Update Schedule	This drop-down menu is used to configure the frequency of the automatic pattern file update. Choices are **1 hr**, **12 hr** and **24 hr**.
Manually Update Virus Information	Click **Update Now** to download and update to the latest pattern file.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to return to the previously saved settings.

17.5.1 Updating the Anti Virus Packet Scan

Follow the steps below to update the virus scan on the Prestige manually.

Note: Do not turn off the Prestige while the virus scan update is in progress!

1 In the **Registration and Virus Information Update** screen, click **Update Now**. An update progress screen displays as shown.

Figure 88 Virus Scan Update in Progress

2 After the virus scan update is successful, a screen displays as shown.

Figure 89 Virus Scan Update Successful

Note: The Prestige automatically restarts after the virus scan update is complete.

CHAPTER 18
Introduction to IPSec

This chapter introduces the basics of IPSec VPNs.

18.1 VPN Overview

A VPN (Virtual Private Network) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing technologies/services used to transport traffic over the Internet or any insecure network that uses the TCP/IP protocol suite for communication.

18.1.1 IPSec

Internet Protocol Security (IPSec) is a standards-based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer.

18.1.2 Security Association

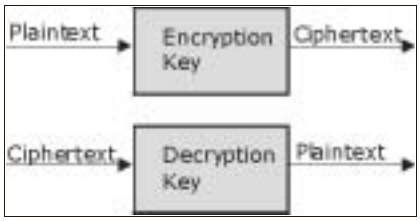
A Security Association (SA) is a contract between two parties indicating what security parameters, such as keys and algorithms they will use.

18.1.3 Other Terminology

18.1.3.1 Encryption

Encryption is a mathematical operation that transforms data from "plaintext" (readable) to "ciphertext" (scrambled text) using a "key". The key and clear text are processed by the encryption operation, which leads to the data scrambling that makes encryption secure. Decryption is the opposite of encryption: it is a mathematical operation that transforms “ciphertext” to plaintext. Decryption also requires a key.

Figure 90 Encryption and Decryption



18.1.3.2 Data Confidentiality

The IPSec sender can encrypt packets before transmitting them across a network.

18.1.3.3 Data Integrity

The IPSec receiver can validate packets sent by the IPSec sender to ensure that the data has not been altered during transmission.

18.1.3.4 Data Origin Authentication

The IPSec receiver can verify the source of IPSec packets. This service depends on the data integrity service.

18.1.4 VPN Applications

The Prestige supports the following VPN applications.

- Linking Two or More Private Networks Together

  Connect branch offices and business partners over the Internet with significant cost savings and improved performance when compared to leased lines between sites.

- Accessing Network Resources When NAT Is Enabled

  When NAT is enabled, remote users are not able to access hosts on the LAN unless the host is designated a public LAN server for that specific protocol. Since the VPN tunnel terminates inside the LAN, remote users will be able to access all computers that use private IP addresses on the LAN.

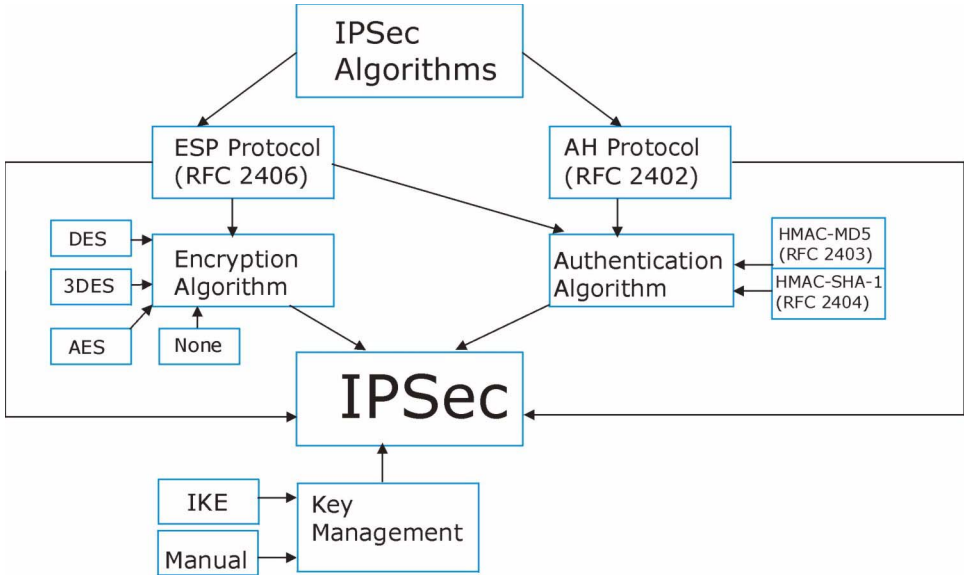
- Unsupported IP Applications

  A VPN tunnel may be created to add support for unsupported emerging IP applications. See the chapter on *Getting to Know Your Prestige* for an example of a VPN application.

18.2 IPSec Architecture

The overall IPSec architecture is shown as follows.

Figure 91 IPSec Architecture



18.2.1 IPSec Algorithms

The **ESP** (Encapsulating Security Payload) Protocol (RFC 2406) and **AH** (Authentication Header) protocol (RFC 2402) describe the packet formats and the default standards for packet structure (including implementation algorithms).

The Encryption Algorithm describes the use of encryption techniques such as DES (Data Encryption Standard) and Triple DES algorithms.

The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404, provide an authentication mechanism for the **AH** and **ESP** protocols. Please see the IPSec Algorithms section for more information.

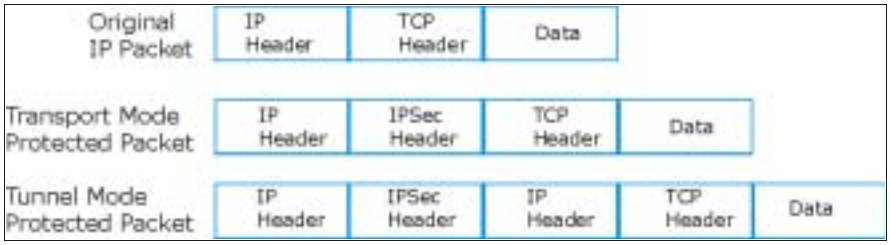
18.2.2 Key Management

Key management allows you to determine whether to use IKE (ISAKMP) or manual key configuration in order to set up a VPN.

18.3 Encapsulation

The two modes of operation for IPSec VPNs are **Transport** mode and **Tunnel** mode.

Figure 92 Transport and Tunnel Mode IPSec Encapsulation



18.3.1 Transport Mode

Transport mode is used to protect upper layer protocols and only affects the data in the IP packet. In **Transport** mode, the IP packet contains the security protocol (**AH** or **ESP**) located after the original IP header and options, but before any upper layer protocols contained in the packet (such as TCP and UDP).

With **ESP,** protection is applied only to the upper layer protocols contained in the packet. The IP header information and options are not used in the authentication process. Therefore, the originating IP address cannot be verified for integrity against the data.

With the use of **AH** as the security protocol, protection is extended forward into the IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process.

18.3.2 Tunnel Mode

Tunnel mode encapsulates the entire IP packet to transmit it securely. A **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation. **Tunnel** mode is required for gateway to gateway and host to gateway communications. **Tunnel** mode communications have two sets of IP headers:

- **Outside header**: The outside IP header contains the destination IP address of the VPN gateway.
- **Inside header**: The inside IP header contains the destination IP address of the final system behind the VPN gateway. The security protocol appears after the outer IP header and before the inside IP header.

18.4 IPSec and NAT

Read this section if you are running IPSec on a host computer behind the Prestige.

NAT is incompatible with the **AH** protocol in both **Transport** and **Tunnel** mode. An IPSec VPN using the **AH** protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet. When using **AH** protocol, packet contents (the data payload) are not encrypted.

A NAT device in between the IPSec endpoints will rewrite either the source or destination address with one of its own choosing. The VPN device at the receiving end will verify the integrity of the incoming packet by computing its own hash value, and complain that the hash value appended to the received packet doesn't match. The VPN device at the receiving end doesn't know about the NAT in the middle, so it assumes that the data has been maliciously altered.

IPSec using **ESP** in **Tunnel** mode encapsulates the entire original packet (including headers) in a new IP packet. The new IP packet's source address is the outbound address of the sending VPN gateway, and its destination address is the inbound address of the VPN device at the receiving end. When using **ESP** protocol with authentication, the packet contents (in this case, the entire original packet) are encrypted. The encrypted contents, but not the new headers, are signed with a hash value appended to the packet.

Tunnel mode **ESP** with authentication is compatible with NAT because integrity checks are performed over the combination of the "original header plus original payload," which is unchanged by a NAT device.

Transport mode **ESP** with authentication is not compatible with NAT, although NAT traversal provides a way to use **Transport** mode **ESP** when there is a NAT router between the IPSec endpoints (see the NAT Traversal section for details).

Table 65 VPN and NAT

SECURITY PROTOCOL	MODE	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	N
ESP	Tunnel	Y

CHAPTER 19
VPN Screens

This chapter introduces the VPN screens. See the Logs chapter for information on viewing logs and the appendix for IPSec log descriptions.

19.1 VPN/IPSec Overview

Use the screens documented in this chapter to configure rules for VPN connections and manage VPN connections.

19.2 IPSec Algorithms

The **ESP** and **AH** protocols are necessary to create a Security Association (SA), the foundation of an IPSec VPN. An SA is built from the authentication provided by the **AH** and **ESP** protocols. The primary function of key management is to establish and maintain the SA between systems. Once the SA is established, the transport of data may commence.

19.2.1 AH (Authentication Header) Protocol

AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and non-repudiation but not for confidentiality, for which the **ESP** was designed.

In applications where confidentiality is not required or not sanctioned by government encryption restrictions, an **AH** can be employed to ensure integrity. This type of implementation does not protect the information from dissemination but will allow for verification of the integrity of the information and authentication of the originator.

19.2.2 ESP (Encapsulating Security Payload) Protocol

The **ESP** protocol (RFC 2406) provides encryption as well as some of the services offered by **AH**. **ESP** authenticating properties are limited compared to the **AH** due to the non-inclusion of the IP header information during the authentication process. However, **ESP** is sufficient if only the upper layer protocols need to be authenticated.

An added feature of the **ESP** is payload padding, which further protects communications by concealing the size of the packet being transmitted.

Table 66 AH and ESP

ESP	AH
DES (default) Data Encryption Standard (DES) is a widely used method of data encryption using a private (secret) key. DES applies a 56-bit key to each 64-bit block of data.	**MD5** (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
3DES Triple DES (3DES) is a variant of DES, which iterates three times with three separate keys (3 x 56 = 168 bits), effectively doubling the strength of DES.	**SHA1** SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.
AES Advanced Encryption Standard is a newer method of data encryption that also uses a secret key. This implementation of AES applies a 128-bit key to 128-bit blocks of data. AES is faster than 3DES.	
Select **DES** for minimal security and **3DES** or **AES** for maximum. Select **NULL** to set up a tunnel without encryption.	Select **MD5** for minimal security and **SHA-1** for maximum security.

19.3 My IP Address

My IP Address is the WAN IP address of the Prestige. The Prestige has to rebuild the VPN tunnel if the My IP Address changes after setup.

The following applies if this field is configured as **0.0.0.0**:

- The Prestige uses the current Prestige WAN IP address (static or dynamic) to set up the VPN tunnel.
- If the WAN connection goes down, the Prestige uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. See the chapter on WAN for details on dial backup and traffic redirect.

19.4 Secure Gateway Address

Secure Gateway Address is the WAN IP address or domain name of the remote IPSec router (secure gateway).

If the remote secure gateway has a static WAN IP address, enter it in the **Secure Gateway Address** field. You may alternatively enter the remote secure gateway's domain name (if it has one) in the **Secure Gateway Address** field.

You can also enter a remote secure gateway's domain name in the **Secure Gateway Address** field if the remote secure gateway has a dynamic WAN IP address and is using DDNS. The Prestige has to rebuild the VPN tunnel each time the remote secure gateway's WAN IP address changes (there may be a delay until the DDNS servers are updated with the remote gateway's new WAN IP address).

19.4.1 Dynamic Secure Gateway Address

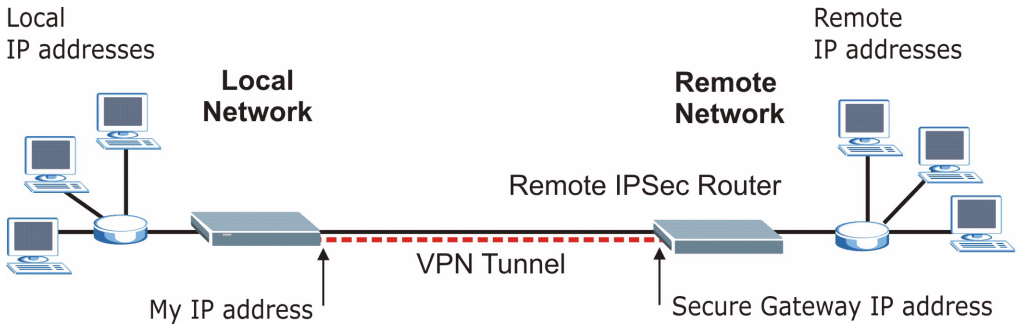
If the remote secure gateway has a dynamic WAN IP address and does not use DDNS, enter 0.0.0.0 as the secure gateway's address. In this case only the remote secure gateway can initiate SAs. This may be useful for telecommuters initiating a VPN tunnel to the company network (see the Telecommuter VPN/IPSec Examples section for configuration examples).

The Secure Gateway IP Address may be configured as 0.0.0.0 only when using **IKE** key management and not **Manual** key management.

19.5 VPN Summary Screen

The following figure helps explain the main fields in the web configurator.

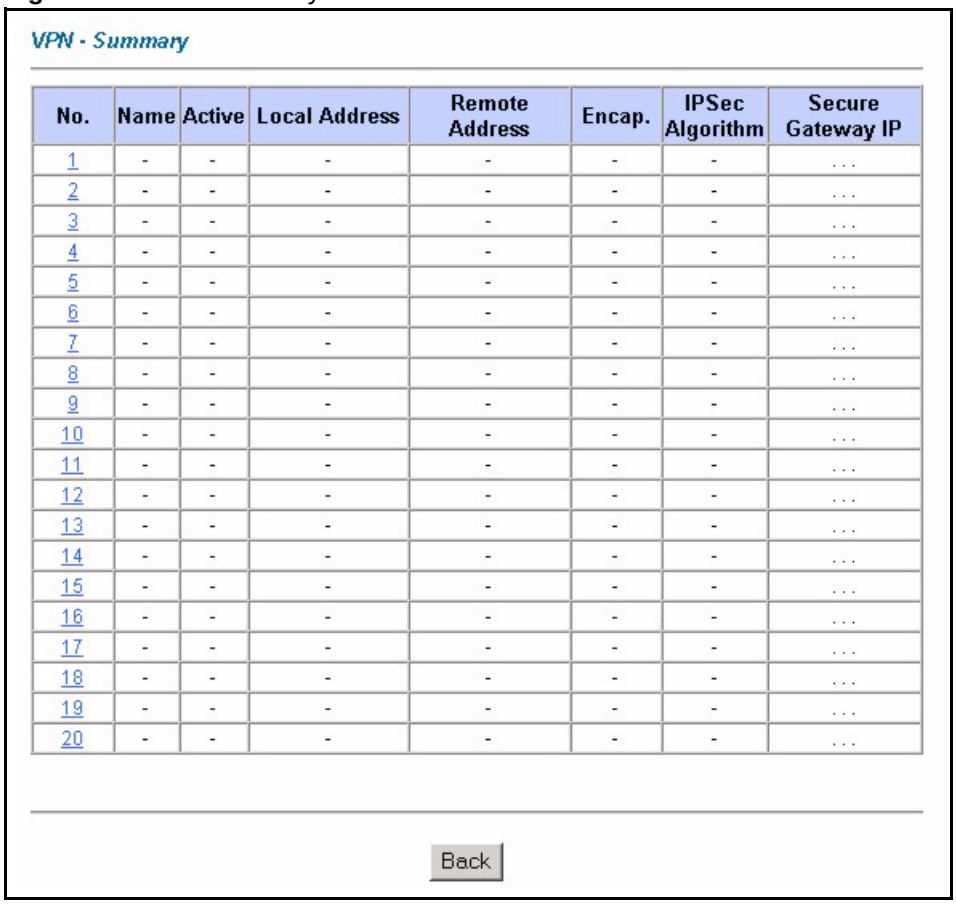
Figure 93 IPSec Summary Fields



Local and remote IP addresses must be static.

Click **VPN** and **Setup** to open the **VPN Summary** screen. This is a read-only menu of your IPSec rules (tunnels). The IPSec summary menu is read-only. Edit a VPN by selecting an index number and then configuring its associated submenus.

Figure 94 VPN Summary



The following table describes the fields in this screen.

Table 67 VPN Summary

LABEL	DESCRIPTION
No.	This is the VPN policy index number. Click a number to edit VPN policies.
Name	This field displays the identification name for this VPN policy.
Active	This field displays whether the VPN policy is active or not. A **Yes** signifies that this VPN policy is active. **No** signifies that this VPN policy is not active.
Local Address	This is the IP address(es) of computer(s) on your local network behind your Prestige. The same (static) IP address is displayed twice when the **Local Address Type** field in the **VPN-IKE** (or **VPN-Manual Key**) screen is configured to **Single**. The beginning and ending (static) IP addresses, in a range of computers are displayed when the **Local Address Type** field in the **VPN-IKE** (or **VPN-Manual Key**) screen is configured to **Range**. A (static) IP address and a subnet mask are displayed when the **Local Address Type** field in the **VPN-IKE** (or **VPN-Manual Key**) screen is configured to **Subnet**.

Table 67 VPN Summary (continued)

LABEL	DESCRIPTION
Remote Address	This is the IP address(es) of computer(s) on the remote network behind the remote IPSec router. This field displays **N/A** when the **Secure Gateway Address** field displays **0.0.0.0**. In this case only the remote IPSec router can initiate the VPN. The same (static) IP address is displayed twice when the **Remote Address Type** field in the **VPN-IKE** (or **VPN-Manual Key**) screen is configured to **Single**. The beginning and ending (static) IP addresses, in a range of computers are displayed when the **Remote Address Type** field in the **VPN-IKE** (or **VPN-Manual Key**) screen is configured to **Range**. A (static) IP address and a subnet mask are displayed when the **Remote Address Type** field in the **VPN-IKE** (or **VPN-Manual Key**) screen is configured to **Subnet**.
Encap.	This field displays **Tunnel** or **Transport** mode (**Tunnel** is the default selection).
IPSec Algorithm	This field displays the security protocols used for an SA. Both **AH** and **ESP** increase Prestige processing requirements and communications latency (delay).
Secure Gateway IP	This is the static WAN IP address or URL of the remote IPSec router. This field displays **0.0.0.0** when you configure the **Secure Gateway Address** field in the **VPN-IKE** screen to **0.0.0.0.**
Back	Click **Back** to return to the previous screen.

19.6 Keep Alive

When you initiate an IPSec tunnel with keep alive enabled, the Prestige automatically renegotiates the tunnel when the IPSec SA lifetime period expires (see the IKE Phases section for more on the IPSec SA lifetime). In effect, the IPSec tunnel becomes an "always on" connection after you initiate it. Both IPSec routers must have a Prestige-compatible keep alive feature enabled in order for this feature to work.

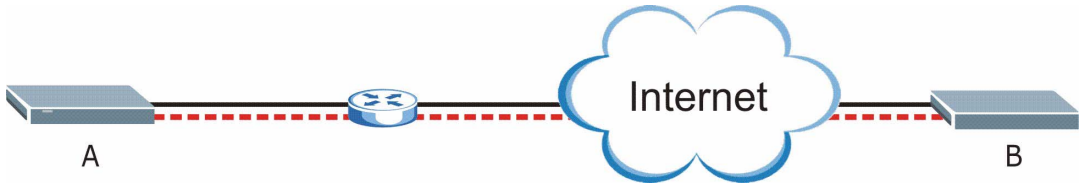
If the Prestige has its maximum number of simultaneous IPSec tunnels connected to it and they all have keep alive enabled, then no other tunnels can take a turn connecting to the Prestige because the Prestige never drops the tunnels that are already connected. Refer to the Features of the Prestige section to see how many simultaneous IPSec SAs your Prestige model can support.

When there is outbound traffic with no inbound traffic, the Prestige automatically drops the tunnel after two minutes.

19.7 NAT Traversal

NAT traversal allows you to set up a VPN connection when there are NAT routers between the two IPSec routers.

Figure 95 NAT Router Between IPSec Routers



Normally you cannot set up a VPN connection with a NAT router between the two IPSec routers because the NAT router changes the header of the IPSec packet. In the previous figure, IPSec router A sends an IPSec packet in an attempt to initiate a VPN. The NAT router changes the IPSec packet's header so it does not match the header for which IPSec router B is checking. Therefore, IPSec router B does not respond and the VPN connection cannot be built.

NAT traversal solves the problem by adding a UDP port 500 header to the IPSec packet. The NAT router forwards the IPSec packet with the UDP port 500 header unchanged. IPSec router B checks the UDP port 500 header and responds. IPSec routers A and B build a VPN connection.

19.7.1 NAT Traversal Configuration

For NAT traversal to work you must:

- Use ESP security protocol (in either transport or tunnel mode).
- Use IKE keying mode.
- Enable NAT traversal on both IPSec endpoints.

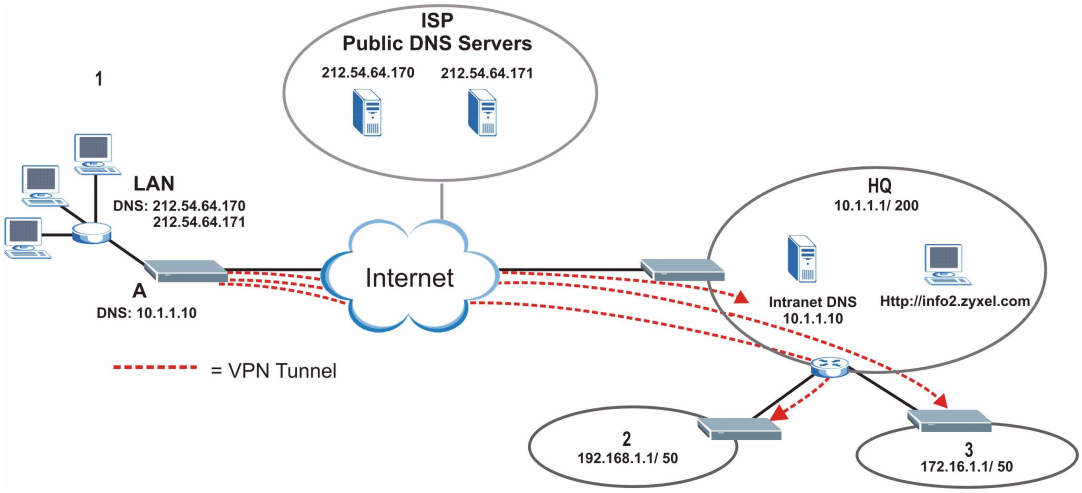
In order for IPSec router A (see the figure) to receive an initiating IPSec packet from IPSec router B, set the NAT router to forward UDP port 500 to IPSec router A.

19.7.2 Remote DNS Server

In cases where you want to use domain names to access Intranet servers on a remote network that has a DNS server, you must identify that DNS server. You cannot use DNS servers on the LAN or from the ISP since these DNS servers cannot resolve domain names to private IP addresses on the remote network

The following figure depicts an example where three VPN tunnels are created from Prestige A; one to branch office 2, one to branch office 3 and another to headquarters. In order to access computers that use private domain names on the headquarters (HQ) network, the Prestige at branch office 1 uses the Intranet DNS server in headquarters. The DNS server feature for VPN does not work with Windows 2000 or Windows XP.

Figure 96 VPN Host using Intranet DNS Server Example



If you do not specify an Intranet DNS server on the remote network, then the VPN host must use IP addresses to access the computers on the remote network.

19.8 ID Type and Content

With aggressive negotiation mode (see the Negotiation Mode section), the Prestige identifies incoming SAs by ID type and content since this identifying information is not encrypted. This enables the Prestige to distinguish between multiple rules for SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. Telecommuters can use separate passwords to simultaneously connect to the Prestige from IPSec routers with dynamic IP addresses (see the Telecommuter VPN/IPSec Examples section for a telecommuter configuration example).

Regardless of the ID type and content configuration, the Prestige does not allow you to save multiple active rules with overlapping local and remote IP addresses.

With main mode (see the Negotiation Mode section), the ID type and content are encrypted to provide identity protection. In this case the Prestige can only distinguish between up to 12 different incoming SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. The Prestige can distinguish up to 12 incoming SAs because you can select between three encryption algorithms (DES, 3DES and AES), two authentication algorithms (MD5 and SHA1) and two key groups (DH1 and DH2) when you configure a VPN rule (see the Configuring Advanced IKE Settings section). The ID type and content act as an extra level of identification for incoming SAs.

The type of ID can be a domain name, an IP address or an e-mail address. The content is the IP address, domain name, or e-mail address.

Table 68 Local ID Type and Content Fields

LOCAL ID TYPE=	CONTENT=
IP	Type the IP address of your computer or leave the field blank to have the Prestige automatically use its own IP address.
DNS	Type a domain name (up to 31 characters) by which to identify this Prestige.
E-mail	Type an e-mail address (up to 31 characters) by which to identify this Prestige.
	The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address.

Table 69 Peer ID Type and Content Fields

PEER ID TYPE=	CONTENT=
IP	Type the IP address of the computer with which you will make the VPN connection or leave the field blank to have the Prestige automatically use the address in the **Secure Gateway** field.
DNS	Type a domain name (up to 31 characters) by which to identify the remote IPSec router.
E-mail	Type an e-mail address (up to 31 characters) by which to identify the remote IPSec router.
	The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address. The domain name also does not have to match the remote router's IP address or what you configure in the **Secure Gateway Addr** field below.

19.8.1 ID Type and Content Examples

Two IPSec routers must have matching ID type and content configuration in order to set up a VPN tunnel.

The two Prestiges in this example can complete negotiation and establish a VPN tunnel.

Table 70 Matching ID Type and Content Configuration Example

PRESTIGE A	PRESTIGE B
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.2	Peer ID content: tom@yourcompany.com

The two Prestiges in this example cannot complete their negotiation because Prestige B's **Local ID type** is **IP**, but Prestige A's **Peer ID type** is set to **E-mail**. An "ID mismatched" message displays in the IPSEC LOG.

Table 71 Mismatching ID Type and Content Configuration Example

PRESTIGE A	PRESTIGE B
Local ID type: IP	Local ID type: IP
Local ID content: 1.1.1.10	Local ID content: 1.1.1.10
Peer ID type: E-mail	Peer ID type: IP
Peer ID content: aa@yahoo.com	Peer ID content: N/A

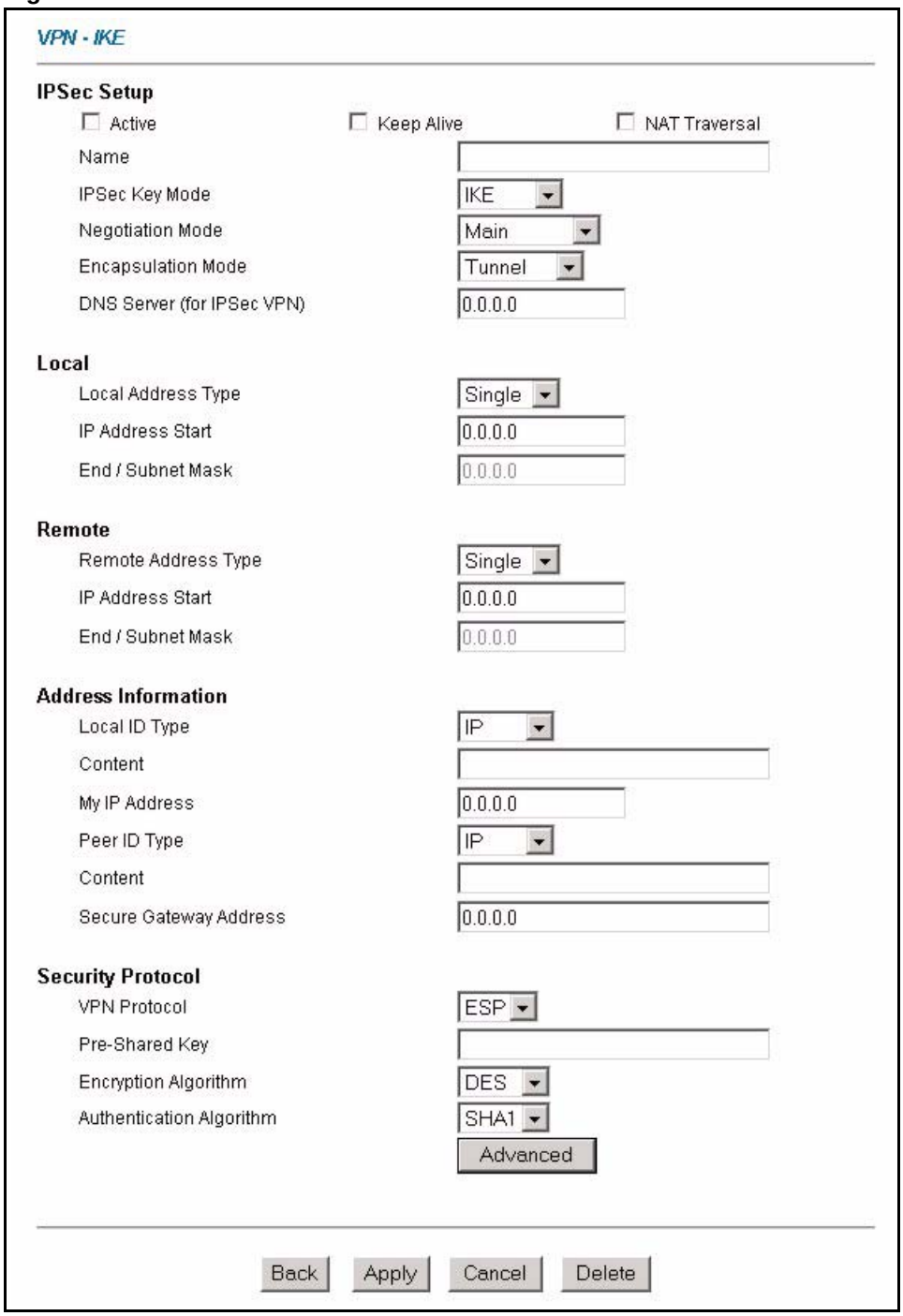
19.9 Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation (see the IKE Phases section for more on IKE phases). It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.

19.10 Editing VPN Policies

Click a number (**No.**) on the **Summary** screen to edit VPN policies.

Figure 97 VPN IKE



The following table describes the fields in this screen.

Table 72 VPN IKE

LABEL	DESCRIPTION
IPSec Setup	
Active	Select this check box to activate this VPN policy. This option determines whether a VPN rule is applied before a packet leaves the firewall.
Keep Alive	Select either **Yes** or **No** from the drop-down list box. Select **Yes** to have the Prestige automatically reinitiate the SA after the SA lifetime times out, even if there is no traffic. The remote IPSec router must also have keep alive enabled in order for this feature to work.
NAT Traversal	Select this check box to enable NAT traversal. NAT traversal allows you to set up a VPN connection when there are NAT routers between the two IPSec routers. The remote IPSec router must also have NAT traversal enabled. You can use NAT traversal with **ESP** protocol using **Transport** or **Tunnel** mode, but not with **AH** protocol nor with manual key management. In order for an IPSec router behind a NAT router to receive an initiating IPSec packet, set the NAT router to forward UDP port 500 to the IPSec router behind the NAT router.
Name	Type up to 32 characters to identify this VPN policy. You may use any character, including spaces, but the Prestige drops trailing spaces.
IPSec Key Mode	Select **IKE** or **Manual** from the drop-down list box. **IKE** provides more protection so it is generally recommended. **Manual** is a useful option for troubleshooting if you have problems using **IKE** key management.
Negotiation Mode	Select **Main** or **Aggressive** from the drop-down list box. Multiple SAs connecting through a secure gateway must have the same negotiation mode.
Encapsulation Mode	Select **Tunnel** mode or **Transport** mode from the drop-down list box.
DNS Server (for IPSec VPN)	If there is a private DNS server that services the VPN, type its IP address here. The Prestige assigns this additional DNS server to the Prestige's DHCP clients that have IP addresses in this IPSec rule's range of local addresses. A DNS server allows clients on the VPN to find other computers and servers on the VPN by their (private) domain names.
Local	Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses. Two active SAs can have the same configured local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time. In order to have more than one active rule with the **Secure Gateway Address** field set to **0.0.0.0**, the ranges of the local IP addresses cannot overlap between rules. If you configure an active rule with **0.0.0.0** in the **Secure Gateway Address** field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the **Secure Gateway Address** field set to **0.0.0.0**.
Local Address Type	Use the drop-down menu to choose **Single**, **Range**, or **Subnet**. Select **Single** for a single IP address. Select **Range** for a specific range of IP addresses. Select **Subnet** to specify IP addresses on a network by their subnet mask.
IP Address Start	When the **Local Address Type** field is configured to **Single**, enter a (static) IP address on the LAN behind your Prestige. When the **Local Address Type** field is configured to **Range**, enter the beginning (static) IP address, in a range of computers on your LAN behind your Prestige. When the **Local Address Type** field is configured to **Subnet**, this is a (static) IP address on the LAN behind your Prestige.

Table 72 VPN IKE (continued)

LABEL	DESCRIPTION
End / Subnet Mask	When the **Local Address Type** field is configured to **Single**, this field is N/A. When the **Local Address Type** field is configured to **Range**, enter the end (static) IP address, in a range of computers on the LAN behind your Prestige. When the **Local Address Type** field is configured to **Subnet**, this is a subnet mask on the LAN behind your Prestige.
Remote	Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. The remote fields do not apply when the **Secure Gateway IP Address** field is configured to **0.0.0.0**. In this case only the remote IPSec router can initiate the VPN. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Remote Address Type	Use the drop-down menu to choose **Single**, **Range**, or **Subnet**. Select **Single** with a single IP address. Select **Range** for a specific range of IP addresses. Select **Subnet** to specify IP addresses on a network by their subnet mask.
IP Address Start	When the **Remote Address Type** field is configured to **Single**, enter a (static) IP address on the network behind the remote IPSec router. When the **Remote Address Type** field is configured to **Range**, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Remote Address Type** field is configured to **Subnet**, enter a (static) IP address on the network behind the remote IPSec router.
End / Subnet Mask	When the **Remote Address Type** field is configured to **Single**, this field is N/A. When the **Remote Address Type** field is configured to **Range**, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Remote Address Type** field is configured to **Subnet**, enter a subnet mask on the network behind the remote IPSec router.
Address Information	
Local ID Type	Select **IP** to identify this Prestige by its IP address. Select **DNS** to identify this Prestige by a domain name. Select **E-mail** to identify this Prestige by an e-mail address.
Content	When you select **IP** in the **Local ID Type** field, type the IP address of your computer in the local **Content** field. The Prestige automatically uses the IP address in the **My IP Address** field (refer to the **My IP Address** field description) if you configure the local **Content** field to **0.0.0.0** or leave it blank. It is recommended that you type an IP address other than **0.0.0.0** in the local **Content** field or use the **DNS** or **E-mail** ID type in the following situations. When there is a NAT router between the two IPSec routers. When you want the remote IPSec router to be able to distinguish between VPN connection requests that come in from IPSec routers with dynamic WAN IP addresses. When you select **DNS** or **E-mail** in the **Local ID Type** field, type a domain name or e-mail address by which to identify this Prestige in the local **Content** field. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string.

Table 72 VPN IKE (continued)

LABEL	DESCRIPTION
My IP Address	Enter the WAN IP address of your Prestige. The VPN tunnel has to be rebuilt if this IP address changes. The following applies if this field is configured as **0.0.0.0**: The Prestige uses the current Prestige WAN IP address (static or dynamic) to set up the VPN tunnel. If the WAN connection goes down, the Prestige uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. See the chapter on WAN for details on dial backup and traffic redirect.
Peer ID Type	Select **IP** to identify the remote IPSec router by its IP address. Select **DNS** to identify the remote IPSec router by a domain name. Select **E-mail** to identify the remote IPSec router by an e-mail address.
Content	The configuration of the peer content depends on the peer ID type. For **IP**, type the IP address of the computer with which you will make the VPN connection. If you configure this field to **0.0.0.0** or leave it blank, the Prestige will use the address in the **Secure Gateway Address** field (refer to the **Secure Gateway Address** field description). For **DNS** or **E-mail**, type a domain name or e-mail address by which to identify the remote IPSec router. Use up to 31 ASCII characters including spaces, although trailing spaces are truncated. The domain name or e-mail address is for identification purposes only and can be any string. It is recommended that you type an IP address other than **0.0.0.0** or use the **DNS** or **E-mail** ID type in the following situations: When there is a NAT router between the two IPSec routers. When you want the Prestige to distinguish between VPN connection requests that come in from remote IPSec routers with dynamic WAN IP addresses.
Secure Gateway Address	Type the WAN IP address or the URL (up to 31 characters) of the IPSec router with which you're making the VPN connection. Set this field to **0.0.0.0** if the remote IPSec router has a dynamic WAN IP address (the **Key Management** field must be set to **IKE**). In order to have more than one active rule with the **Secure Gateway Address** field set to **0.0.0.0**, the ranges of the local IP addresses cannot overlap between rules. If you configure an active rule with **0.0.0.0** in the **Secure Gateway Address** field and the LAN's full IP address range as the local IP address, then you cannot configure any other active rules with the **Secure Gateway Address** field set to **0.0.0.0**.
Security Protocol	
VPN Protocol	Select **ESP** if you want to use ESP (Encapsulation Security Payload). The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by **AH**. If you select **ESP** here, you must select options from the **Encryption Algorithm** and **Authentication Algorithm** fields (described below).

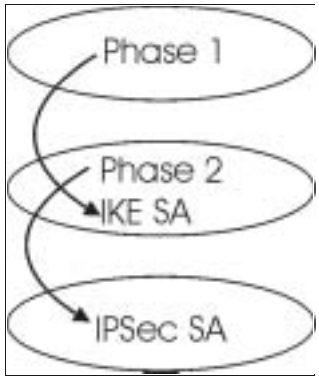
Table 72 VPN IKE (continued)

LABEL	DESCRIPTION
Pre-Shared Key	Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection. Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x" (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in "0x0123456789ABCDEF", "0x" denotes that the key is hexadecimal and "0123456789ABCDEF" is the key itself. Both ends of the VPN tunnel must use the same pre-shared key. You will receive a "PYLD_MALFORMED" (payload malformed) packet if the same pre-shared key is not used on both ends.
Encryption Algorithm	Select **DES**, **3DES**, **AES** or **NULL** from the drop-down list box. When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on **DES** that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of **AES** uses a 128-bit key. **AES** is faster than **3DES**. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter an encryption key.
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security.
Advanced	Click **Advanced** to configure more detailed settings of your IKE key management.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Delete	Click **Delete** to delete the current rule.

19.11 IKE Phases

There are two phases to every IKE (Internet Key Exchange) negotiation – phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA and the second one uses that SA to negotiate SAs for IPSec.

Figure 98 Two Phases to Set Up the IPSec SA



In phase 1 you must:

- Choose a negotiation mode.
- Authenticate the connection by entering a pre-shared key.
- Choose an encryption algorithm.
- Choose an authentication algorithm.
- Choose a Diffie-Hellman public-key cryptography key group (**DH1** or **DH2**).
- Set the IKE SA lifetime. This field allows you to determine how long an IKE SA should stay up before it times out. An IKE SA times out when the IKE SA lifetime period expires. If an IKE SA times out when an IPSec SA is already established, the IPSec SA stays connected.

In phase 2 you must:

- Choose which protocol to use (**ESP** or **AH**) for the IKE key exchange.
- Choose an encryption algorithm.
- Choose an authentication algorithm
- Choose whether to enable Perfect Forward Secrecy (PFS) using Diffie-Hellman public-key cryptography – see the Perfect Forward Secrecy (PFS) section . Select **None** (the default) to disable PFS.
- Choose **Tunnel** mode or **Transport** mode.
- Set the IPSec SA lifetime. This field allows you to determine how long the IPSec SA should stay up before it times out. The Prestige automatically renegotiates the IPSec SA if there is traffic when the IPSec SA lifetime period expires. The Prestige also automatically renegotiates the IPSec SA if both IPSec routers have keep alive enabled, even if there is no traffic. If an IPSec SA times out, then the IPSec router must renegotiate the SA the next time someone attempts to send traffic.

19.11.1 Negotiation Mode

The phase 1 **Negotiation Mode** you select determines how the Security Association (SA) will be established for each connection through IKE negotiations.

- **Main Mode** ensures the highest level of security when the communicating parties are negotiating authentication (phase 1). It uses 6 messages in three round trips: SA negotiation, Diffie-Hellman exchange and an exchange of nonces (a nonce is a random number). This mode features identity protection (your identity is not revealed in the negotiation).
- **Aggressive Mode** is quicker than **Main Mode** because it eliminates several steps when the communicating parties are negotiating authentication (phase 1). However the trade-off is that faster speed limits its negotiating power and it also does not provide identity protection. It is useful in remote access situations where the address of the initiator is not know by the responder and both parties want to use pre-shared key authentication.

19.11.2 Diffie-Hellman (DH) Key Groups

Diffie-Hellman (DH) is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE SA setup to establish session keys. 768-bit (Group 1 - **DH1**) and 1024-bit (Group 2 – **DH2**) Diffie-Hellman groups are supported. Upon completion of the Diffie-Hellman exchange, the two peers have a shared secret, but the IKE SA is not authenticated. For authentication, use pre-shared keys.

19.11.3 Perfect Forward Secrecy (PFS)

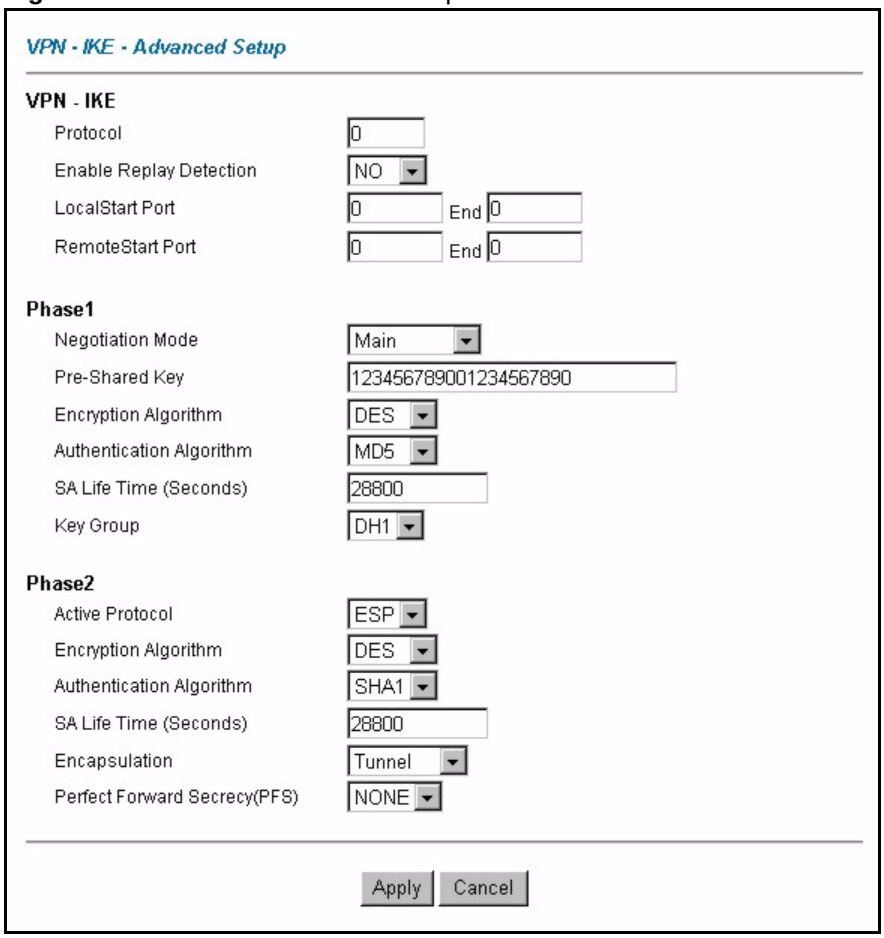
Enabling PFS means that the key is transient. The key is thrown away and replaced by a brand new key using a new Diffie-Hellman exchange for each new IPSec SA setup. With PFS enabled, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys. The (time-consuming) Diffie-Hellman exchange is the trade-off for this extra security.

This may be unnecessary for data that does not require such security, so PFS is disabled (**None**) by default in the Prestige. Disabling PFS means new authentication and encryption keys are derived from the same root secret (which may have security implications in the long run) but allows faster SA setup (by bypassing the Diffie-Hellman key exchange).

19.12 Configuring Advanced IKE Settings

Click **Advanced** in the **VPN IKE** screen. This is the **VPN IKE- Advanced Setup** screen as shown next.

Figure 99 VPN IKE: Advanced Setup



The following table describes the fields in this screen.

Table 73 VPN IKE: Advanced Setup

LABEL	DESCRIPTION
VPN - IKE	
Protocol	Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol.
Enable Replay Protection	As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DoS) attacks The IPSec receiver can detect and reject old or duplicate packets to protect against replay attacks. Select **YES** from the drop-down menu to enable replay detection, or select **NO** to disable it.
Local Start Port	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. If **Local Start Port** is left at 0, **End** will also remain at 0.
Remote Start Port	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.

Table 73 VPN IKE: Advanced Setup (continued)

LABEL	DESCRIPTION
End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. If **Remote Start Port** is left at 0, **End** will also remain at 0.
Phase 1	
Negotiation Mode	Select **Main** or **Aggressive** from the drop-down list box. Multiple SAs connecting through a secure gateway must have the same negotiation mode.
Pre-Shared Key	Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection. Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x" (zero x), which is not counted as part of the 16 to 62-character range for the key. For example, in "0x0123456789ABCDEF", "0x" denotes that the key is hexadecimal and "0123456789ABCDEF" is the key itself. Both ends of the VPN tunnel must use the same pre-shared key. You will receive a "PYLD_MALFORMED" (payload malformed) packet if the same pre-shared key is not used on both ends.
Encryption Algorithm	Select **DES**, **3DES** or **AES** from the drop-down list box. When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on **DES** that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of AES uses a 128-bit key. **AES** is faster than **3DES**.
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security.
SA Life Time (Seconds)	Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Key Group	You must choose a key group for phase 1 IKE setup. **DH1** (default) refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number.
Phase 2	
Active Protocol	Use the drop-down list box to choose from **ESP** or **AH**.

Table 73 VPN IKE: Advanced Setup (continued)

LABEL	DESCRIPTION
Encryption Algorithm	This field is available when you select **ESP** in the **Active Protocol** field. Select **DES**, **3DES**, **AES** or **NULL** from the drop-down list box. When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on DES that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of AES uses a 128-bit key. **AES** is faster than **3DES**. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter an encryption key.
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The SHA1 algorithm is generally considered stronger than MD5, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security.
SA Life Time (Seconds)	Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.
Encapsulation	Select **Tunnel** mode or **Transport** mode from the drop-down list box.
Perfect Forward Secrecy (PFS)	Perfect Forward Secrecy (PFS) is disabled (**NONE**) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure. Choose **DH1** or **DH2** from the drop-down list box to enable PFS. **DH1** refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number (more secure, yet slower).
Apply	Click **Apply** to save your changes back to the Prestige and return to the **VPN-IKE** screen.
Cancel	Click **Cancel** to return to the **VPN-IKE** screen without saving your changes.

19.13 Manual Key Setup

Manual key management is useful if you have problems with **IKE** key management.

19.13.1 Security Parameter Index (SPI)

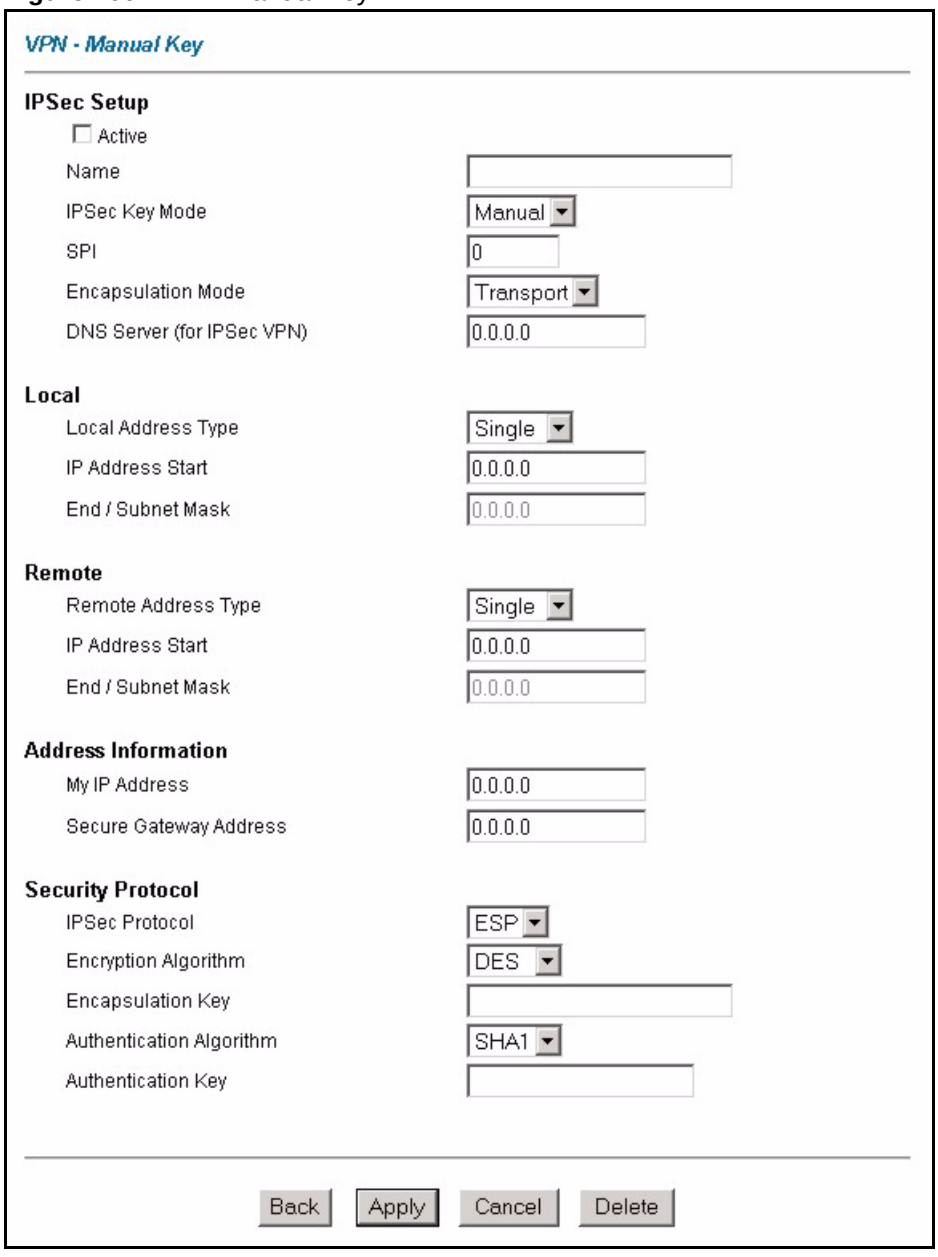
An SPI is used to distinguish different SAs terminating at the same destination and using the same IPSec protocol. This data allows for the multiplexing of SAs to a single gateway. The **SPI** (Security Parameter Index) along with a destination IP address uniquely identify a particular Security Association (SA). The **SPI** is transmitted from the remote VPN gateway to the local VPN gateway. The local VPN gateway then uses the network, encryption and key values that the administrator associated with the SPI to establish the tunnel.

Current ZyXEL implementation assumes identical outgoing and incoming SPIs.

19.14 Configuring Manual Key

You only configure **VPN Manual Key** when you select **Manual** in the **IPSec Key Mode** field on the **VPN IKE** screen. This is the **VPN Manual Key** screen as shown next.

Figure 100 VPN: Manual Key



The following table describes the fields in this screen.

Table 74 VPN: Manual Key

LABEL	DESCRIPTION
IPSec Setup	
Active	Select this check box to activate this VPN policy.
Name	Type up to 32 characters to identify this VPN policy. You may use any character, including spaces, but the Prestige drops trailing spaces.
IPSec Key Mode	Select **IKE** or **Manual** from the drop-down list box. **Manual** is a useful option for troubleshooting if you have problems using **IKE** key management.
SPI	Type a number (base 10) from 1 to 999999 for the Security Parameter Index.
Encapsulation Mode	Select **Tunnel** mode or **Transport** mode from the drop-down list box.
DNS Server (for IPSec VPN)	If there is a private DNS server that services the VPN, type its IP address here. The Prestige assigns this additional DNS server to the Prestige 's DHCP clients that have IP addresses in this IPSec rule's range of local addresses. A DNS server allows clients on the VPN to find other computers and servers on the VPN by their (private) domain names.
Local	Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Local Address Type	Use the drop-down menu to choose **Single**, **Range**, or **Subnet**. Select **Single** for a single IP address. Select **Range** for a specific range of IP addresses. Select **Subnet** to specify IP addresses on a network by their subnet mask.
IP Address Start	When the **Local Address Type** field is configured to **Single**, enter a (static) IP address on the LAN behind your Prestige. When the **Local Address Type** field is configured to **Range**, enter the beginning (static) IP address, in a range of computers on your LAN behind your Prestige. When the **Local Address Type** field is configured to **Subnet**, this is a (static) IP address on the LAN behind your Prestige.
End / Subnet Mask	When the **Local Address Type** field is configured to **Single**, this field is N/A. When the **Local Address Type** field is configured to **Range**, enter the end (static) IP address, in a range of computers on the LAN behind your Prestige. When the **Local Address Type** field is configured to **Subnet**, this is a subnet mask on the LAN behind your Prestige.
Remote	Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Remote Address Type	Use the drop-down menu to choose **Single**, **Range**, or **Subnet**. Select **Single** with a single IP address. Select **Range** for a specific range of IP addresses. Select **Subnet** to specify IP addresses on a network by their subnet mask.
IP Address Start	When the **Remote Address Type** field is configured to Single, enter a (static) IP address on the network behind the remote IPSec router. When the **Remote Address Type** field is configured to **Range**, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Remote Address Type** field is configured to **Subnet**, enter a (static) IP address on the network behind the remote IPSec router.

Table 74 VPN: Manual Key (continued)

LABEL	DESCRIPTION
End / Subnet Mask	When the **Remote Address Type** field is configured to **Single**, this field is N/A. When the **Remote Address Type** field is configured to **Range**, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Remote Address Type** field is configured to **Subnet**, enter a subnet mask on the network behind the remote IPSec router.
Address Information	
My IP Address	Enter the WAN IP address of your Prestige. The VPN tunnel has to be rebuilt if this IP address changes. The following applies if this field is configured as **0.0.0.0**: The Prestige uses the current Prestige WAN IP address (static or dynamic) to set up the VPN tunnel. If the WAN connection goes down, the Prestige uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. See the chapter on WAN for details on dial backup and traffic redirect.
Secure Gateway Address	Type the WAN IP address or the URL (up to 31 characters) of the IPSec router with which you're making the VPN connection.
Security Protocol	
IPSec Protocol	Select **ESP** if you want to use ESP (Encapsulation Security Payload). The ESP protocol (RFC 2406) provides encryption as well as some of the services offered by **AH**. If you select ESP here, you must select options from the **Encryption Algorithm** and **Authentication Algorithm** fields (described next).
Encryption Algorithm	Select **DES**, **3DES** or **NULL** from the drop-down list box. When **DES** is used for data communications, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The **DES** encryption algorithm uses a 56-bit key. Triple DES (**3DES**) is a variation on **DES** that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in increased latency and decreased throughput. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter an encryption key.
Encapsulation Key (only with ESP)	With **DES**, type a unique key 8 characters long. With **3DES**, type a unique key 24 characters long. Any characters may be used, including spaces, but trailing spaces are truncated.
Authentication Algorithm	Select **SHA1** or **MD5** from the drop-down list box. **MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slower. Select **MD5** for minimal security and **SHA-1** for maximum security.
Authentication Key	Type a unique authentication key to be used by IPSec if applicable. Enter 16 characters for **MD5** authentication or 20 characters for **SHA-1** authentication. Any characters may be used, including spaces, but trailing spaces are truncated.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to begin configuring this screen afresh.
Delete	Click **Delete** to remove the current rule.

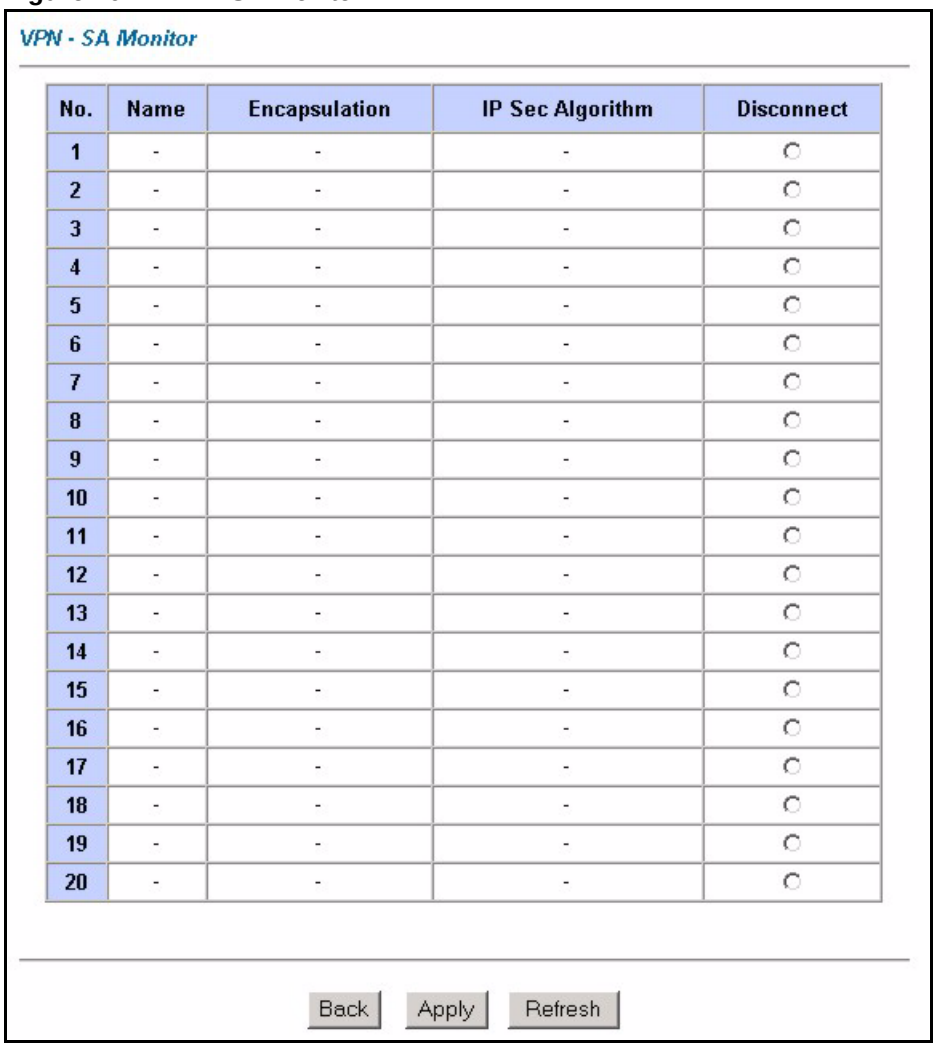
19.15 Viewing SA Monitor

Click **VPN** and **Monitor** to open the **SA Monitor** screen as shown. Use this screen to display and manage active VPN connections.

A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This screen displays active VPN connections. Use **Refresh** to display active VPN connections. This screen is read-only. The following table describes the fields in this tab.

When there is outbound traffic but no inbound traffic, the SA times out automatically after two minutes. A tunnel with no outbound or inbound traffic is "idle" and does not timeout until the SA lifetime period expires. See the Keep Alive section on keep alive to have the Prestige renegotiate an IPSec SA when the SA lifetime expires, even if there is no traffic.

Figure 101 VPN: SA Monitor



The following table describes the fields in this screen.

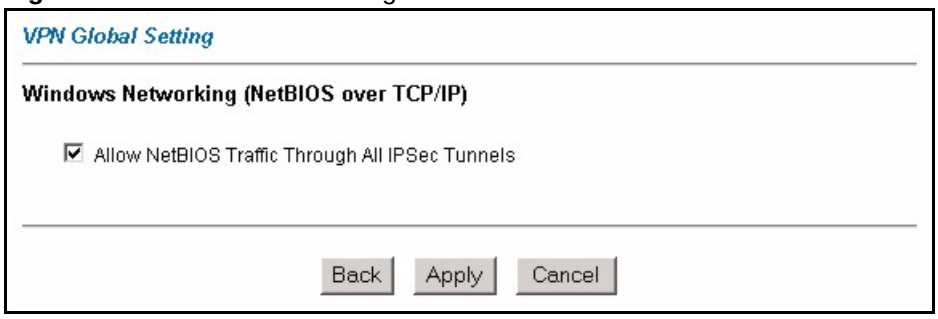
Table 75

LABEL	DESCRIPTION
No	This is the security association index number.
Name	This field displays the identification name for this VPN policy.
Encapsulation	This field displays **Tunnel** or **Transport** mode.
IPSec Algorithm	This field displays the security protocols used for an SA. Both **AH** and **ESP** increase Prestige processing requirements and communications latency (delay).
Disconnect	Select **Disconnect** next to a security association and then click **Apply** to stop that security association.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the Prestige.
Refresh	Click **Refresh** to display the current active VPN connection(s).

19.16 Configuring Global Setting

To change your Prestige's global settings, click **VPN** and then **Global Setting**. The screen appears as shown.

Figure 102 VPN: Global Setting



The following table describes the fields in this screen.

Table 76 VPN: Global Setting

LABEL	DESCRIPTION
Windows Networking (NetBIOS over TCP/IP)	NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to find other computers. It may sometimes be necessary to allow NetBIOS packets to pass through VPN tunnels in order to allow local computers to find computers on the remote network and vice versa.
Allow NetBIOS Traffic Through All IP/Sec Tunnels	Select this check box to send NetBIOS packets through the VPN connection.
Back	Click **Back** to return to the previous screen.

Table 76 VPN: Global Setting (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to begin configuring this screen afresh.

19.17 Telecommuter VPN/IPSec Examples

The following examples show how multiple telecommuters can make VPN connections to a single Prestige at headquarters. The telecommuters use IPSec routers with dynamic WAN IP addresses. The Prestige at headquarters has a static public IP address.

19.17.1 Telecommuters Sharing One VPN Rule Example

See the following figure and table for an example configuration that allows multiple telecommuters (A, B and C in the figure) to use one VPN rule to simultaneously access a Prestige at headquarters (HQ in the figure). The telecommuters do not have domain names mapped to the WAN IP addresses of their IPSec routers. The telecommuters must all use the same IPSec parameters but the local IP addresses (or ranges of addresses) should not overlap.

Figure 103 Telecommuters Sharing One VPN Rule Example

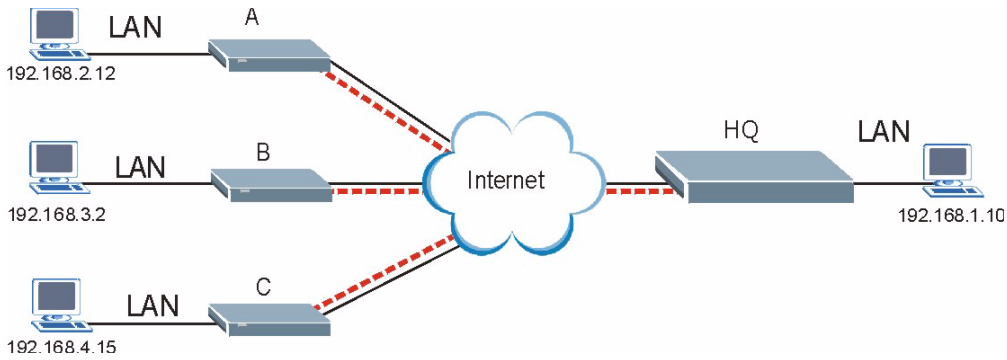


Table 77 Telecommuters Sharing One VPN Rule Example

FIELDS	TELECOMMUTERS	HEADQUARTERS
My IP Address:	0.0.0.0 (dynamic IP address assigned by the ISP)	Public static IP address
Secure Gateway IP Address:	Public static IP address	0.0.0.0 With this IP address only the telecommuter can initiate the IPSec tunnel.
Local IP Address:	Telecommuter A: 192.168.2.12 Telecommuter B: 192.168.3.2 Telecommuter C: 192.168.4.15	192.168.1.10
Remote IP Address:	192.168.1.10	0.0.0.0 (N/A)

19.17.2 Telecommuters Using Unique VPN Rules Example

In this example the telecommuters (A, B and C in the figure) use IPSec routers with domain names that are mapped to their dynamic WAN IP addresses (use Dynamic DNS to do this).

With aggressive negotiation mode (see the Negotiation Mode section), the Prestige can use the ID types and contents to distinguish between VPN rules. Telecommuters can each use a separate VPN rule to simultaneously access a Prestige at headquarters. They can use different IPSec parameters. The local IP addresses (or ranges of addresses) of the rules configured on the Prestige at headquarters can overlap. The local IP addresses of the rules configured on the telecommuters' IPSec routers should not overlap.

See the following table and figure for an example where three telecommuters each use a different VPN rule for a VPN connection with a Prestige located at headquarters. The Prestige at headquarters (HQ in the figure) identifies each incoming SA by its ID type and content and uses the appropriate VPN rule to establish the VPN connection.

The Prestige at headquarters can also initiate VPN connections to the telecommuters since it can find the telecommuters by resolving their domain names.

Figure 104 Telecommuters Using Unique VPN Rules Example

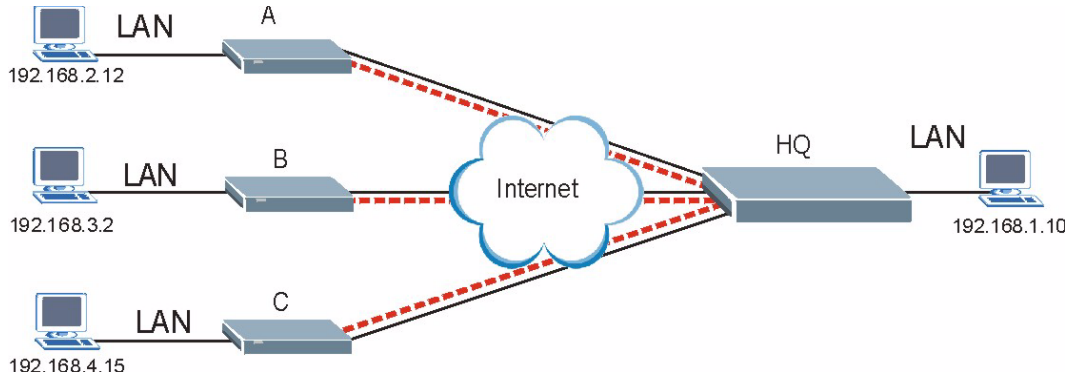


Table 78 Telecommuters Using Unique VPN Rules Example

TELECOMMUTERS	HEADQUARTERS
All Telecommuter Rules:	All Headquarters Rules:
My IP Address 0.0.0.0	My IP Address: bigcompanyhq.com
Secure Gateway Address: bigcompanyhq.com	Local IP Address: 192.168.1.10
Remote IP Address: 192.168.1.10	Local ID Type: E-mail
Peer ID Type: E-mail	Local ID Content: bob@bigcompanyhq.com
Peer ID Content: bob@bigcompanyhq.com	
Telecommuter A (telecommutera.dydns.org)	Headquarters Prestige Rule 1:
Local ID Type: IP	Peer ID Type: IP
Local ID Content: 192.168.2.12	Peer ID Content: 192.168.2.12
Local IP Address: 192.168.2.12	Secure Gateway Address: telecommuter1.com
	Remote Address 192.168.2.12
Telecommuter B (telecommuterb.dydns.org)	Headquarters Prestige Rule 2:
Local ID Type: DNS	Peer ID Type: DNS
Local ID Content: telecommuterb.com	Peer ID Content: telecommuterb.com
Local IP Address: 192.168.3.2	Secure Gateway Address: telecommuterb.com
	Remote Address 192.168.3.2
Telecommuter C (telecommuterc.dydns.org)	Headquarters Prestige Rule 3:
Local ID Type: E-mail	Peer ID Type: E-mail
Local ID Content: myVPN@myplace.com	Peer ID Content: myVPN@myplace.com
Local IP Address: 192.168.4.15	Secure Gateway Address: telecommuterc.com
	Remote Address 192.168.4.15

19.18 VPN and Remote Management

If a VPN tunnel uses Telnet, FTP, WWW, then you should configure remote management (**Remote Management**) to allow access for that service.

CHAPTER 20
Remote Management Configuration

This chapter provides information on configuring remote management.

20.1 Remote Management Overview

Remote management allows you to determine which services/protocols can access which Prestige interface (if any) from which computers.

When you configure remote management to allow management from the WAN, you still need to configure a firewall rule to allow access. See the firewall chapters for details on configuring firewall rules.

You may manage your Prestige from a remote location via:

- Internet (WAN only)
- ALL (LAN and WAN)
- LAN only,
- Neither (Disable).

When you Choose **WAN only** or **ALL** (LAN & WAN), you still need to configure a firewall rule to allow access.

To disable remote management of a service, select **Disable** in the corresponding **Server Access** field.

You may only have one remote management session running at a time. The Prestige automatically disconnects a remote management session of lower priority when another remote management session of higher priority starts. The priorities for the different types of remote management sessions are as follows.

1. Telnet
2. HTTP

20.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

- A filter in SMT menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
- You have disabled that service in one of the remote management screens.
- The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the Prestige will disconnect the session immediately.
- There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.
- There is a firewall rule that blocks it.

20.1.2 Remote Management and NAT

When NAT is enabled:

- Use the Prestige's WAN IP address when configuring from the WAN.
- Use the Prestige's LAN IP address when configuring from the LAN.

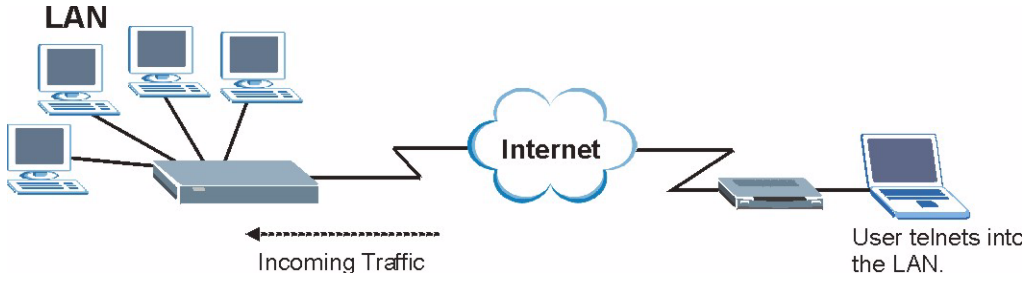
20.1.3 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The Prestige automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling.

20.2 Telnet

You can configure your Prestige for remote Telnet access as shown next.

Figure 105 Telnet Configuration on a TCP/IP Network



20.3 FTP

You can upload and download Prestige firmware and configuration files using FTP. To use this feature, your computer must have an FTP client.

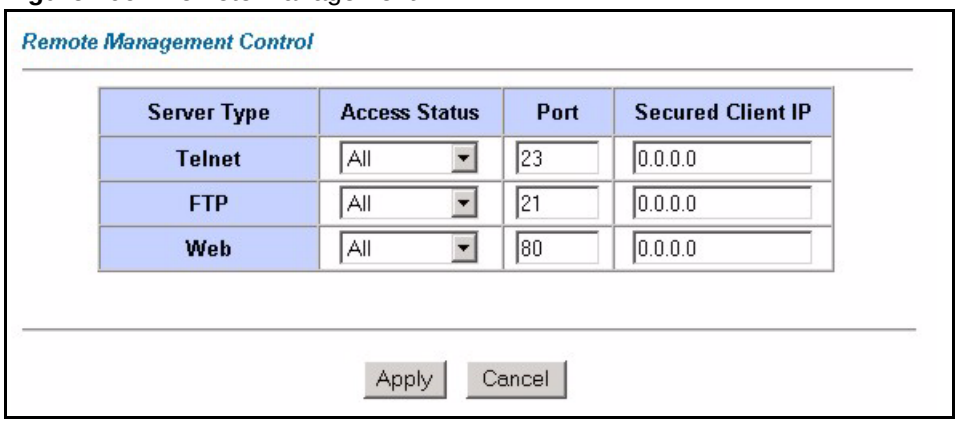
20.4 Web

You can use the Prestige's embedded web configurator for configuration and file management. See the online help for details.

20.5 Configuring Remote Management

Click **Remote Management** to open the following screen.

Figure 106 Remote Management



The following table describes the fields in this screen.

Table 79 Remote Management

LABEL	DESCRIPTION
Server Type	Each of these labels denotes a service that you may use to remotely manage the Prestige.
Access Status	Select the access interface. Choices are **All**, **LAN Only**, **WAN Only** and **Disable**.
Port	This field shows the port number for the remote management service. You may change the port number for a service in this field, but you must use the same port number to use that service for remote management.
Secured Client IP	The default 0.0.0.0 allows any client to use this service to remotely manage the Prestige. Type an IP address to restrict access to a client with a matching IP address.
Apply	Click **Apply** to save your settings back to the Prestige.
Cancel	Click **Cancel** to begin configuring this screen afresh.

CHAPTER 21
Universal Plug-and-Play (UPnP)

This chapter introduces the UPnP feature in the web configurator.

21.1 Introducing Universal Plug and Play

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

21.1.1 How do I know if I'm using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

21.1.2 NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See the Network Address Translation (NAT) Screens chapter for further information about NAT.

21.1.3 Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

21.2 UPnP and ZyXEL

ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum Creates UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports IGD 1.0 (Internet Gateway Device). At the time of writing ZyXEL's UPnP implementation supports Windows Messenger 4.6 and 4.7 while Windows Messenger 5.0 and Xbox are still being tested.

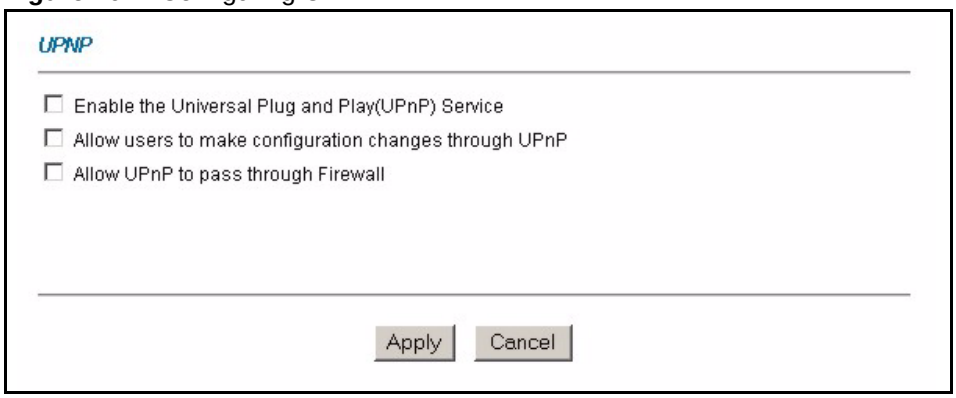
UPnP broadcasts are only allowed on the LAN.

See later sections for examples of installing UPnP in Windows XP and Windows Me as well as an example of using UPnP in Windows.

21.2.1 Configuring UPnP

From the **Site Map** in the main menu, click **UPnP** under **Advanced Setup** to display the screen shown next.

Figure 107 Configuring UPnP



The following table describes the fields in this screen.

Table 80 Configuring UPnP

LABEL	DESCRIPTION
Enable the Universal Plug and Play (UPnP) Service	Select this checkbox to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the Prestige's IP address (although you must still enter the password to access the web configurator).
Allow users to make configuration changes through UPnP	Select this check box to allow UPnP-enabled applications to automatically configure the Prestige so that they can communicate through the Prestige, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.
Allow UPnP to pass through Firewall	Select this check box to allow traffic from UPnP-enabled applications to bypass the firewall. Clear this check box to have the firewall block all UPnP application packets (for example, MSN packets).
Apply	Click **Apply** to save the setting to the Prestige.
Cancel	Click **Cancel** to return to the previously saved settings.

21.3 Installing UPnP in Windows Example

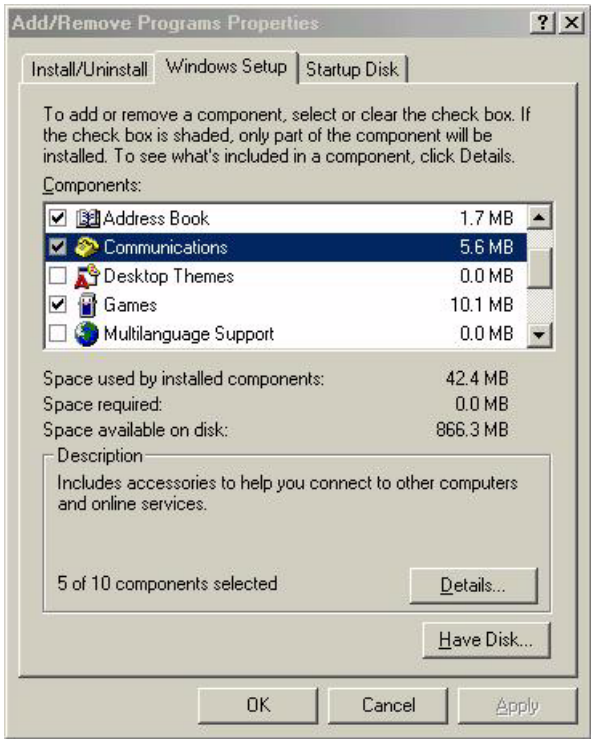
This section shows how to install UPnP in Windows Me and Windows XP.

Installing UPnP in Windows Me

Follow the steps below to install the UPnP in Windows Me.

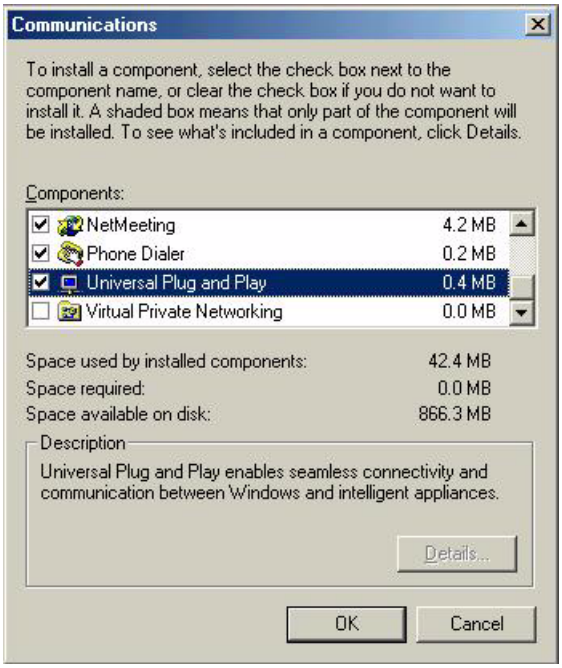
1. Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.
2. Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.

Figure 108 Add/Remove Programs: Windows Setup: Communication



3 In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.

Figure 109 Add/Remove Programs: Windows Setup: Communication: Components



4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.

5 Restart the computer when prompted.

Installing UPnP in Windows XP

Follow the steps below to install the UPnP in Windows XP.

1 Click **Start** and **Control Panel**.

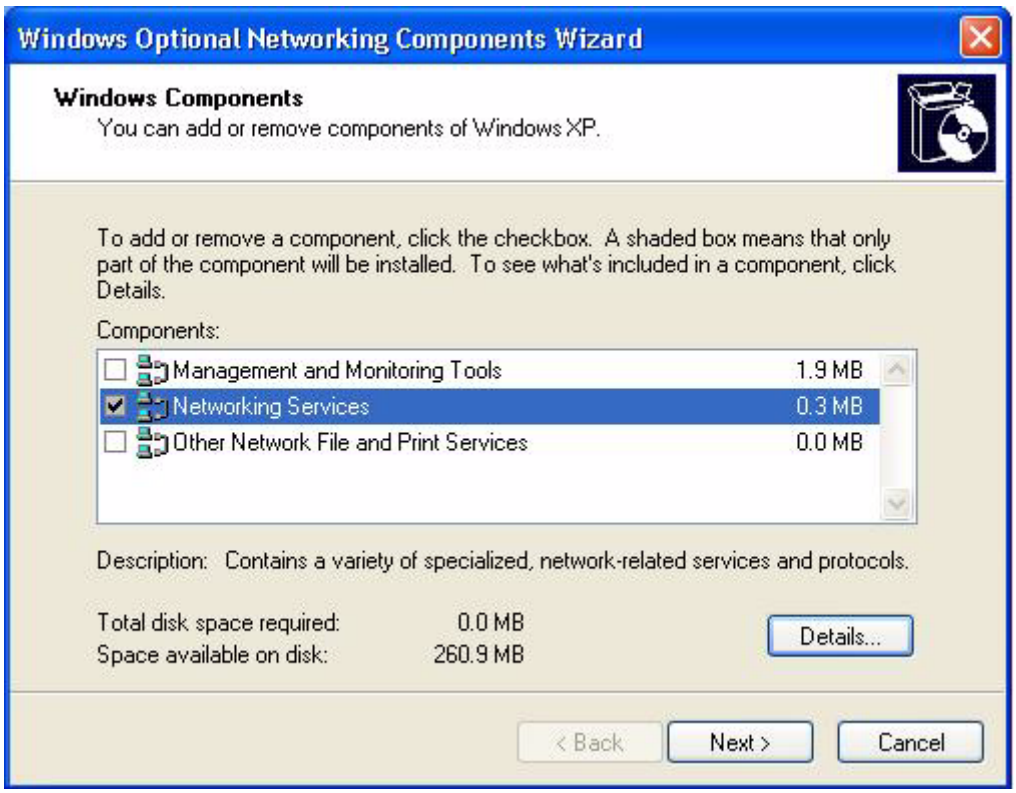
2 Double-click **Network Connections**.

3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ….**

Figure 110 Network Connections

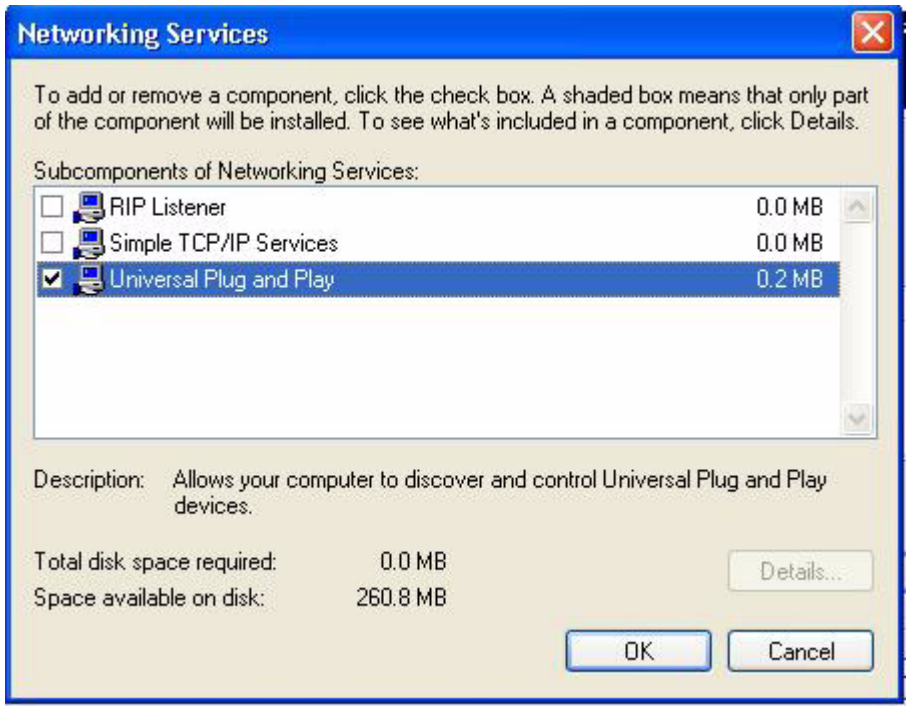
4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.

Figure 111 Windows Optional Networking Components Wizard



5 In the **Networking Services** window, select the **Universal Plug and Play** check box.

Figure 112 Networking Services



6 Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.

21.4 Using UPnP in Windows XP Example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the Prestige.

Make sure the computer is connected to a LAN port of the Prestige. Turn on your computer and the Prestige.

Auto-discover Your UPnP-enabled Network Device

1 Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.

2 Right-click the icon and select **Properties**.

Figure 113 Network Connections

3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

Figure 114 Internet Connection Properties

4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

Figure 115 Internet Connection Properties: Advanced Settings

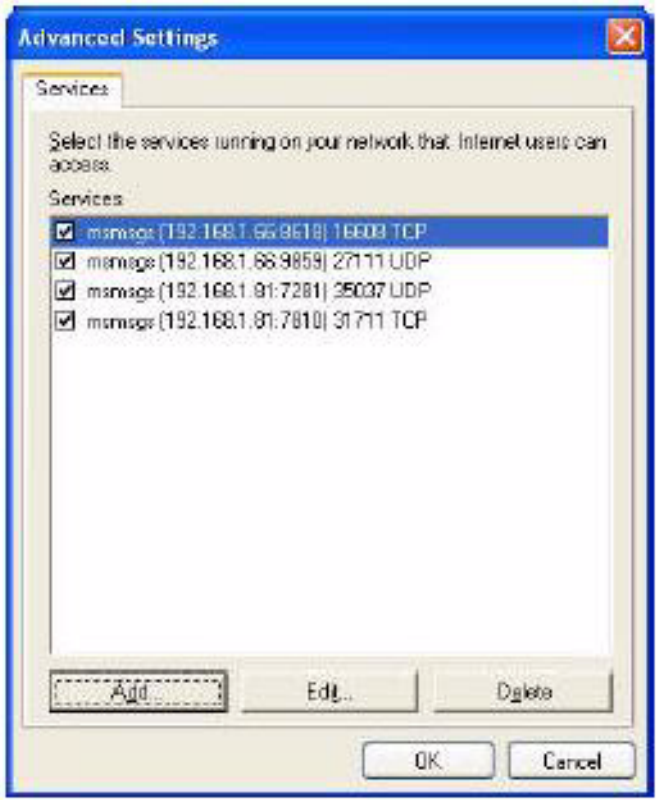
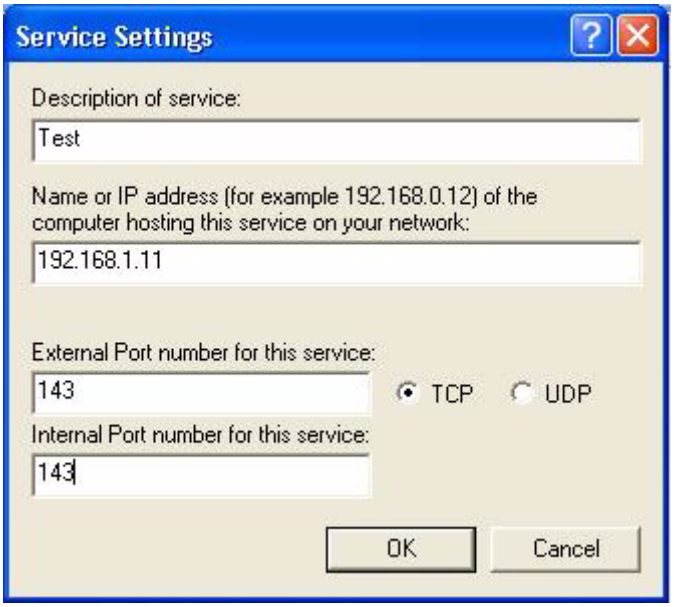


Figure 116 Internet Connection Properties: Advanced Settings: Add



5 When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

6 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.

Figure 117 System Tray Icon

7 Double-click on the icon to display your current Internet connection status.

Figure 118 Internet Connection Status

Web Configurator Easy Access

With UPnP, you can access the web-based configurator on the Prestige without finding out the IP address of the Prestige first. This comes helpful if you do not know the IP address of the Prestige.

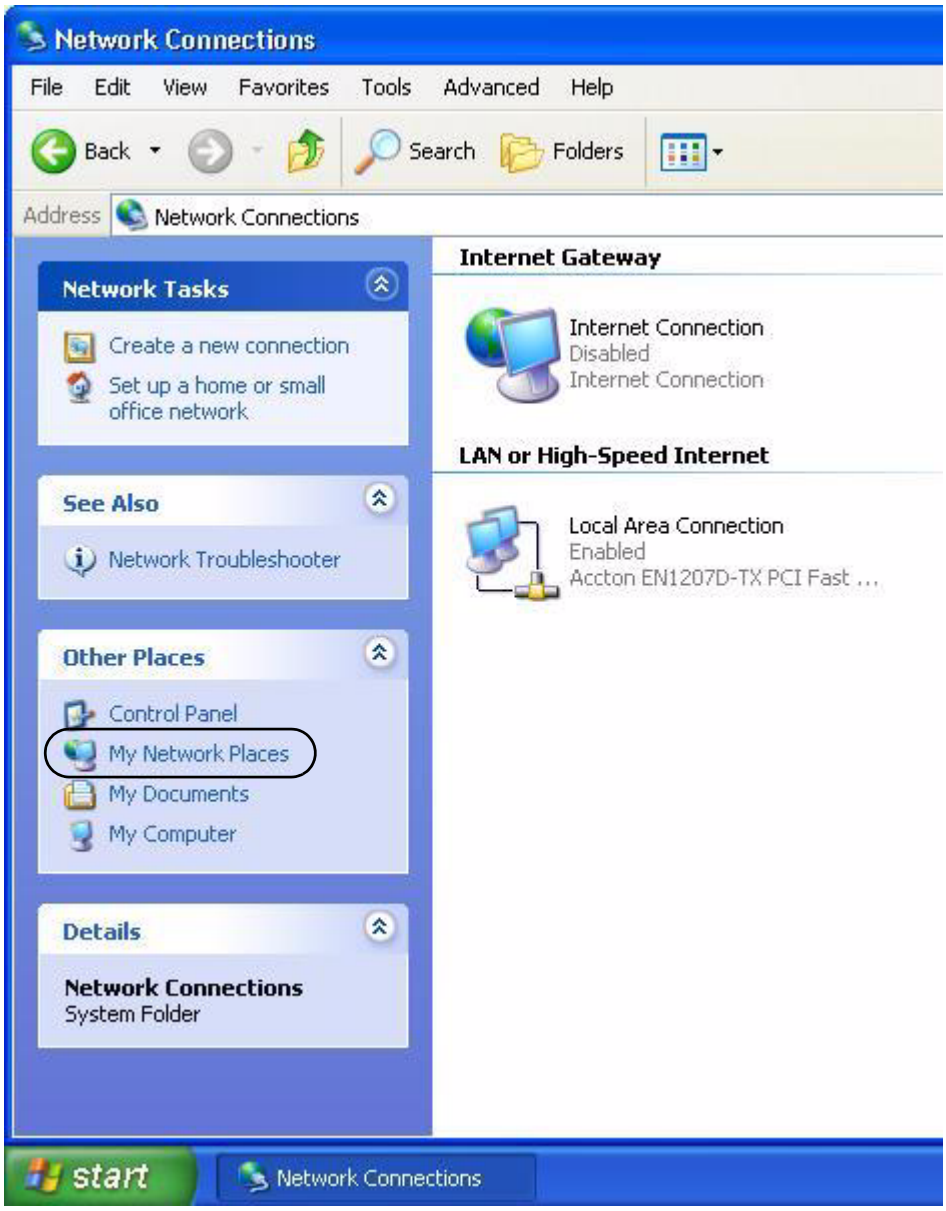
Follow the steps below to access the web configurator.

1 Click **Start** and then **Control Panel**.

2 Double-click **Network Connections**.

3 Select **My Network Places** under **Other Places**.

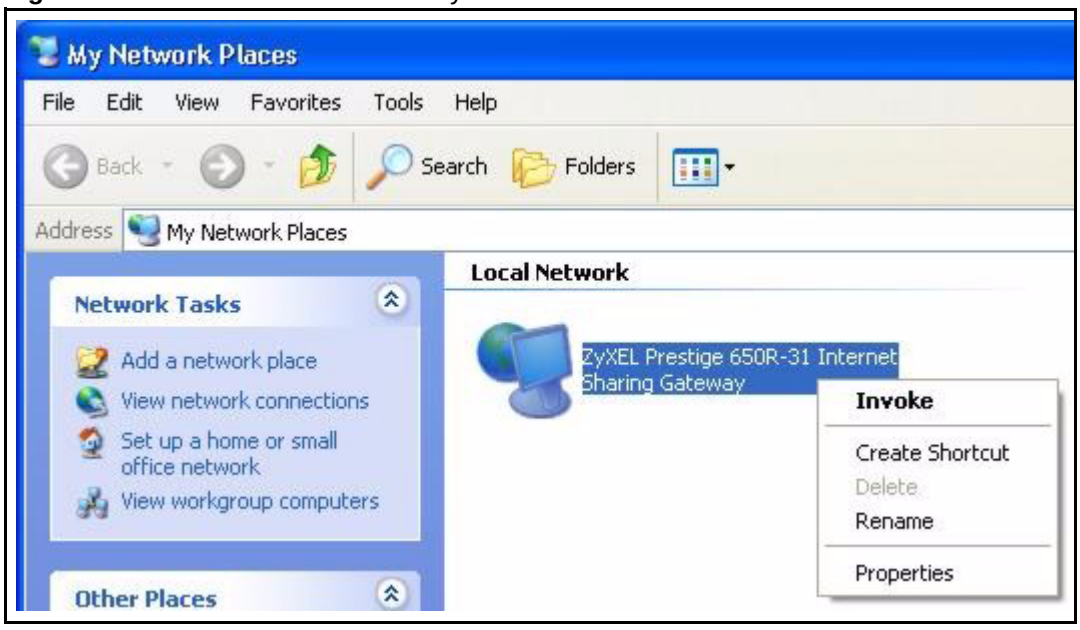
Figure 119 Network Connections



4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

5 Right-click on the icon for your Prestige and select **Invoke**. The web configurator login screen displays.

Figure 120 Network Connections: My Network Places



6 Right-click on the icon for your Prestige and select **Properties**. A properties window displays with basic information about the Prestige.

Figure 121 Network Connections: My Network Places: Properties: Example

CHAPTER 22
Logs Screens

This chapter contains information about configuring general log settings and viewing the Prestige's logs. Refer to the appendix for example log message explanations.

22.1 Logs Overview

The web configurator allows you to choose which categories of events and/or alerts to have the Prestige log and then display the logs or have the Prestige send them to an administrator (as e-mail) or to a syslog server.

22.1.1 Alerts and Logs

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

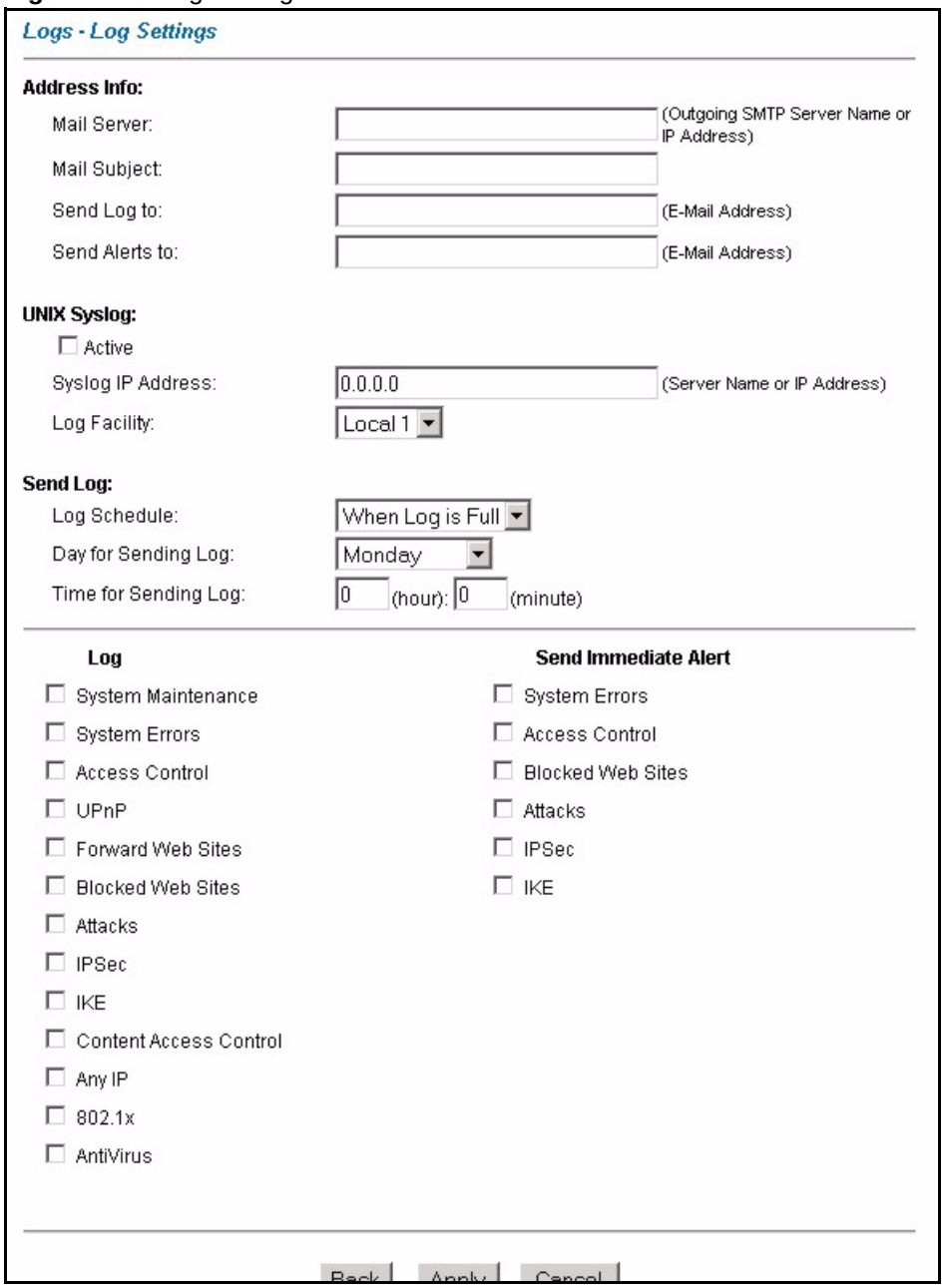
22.2 Configuring Log Settings

Use the **Log Settings** screen to configure to where the Prestige is to send logs; the schedule for when the Prestige is to send the logs and which logs and/or immediate alerts the Prestige is to record.

To change your Prestige's log settings, click **Logs**, then the **Log Settings**. The screen appears as shown.

Alerts are e-mailed as soon as they happen. Logs may be e-mailed as soon as the log is full (see **Log Schedule**). Selecting many alert and/or log categories (especially **Access Control**) may result in many e-mails being sent.

Figure 122 Log Settings



The following table describes the fields in this screen.

Table 81 Log Settings

LABEL	DESCRIPTION
Address Info	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via e-mail.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the Prestige sends.

Table 81 Log Settings (continued)

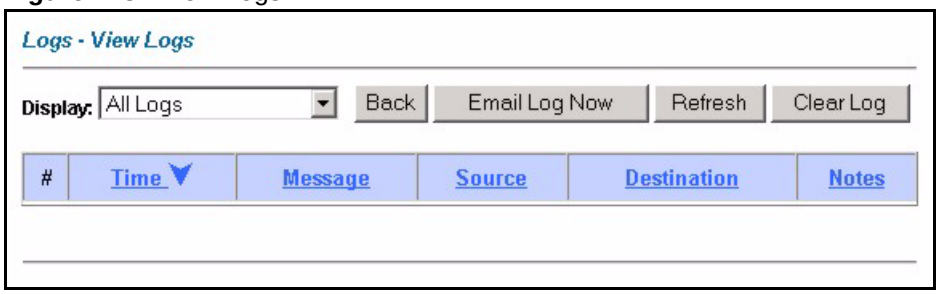
LABEL	DESCRIPTION
Send log to	Logs are sent to the e-mail address specified in this field. If this field is left blank, logs will not be sent via e-mail.
Send alerts to	Alerts are sent to the e-mail address specified in this field. If this field is left blank, alerts will not be sent via e-mail.
UNIX Syslog	Syslog logging sends a log to an external syslog server used to store logs.
Active	Click **Active** to enable syslog logging.
Syslog IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Send Log	
Log Schedule	This drop-down menu is used to configure the frequency of log messages being sent as E-mail: Daily Weekly Hourly When Log is Full None. If you select **Weekly** or **Daily**, specify a time of day when the E-mail should be sent. If you select **Weekly**, then also specify which day of the week the E-mail should be sent. If you select **When Log is Full**, an alert is sent when the log fills up. If you select **None**, no log messages are sent
Day for Sending Log	Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Log	Select the categories of logs that you want to record. Logs include alerts.
Send Immediate Alert	Select the categories of alerts for which you want the Prestige to instantly e-mail alerts to the e-mail address specified in the **Send Alerts To** field.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to return to the previously saved settings.

22.3 Displaying the Logs

Click **Logs** and then **View Log** to open the **View Logs** screen. Use the **View Logs** screen to see the logs for the categories that you selected in the **Log Settings** screen (see the Configuring Log Settings section).

Log entries in red indicate alerts. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.

Figure 123 View Logs



The following table describes the fields in this screen.

Table 82 View Logs

LABEL	DESCRIPTION
Display	The categories that you select in the **Log Settings** screen (see *section*) display in the drop-down list box. Select a category of logs to view; select **All Logs** to view logs from all of the log categories that you selected in the **Log Settings** page.
Time	This field displays the time the log was recorded. See the chapter on system maintenance and information to configure the Prestige's time and date.
Message	This field states the reason for the log.
Source	This field lists the source IP address and the port number of the incoming packet.
Destination	This field lists the destination IP address and the port number of the incoming packet.
Notes	This field displays additional information about the log entry.
Back	Click **Back** to return to the previous screen
Email Log Now	Click **Email Log Now** to send the log screen to the e-mail address specified in the **Log Settings** page (make sure that you have first filled in the **Address Info** fields in **Log Settings**, see *the Configuring Log Settings section*).
Refresh	Click **Refresh** to renew the log screen.
Clear Log	Click **Clear Log** to delete all the logs.

22.4 SMTP Error Messages

If there are difficulties in sending e-mail the following error messages appear.

E-mail error messages appear in SMT menu 24.3.1 as "SMTP action request failed. ret= ??". The "??"are described in the following table.

Table 83 SMTP Error Messages

-1 means Prestige out of socket
-2 means tcp SYN fail
-3 means smtp server OK fail

Table 83 SMTP Error Messages (continued)

-4 means HELO fail
-5 means MAIL FROM fail
-6 means RCPT TO fail
-7 means DATA fail
-8 means mail data send fail

22.4.1 Example E-mail Log

An "End of Log" message displays for each mail in which a complete log has been sent. The following is an example of a log sent by e-mail.

- You may edit the subject title.
- The date format here is Day-Month-Year.
- The date format here is Month-Day-Year. The time format is Hour-Minute-Second.
- "`End of Log`" message shows that a complete log has been sent.

Figure 124 E-mail Log Example

```
Subject:
        Firewall Alert From Prestige
   Date:
        Fri, 07 Apr 2000 10:05:42
   From:
        user@zyxel.com
     To:
        user@zyxel.com
  1|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |default policy
|forward
   | 09:54:03 |UDP     src port:00520 dest port:00520  |<1,00>          |
  2|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |default policy
|forward
   | 09:54:17 |UDP     src port:00520 dest port:00520  |<1,00>          |
  3|Apr  7 00 |From:192.168.1.6     To:10.10.10.10 |match           |forward
   | 09:54:19 |UDP     src port:03516 dest port:00053  |<1,01>          |
……..{snip}……..
……..{snip}……..
126|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match          |forward
   | 10:05:00 |UDP     src port:00520 dest port:00520  |<1,02>          |
127|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |match          |forward
   | 10:05:17 |UDP     src port:00520 dest port:00520  |<1,02>          |
128|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match          |forward
   | 10:05:30 |UDP     src port:00520 dest port:00520  |<1,02>          |
End of Firewall Log
```

CHAPTER 23
Media Bandwidth Management Advanced Setup

This chapter describes the functions and advanced configuration of bandwidth management.

23.1 Bandwidth Management Advanced Setup Overview

Bandwidth management allows you to allocate an interface's outgoing capacity to specific types of traffic. It can also help you make sure that the Prestige forwards certain types of traffic (especially real-time applications) with minimum delay. With the use of real-time applications such as Voice-over-IP (VoIP) increasing, the requirement for bandwidth allocation is also increasing.

Bandwidth management addresses questions such as:

- Who gets how much access to specific applications?
- What priority level should you give to each type of traffic?
- Which traffic must have guaranteed delivery?
- How much bandwidth should be allotted to guarantee delivery?

Bandwidth management also allows you to configure the allowed output for an interface to match what the network can handle. This helps reduce delays and dropped packets at the next routing device. For example, you can set the WAN interface speed to 1000kbps if the ADSL connection has an upstream speed of 1000kbps. All configuration screens display measurements in kbps (kilobits per second), but this *User's Guide* also uses Mbps (megabits per second) for brevity's sake.

You can use the wizard setup screens to configure basic bandwidth management. Refer to Chapter 4 Wizard Setup for Media Bandwidth Management for more information.

23.2 Bandwidth Classes and Filters

Use bandwidth classes and child-classes to allocate specific amounts of bandwidth capacity (bandwidth budgets). Configure a bandwidth filter to define a bandwidth class (or child-class) based on a specific application and/or subnet. Use the **Class Configuration** screen (see the Configuring Class Setup section) to set up a bandwidth class's name, bandwidth allotment, and bandwidth filter. You can configure up to one bandwidth filter per bandwidth class. You can also configure bandwidth classes without bandwidth filters. However, it is recommended

that you configure child-classes with filters for any classes that you configure without filters. The Prestige leaves the bandwidth budget allocated and unused for a class that does not have a filter itself or child-classes with filters. View your configured bandwidth classes and child-classes in the **Class Setup** screen (see the Configuring Class Setup section for details).

The total of the configured bandwidth budgets for child-classes cannot exceed the configured bandwidth budget speed of the parent class.

23.3 Proportional Bandwidth Allocation

Bandwidth management allows you to define how much bandwidth each class gets; however, the actual bandwidth allotted to each class decreases or increases in proportion to actual available bandwidth.

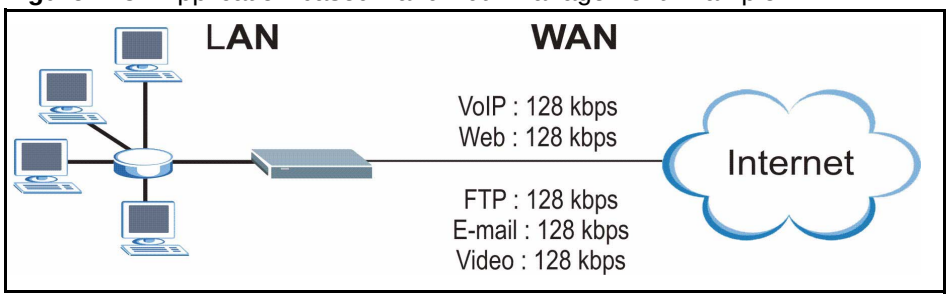
23.4 Bandwidth Management Usage Examples

These examples show bandwidth management allotments on a WAN interface that is configured for 640Kbps.

23.4.1 Application-based Bandwidth Management Example

The bandwidth classes in the following example are based solely on application. Each bandwidth class (VoIP, Web, FTP, E-mail and Video) is allotted 128kbps.

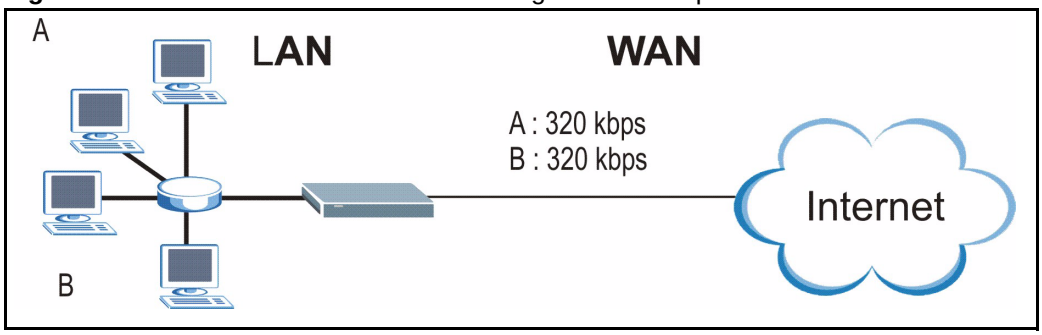
Figure 125 Application-based Bandwidth Management Example



23.4.2 Subnet-based Bandwidth Management Example

The following example uses bandwidth classes based solely on LAN subnets. Each bandwidth class (Subnet A and Subnet B) is allotted 320kbps.

Figure 126 Subnet-based Bandwidth Management Example



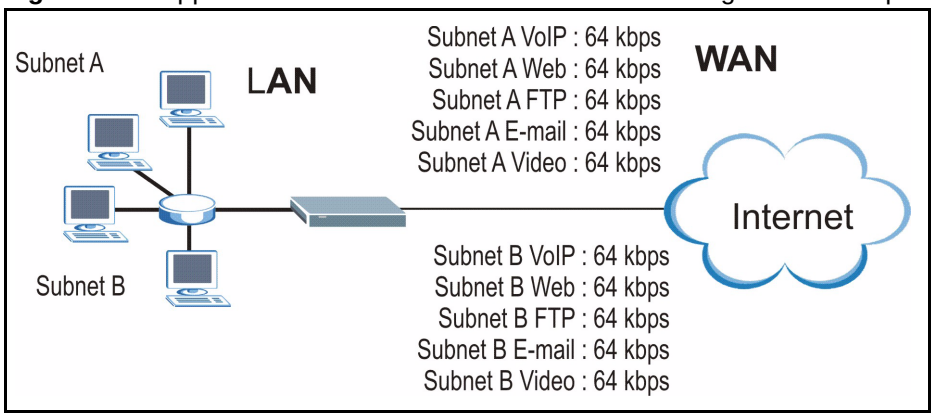
23.4.3 Application and Subnet-based Bandwidth Management Example

The following example uses bandwidth classes based on LAN subnets and applications (specific applications in each subnet are allotted bandwidth).

Table 84 Application and Subnet-based Bandwidth Management Example

TRAFFIC TYPE	FROM SUBNET A	FROM SUBNET B
VoIP	64 kbps	64 kbps
Web	64 kbps	64 kbps
FTP	64 kbps	64 kbps
E-mail	64 kbps	64 kbps
Video	64 kbps	64 kbps

Figure 127 Application and Subnet-based Bandwidth Management Example



23.5 Scheduler

The scheduler divides up an interface's bandwidth among the bandwidth classes. The Prestige has two types of scheduler: fairness-based and priority-based.

23.5.1 Priority-based Scheduler

With the priority-based scheduler, the Prestige forwards traffic from bandwidth classes according to the priorities that you assign to the bandwidth classes. The larger a bandwidth class's priority number is, the higher the priority. Assign real-time applications (like those using audio or video) a higher priority number to provide smoother operation.

23.5.2 Fairness-based Scheduler

The Prestige divides bandwidth equally among bandwidth classes when using the fairness-based scheduler; thus preventing one bandwidth class from using all of the interface's bandwidth.

23.6 Maximize Bandwidth Usage

The maximize bandwidth usage option (see the Maximize Bandwidth Usage With Bandwidth Borrowing section) allows the Prestige to divide up any available bandwidth on the interface (including unallocated bandwidth and any allocated bandwidth that a class is not using) among the bandwidth classes that require more bandwidth.

When you enable maximize bandwidth usage, the Prestige first makes sure that each bandwidth class gets up to its bandwidth allotment. Next, the Prestige divides up an interface's available bandwidth (bandwidth that is unbudgeted or unused by the classes) depending on how many bandwidth classes require more bandwidth and on their priority levels. When only one class requires more bandwidth, the Prestige gives extra bandwidth to that class.

When multiple classes require more bandwidth, the Prestige gives the highest priority classes the available bandwidth first (as much as they require, if there is enough available bandwidth), and then to lower priority classes if there is still bandwidth available. The Prestige distributes the available bandwidth equally among classes with the same priority level.

23.6.1 Reserving Bandwidth for Non-Bandwidth Class Traffic

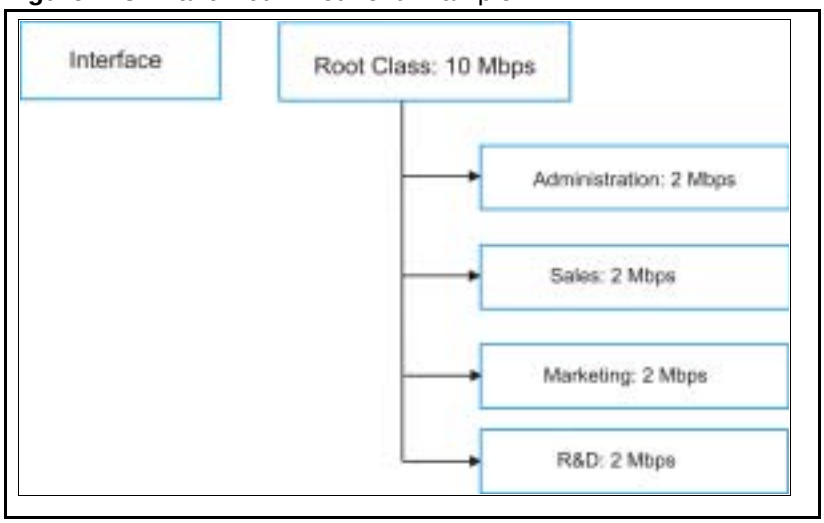
Do the following three steps to configure the Prestige to allow bandwidth for traffic that is not defined in a bandwidth filter.

1. Leave some of the interface's bandwidth unbudgeted.
2. Do not enable the interface's **Maximize Bandwidth Usage** option.
3. Do not enable bandwidth borrowing on the child-classes that have the root class as their parent (see the Bandwidth Borrowing section).

23.6.2 Maximize Bandwidth Usage Example

Here is an example of a Prestige that has maximized bandwidth usage enabled on an interface. The first figure shows each bandwidth class's bandwidth budget and priority. The classes are set up based on subnets. The interface is set to 10 Mbps. Each subnet is allocated 2 Mbps. The unbudgeted 2 Mbps allows traffic not defined in one of the bandwidth filters to go out when you do not select the maximize bandwidth option.

Figure 128 Bandwidth Allotment Example

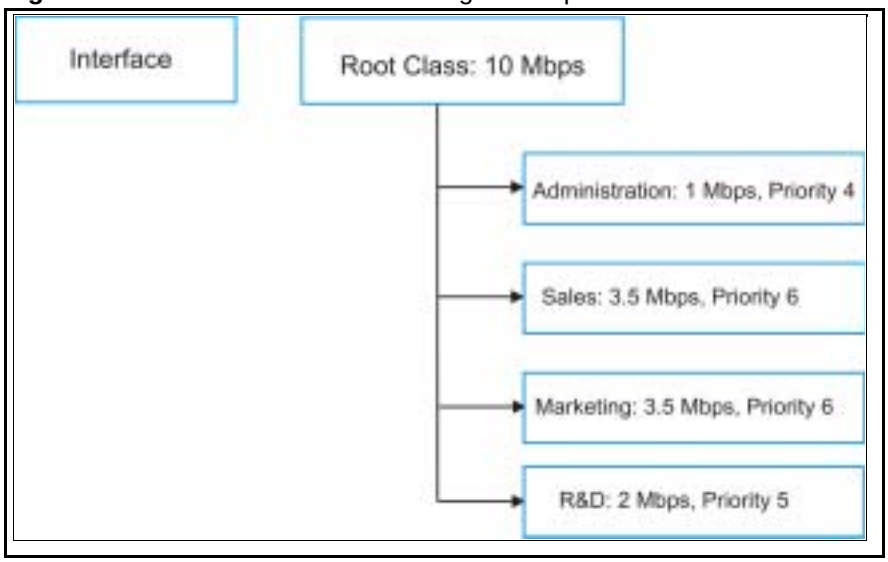


The following figure shows the bandwidth usage with the maximize bandwidth usage option enabled. The Prestige divides up the unbudgeted 2 Mbps among the classes that require more bandwidth. If the administration department only uses 1 Mbps of the budgeted 2 Mbps, the Prestige also divides the remaining 1 Mbps among the classes that require more bandwidth. Therefore, the Prestige divides a total of 3 Mbps total of unbudgeted and unused bandwidth among the classes that require more bandwidth.

In this case, suppose that all of the classes except for the administration class need more bandwidth.

- Each class gets up to its budgeted bandwidth. The administration class only uses 1 Mbps of its budgeted 2 Mbps.
- Sales and Marketing are first to get extra bandwidth because they have the highest priority (6). If they each require 1.5 Mbps or more of extra bandwidth, the Prestige divides the total 3 Mbps total of unbudgeted and unused bandwidth equally between the sales and marketing departments (1.5 Mbps extra to each for a total of 3.5 Mbps for each) because they both have the highest priority level.
- R&D requires more bandwidth but only gets its budgeted 2 Mbps because all of the unbudgeted and unused bandwidth goes to the higher priority sales and marketing classes.
- The Prestige does not send any traffic that is not defined in the bandwidth filters because all of the unbudgeted bandwidth goes to the classes that need it.

Figure 129 Maximize Bandwidth Usage Example



23.7 Bandwidth Borrowing

Bandwidth borrowing allows a child-class to borrow unused bandwidth from its parent class, whereas maximize bandwidth usage allows bandwidth classes to borrow any unused or unbudgeted bandwidth on the whole interface.

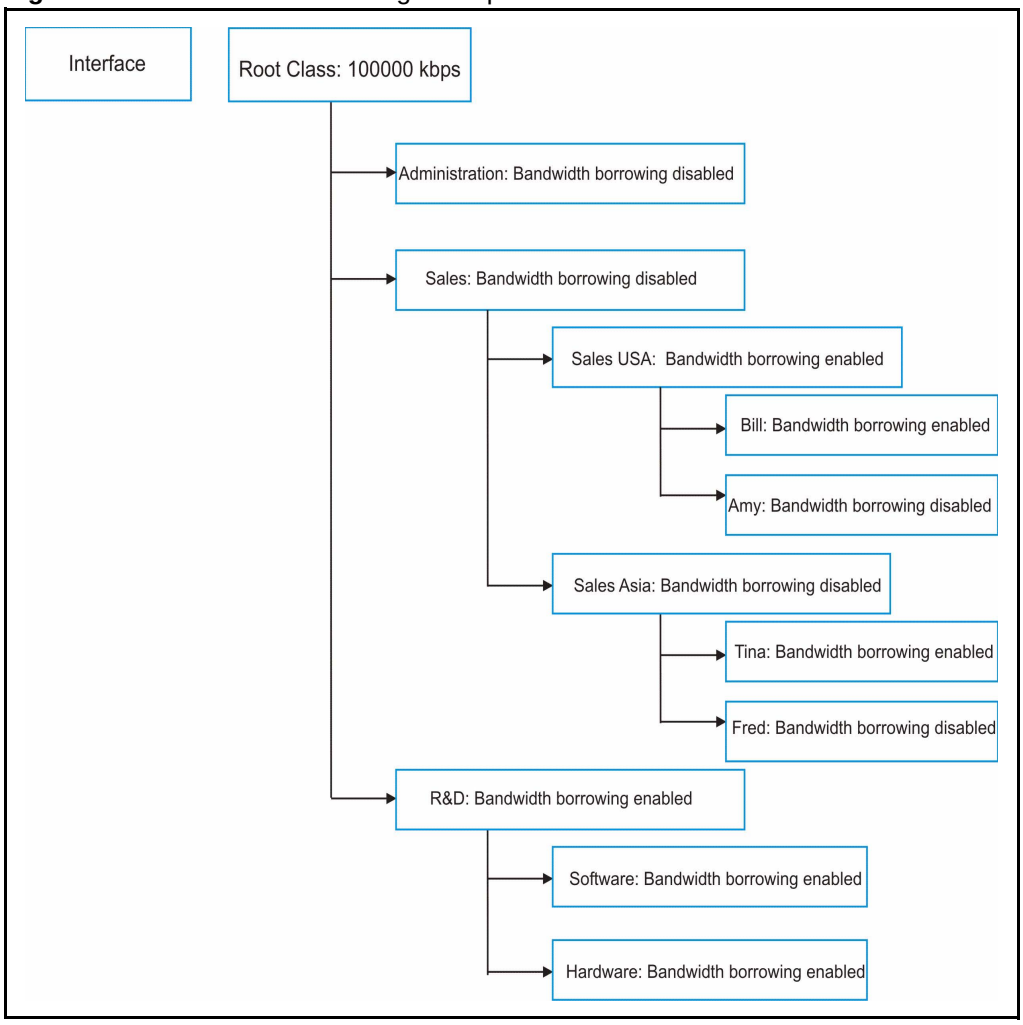
Enable bandwidth borrowing on a child-class to allow the child-class to use its parent class's unused bandwidth. A parent class's unused bandwidth is given to the highest priority child-class first. The child-class can also borrow bandwidth from a higher parent class (grandparent class) if the child-class's parent class is also configured to borrow bandwidth from its parent class. This can go on for as many levels as are configured to borrow bandwidth from their parent class (see the Bandwidth Borrowing Example section).

The total of the bandwidth allotments for child-classes cannot exceed the bandwidth allotment of their parent class. The Prestige uses the scheduler to divide a parent class's unused bandwidth among the child-classes.

23.7.1 Bandwidth Borrowing Example

Here is an example of bandwidth management with classes configured for bandwidth borrowing. The classes are set up based on departments and individuals within certain departments.

Figure 130 Bandwidth Borrowing Example



- The Bill class can borrow unused bandwidth from the Sales USA class because the Bill class has bandwidth borrowing enabled.
- The Bill class can also borrow unused bandwidth from the Sales class because the Sales USA class also has bandwidth borrowing enabled.
- The Bill class cannot borrow unused bandwidth from the Root class because the Sales class has bandwidth borrowing disabled.
- The Amy class cannot borrow unused bandwidth from the Sales USA class because the Amy class has bandwidth borrowing disabled.
- The R&D Software and Hardware classes can both borrow unused bandwidth from the R&D class because the R&D Software and Hardware classes both have bandwidth borrowing enabled.
- The R&D Software and Hardware classes can also borrow unused bandwidth from the Root class because the R&D class also has bandwidth borrowing enabled.

23.7.2 Maximize Bandwidth Usage With Bandwidth Borrowing

If you configure both maximize bandwidth usage (on the interface) and bandwidth borrowing (on individual child-classes), the Prestige functions as follows.

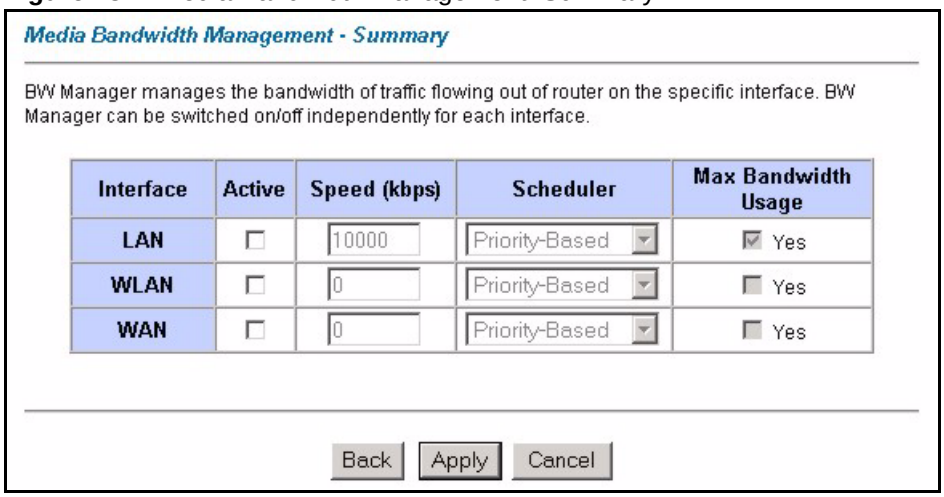
1. The Prestige sends traffic according to each bandwidth class's bandwidth budget.
2. The Prestige assigns a parent class's unused bandwidth to its child-classes that have more traffic than their budgets and have bandwidth borrowing enabled. The Prestige gives priority to bandwidth child-classes of higher priority and treats bandwidth classes of the same priority equally.
3. The Prestige assigns any remaining unused or unbudgeted bandwidth on the interface to any bandwidth class that requires it. The Prestige gives priority to bandwidth classes of higher priority and treats bandwidth classes of the same level equally.
4. The Prestige assigns any remaining unbudgeted bandwidth to traffic that does not match any of the bandwidth classes.

23.8 Configuring Summary

Click **Media Bandwidth Management**, **Summary** to open the screen as shown next.

Enable bandwidth management on an interface and set the maximum allowed bandwidth for that interface.

Figure 131 Media Bandwidth Management: Summary



The following table describes the labels in this screen.

Table 85 Media Bandwidth Management: Summary

LABEL	DESCRIPTION
LAN WLAN WAN	These read-only labels represent the physical interfaces. Select an interface's check box to enable bandwidth management on that interface. Bandwidth management applies to all traffic flowing out of the router through the interface, regardless of the traffic's source. Traffic redirect or IP alias may cause LAN-to-LAN traffic to pass through the Prestige and be managed by bandwidth management.
Active	Select an interface's check box to enable bandwidth management on that interface.
Speed (kbps)	Enter the amount of bandwidth for this interface that you want to allocate using bandwidth management. This appears as the bandwidth budget of the interface's root class. The recommendation is to set this speed to match what the interface's connection can handle. For example, set the WAN interface speed to 1000 kbps if the ADSL connection has an upstream speed of 1000 kbps.
Scheduler	Select either **Priority-Based** or **Fairness-Based** from the drop-down menu to control the traffic flow. Select **Priority-Based** to give preference to bandwidth classes with higher priorities. Select **Fairness-Based** to treat all bandwidth classes equally. .
Maximize Bandwidth Usage	Select this check box to have the Prestige divide up all of the interface's unallocated and/or unused bandwidth among the bandwidth classes that require bandwidth. Do not select this if you want to reserve bandwidth for traffic that does not match a bandwidth class or you want to limit the speed of this interface (see the **Speed** field description).
Back	Click **Back** to go to the main **Media Bandwidth Management** screen.
Apply	Click **Apply** to save your settings back to the Prestige.
Cancel	Click **Cancel** to begin configuring this screen afresh.

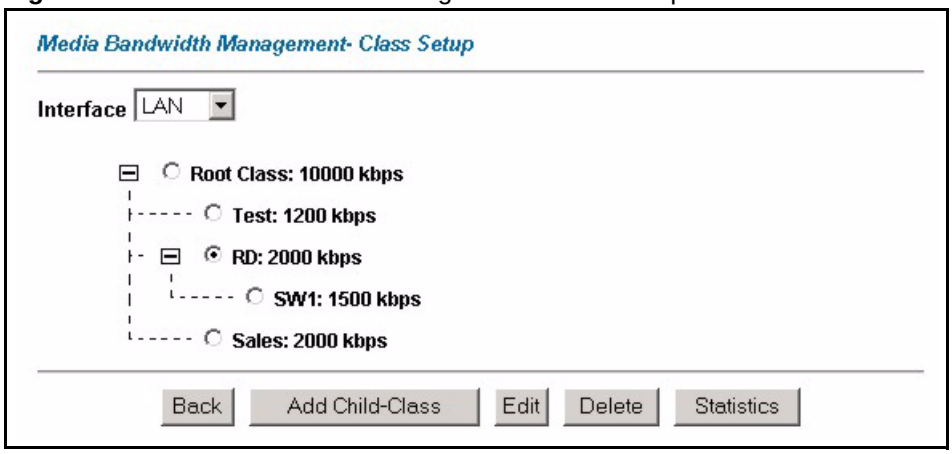
23.9 Configuring Class Setup

The class setup screen displays the configured bandwidth classes by individual interface. Select an interface and click the buttons to perform the actions described next. Click "+" to expand the class tree or click "-" to collapse the class tree. Each interface has a permanent root class. The bandwidth budget of the root class is equal to the speed you configured on the interface (see the Configuring Summary section to configure the speed of the interface). Configure child-class layers for the root class.

To add or delete child classes on an interface, click **Media Bandwidth Management**, then **Class Setup**. The screen appears as shown (with example classes).

The example reserves 10 Mbps of unbudgeted bandwidth for traffic that is not defined in the bandwidth filters (see the Reserving Bandwidth for Non-Bandwidth Class Traffic section). The Administration and Sales USA bandwidth classes each have bigger bandwidth budgets than the total of the budgets of their child-classes. The child-classes can borrow the extra bandwidth as long as they have bandwidth borrowing enabled (see the Bandwidth Borrowing section).

Figure 132 Media Bandwidth Management: Class Setup



The following table describes the labels in this screen.

Table 86 Media Bandwidth Management: Class Setup

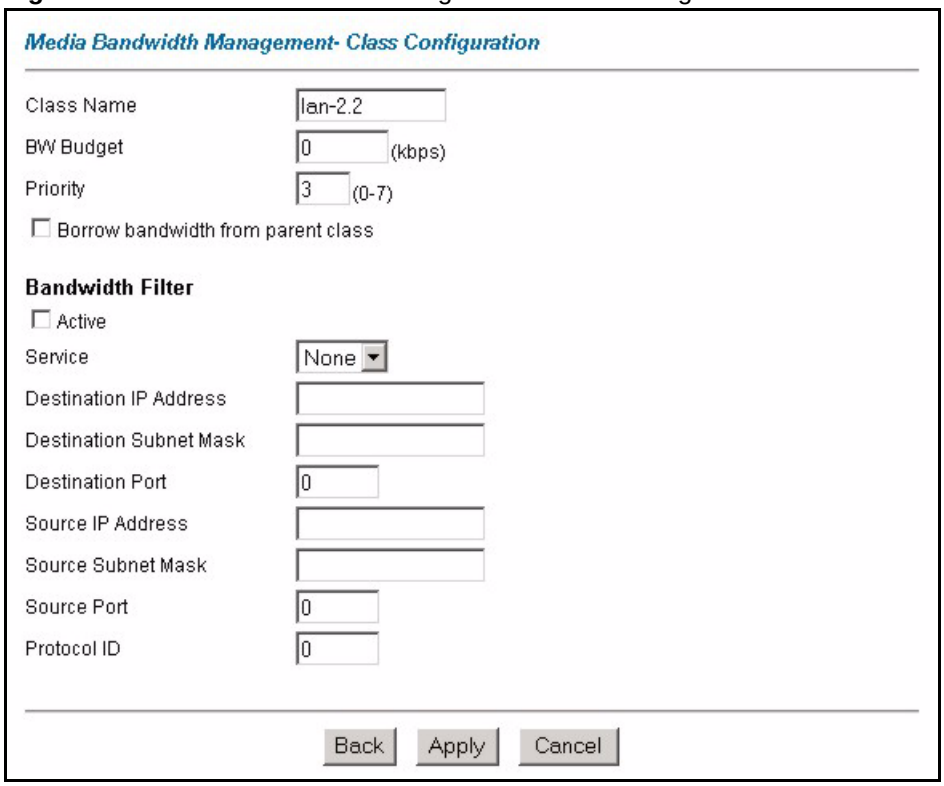
LABEL	DESCRIPTION
Interface	Select an interface from the drop-down list box for which you wish to set up classes.
Back	Click **Back** to go to the main **Media Bandwidth Management** screen.
Add Child-Class	Click **Add Child-class** to add a sub-class.
Edit	Click **Edit** to configure the selected class. You cannot edit the root class.
Delete	Click **Delete** to delete the class and all its child-classes. You cannot delete the root class.
Statistics	Click **Statistics** to display the status of the selected class.

23.9.1 Media Bandwidth Management Class Configuration

Configure a bandwidth management class in the **Class Configuration** screen. You must use the **Media Bandwidth Management - Summary** screen to enable bandwidth management on an interface before you can configure classes for that interface.

To add a child class, click **Media Bandwidth Management**, then **Class Setup**. Click the **Add Child-Class** button to open the following screen.

Figure 133 Media Bandwidth Management: Class Configuration



The following table describes the labels in this screen

Table 87 Media Bandwidth Management: Class Configuration

LABEL	DESCRIPTION
Class Name	Use the auto-generated name or enter a descriptive name of up to 20 alphanumeric characters, including spaces.
BW Budget (kbps)	Specify the maximum bandwidth allowed for the class in kbps. The recommendation is a setting between 20 kbps and 20000 kbps for an individual class.
Priority	Enter a number between 0 and 7 to set the priority of this class. The higher the number, the higher the priority. The default setting is 3.
Borrow bandwidth from parent class	Select this option to allow a child-class to borrow bandwidth from its parent class if the parent class is not using up its bandwidth budget. Bandwidth borrowing is governed by the priority of the child-classes. That is, a child-class with the highest priority (7) is the first to borrow bandwidth from its parent class. Do not select this for the classes directly below the root class if you want to leave bandwidth available for other traffic types or you want to set the interface's speed to match what the next device in network can handle (see the **Speed** field description in the **Summary** screen).
Bandwidth Filter The Prestige uses a bandwidth filter to identify the traffic that belongs to a bandwidth class.	
Active	Select the check box to have the Prestige use this bandwidth filter when it performs bandwidth management.

Table 87 Media Bandwidth Management: Class Configuration (continued)

LABEL	DESCRIPTION
Service	You can select a predefined service instead of configuring the **Destination Port**, **Source Port** and **Protocol ID** fields. SIP (Session Initiation Protocol) is a signaling protocol used in Internet telephony, instant messaging and other VoIP (Voice over IP) applications. Select **SIP** from the drop-down list box to configure this bandwidth filter for traffic that uses SIP. File Transfer Protocol (FTP) is an Internet file transfer service that operates on the Internet and over TCP/IP networks. A system running the FTP server accepts commands from a system running an FTP client. The service allows users to send commands to the server for uploading and downloading files. Select **FTP** from the drop-down list box to configure this bandwidth filter for FTP traffic. H.323 is a standard teleconferencing protocol suite that provides audio, data and video conferencing. It allows for real-time point-to-point and multipoint communication between client computers over a packet-based network that does not provide a guaranteed quality of service. Select **H.323** from the drop-down list box to configure this bandwidth filter for traffic that uses H.323. When you select **None**, the bandwidth class applies to all services unless you specify one by configuring the **Destination Port**, **Source Port** and **Protocol ID** fields.
Destination IP Address	Enter the destination IP address in dotted decimal notation. A blank destination IP address means any destination IP address.
Destination Subnet Mask	Enter the destination subnet mask. This field is N/A if you do not specify a **Destination IP Address**. Refer to the appendix for more information on IP subnetting.
Destination Port	Enter the port number of the destination. A blank destination port means any destination port.
Source IP Address	Enter the source IP address. A blank source IP address means any source IP address.
Source Subnet Mask	Enter the source subnet mask. This field is N/A if you do not specify a **Source IP Address**. Refer to the appendix for more information on IP subnetting.
Source Port	Enter the port number of the source. See the following table for some common services and port numbers. A blank source port means any source port number.
Protocol ID	Enter the protocol ID (service type) number, for example: 1 for ICMP, 6 for TCP or 17 for UDP. A blank protocol ID means any protocol number.
Back	Click **Back** to go to the main **Media Bandwidth Management** screen.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Table 88 Services and Port Numbers

SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53

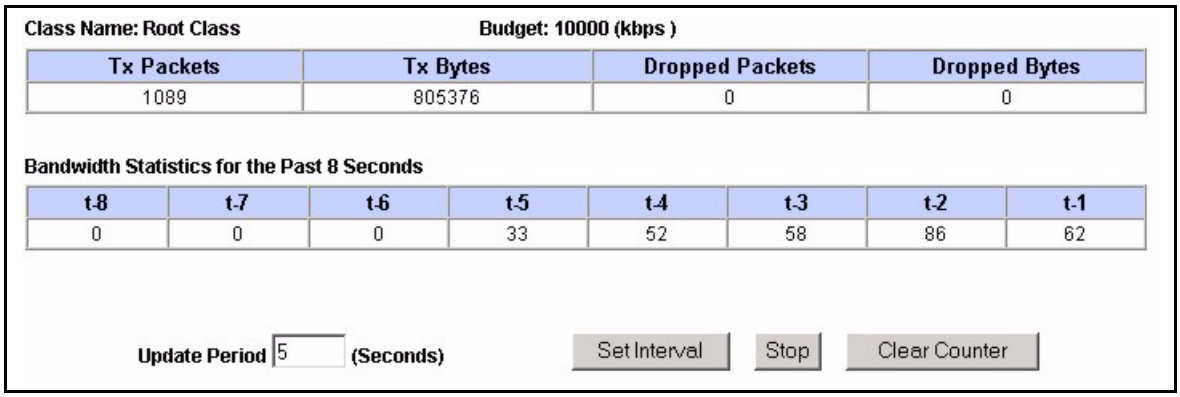
Table 88 Services and Port Numbers

SERVICES	PORT NUMBER
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

23.9.2 Media Bandwidth Management Statistics

Use the **Media Bandwidth Management Statistics** screen to view network performance information. Click the **Statistics** button in the **Class Setup** screen to open the **Statistics** screen.

Figure 134 Media Bandwidth Management Statistics



The following table describes the labels in this screen.

Table 89 Media Bandwidth Management Statistics

LABEL	DESCRIPTION
Class Name	This field displays the name of the class the statistics page is showing.
Budget (kbps)	This field displays the amount of bandwidth allocated to the class.
Tx Packets	This field displays the total number of packets transmitted.
Tx Bytes	This field displays the total number of bytes transmitted.
Dropped Packets	This field displays the total number of packets dropped.
Dropped Bytes	This field displays the total number of bytes dropped.
Bandwidth Statistics for the Past 8 Seconds (t-8 to t-1)	
This field displays the bandwidth statistics (in bps) for the past one to eight seconds. For example, t-1 means one second ago.	
Update Period (seconds)	Enter the time interval in seconds to define how often the information should be refreshed.

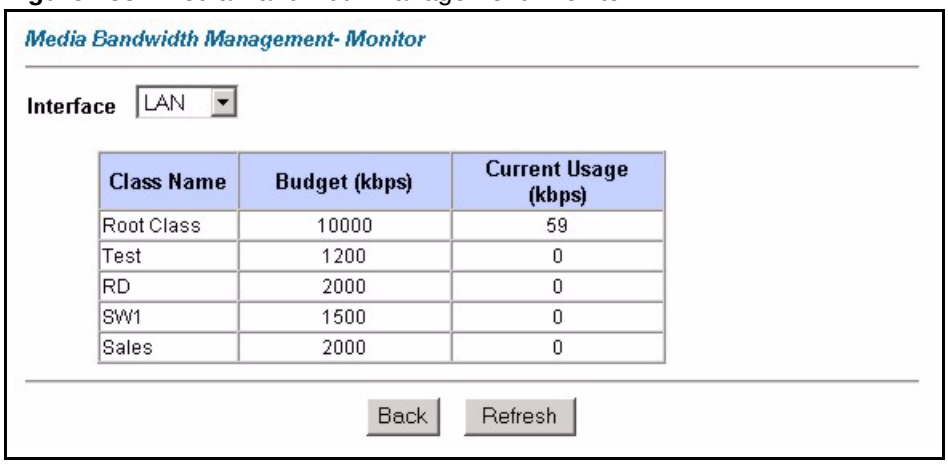
Table 89 Media Bandwidth Management Statistics

LABEL	DESCRIPTION
Set Interval	Click **Set Interval** to apply the new update period you entered in the **Update Period** field above.
Stop Update	Click **Stop Update** to stop the browser from refreshing bandwidth management statistics.
Clear Counter	Click **Clear Counter** to clear all of the bandwidth management statistics.

23.10 Bandwidth Monitor

To view the Prestige's bandwidth usage and allotments, click **Media Bandwidth Management**, then **Monitor**. The screen appears as shown.

Figure 135 Media Bandwidth Management: Monitor



The following table describes the labels in this screen.

Table 90 Media Bandwidth Management: Monitor

LABEL	DESCRIPTION
Interface	Select an interface from the drop-down list box to view the bandwidth usage of its bandwidth classes.
Class Name	This field displays the name of the class.
Budget (kbps)	This field displays the amount of bandwidth allocated to the class.
Current Usage (kbps)	This field displays the amount of bandwidth that each class is using.
Back	Click **Back** to go to the main **Media Bandwidth Management** screen.
Refresh	Click **Refresh** to update the page.

CHAPTER 24
Maintenance

This chapter displays system information such as ZyNOS firmware, port IP addresses and port traffic statistics.

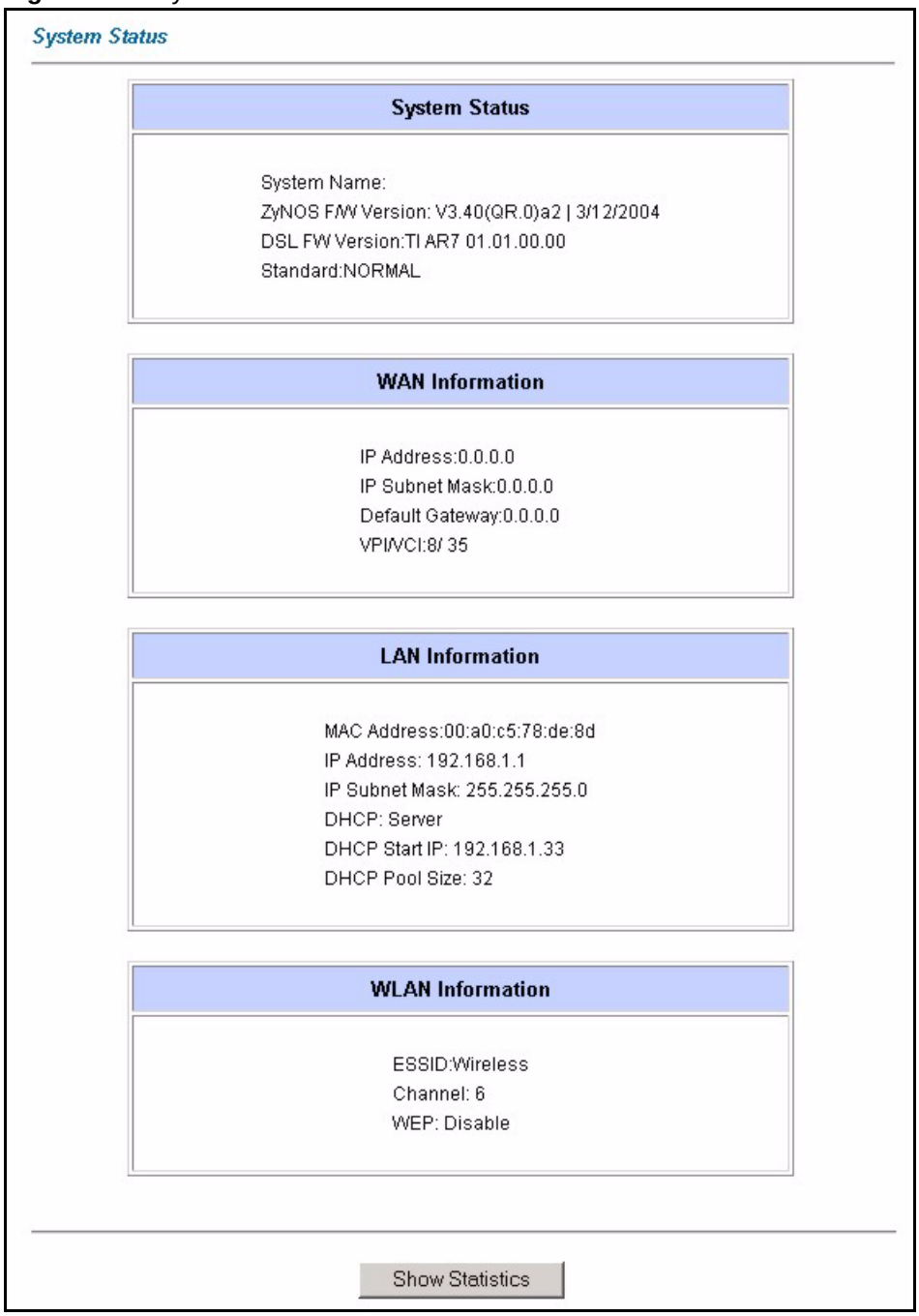
24.1 Maintenance Overview

The maintenance screens can help you view system information, upload new firmware, manage configuration and restart your Prestige.

24.2 System Status Screen

Click **System Status** to open the following screen, where you can use to monitor your Prestige. Note that these fields are READ-ONLY and only for diagnostic purposes.

Figure 136 System Status



The following table describes the fields in this screen.

Table 91 System Status

LABEL	DESCRIPTION
System Status	
System Name	This is the name of your Prestige. It is for identification purposes.

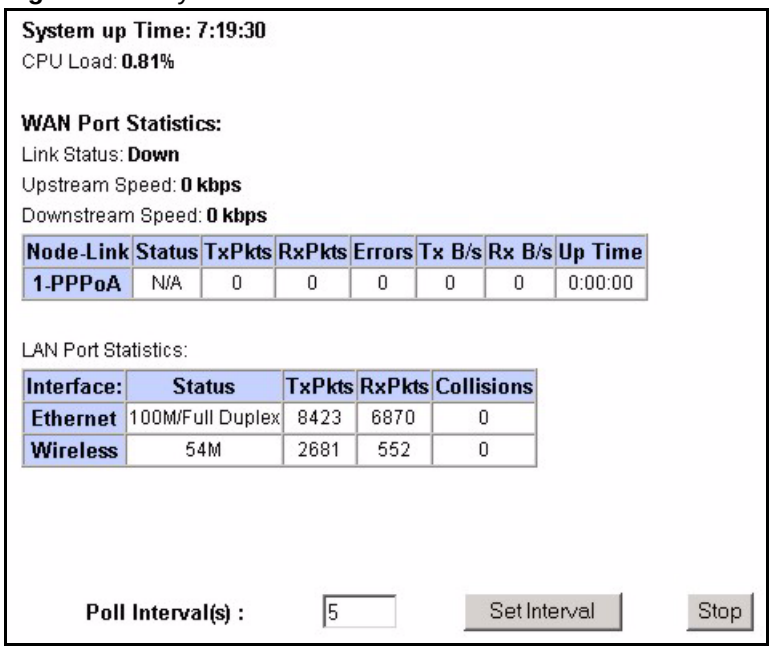
Table 91 System Status (continued)

LABEL	DESCRIPTION
ZyNOS Firmware Version	This is the ZyNOS firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design.
DSL FW Version	This is the DSL firmware version associated with your Prestige.
Standard	This is the standard that your Prestige is using.
WAN Information	
IP Address	This is the WAN port IP address.
IP Subnet Mask	This is the WAN port IP subnet mask.
Default Gateway	This is the IP address of the default gateway, if applicable.
VPI/VCI	This is the Virtual Path Identifier and Virtual Channel Identifier that you entered in the first Wizard screen.
LAN Information	
MAC Address	This is the MAC (Media Access Control) or Ethernet address unique to your Prestige.
IP Address	This is the LAN port IP address.
IP Subnet Mask	This is the LAN port IP subnet mask.
DHCP	This is the WAN port DHCP role - **Server**, **Relay** (not all Prestige models) or **None**.
DHCP Start IP	This is the first of the contiguous addresses in the IP address pool.
DHCP Pool Size	This is the number of IP addresses in the IP address pool.
WLAN Information	
ESSID	This is the descriptive name used to identify the Prestige in the wireless LAN.
Channel	This is the channel number used by the Prestige now.
WEP	This displays the status of WEP data encryption.
Show Statistics	Click **Show Statistics** to see the performance statistics such as number of packets sent and number of packets received for each port.

24.2.1 System Statistics

Click **Show Statistics** in the **System Status** screen to open the following screen. Read-only information here includes port status and packet specific statistics. Also provided are "system up time" and "poll interval(s)". The **Poll Interval(s)** field is configurable.

Figure 137 System Status: Show Statistics



The following table describes the fields in this screen.

Table 92 System Status: Show Statistics

LABEL	DESCRIPTION
System up Time	This is the elapsed time the system has been up.
CPU Load	This field specifies the percentage of CPU utilization.
LAN or WAN Port Statistics	This is the WAN or LAN port.
Link Status	This is the status of your WAN link.
Upstream Speed	This is the upstream speed of your Prestige.
Downstream Speed	This is the downstream speed of your Prestige.
Node-Link	This field displays the remote node index number and link type. Link types are PPPoA, ENET, RFC 1483 and PPPoE.
Interface	This field displays the type of port.
Status	For the WAN port, this displays the port speed and duplex setting if you're using Ethernet encapsulation and **down** (line is down), **idle** (line (ppp) idle), **dial** (starting to trigger a call) and **drop** (dropping a call) if you're using PPPoE encapsulation. For a LAN port, this shows the port speed and duplex setting.
TxPkts	This field displays the number of packets transmitted on this port.
RxPkts	This field displays the number of packets received on this port.
Errors	This field displays the number of error packets on this port.
Tx B/s	This field displays the number of bytes transmitted in the last second.
Rx B/s	This field displays the number of bytes received in the last second.
Up Time	This field displays the elapsed time this port has been up.
Collisions	This is the number of collisions on this port.

Table 92 System Status: Show Statistics (continued)

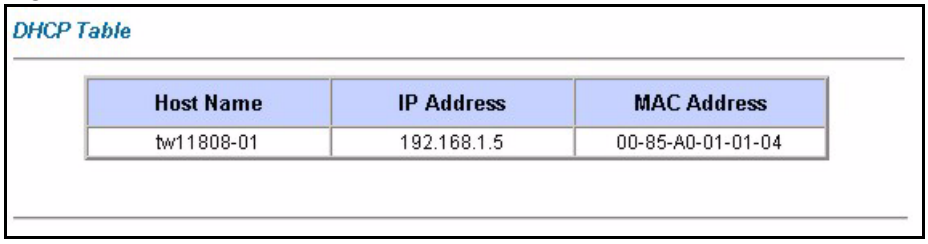
LABEL	DESCRIPTION
Poll Interval(s)	Type the time interval for the browser to refresh system statistics.
Set Interval	Click this button to apply the new poll interval you entered in the **Poll Interval** field above.
Stop	Click this button to halt the refreshing of the system statistics.

24.3 DHCP Table Screen

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the Prestige as a DHCP server or disable it. When configured as a server, the Prestige provides the TCP/IP configuration for the clients. If set to **None**, DHCP service will be disabled and you must have another DHCP server on your LAN, or else the computer must be manually configured.

Click **Maintenance**, and then the **DHCP Table** tab. Read-only information here relates to your DHCP status. The DHCP table shows current DHCP Client information (including **IP Address**, **Host Name** and **MAC Address**) of all network clients using the DHCP server.

Figure 138 DHCP Table



The following table describes the fields in this screen.

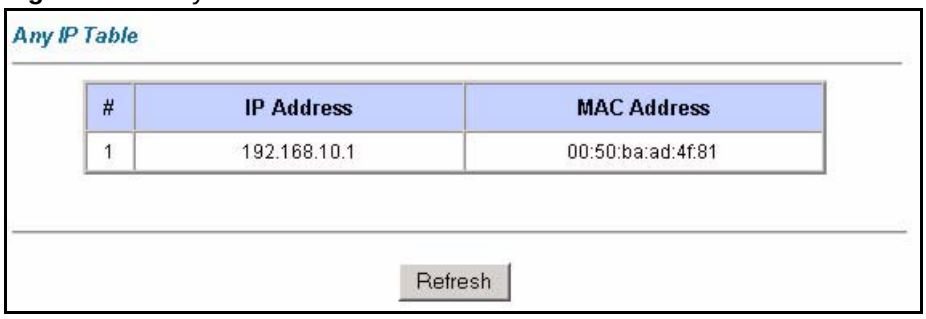
Table 93 DHCP Table

LABEL	DESCRIPTION
Host Name	This is the name of the host computer.
IP Address	This field displays the IP address relative to the **Host Name** field.
MAC Address	This field displays the MAC (Media Access Control) address of the computer with the displayed host name. Every Ethernet device has a unique MAC address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

24.4 Any IP Table Screen

Click **Maintenance**, **Any IP**. The Any IP table shows current read-only information (including the IP address and the MAC address) of all network devices that use the Any IP feature to communicate with the Prestige. Refer to the Any IP section for more information.

Figure 139 Any IP Table



The following table describes the labels in this screen.

Table 94 Any IP Table

LABEL	DESCRIPTION
#	This field displays the index number.
IP Address	This field displays the IP address of the network device.
MAC Address	This field displays the MAC (Media Access Control) address of the computer with the displayed IP address. Every Ethernet device has a unique MAC address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
Refresh	Click **Refresh** to update this screen.

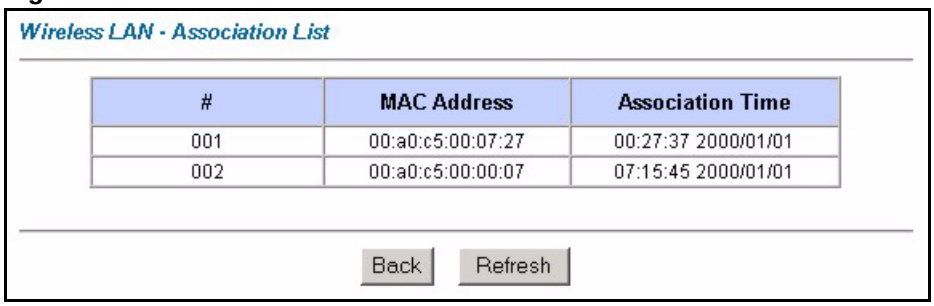
24.5 Wireless Screen

The read-only screen displays information about the Prestige's wireless LAN.

24.5.1 Association List

This screen displays the MAC address(es) of the wireless stations that are currently logged in to the network. Click **Wireless LAN** and then **Association List** to open the screen shown next.

Figure 140 Association List



The following table describes the fields in this screen.

Table 95 Association List

LABEL	DESCRIPTION
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC (Media Access Control) address of an associated wireless station. Every Ethernet device has a unique MAC address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
Association Time	This field displays the time a wireless station is associated to the Prestige.
Back	Click **Back** to return to the previous screen.
Refresh	Click **Refresh** to renew the information in the table.

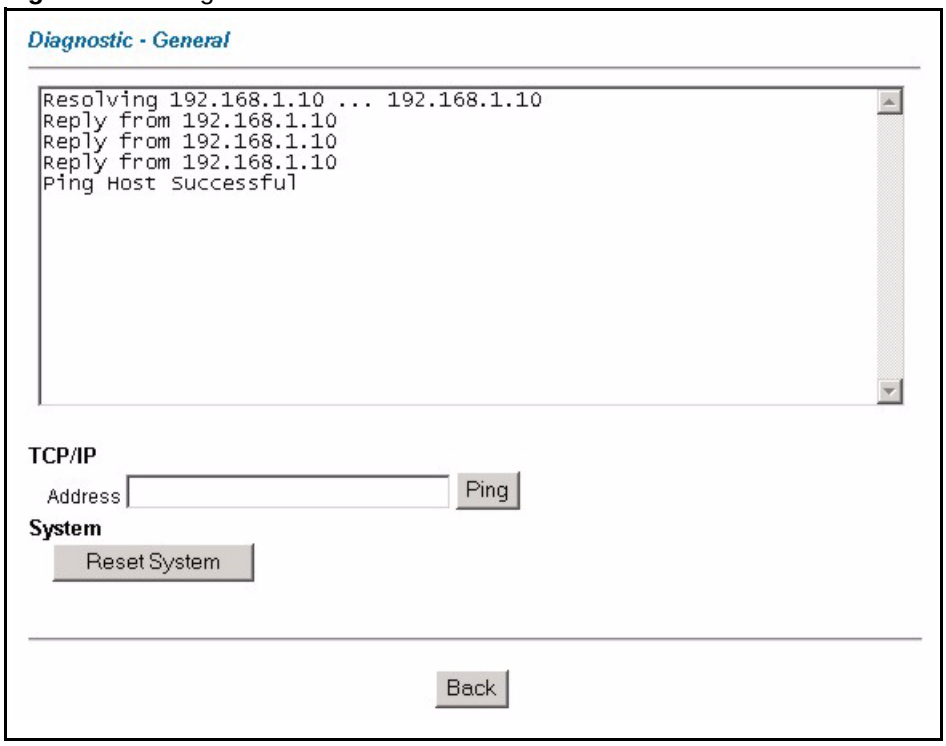
24.6 Diagnostic Screens

These read-only screens display information to help you identify problems with the Prestige.

24.6.1 Diagnostic General Screen

Click **Diagnostic** and then **General** to open the screen shown next.

Figure 141 Diagnostic: General



The following table describes the fields in this screen.

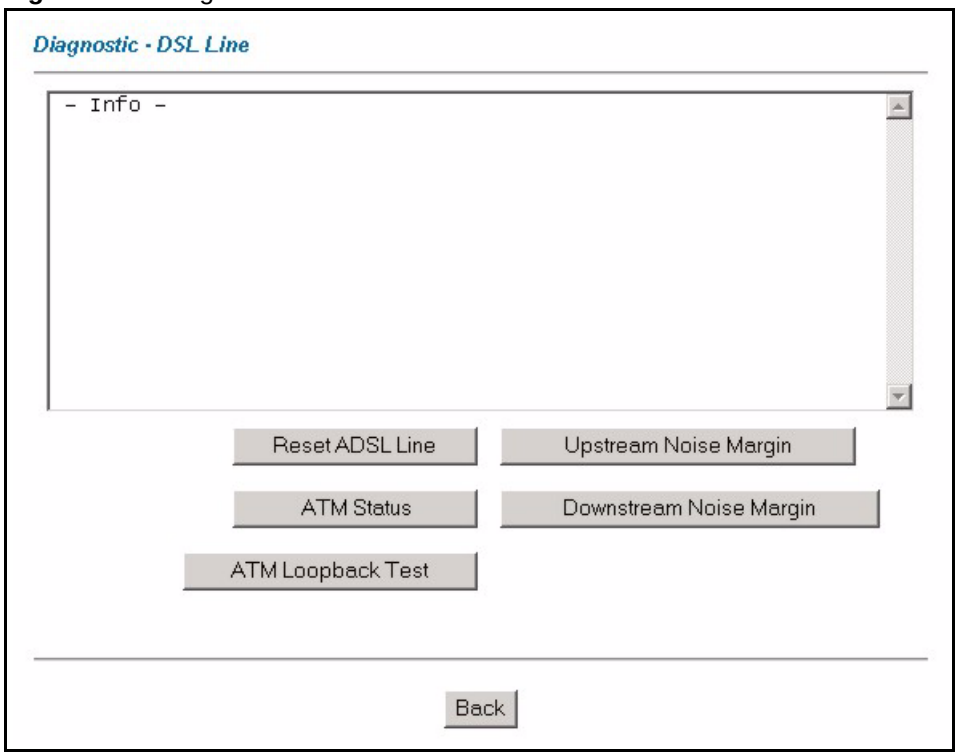
Table 96 Diagnostic: General

LABEL	DESCRIPTION
TCP/IP Address	Type the IP address of a computer that you want to ping in order to test a connection.
Ping	Click this button to ping the IP address that you entered.
Reset System	Click this button to reboot the Prestige. A warning dialog box is then displayed asking you if you're sure you want to reboot the system. Click **OK** to proceed.
Back	Click this button to go back to the main **Diagnostic** screen.

24.6.2 Diagnostic DSL Line Screen

Click **Diagnostic** and then **DSL Line** to open the screen shown next.

Figure 142 Diagnostic: DSL Line



The following table describes the fields in this screen.

Table 97 Diagnostic: DSL Line

LABEL	DESCRIPTION

Reset ADSL Line	Click this button to reinitialize the ADSL line. The large text box above then displays the progress and results of this operation, for example:
	`"Start to reset ADSL`
	`Loading ADSL modem F/W...`
	`Reset ADSL Line Successfully!"`

ATM Status	Click this button to view ATM status.
ATM Loopback Test	Click this button to start the ATM loopback test. Make sure you have configured at least one PVC with proper VPIs/VCIs before you begin this test. The Prestige sends an OAM F5 packet to the DSLAM/ATM switch and then returns it (loops it back) to the Prestige. The ATM loopback test is useful for troubleshooting problems with the DSLAM and ATM network.
Upstream Noise Margin	Click this button to display the upstream noise margin.
Downstream Noise Margin	Click this button to display the downstream noise margin.
Back	Click this button to go back to the main **Diagnostic** screen.

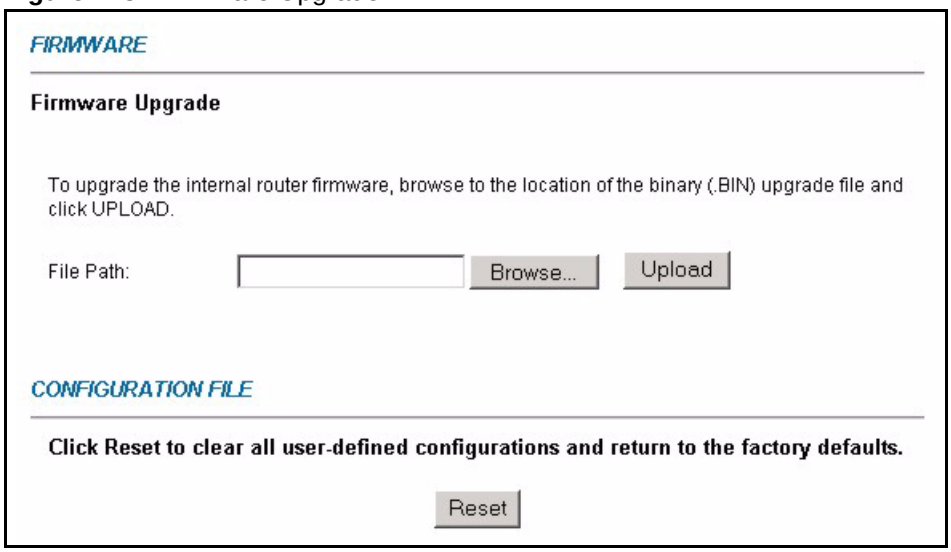
24.7 Firmware Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a "*.bin" extension, e.g., "Prestige.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. See Chapter 40 Firmware and Configuration File Maintenance in the parts that document the SMT for upgrading firmware using FTP/TFTP commands.

Only use firmware for your device's specific model. Refer to the label on the bottom of your device.

Click **Firmware** to open the following screen. Follow the instructions in this screen to upload firmware to your Prestige.

Figure 143 Firmware Upgrade



The following table describes the labels in this screen.

Table 98 Firmware Upgrade

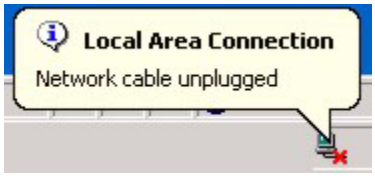
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.
Reset	Click this button to clear all user-entered configuration information and return the Prestige to its factory defaults. Refer to the *Resetting the Prestige* section.

Note: Do not turn off the Prestige while firmware upload is in progress!

After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the Prestige again.

The Prestige automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 144 Network Temporarily Disconnected



After two minutes, log in again and check your new firmware version in the **System Status** screen.

If the upload was not successful, the following screen will appear. Click **Back** to go back to the **Firmware** screen.

Figure 145 Error Message

CHAPTER 25
Introducing the SMT

This chapter explains how to access and navigate the System Management Terminal and gives an overview of its menus.

25.1 SMT Introduction

The Prestige's SMT (System Management Terminal) is a menu-driven interface that you can access from a terminal emulator over a telnet connection. This chapter shows you how to access the SMT (System Management Terminal) menus via Telnet, how to navigate the SMT and how to configure SMT menus.

25.1.1 Procedure for SMT Configuration via Telnet

The following procedure details how to telnet into your Prestige.

1. In Windows, click **Start** (usually in the bottom left corner), **Run** and then type "`telnet 192.168.1.1`" (the default IP address) and click **OK**.
2. Enter "`1234`" in the **Password** field.
3. After entering the password you will see the main menu.

Please note that if there is no activity for longer than five minutes (default timeout period) after you log in, your Prestige will automatically log you out. You will then have to telnet into the Prestige again.

25.1.2 Entering Password

The login screen appears after you press [ENTER], prompting you to enter the password, as shown next.

For your first login, enter the default password "`1234`". As you type the password, the screen displays an asterisk "`*`" for each character you type.

Please note that if there is no activity for longer than five minutes after you log in, your Prestige will automatically log you out.

Figure 146 Login Screen

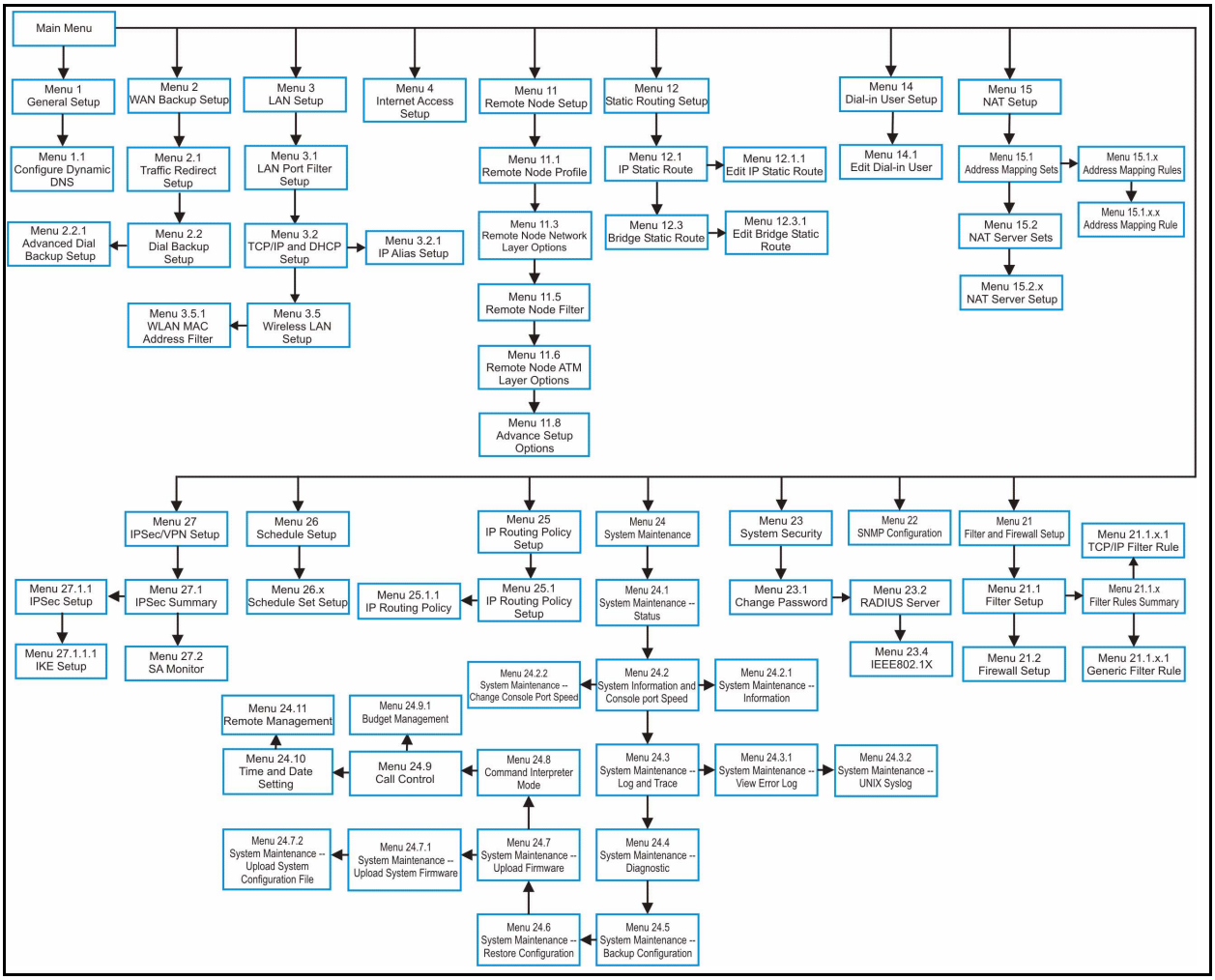
```
Enter Password : ****
```

25.1.3 Prestige SMT Menu Overview

We use the Prestige 662HW-61 SMT menus in this guide as an example. The SMT menus vary slightly for different Prestige models.

The following figure gives you an overview of the various SMT menu screens of your Prestige.

Figure 147 Prestige SMT Menu Overview



25.2 Navigating the SMT Interface

The SMT (System Management Terminal) is the interface that you use to configure your Prestige.

Several operations that you should be familiar with before you attempt to modify the configuration are listed in the table below.

Table 99 Navigating the SMT Interface

OPERATION	KEY STROKE	DESCRIPTION
Move down to another menu	[ENTER]	To move forward to a submenu, type in the number of the desired submenu and press [ENTER].
Move up to a previous menu	[ESC]	Press [ESC] to move back to the previous menu.
Move to a hidden menu	Press [SPACE BAR] to change **No** to **Yes** then press [ENTER].	Fields beginning with "Edit" lead to hidden menus and have a default setting of **No**. Press [SPACE BAR] once to change **No** to **Yes**, then press [ENTER] to go to the "hidden" menu.
Move the cursor	[ENTER] or [UP]/ [DOWN] arrow keys.	Within a menu, press [ENTER] to move to the next field. You can also use the [UP]/[DOWN] arrow keys to move to the previous and the next field, respectively.
Entering information	Type in or press [SPACE BAR], then press [ENTER].	You need to fill in two types of fields. The first requires you to type in the appropriate information. The second allows you to cycle through the available choices by pressing [SPACE BAR].
Required fields	<? > or **ChangeMe**	All fields with the symbol <?> must be filled in order to be able to save the new configuration. All fields with **ChangeMe** must not be left blank in order to be able to save the new configuration.
N/A fields	<N/A>	Some of the fields in the SMT will show a <N/A>. This symbol refers to an option that is Not Applicable.
Save your configuration	[ENTER]	Save your configuration by pressing [ENTER] at the message "Press ENTER to confirm or ESC to cancel". Saving the data on the screen will take you, in most cases to the previous menu.
Exit the SMT		Type 99, then press [ENTER].Type 99 at the main menu prompt and press [ENTER] to exit the SMT interface.

After you enter the password, the SMT displays the main menu, as shown next.

Table 100 SMT Main Menu

```
            Copyright (c) 1994 - 2004 ZyXEL Communications Corp.

            Prestige 662HW-61 Main Menu
Getting Started                      Advanced Management
  1. General Setup                     21. Filter and Firewall Setup
  2. WAN Backup Setup                  22. SNMP Configuration
  3. LAN Setup                         23. System Security
  4. Internet Access Setup             24. System Maintenance
                                       25. IP Routing Policy Setup
Advanced Applications                  26. Schedule Setup
  11. Remote Node Setup                27. VPN/IPSec Setup
  12. Static Routing Setup
  14. Dial-in User Setup               99. Exit
  15. NAT Setup
                     Enter Menu Selection Number:
```

25.2.1 System Management Terminal Interface Summary

Table 101 Main Menu Summary

#	MENU TITLE	DESCRIPTION
1	General Setup	Use this menu to set up your general information.
2	WAN Backup Setup	Use this menu to setup traffic redirect and dial-back up.
3	LAN Setup	Use this menu to set up your wireless LAN and LAN connection.
4	Internet Access Setup	A quick and easy way to set up an Internet connection.
11	Remote Node Setup	Use this menu to set up the Remote Node for LAN-to-LAN connection, including Internet connection.
12	Static Routing Setup	Use this menu to set up static routes.
14	Dial-in User Setup	Use this menu to set up local user profiles on the Prestige.
15	NAT Setup	Use this menu to specify inside servers when NAT is enabled.
21	Filter and Firewall Setup	Use this menu to configure filters, activate/deactivate the firewall and view the firewall log.
22	SNMP Configuration	Use this menu to set up SNMP related parameters.
23	System Security	Use this menu to set up wireless security and change your password.
24	System Maintenance	This menu provides system status, diagnostics, software upload, etc.
25	IP Routing Policy Setup	Use this menu to configure your IP routing policy.
26	Schedule Setup	Use this menu to schedule outgoing calls.
27	VPN/IPSec	Use this menu to configure VPN connections.
99	Exit	Use this to exit from SMT and return to a blank screen.

25.3 Changing the System Password

Change the Prestige default password by following the steps shown next.

1. Enter 23 in the main menu to display **Menu 23 - System Security**.
2. Enter 1 to display **Menu 23.1 - System Security - Change Password** as shown next.
3. Type your existing system password in the **Old Password** field, for example "1234", and press [ENTER].

Figure 148 Menu 23.1 Change Password

```
            Menu 23.1 - System Security - Change Password
                Old Password= ?
                New Password= ?
                Retype to confirm= ?
            Enter here to CONFIRM or ESC to CANCEL:
```

4 Type your new system password in the **New Password** field (up to 30 characters), and press [ENTER].

5 Re-type your new system password in the **Retype to confirm** field for confirmation and press [ENTER].

Note: Note that as you type a password, the screen displays an "*" for each character you type.

CHAPTER 26
Menu 1 General Setup

Menu 1 - General Setup *contains administrative and system-related information.*

26.1 General Setup

Menu 1 — General Setup contains administrative and system-related information (shown next). The **System Name** field is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

- In Windows 95/98 click **Start**, **Settings**, **Control Panel**, **Network**. Click the **Identification** tab, note the entry for the **Computer name** field and enter it as the Prestige **System Name**.
- In Windows 2000 click **Start**, **Settings**, **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the Prestige **System Name**.
- In Windows XP, click **start**, **My Computer**, **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the Prestige **System Name**.

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (System Name) on each individual computer, the domain name can be assigned from the Prestige via DHCP.

26.2 Procedure To Configure Menu 1

Enter 1 in the Main Menu to open **Menu 1 — General Setup** (shown next).

Figure 149 Menu 1 General Setup

```
                  Menu 1 General Setup
                        System Name= ?
                        Location=
                        Contact Person's Name=
                        Domain Name=
                        Edit Dynamic DNS= No
                        Route IP= Yes
                        Bridge= No
            Press ENTER to Confirm or ESC to Cancel:
```

Fill in the required fields. Refer to the table shown next for more information about these fields.

Table 102 Menu 1 General Setup

FIELD	DESCRIPTION
System Name	Choose a descriptive name for identification purposes. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Location (optional)	Enter the geographic location (up to 31 characters) of your Prestige.
Contact Person's Name (optional)	Enter the name (up to 30 characters) of the person in charge of this Prestige.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. You can go to menu 24.8 and type "sys domainname" to see the current domain name used by your gateway. If you want to clear this field just press the [SPACE BAR]. The domain name entered by you is given priority over the ISP assigned domain name.
Edit Dynamic DNS	Press the [SPACE BAR] to select **Yes** or **No** (default). Select **Yes** to configure **Menu 1.1 — Configure Dynamic DNS** (discussed next).
Route IP	Set this field to **Yes** to enable or **No** to disable IP routing. You must enable IP routing for Internet access.
Bridge	Turn on/off bridging for protocols not supported (for example, SNA) or not turned on in the previous **Route IP** field. Select **Yes** to turn bridging on; select **No** to turn bridging off.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

26.2.1 Procedure to Configure Dynamic DNS

Note: If you have a private WAN IP address, then you cannot use dynamic DNS.

To configure dynamic DNS, go to **Menu 1 — General Setup** and select **Yes** in the **Edit Dynamic DNS** field. Press [ENTER] to display **Menu 1.1— Configure Dynamic DNS** as shown next.

Figure 150 Menu 1.1 Configure Dynamic DNS

```
                Menu 1.1 - Configure Dynamic DNS
           Service Provider= WWW.DynDNS.ORG
           Active= No
           Host=
           EMAIL=
           USER=
           Password= ********
           Enable Wildcard= No
                Press ENTER to Confirm or ESC to Cancel:
```

Follow the instructions in the next table to configure dynamic DNS parameters.

Table 103 Menu 1.1 Configure Dynamic DNS

FIELD	DESCRIPTION
Service Provider	This is the name of your dynamic DNS service provider.
Active	Press [SPACE BAR] to select **Yes** and then press [ENTER] to make dynamic DNS active.
Host	Enter the domain name assigned to your Prestige by your dynamic DNS provider.
EMAIL	Enter your e-mail address.
User	Enter your user name.
Password	Enter the password assigned to you.
Enable Wildcard	Your Prestige supports DYNDNS Wildcard. Press [SPACE BAR] and then [ENTER] to select **Yes** or **No** This field is **N/A** when you choose DDNS client as your service provider.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

CHAPTER 27
Menu 2 WAN Backup Setup

This chapter describes how to configure traffic redirect and dial-backup using menu 2 and 2.1.

27.1 Introduction to WAN Backup Setup

This chapter explains how to configure the Prestige for traffic redirect and dial backup connections.

27.2 Configuring Dial Backup in Menu 2

From the main menu, enter 2 to open menu 2.

Figure 151 Menu 2 WAN Backup Setup

```
                    Menu 2 - Wan Backup Setup
                Check Mechanism = DSL Link
                Check WAN IP Address1 = 0.0.0.0
                Check WAN IP Address2 = 0.0.0.0
                Check WAN IP Address3 = 0.0.0.0
                  KeepAlive Fail Tolerance = 0
                  Recovery Interval(sec) = 0
                  ICMP Timeout(sec) = 0
                Traffic Redirect = No
                Dial Backup = No
              Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 104 Menu 2 WAN Backup Setup

FIELD	DESCRIPTION
Check Mechanism	Press [SPACE BAR] and then press [ENTER] to select the method that the Prestige uses to check the DSL connection. Select **DSL Link** to have the Prestige check the DSL connection's physical layer. Select **ICMP** to have the Prestige periodically ping the IP addresses configured in the **Check WAN IP Address** fields.
Check WAN IP Address1-3	Configure this field to test your Prestige's WAN accessibility. Type the IP address of a reliable nearby computer (for example, your ISP's DNS server address). When using a WAN backup connection, the Prestige periodically pings the addresses configured here and uses the other WAN backup connection (if configured) if there is no response.

Table 104 Menu 2 WAN Backup Setup (continued)

FIELD	DESCRIPTION
KeepAlive Fail Tolerance	Type the number of times (2 recommended) that your Prestige may ping the IP addresses configured in the **Check WAN IP Address** field without getting a response before switching to a WAN backup connection (or a different WAN backup connection).
Recovery Interval(sec)	When the Prestige is using a lower priority connection (usually a WAN backup connection), it periodically checks to whether or not it can use a higher priority connection. Type the number of seconds (30 recommended) for the Prestige to wait between checks. Allow more time if your destination IP address handles lots of traffic.
ICMP Timeout	Type the number of seconds for an ICMP session to wait for the ICMP response
Traffic Redirect	Press [SPACE BAR] to select **Yes** or **No**. Select **Yes** and press [ENTER] to configure **Menu 2.1 Traffic Redirect Setup**. Select **No** (default) if you do not want to configure this feature.
Dial Backup	Press [SPACE BAR] to select **Yes** or **No**. Select **Yes** and press [ENTER] to configure **Menu 2.2 Dial Backup Setup**. Select **No** (default) if you do not want to configure this feature.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

27.2.1 Traffic Redirect Setup

Configure parameters that determine when the Prestige will forward WAN traffic to the backup gateway using **Menu 2.1 — Traffic Redirect Setup**.

Figure 152 Menu 2.1Traffic Redirect Setup

```
                    Menu 2.1 - Traffic Redirect Setup
                Active= No
                Configuration:
                  Backup Gateway IP Address= 0.0.0.0
                  Metric= 15
                Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 105 Menu 2.1Traffic Redirect Setup

FIELD	DESCRIPTION
Active.	Press [SPACE BAR] and select **Yes** (to enable) or **No** (to disable) traffic redirect setup. The default is **No**
Configuration	
Backup Gateway IP Address	Enter the IP address of your backup gateway in dotted decimal notation. The Prestige automatically forwards traffic to this IP address if the Prestige's Internet connection terminates.

Table 105 Menu 2.1Traffic Redirect Setup

FIELD	DESCRIPTION
Metric	This field sets this route's priority among the routes the Prestige uses. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost"
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

27.3 Configuring Dial Backup Setup

1. From the main menu, enter 2 to open menu 2. Then move the cursor to the **Dial Backup** field in
2. **Menu 2 - WAN Backup Setup**, press the [SPACE BAR] to select **Yes** and then press [ENTER].

Figure 153 Menu 2.2 Dial Backup Setup

```
            Menu 2.2 - Dial Backup Setup

                        Dial-Backup:
                          Active= No
                          Port Speed= 115200
                        AT Command String:
                          Init= at&fs0=0
                          Edit Advanced Setup= No
            Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 106 Menu 2.2 Dial Backup Setup

FIELD	DESCRIPTION
Dial-Backup:	
Active	Use this field to turn the dial-backup feature on (**Yes**) or off (**No**).
Port Speed	Press [SPACE BAR] and then press [ENTER] to select the speed of the connection between the Dial Backup port and the external device. Available speeds are:**9600**, **19200**, **38400**, **57600**, **115200** or **230400** bps.
AT Command String:	
Init	Enter the AT command string to initialize the WAN device. Consult the manual of your WAN device connected to your Dial Backup port for specific AT commands.

Table 106 Menu 2.2 Dial Backup Setup (continued)

FIELD	DESCRIPTION
Edit Advanced Setup	To edit the advanced setup for the Dial Backup port, move the cursor to this field; press the [SPACE BAR] to select **Yes** and then press [ENTER] to go to **Menu 2.2.1 Advanced Dial Backup Setup**.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

27.4 Advanced Dial Backup Setup

Note: Consult the manual of your WAN device connected to your Dial Backup port for specific AT commands.

To edit the advanced setup for the dial backup port, move the cursor to the **Edit Advanced Setup** field in **Menu 2.2 Dial Backup Setup**, press the [SPACE BAR] to select **Yes** and then press [ENTER].

Figure 154 Menu 2.2.1 Advanced Dial Backup Setup

```
             Menu 2.2.1 - Advanced Dial Backup Setup

AT Command Strings:                    Call Control:
Dial= atd                              Dial Timeout(sec)= 60
     Drop= ~~+++~~ath                       Retry Count= 0
     Answer= ata                            Retry Interval(sec)= N/A
                                            Drop Timeout(sec)= 20
   Drop DTR When Hang Up= No                Call Back Delay(sec)= 15
   AT Response Strings:
     CLID= NMBR =
     Called Id=
     Speed= CONNECT
              Press ENTER to Confirm or ESC to Cancel:
```

The following table describes fields in this menu.

Table 107 Menu 2.2.1 Advanced Dial Backup Setup: AT Commands Fields

FIELD	DESCRIPTION
AT Command Strings:	
Dial	Enter the AT Command string to make a call.
Drop	Enter the AT Command string to drop a call. "~" represents a one second wait, e.g., "`~~~+++~~ath`" can be used if your modem has a slow response time.
Answer	Enter the AT Command string to answer a call.
Drop DTR When Hang Up	Press the [SPACE BAR] to choose either **Yes** or **No**. When **Yes** is selected (the default), the DTR (Data Terminal Ready) signal is dropped after the "`AT Command String: Drop`" is sent out.
AT Response Strings:	
CLID (Calling Line Identification)	Enter the keyword that precedes the CLID (Calling Line Identification) in the AT response string. This lets the Prestige capture the CLID in the AT response string that comes from the WAN device. CLID is required for CLID authentication.
Called Id	Enter the keyword preceding the dialed number.
Speed	Enter the keyword preceding the connection speed.

Table 108 Menu 2.2.1 Advanced Dial Backup Setup: Call Control Parameters

FIELD	DESCRIPTION
Call Control	
Dial Timeout (sec)	Enter a number of seconds for the Prestige to keep trying to set up an outgoing call before timing out (stopping). The Prestige times out and stops if it cannot set up an outgoing call within the timeout value.
Retry Count	Enter a number of times for the Prestige to retry a busy or no-answer phone number before blacklisting the number.
Retry Interval (sec)	Enter a number of seconds for the Prestige to wait before trying another call after a call has failed. This applies before a phone number is blacklisted.

Table 108 Menu 2.2.1 Advanced Dial Backup Setup: Call Control Parameters

FIELD	DESCRIPTION
Drop Timeout (sec)	Enter a number of seconds for the Prestige to wait before dropping the DTR signal if it does not receive a positive disconnect confirmation.
Call Back Delay (sec)	Enter a number of seconds for the Prestige to wait between dropping a callback request call and dialing the co-responding callback call.

CHAPTER 28
Menu 3 LAN Setup

This chapter covers how to configure your wired Local Area Network (LAN) settings.

28.1 LAN Setup

This section describes how to configure the Ethernet using **Menu 3 — LAN Setup**. From the main menu, enter 3 to display menu 3.

Figure 155 Menu 3 LAN Setup

```
Menu 3 - LAN Setup
1. LAN Port Filter Setup
2. TCP/IP and DHCP Setup
5. Wireless LAN Setup
Enter Menu Selection Number:
```

28.1.1 General Ethernet Setup

This menu allows you to specify filter set(s) that you wish to apply to the Ethernet traffic. You seldom need to filter Ethernet traffic; however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches.

Figure 156 Menu 3.1 LAN Port Filter Setup

```
Menu 3.1 - LAN Port Filter Setup
  Input Filter Sets:
    protocol filters=
    device filters=
  Output Filter Sets:
    protocol filters=
    device filters=
Press ENTER to Confirm or ESC to Cancel:
```

If you need to define filters, please read Chapter 36 Filter Configuration first, then return to this menu to define the filter sets.

28.2 Protocol Dependent Ethernet Setup

Depending on the protocols for your applications, you need to configure the respective Ethernet Setup, as outlined below.

- For TCP/IP Ethernet setup refer to the Internet Access Configuration section .
- For bridging Ethernet setup refer to Chapter 33 Bridging Setup .

28.3 CP/IP Ethernet Setup and DHCP

Use menu 3.2 to configure your Prestige for TCP/IP.

To edit menu 3.2, enter 3 from the main menu to display **Menu 3 — LAN Setup**. When menu 3 appears, press 2 and press [ENTER] to display **Menu 3.2 — TCP/IP and DHCP Ethernet Setup**, as shown next:

Figure 157 Menu 3.2 TCP/IP and DHCP Ethernet Setup

```
                        Menu 3.2 - TCP/IP and DHCP Setup
                    DHCP Setup
                      DHCP= Server
                      Client IP Pool Starting Address= 192.168.1.33
                      Size of Client IP Pool= 32
                      Primary DNS Server= 0.0.0.0
                      Secondary DNS Server= 0.0.0.0
                      Remote DHCP Server= N/A
                    TCP/IP Setup:
                      IP Address= 192.168.1.1
                      IP Subnet Mask= 255.255.255.0
                      RIP Direction= None
                        Version= N/A
                      Multicast= None
                      IP Policies=
                      Edit IP Alias= No
                    Press ENTER to Confirm or ESC to Cancel:
```

Follow the instructions in the following table on how to configure the DHCP fields.

Table 109 DHCP Ethernet Setup

FIELD	DESCRIPTION
DHCP Setup	
DHCP	If set to **Server**, your Prestige can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client. If set to **None**, the DHCP server will be disabled. If set to **Relay**, the Prestige acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the Remote DHCP Server in this case. When DHCP server is used, the following items need to be set:
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Size of Client IP Pool	This field specifies the size or count of the IP address pool.
Primary DNS Server Secondary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Remote DHCP Serve	If **Relay** is selected in the **DHCP** field above then enter the IP address of the actual remote DHCP server here.

Follow the instructions in the following table to configure TCP/IP parameters for the Ethernet port.

Table 110 TCP/IP Ethernet Setup

FIELD	DESCRIPTION
TCP/IP Setup	
IP Address	Enter the (LAN) IP address of your Prestige in dotted decimal notation

Table 110 TCP/IP Ethernet Setup (continued)

FIELD	DESCRIPTION
IP Subnet Mask	Your Prestige will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Prestige (refer to the IP Subnetting appendix for more information).
RIP Direction	Press [SPACE BAR] to select the RIP direction. Choices are **Both**, **In Only**, **Out Only** or **None**.
Version	Press [SPACE BAR] to select the RIP version. Choices are **RIP-1**, **RIP-2B** or **RIP-2M**.
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group. The Prestige supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). Press the [SPACE BAR] to enable IP Multicasting or select **None** to disable it.
IP Policies	Create policies using SMT menu 25 (see Chapter 43 IP Policy Routing) and apply them on the Prestige LAN interface here. You can apply up to four IP Policy sets (from twelve) by entering their numbers separated by commas.
Edit IP Alias	The Prestige supports three logical LAN interfaces via its single physical Ethernet interface with the Prestige itself as the gateway for each LAN network. Press [SPACE BAR] to change **No** to **Yes** and press [ENTER] to display Menu 3.2.1.

CHAPTER 29
Wireless LAN Setup

This chapter covers how to configure wireless LAN settings in SMT menu 3.5.

29.1 Wireless LAN Overview

Refer to the chapter on the wireless LAN screens for wireless LAN background information.

29.2 Wireless LAN Setup

Use menu 3.5 to set up your Prestige as the wireless access point. To edit menu 3.5, enter 3 from the main menu to display **Menu 3 – LAN Setup**. When menu 3 appears, press 5 and then press [ENTER] to display **Menu 3.5 – Wireless LAN Setup** as shown next.

Figure 158 Menu 3.5 - Wireless LAN Setup

```
            Menu 3.5- Wireless LAN Setup
                        ESSID= Wireless
                        Hide ESSID= No
                        Channel ID= CH06 2437MHz
                        RTS Threshold= 2432
                        Frag. Threshold= 2432
                        WEP= Disable
                          Default Key= N/A
                          Key1= N/A
                          Key2= N/A
                          Key3= N/A
                          Key4= N/A
                        Edit MAC Address Filter= No

            Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 111 Menu 3.5 - Wireless LAN Setup

FIELD	DESCRIPTION
ESSID	The ESSID (Extended Service Set IDentifier) identifies the AP to which the wireless stations associate. Wireless stations associating to the Access Point must have the same ESSID. Enter a descriptive name of up to 32 printable 7-bit ASCII characters.
Hide ESSID	Press [SPACE BAR] and select **Yes** to hide the ESSID in the outgoing beacon frame so a station cannot obtain the ESSID through passive scanning.

Table 111 Menu 3.5 - Wireless LAN Setup (continued)

FIELD	DESCRIPTION
Channel ID	Press [SPACE BAR] to select a channel. This allows you to set the operating frequency/ channel depending on your particular region.
RTS Threshold	RTS(Request To Send) threshold (number of bytes) enables RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC Service Data Unit) size turns off the RTS/CTS handshake. Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between 0 and 2432.
Frag. Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between 256 and 2432.
WEP	WEP (Wired Equivalent Privacy) provides data encryption to prevent wireless stations from accessing data transmitted over the wireless network. Select **Disable** allows wireless stations to communicate with the access points without any data encryption. Select **64-bit WEP** or **128-bit WEP** to for the type of data encryption. WEP causes performance degradation.
Default Key	Enter the number of the key as an active key.
Key 1 to Key 4	If you chose **64-bit WEP** in the **WEP Encryption** field, then enter 5 characters or 10 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key (1-4). If you chose **128-bit WEP** in the **WEP Encryption** field, then enter 13 characters or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key (1-4). There are four data encryption keys to secure your data from eavesdropping by unauthorized wireless users. The values for the keys must be set up exactly the same on the access points as they are on the wireless stations.
Edit MAC Address Filter	To edit MAC address filtering table, press [SPACE BAR] to select **Yes** and press [ENTER] to open menu 3.5.1.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

29.2.1 Wireless LAN MAC Address Filter

The next layer of security is MAC address filter. To allow a wireless station to associate with the Prestige, enter the MAC address of the wireless LAN adapter on that wireless station in the MAC address table.

Figure 159 Menu 3.5.1 WLAN MAC Address Filtering

```
                  Menu 3.5.1 - WLAN MAC Address Filter
                Active= No
                Filter Action= Allowed Association
------------------------------------------------------------------------------
  1=   00:00:00:00:00:00   13=   00:00:00:00:00:00   25=   00:00:00:00:00:00
  2=   00:00:00:00:00:00   14=   00:00:00:00:00:00   26=   00:00:00:00:00:00
  3=   00:00:00:00:00:00   15=   00:00:00:00:00:00   27=   00:00:00:00:00:00
  4=   00:00:00:00:00:00   16=   00:00:00:00:00:00   28=   00:00:00:00:00:00
  5=   00:00:00:00:00:00   17=   00:00:00:00:00:00   29=   00:00:00:00:00:00
  6=   00:00:00:00:00:00   18=   00:00:00:00:00:00   30=   00:00:00:00:00:00
  7=   00:00:00:00:00:00   19=   00:00:00:00:00:00   31=   00:00:00:00:00:00
  8=   00:00:00:00:00:00   20=   00:00:00:00:00:00   32=   00:00:00:00:00:00
  9=   00:00:00:00:00:00   21=   00:00:00:00:00:00
 10=   00:00:00:00:00:00   22=   00:00:00:00:00:00
 11=   00:00:00:00:00:00   23=   00:00:00:00:00:00
 12=   00:00:00:00:00:00   24=   00:00:00:00:00:00
------------------------------------------------------------------------------
                    Enter here to CONFIRM or ESC to CANCEL:
```

The following table describes the fields in this menu.

Table 112 Menu 3.5.1 WLAN MAC Address Filtering

FIELD	DESCRIPTION
Active	To enable MAC address filtering, press [SPACE BAR] to select **Yes** and press [ENTER].
Filter Action	Define the filter action for the list of MAC addresses in the MAC address filter table. To deny access to the Prestige, press [SPACE BAR] to select **Deny Association** and press [ENTER]. MAC addresses not listed will be allowed to access the router. The default action, **Allowed Association**, permits association with the Prestige. MAC addresses not listed will be denied access to the router.
MAC Address Filter	
Address 1.	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless stations that are allowed or denied access to the Prestige in these address fields.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

CHAPTER 30
Internet Access

This chapter shows you how to configure the LAN and WAN of your Prestige for Internet access.

30.1 Internet Access Overview

Refer to the chapters on the web configurator's wizard, LAN and WAN screens for more background information on fields in the SMT screens covered in this chapter.

30.2 IP Policies

Traditionally, routing is based on the destination address *only* and the router takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing. Create policies using SMT menu 25 (see Chapter 43 IP Policy Routing) and apply them on the Prestige LAN and/or WAN interfaces using menus 3.2 (LAN) and 11.3 (WAN).

30.3 IP Alias

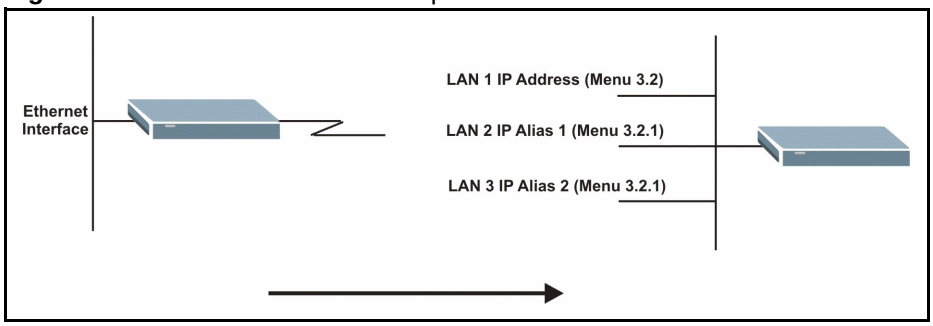
IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The Prestige supports three logical LAN interfaces via its single physical Ethernet interface with the Prestige itself as the gateway for each LAN network.

When you use IP alias, you can also configure firewall rules to control access between the LAN's logical networks (subnets).

Note: Make sure that the subnets of the logical networks do not overlap.

The following figure shows a LAN divided into subnets A, B, and C.

Figure 160 IP Alias Network Example



Use menu 3.2.1 to configure IP Alias on your Prestige.

30.4 IP Alias Setup

Use menu 3.2 to configure the first network. Move the cursor to **Edit IP Alias** field and press [SPACEBAR] to choose **Yes** and press [ENTER] to configure the second and third network.

Figure 161 Menu 3.2 TCP/IP and DHCP Setup

```
                    Menu 3.2 - TCP/IP and DHCP Setup
DHCP Setup
  DHCP= Server
  Client IP Pool Starting Address= 192.168.1.33
  Size of Client IP Pool= 32
  Primary DNS Server= 0.0.0.0
  Secondary DNS Server= 0.0.0.0
  Remote DHCP Server= N/A
TCP/IP Setup:
  IP Address= 192.168.1.1
  IP Subnet Mask= 255.255.255.0
  RIP Direction= None
    Version= N/A
  Multicast= None
  IP Policies=
  Edit IP Alias= No

Press ENTER to Confirm or ESC to Cancel:
```

Pressing [ENTER] displays **Menu 3.2.1 — IP Alias Setup**, as shown next.

Figure 162 Menu 3.2.1 IP Alias Setup

```
            Menu 3.2.1 - IP Alias Setup
              IP Alias 1= No
                IP Address= N/A
                IP Subnet Mask= N/A
                RIP Direction= N/A
                Version= N/A
                Incoming protocol filters= N/A
                Outgoing protocol filters= N/A
              IP Alias 2= No
                IP Address= N/A
                IP Subnet Mask= N/A
                RIP Direction= N/A
                Version= N/A
                Incoming protocol filters= N/A
                Outgoing protocol filters= N/A

                 Enter here to CONFIRM or ESC to CANCEL:
```

Follow the instructions in the following table to configure IP Alias parameters.

Table 113 Menu 3.2.1 IP Alias Setup

FIELD	DESCRIPTION
IP Alias	Choose **Yes** to configure the LAN network for the Prestige.
IP Address	Enter the IP address of your Prestige in dotted decimal notation
IP Subnet Mask	Your Prestige will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Prestige
RIP Direction	Press [SPACE BAR] to select the RIP direction. Choices are **None**, **Both**, **In Only** or **Out Only**.
Version	Press [SPACE BAR] to select the RIP version. Choices are **RIP-1**, **RIP-2B** or **RIP-2M**.
Incoming Protocol Filters	Enter the filter set(s) you wish to apply to the incoming traffic between this node and the Prestige.
Outgoing Protocol Filters	Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the Prestige.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

30.5 Route IP Setup

The first step is to enable the IP routing in **Menu 1 — General Setup**.

To edit menu 1, type 1 in the main menu and press [ENTER]. Set the **Route IP** field to **Yes** by pressing [SPACE BAR].

Figure 163 Menu 1 General Setup

```
            Menu 1 - General Setup
                       System Name= ?
                       Location= location
                       Contact Person's Name=
                       Domain Name=
                       Edit Dynamic DNS= No
                       Route IP= Yes
                       Bridge= No

            Press ENTER to Confirm or ESC to Cancel:
```

30.6 Internet Access Configuration

Menu 4 allows you to enter the Internet Access information in one screen. Menu 4 is actually a simplified setup for one of the remote nodes that you can access in menu 11. Before you configure your Prestige for Internet access, you need to collect your Internet account information.

Use the *Internet Account Information* table in the *Quick Start Guide* to record your. Note that if you are using PPPoA or PPPoE encapsulation, then the only ISP information you need is a login name and password. You only need to know the Ethernet Encapsulation Gateway IP address if you are using ENET ENCAP encapsulation.

From the main menu, type 4 to display **Menu 4 - Internet Access Setup**, as shown next.

Figure 164 Menu 4 Internet Access Setup

```
            Menu 4 - Internet Access Setup
              ISP's Name= MyISP
              Encapsulation= RFC 1483
              Multiplexing= LLC-based
              VPI #= 8
              VCI #= 35
              ATM QoS Type= CBR
                Peak Cell Rate (PCR)= 0
                Sustain Cell Rate (SCR)= 0
                Maximum Burst Size (MBS)= 0
              My Login= N/A
              My Password= N/A
              ENET ENCAP Gateway= N/A
              IP Address Assignment= Static
                IP Address= 0.0.0.0
              Network Address Translation= SUA Only
                Address Mapping Set= N/A

            Press ENTER to Confirm or ESC to Cancel:
```

The following table contains instructions on how to configure your Prestige for Internet access

.

Table 114 Menu 4 Internet Access Setup

FIELD	DESCRIPTION
ISP's Name	Enter the name of your Internet Service Provider (ISP). This information is for identification purposes only.
Encapsulation	Press [SPACE BAR] to select the method of encapsulation used by your ISP. Choices are **PPPoE**, **PPPoA**, **RFC 1483** or **ENET ENCAP**.
Multiplexing	Press [SPACE BAR] to select the method of multiplexing used by your ISP. Choices are **VC-based** or **LLC-based**.
VPI #	Enter the Virtual Path Identifier (VPI) assigned to you.
VCI #	Enter the Virtual Channel Identifier (VCI) assigned to you.
ATM QoS Type	Press [SPACE BAR] and select **CBR** (Continuous Bit Rate) to specify fixed (always-on) bandwidth. Select **UBR** (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select **VBR** (Variable Bit Rate) for bursty traffic and bandwidth sharing with other applications.
Peak Cell Rate (PCR)	This is the maximum rate at which the sender can send cells. Type the PCR.
Sustain Cell Rate (SCR)= 0	Sustained Cell Rate is the mean cell rate of a bursty, on-off traffic source that can be sent at the peak rate, and a parameter for burst-traffic. Type the SCR; it must be less than the PCR.
Maximum Burst Size (MBS)= 0	Refers to the maximum number of cells that can be sent at the peak rate. Type the MBS. The MBS must be less than 65535.
My Login	Configure the **My Login** and **My Password** fields for PPPoA and PPPoE encapsulation only. Enter the login name that your ISP gives you. If you are using PPPoE encapsulation**,** then this field must be of the form user@domain where domain identifies your PPPoE service name.
My Password	Enter the password associated with the login name above.
ENET ENCAP Gateway	Enter the gateway IP address supplied by your ISP when you are using **ENET ENCAP** encapsulation.
Idle Timeout	This value specifies the number of idle seconds that elapse before the Prestige automatically disconnects the PPPoE session.
IP Address Assignment	Press [SPACE BAR] to select **Static** or **Dynamic** address assignment.
IP Address	Enter the IP address supplied by your ISP if applicable.
Network Address Translation	Press [SPACE BAR] to select **None**, **SUA Only** or **Full Feature**. Please see Chapter 34 Network Address Translation (NAT) for more details on the SUA (Single User Account) feature.
Address Mapping Set	Type the numbers of mapping sets (1-8) to use with NAT. See Chapter 34 Network Address Translation (NAT) for details.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

If all your settings are correct your Prestige should connect automatically to the Internet. If the connection fails, note the error message that you receive on the screen and take the appropriate troubleshooting steps.

CHAPTER 31
Remote Node Configuration

This chapter covers remote node configuration.

31.1 Remote Node Setup Overview

This section describes the protocol-independent parameters for a remote node. A remote node is required for placing calls to a remote gateway. A remote node represents both the remote gateway and the network behind it across a WAN connection. When you use menu 4 to set up Internet access, you are configuring one of the remote nodes.

You first choose a remote node in **Menu 11- Remote Node Setup**. You can then edit that node's profile in menu 11.1, as well as configure specific settings in three submenus: edit IP and bridge options in menu 11.3; edit ATM options in menu 11.6; and edit filter sets in menu 11.5.

31.2 Remote Node Setup

This section describes the protocol-independent parameters for a remote node.

31.2.1 Remote Node Profile

To configure a remote node, follow these steps:

1. From the main menu, enter 11 to display **Menu 11 - Remote Node Setup.**
2. When menu 11 appears, as shown in the following figure, type the number of the remote node that you want to configure.

Figure 165 Menu 11 Remote Node Setup

```
                Menu 11 - Remote Node Setup
          1. MyISP (ISP, SUA)
          2. _________
          3. _________
          4. _________
          5. _________
          6. _________
          7. _________
          8. _________

                   Enter Node # to Edit:
```

31.2.2 Encapsulation and Multiplexing Scenarios

For Internet access you should use the encapsulation and multiplexing methods used by your ISP. Consult your telephone company for information on encapsulation and multiplexing methods for LAN-to-LAN applications, for example between a branch office and corporate headquarters. There must be prior agreement on encapsulation and multiplexing methods because they cannot be automatically determined. What method(s) you use also depends on how many VCs you have and how many different network protocols you need. The extra overhead that ENET ENCAP encapsulation entails makes it a poor choice in a LAN-to-LAN application. Here are some examples of more suitable combinations in such an application.

31.2.2.1 Scenario 1: One VC, Multiple Protocols

PPPoA (RFC-2364) encapsulation with **VC-based** multiplexing is the best combination because no extra protocol identifying headers are needed. The **PPP** protocol already contains this information.

31.2.2.2 Scenario 2: One VC, One Protocol (IP)

Selecting **RFC-1483** encapsulation with **VC-based** multiplexing requires the least amount of overhead (0 octets). However, if there is a potential need for multiple protocol support in the future, it may be safer to select **PPPoA** encapsulation instead of **RFC-1483**, so you do not need to reconfigure either computer later.

31.2.2.3 Scenario 3: Multiple VCs

If you have an equal number (or more) of VCs than the number of protocols, then select **RFC-1483** encapsulation and **VC-based** multiplexing.

Figure 166 Menu 11.1 Remote Node Profile

```
             Menu 11.1 - Remote Node Profile
Rem Node Name= MyISP                 Route= IP
Active= Yes                          Bridge= No
Encapsulation= RFC 1483              Edit IP/Bridge= No
Multiplexing= LLC-based              Edit ATM Options= No
Service Name= N/A                    Edit Advance Options= N/A
Incoming:                            Telco Option:
  Rem Login= N/A                       Allocated Budget(min)= N/A
  Rem Password= N/A                    Period(hr)= N/A
Outgoing:                              Schedule Sets= N/A
  My Login= N/A                        Nailed-Up Connection= N/A
  My Password= N/A                   Session Options:
  Authen= N/A                          Edit Filter Sets= No
                                         Idle Timeout(sec)= N/A

             Press ENTER to Confirm or ESC to Cancel:
```

In **Menu 11.1 – Remote Node Profile**, fill in the fields as described in the following table.

Table 115 Menu 11.1 Remote Node Profile

FIELD	DESCRIPTION
Rem Node Name	Type a unique, descriptive name of up to eight characters for this node.
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** to activate or **No** to deactivate this node. Inactive nodes are displayed with a minus sign –" in SMT menu 11.
Encapsulation	**PPPoA** refers to RFC-2364 (PPP Encapsulation over ATM Adaptation Layer 5). If RFC-1483 (Multiprotocol Encapsulation over ATM Adaptation Layer 5) of **ENET ENCAP** are selected, then the **Rem Login**, **Rem Password**, **My Login**, **My Password** and **Authen** fields are not applicable (**N/A**).
Multiplexing	Press [SPACE BAR] and then [ENTER] to select the method of multiplexing that your ISP uses, either **VC-based** or **LLC-based**.
Service Name	When using **PPPoE** encapsulation, type the name of your PPPoE service here.
Incoming:	
Rem Login	Type the login name that this remote node will use to call your Prestige. The login name and the **Rem Password** will be used to authenticate this node.
Rem Password	Type the password used when this remote node calls your Prestige.
Outgoing:	
My Login	Type the login name assigned by your ISP when the Prestige calls this remote node.
My Password	Type the password assigned by your ISP when the Prestige calls this remote node.
Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are:
	CHAP/**PAP** – Your Prestige will accept either **CHAP** or **PAP** when requested by this remote node.
	CHAP – accept **CHAP** (Challenge Handshake Authentication Protocol) only.

Table 115 Menu 11.1 Remote Node Profile (continued)

FIELD	DESCRIPTION
	PAP – accept PAP (Password Authentication Protocol) only.
Route	This field determines the protocol used in routing. Options are **IP** and **None.**
Bridge	When bridging is enabled, your Prestige will forward any packet that it does not route to this remote node; otherwise, the packets are discarded. Select **Yes** to enable and **No** to disable.
Edit IP/Bridge	Press [SPACE BAR] to select **Yes** and press [ENTER] to display **Menu 11.3 – Remote Node Network Layer Options**.
Edit ATM Options	Press [SPACE BAR] to select **Yes** and press [ENTER] to display **Menu 11.6 – Remote Node ATM Layer Options**.
Edit Advance Options	This field is only available when you select **PPPoE** in the **Encapsulation** field. Press [SPACE BAR] to select **Yes** and press [ENTER] to display **Menu 11.8 – Advance Setup Options**.
Telco Option	
Allocated Budget (min)	This sets a ceiling for outgoing call time for this remote node. The default for this field is 0 meaning no budget control.
Period (hr)	This field is the time period that the budget should be reset. For example, if we are allowed to call this remote node for a maximum of 10 minutes every hour, then the **Allocated Budget** is (10 minutes) and the **Period (hr)** is 1 (hour).
Schedule Sets	This field is only applicable for **PPPoE** and **PPPoA** encapsulation. You can apply up to four schedule sets here. For more details please refer to Chapter 44 Call Scheduling .
Nailed up Connection	This field is only applicable for **PPPoE** and **PPPoA** encapsulation. This field specifies if you want to make the connection to this remote node a nailed-up connection. More details are given earlier in this section.
Session Options	
Edit Filter Sets	Use [SPACE BAR] to choose **Yes** and press [ENTER] to open menu 11.5 to edit the filter sets. See the *Remote Node Filter* section for more details.
Idle Timeout (sec)	Type the number of seconds (0-9999) that can elapse when the Prestige is idle (there is no traffic going to the remote node), before the Prestige automatically disconnects the remote node. 0 means that the session will not timeout.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

31.2.3 Outgoing Authentication Protocol

For obvious reasons, you should employ the strongest authentication protocol possible. However, some vendors' implementation includes specific authentication protocol in the user profile. It will disconnect if the negotiated protocol is different from that in the user profile, even when the negotiated protocol is stronger than specified. If the peer disconnects right after a successful authentication, make sure that you specify the correct authentication protocol when connecting to such an implementation.

31.3 Remote Node Network Layer Options

For the TCP/IP parameters, perform the following steps to edit **Menu 11.3 – Remote Node Network Layer Options** as shown next.

1. In menu 11.1, make sure **IP** is among the protocols in the **Route** field.
2. Move the cursor to the **Edit IP/Bridge** field, press [SPACE BAR] to select **Yes,** then press [ENTER] to display **Menu 11.3 – Remote Node Network Layer Options.**

Figure 167 Menu 11.3 Remote Node Network Layer Options

```
            Menu 11.3 - Remote Node Network Layer Options
IP Options:                          Bridge Options:
  IP Address Assignment = Static       Ethernet Addr Timeout(min)= N/A
  Rem IP Addr = 0.0.0.0
  Rem Subnet Mask= 0.0.0.0
  My WAN Addr= 0.0.0.0
  NAT= SUA Only
    Address Mapping Set= N/A
  Metric= 2
  Private= No
  RIP Direction= None
    Version= RIP-1
  Multicast= None
  IP Policies=

            Enter here to CONFIRM or ESC to CANCEL:
```

The next table explains fields in **Menu 11.3 – Remote Node Network Layer Options**.

Table 116 Menu 11.3 Remote Node Network Layer Options

FIELD	DESCRIPTION
IP Address Assignment	Press [SPACE BAR] and then [ENTER] to select **Dynamic** if the remote node is using a dynamically assigned IP address or **Static** if it is using a static (fixed) IP address. You will only be able to configure this in the ISP node (also the one you configure in menu 4), all other nodes are set to **Static**.
Rem IP Addr	This is the IP address you entered in the previous menu.
Rem Subnet Mask	Type the subnet mask assigned to the remote node.
My WAN Addr	Some implementations, especially UNIX derivatives, require separate IP network numbers for the WAN and LAN links and each end to have a unique address within the WAN network number. In that case, type the IP address assigned to the WAN port of your Prestige. NOTE: Refers to local Prestige address, not the remote router address.
NAT	Press [SPACE BAR] and then [ENTER] to select **Full Feature** if you have multiple public WAN IP addresses for your Prestige.
	Select **SUA Only** if you have just one public WAN IP address for your Prestige. The SMT uses Address Mapping Set 255 (see Figure 185). Select **None** to disable NAT.

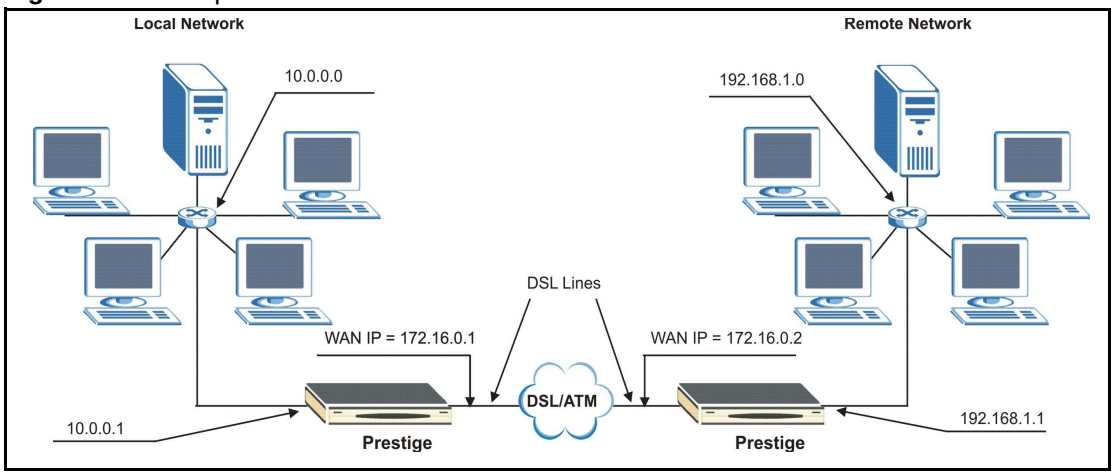
Table 116 Menu 11.3 Remote Node Network Layer Options (continued)

FIELD	DESCRIPTION
Address Mapping Set	When **Full Feature** is selected in the **NAT** field, configure address mapping sets in menu 15.1. Select one of the NAT server sets (2-10) in menu 15.2 (see Chapter 34 Network Address Translation (NAT) for details) and type that number here. When **SUA Only** is selected in the NAT field, the SMT uses NAT server set 1 in menu 15.2 (see Chapter 34 Network Address Translation (NAT) for details).
Metric	The metric represents the cost of transmission for routing purposes. IP routing uses hop count as the cost measurement, with a minimum of 1 for directly connected networks. Type 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.
Private	This determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and not included in RIP broadcast. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP Direction. Options are **Both**, **In Only**, **Out Only** or **None**.
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are **RIP-1**, **RIP-2B** or **RIP-2M**.
Multicast	**IGMP-v1** sets IGMP to version 1, **IGMP-v2** sets IGMP to version 2 and **None** disables IGMP.
IP Policies	You can apply up to four IP Policy sets (from 12) by typing in their numbers separated by commas. Configure the filter sets in menu 25 first (see Chapter 43 IP Policy Routing) and then apply them here.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

31.3.1 My WAN Addr Sample IP Addresses

The following figure uses sample IP addresses to help you understand the field of **My WAN Addr** in menu 11.3. Refer to the previous Figure 19 in the web configurator chapter on LAN setup for a brief review of what a WAN IP is. **My WAN Addr** indicates the local Prestige WAN IP (172.16.0.1 in the following figure) while **Rem IP Addr** indicates the peer WAN IP (172.16.0.2 in the following figure).

Figure 168 Sample IP Addresses for a TCP/IP LAN-to-LAN Connection



31.4 Remote Node Filter

Move the cursor to the **Edit Filter Sets** field in menu 11.1, then press [SPACE BAR] to select **Yes**. Press [ENTER] to display **Menu 11.5 – Remote Node Filter**.

Use **Menu 11.5 – Remote Node Filter** to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the Prestige and also to prevent certain packets from triggering calls. You can specify up to 4 filter sets separated by comma, for example, 1, 5, 9, 12, in each filter field.

Note that spaces are accepted in this field. The Prestige has a prepackaged filter set, NetBIOS_WAN, that blocks NetBIOS packets. Include this in the call filter sets if you want to prevent NetBIOS packets from triggering calls to a remote node.

Figure 169 Menu 11.5 Remote Node Filter (RFC 1483 or ENET Encapsulation)

```
            Menu 11.5 - Remote Node Filter
                    Input Filter Sets:
                      protocol filters=
                        device filters=
                    Output Filter Sets:
                      protocol filters=
                        device filters=

                     Enter here to CONFIRM or ESC to CANCEL:
```

Figure 170 Menu 11.5 Remote Node Filter (PPPoA or PPPoE Encapsulation)

```
                        Menu 11.5 - Remote Node Filter
                  Input Filter Sets:
                    protocol filters=
                      device filters=
                  Output Filter Sets:
                    protocol filters=
                      device filters=
                  Call Filter Sets:
                    protocol filters=
                      device filters=

                   Enter here to CONFIRM or ESC to CANCEL:
```

31.5 Editing ATM Layer Options

Follow the steps shown next to edit **Menu 11.6 – Remote Node ATM Layer Options**.

In menu 11.1, move the cursor to the **Edit ATM Options** field and then press [SPACE BAR] to select **Yes**. Press [ENTER] to display **Menu 11.6 – Remote Node ATM Layer Options**.

There are two versions of menu 11.6 for the Prestige, depending on whether you chose **VC-based/LLC-based** multiplexing and **PPP** encapsulation in menu 11.1.

31.5.1 VC-based Multiplexing (non-PPP Encapsulation)

For **VC-based** multiplexing, by prior agreement, a protocol is assigned a specific virtual circuit, for example, VC1 will carry IP. Separate VPI and VCI numbers must be specified for each protocol.

Figure 171 Menu 11.6 for VC-based Multiplexing

```
            Menu 11.6 - Remote Node ATM Layer Options
            VPI/VCI (VC-Multiplexing)

   VC Options for IP:              VC Options for Bridge:
     VPI #= 8                        VPI #= 1
     VCI #= 35                       VCI #= 36
     ATM QoS Type= UBR               ATM QoS Type= N/A
     Peak Cell Rate (PCR)= 0         Peak Cell Rate (PCR)= N/A
     Sustain Cell Rate (SCR)= 0      Sustain Cell Rate (SCR)= N/A
     Maximum Burst Size (MBS)= 0     Maximum Burst Size (MBR)= N/A

                 Enter here to CONFIRM or ESC to CANCEL:
```

31.5.2 LLC-based Multiplexing or PPP Encapsulation

For **LLC-based** multiplexing or **PPP** encapsulation, one VC carries multiple protocols with protocol identifying information being contained in each packet header.

Figure 172 Menu 11.6 for LLC-based Multiplexing or PPP Encapsulation

```
            Menu 11.6 - Remote Node ATM Layer Options
            VPI/VCI (LLC-Multiplexing or PPP-Encapsulation)
                                VPI #= 8
                                VCI #= 35
                                ATM QoS Type= UBR
                                Peak Cell Rate (PCR)= 0
                                Sustain Cell Rate (SCR)= 0
                                Maximum Burst Size (MBS)= 0

            ENTER here to CONFIRM or ESC to CANCEL:
```

In this case, only one set of VPI and VCI numbers need be specified for all protocols. The valid range for the VPI is 0 to 255 and for the VCI is 32 to 65535 (1 to 31 is reserved for local management of ATM traffic).

31.5.3 Advance Setup Options

In menu 11.1, select **PPPoE** in the **Encapsulation** field.

Figure 173 Menu 11.1 Remote Node Profile

```
                  Menu 11.1 - Remote Node Profile
Rem Node Name= MyISP                  Route= IP
Active= Yes                           Bridge= No
Encapsulation= PPPoE                Edit IP/Bridge= No
Multiplexing= LLC-based               Edit ATM Options= No
Service Name=                         Edit Advance Options= Yes
Incoming:                             Telco Option:
  Rem Login=                            Allocated Budget(min)= 0
  Rem Password= ********                Period(hr)= 0
Outgoing:                               Schedule Sets=
  My Login= ?                           Nailed-Up Connection= No
  My Password= ?                      Session Options:
  Authen= CHAP/PAP                      Edit Filter Sets= No
                                        Idle Timeout(sec)= 0

               Press ENTER to Confirm or ESC to Cancel:
```

Move the cursor to the **Edit Advance Options** field, press [SPACE BAR] to select **Yes,** then press [ENTER] to display **Menu 11.8 – Advance Setup Options**.

Figure 174 Menu 11.8 Advance Setup Options

```
                        Menu 11.8 - Advance Setup Options

                    PPPoE pass-through= No

                    Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 117 Menu 11.8 Advance Setup Options

FIELD	DESCRIPTION
PPPoE pass-through	Press [SPACE BAR] to select **Yes** and press [ENTER] to enable PPPoE pass through. In addition to the Prestige's built-in PPPoE client, you can enable PPPoE pass through to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the Prestige. Each host can have a separate account and a public WAN IP address. PPPoE pass through is an alternative to NAT for applications where NAT is not appropriate. Press [SPACE BAR] to select **No** and press [ENTER] to disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

CHAPTER 32
Static Route Setup

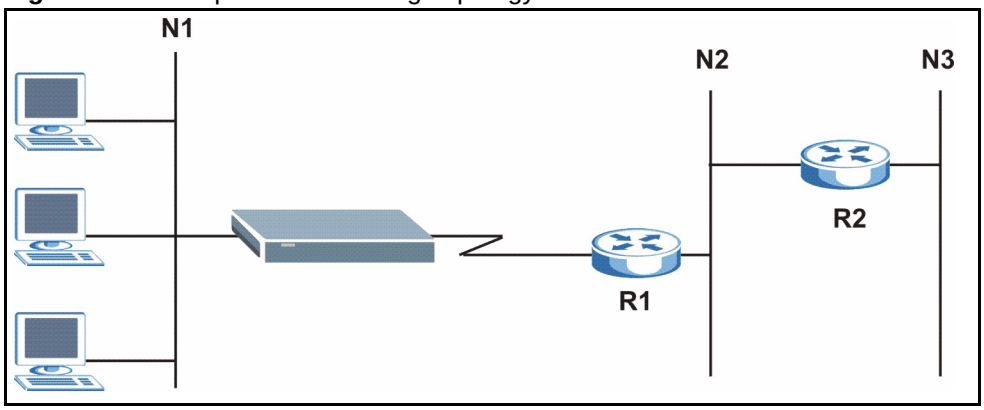
This chapter shows how to setup IP static routes.

32.1 IP Static Route Overview

Static routes tell the Prestige routing information that it cannot learn automatically through other means. This can arise in cases where RIP is disabled on the LAN or a remote network is beyond the one that is directly connected to a remote node.

Each remote node specifies only the network to which the gateway is directly connected and the Prestige has no knowledge of the networks beyond. For instance, the Prestige knows about network N2 in the following figure through remote node Router 1. However, the Prestige is unable to route a packet to network N3 because it does not know that there is a route through remote node Router 1 (via Router 2). The static routes allow you to tell the Prestige about the networks beyond the remote nodes.

Figure 175 Sample Static Routing Topology



32.2 Configuration

To configure an IP static route, use **Menu 12 – Static Route Setup** (shown next).

Figure 176 Menu 12 Static Route Setup

```
                    Menu 12 - Static Route Setup

               1. IP Static Route

               3. Bridge Static Route

                       Please enter selection:
```

From menu 12, select 1 to open **Menu 12.1 — IP Static Route Setup** (shown next).

Figure 177 Menu 12.1 IP Static Route Setup

```
                         Menu 12.1 - IP Static Route Setup
                      1. _________
                      2. _________
                      3. _________
                      4. _________
                      5. _________
                      6. _________
                      7. _________
                      8. _________
                      9. _________
                      10. _________
                      11. _________
                      12. _________
                      13. _________
                      14. _________
                      15. _________
                      16. _________

                   Enter selection number:
```

Now, type the route number of a static route you want to configure.

Figure 178 Menu12.1.1 Edit IP Static Route

```
          Menu 12.1.1 - Edit IP Static Route
                      Route #: 1
                      Route Name= ?
                      Active= No
                      Destination IP Address= ?
                      IP Subnet Mask= ?
                      Gateway IP Address= ?
                      Metric= 2
                      Private= No

           Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields for **Menu 12.1.1 – Edit IP Static Route Setup**.

Table 118 Menu12.1.1 Edit IP Static Route

FIELD	DESCRIPTION
Route #	This is the index number of the static route that you chose in menu 12.1.
Route Name	Type a descriptive name for this route. This is for identification purpose only.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Type the subnet mask for this destination. See the IP Address and Subnet Mask section in this manual.
Gateway IP Address	Type the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Metric	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. Type 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.
Private	This parameter determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and is not included in RIP broadcasts. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

CHAPTER 33
Bridging Setup

This chapter shows you how to configure the bridging parameters of your Prestige.

33.1 Bridging in General

Bridging bases the forwarding decision on the MAC (Media Access Control), or hardware address, while routing does it on the network layer (IP) address. Bridging allows the Prestige to transport packets of network layer protocols that it does not route, for example, SNA, from one network to another. The caveat is that, compared to routing, bridging generates more traffic for the same network layer protocol, and it also demands more CPU cycles and memory.

For efficiency reasons, do *not* turn on bridging unless you need to support protocols other than IP on your network. For IP, enable the routing if you need it; do not bridge what the Prestige can route.

33.2 Bridge Ethernet Setup

Basically, all non-local packets are bridged to the WAN. Your Prestige does not support IPX.

33.2.1 Remote Node Bridging Setup

Follow the procedure in another section to configure the protocol-independent parameters in **Menu 11.1 – Remote Node Profile**. For bridging-related parameters, you need to configure **Menu 11.3 – Remote Node Network Layer Options**.

1. To setup **Menu 11.3 – Remote Node Network Layer Options** shown in the next figure, follow these steps:
2. In menu 11.1, make sure the **Bridge** field is set to **Yes**.

Figure 179 Menu 11.1 Remote Node Profile

```
                Menu 11.1 - Remote Node Profile
  Rem Node Name= ?                      Route= IP
  Active= Yes                           Bridge= Yes
  Encapsulation= ENET ENCAP             Edit IP/Bridge= No
  Multiplexing= VC-based                Edit ATM Options= No
  Service Name= N/A                     Edit Advance Options= N/A
  Incoming:                             Telco Option:
    Rem Login= N/A                        Allocated Budget(min)= N/A
    Rem Password= N/A                     Period(hr)= N/A
  Outgoing:                               Schedule Sets= N/A
    My Login= N/A                         Nailed-Up Connection= N/A
    My Password= N/A                    Session Options:
    Authen= N/A                           Edit Filter Sets= No
                                          Idle Timeout(sec)= N/A

            Press ENTER to Confirm or ESC to Cancel:
```

3 Move the cursor to the **Edit IP/Bridge** field, then press [SPACE BAR] to set the value to **Yes** and press [ENTER] to edit **Menu 11.3 – Remote Node Network Layer Options**.

Figure 180 Menu 11.3 Remote Node Network Layer Options

```
            Menu 11.3 - Remote Node Network Layer Options
 IP Options:                          Bridge Options:
   IP Address Assignment= Static        Ethernet Addr Timeout (min)= 0
   Rem IP Addr: 0.0.0.0
   Rem Subnet Mask= 0.0.0.0
   My WAN Addr= 0.0.0.0
   NAT= Full Feature
     Address Mapping Set=2
   Metric= 2
   Private= No
   RIP Direction= Both
     Version= RIP-2B
   Multicast= IGMP-v2
   IP Policies=

            Press ENTER to Confirm or ESC to Cancel:
```

Table 119 Remote Node Network Layer Options: Bridge Fields

FIELD	DESCRIPTION
Bridge (menu 11.1)	Make sure this field is set to **Yes**.
Edit IP/Bridge (menu 11.1)	Press [SPACE BAR] to select **Yes** and press [ENTER] to display menu 11.3.
Ethernet Addr Timeout (min.) (menu 11.3)	Type the time (in minutes) for the Prestige to retain the Ethernet Address information in its internal tables while the line is down. If this information is retained, your Prestige will not have to recompile the tables when the line comes back up.

33.2.2 Bridge Static Route Setup

Similar to network layer static routes, a bridging static route tells the Prestige the route to a node before a connection is established. You configure bridge static routes in menu 12.3.1 (go to menu 12, choose option 3, then choose a static route to edit) as shown next.

Figure 181 Menu 12.3.1 Edit Bridge Static Route

```
            Menu 12.3.1 - Edit Bridge Static Route
            Route #: 1
            Route Name=
            Active= No
            Ether Address= ?
            IP Address=
            Gateway Node= 1

            Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the **Edit Bridge Static Route** menu.

Table 120 Menu 12.3.1 Edit Bridge Static Route

FIELD	DESCRIPTION
Route #	This is the route index number you typed in **Menu 12.3 – Bridge Static Route Setup**.
Route Name	Type a name for the bridge static route for identification purposes.
Active	Indicates whether the static route is active (**Yes**) or not (**No**).
Ether Address	Type the MAC address of the destination computer that you want to bridge the packets to.
IP Address	If available, type the IP address of the destination computer that you want to bridge the packets to.
Gateway Node	Press [SPACE BAR] and then [ENTER] to select the number of the remote node (one to eight) that is the gateway of this static route.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

CHAPTER 34
Network Address Translation (NAT)

This chapter discusses how to configure NAT on the Prestige.

34.1 Using NAT

You must create a firewall rule in addition to setting up SUA/NAT, to allow traffic from the WAN to be forwarded through the Prestige.

34.1.1 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. See the NAT Setup section or a detailed description of the NAT set for SUA. The Prestige also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types.

- Choose **SUA Only** if you have just one public WAN IP address for your Prestige.
- Choose **Full Feature** if you have multiple public WAN IP addresses for your Prestige.

34.2 Applying NAT

You apply NAT via menus 4 or 11.3 as displayed next. The next figure shows you how to apply NAT for Internet access in menu 4. Enter 4 from the main menu to go to **Menu 4 - Internet Access Setup**.

Figure 182 Menu 4 Applying NAT for Internet Access

```
            Menu 4 - Internet Access Setup
                        ISP's Name= MyISP
                        Encapsulation= RFC 1483
                        Multiplexing= LLC-based
                        VPI #= 8
                        VCI #= 35
                        ATM QoS Type= UBR
                          Peak Cell Rate (PCR)= 0
                          Sustain Cell Rate (SCR)= 0
                          Maximum Burst Size (MBS)= 0
                        My Login= N/A
                        My Password= N/A
                        ENET ENCAP Gateway= N/A
                        IP Address Assignment= Static
                          IP Address= 0.0.0.0
                        Network Address Translation= SUA Only
                          Address Mapping Set= N/A

            Press ENTER to Confirm or ESC to Cancel:
```

The following figure shows how you apply NAT to the remote node in menu 11.1.

1. Enter 11 from the main menu.
2. When menu 11 appears, as shown in the following figure, type the number of the remote node that you want to configure.
3. Move the cursor to the **Edit IP/Bridge** field, press [SPACE BAR] to select **Yes** and then press [ENTER] to bring up **Menu 11.3 - Remote Node Network Layer Options.**

Figure 183 Applying NAT in Menus 4 & 11.3

```
            Menu 11.3 - Remote Node Network Layer Options
IP Options:                          Bridge Options:
  IP Address Assignment = Static       Ethernet Addr Timeout(min)= N/A
  Rem IP Addr = 0.0.0.0
  Rem Subnet Mask= 0.0.0.0
  My WAN Addr= 0.0.0.0
  NAT= SUA Only
    Address Mapping Set= N/A
  Metric= 2
  Private= No
  RIP Direction= Both
    Version= RIP-2B
  Multicast= None
  IP Policies=

            Enter here to CONFIRM or ESC to CANCEL:
```

The following table describes the options for Network Address Translation.

Table 121 Applying NAT in Menus 4 & 11.3

FIELD	DESCRIPTION
NAT	Press [SPACE BAR] and then [ENTER] to select **Full Feature** if you have multiple public WAN IP addresses for your Prestige. The SMT uses the address mapping set that you configure and enter in the **Address Mapping Set** field (see Figure 185).
	Select **None** to disable NAT.
	When you select **SUA Only**, the SMT uses Address Mapping Set 255 (see Figure 186). Choose **SUA Only** if you have just one public WAN IP address for your Prestige.

34.3 NAT Setup

Use the address mapping sets menus and submenus to create the mapping table used to assign global addresses to computers on the LAN. **Set 255** is used for SUA. When you select **Full Feature** in menu 4 or 11.3, the SMT will use **Set 1**. When you select **SUA Only**, the SMT will use the pre-configured **Set 255** (read only).

The server set is a list of LAN servers mapped to external ports. To use this set, a server rule must be set up inside the NAT address mapping set. Please see the section on port forwarding in the chapter on NAT web configurator screens for further information on these menus. To configure NAT, enter 15 from the main menu to bring up the following screen.

Figure 184 Menu 15 NAT Setup

```
            Menu 15 - NAT Setup

                  1. Address Mapping Sets

                  2. NAT Server Sets

            Enter Menu Selection Number:
```

34.3.1 Address Mapping Sets

Enter 1 to bring up **Menu 15.1 — Address Mapping Sets**.

Figure 185 Menu 15.1 Address Mapping Sets

```
              Menu 15.1 - Address Mapping Sets
                       1.
                       2.
                       3.
                       4.
                       5.
                       6.
                       7.
                       8.
                     255. SUA (read only)

              Enter Menu Selection Number:
```

34.3.1.1 SUA Address Mapping Set

Enter 255 to display the next screen (see also section 27.1.1). The fields in this menu cannot be changed.

Figure 186 Menu 15.1.255 SUA Address Mapping Rules

```
             Menu 15.1.255 - Address Mapping Rules
 Set Name=
Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
---  ---------------  ---------------  ---------------  ---------------  ------
 1.  0.0.0.0          255.255.255.255  0.0.0.0                           M-1
 2.                                    0.0.0.0                           Server
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.

               Press ENTER to Confirm or ESC to Cancel:
```

The following table explains the fields in this menu.

Menu 15.1.255 is read-only.

Table 122 SUA Address Mapping Rules

FIELD	DESCRIPTION
Set Name	This is the name of the set you selected in menu 15.1 or enter the name of a new set you want to create.
Idx	This is the index or rule number.
Local Start IP	**Local Start IP** is the starting local IP address (ILA).
Local End IP	**Local End IP** is the ending local IP address (ILA). If the rule is for all local IPs, then the Start IP is 0.0.0.0 and the End IP is 255.255.255.255.

Table 122 SUA Address Mapping Rules (continued)

FIELD	DESCRIPTION
Global Start IP	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global Start IP**.
Global End IP	This is the ending global IP address (IGA).
Type	These are the mapping types. **Server allows us to specify multiple servers of different types behind NAT to this machine. See later for some examples.**
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

34.3.1.2 User-Defined Address Mapping Sets

Now let's look at option 1 in menu 15.1. Enter 1 to bring up this menu. We'll just look at the differences from the previous menu. Note the extra **Action** and **Select Rule** fields mean you can configure rules in this screen. Note also that the [?] in the **Set Name** field means that this is a required field and you must enter a name for the set.

Figure 187 Menu 15.1.1 First Set

```
            Menu 15.1.1 - Address Mapping Rules
 Set Name= NAT_SET
Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
---  ---------------  ---------------  ---------------  ---------------  ----
 1.
 2
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.

            Action= Edit          Select Rule=

            Press ENTER to Confirm or ESC to Cancel:
```

If the **Set Name** field is left blank, the entire set will be deleted.

The Type, Local and Global Start/End IPs are configured in menu 15.1.1.1 (described later) and the values are displayed here.

34.3.1.3 Ordering Your Rules

Ordering your rules is important because the Prestige applies the rules in the order that you specify. When a rule matches the current packet, the Prestige takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule will be pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and now you configure rule number 9. In the set summary screen, the new rule will be rule 7, not 9.

Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so as old rule 5 becomes rule 4, old rule 6 becomes rule 5 and old rule 7 becomes rule 6.

Table 123 Menu 15.1.1 First Set

FIELD	DESCRIPTION
Set Name	Enter a name for this set of rules. This is a required field. If this field is left blank, the entire set will be deleted.
Action	The default is **Edit**. **Edit** means you want to edit a selected rule (see following field). **Insert Before** means to insert a rule before the rule selected. The rules after the selected rule will then be moved down by one rule. **Delete** means to delete the selected rule and then all the rules after the selected one will be advanced one rule. **None** disables the **Select Rule** item.
Select Rule	When you choose **Edit**, **Insert Before** or **Delete** in the previous field the cursor jumps to this field to allow you to select the rule to apply the action in question.

You must press **[ENTER]** at the bottom of the screen to save the whole set. You must do this again if you make any changes to the set – including deleting a rule. No changes to the set take place until this action is taken.

Selecting **Edit** in the **Action** field and then selecting a rule brings up the following menu, **Menu 15.1.1.1 - Address Mapping Rule** in which you can edit an individual rule and configure the **Type**, **Local** and **Global Start/End IPs**.

An End IP address must be numerically greater than its corresponding IP Start address.

Figure 188 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set

```
              Menu 15.1.1.1 Address Mapping Rule
                   Type= One-to-One
                   Local IP:
                     Start=
                     End  = N/A
                   Global IP:
                     Start=
                     End  = N/A
                   Server Mapping Set= N/A

              Press ENTER to Confirm or ESC to Cancel:
```

The following table explains the fields in this menu.

Table 124 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set

FIELD	DESCRIPTION
Type	Press [SPACE BAR] and then [ENTER] to select from a total of five types. These are the mapping types discussed in the chapter on NAT web configurator screens. **Server allows you to specify multiple servers of different types behind NAT to this computer. See *section 27.5.3* for an example.**
Local IP	Only local IP fields are **N/A** for server; Global IP fields MUST be set for **Server**.
Start	This is the starting local IP address (ILA).
End	This is the ending local IP address (ILA). If the rule is for all local IPs, then put the Start IP as 0.0.0.0 and the End IP as 255.255.255.255. This field is **N/A** for One-to-One and Server types.
Global IP	
Start	This is the starting inside global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global IP Start**. Note that **Global IP Start** can be set to 0.0.0.0 only if the types are **Many-to-One** or **Server.**
End	This is the ending inside global IP address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server types**.
Server Mapping Set	Only available when **Type** is set to **Server**. Type a number from 1 to 10 to choose a server set from menu 15.2.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

34.4 Configuring a Server behind NAT

Follow these steps to configure a server behind NAT:

1. Enter 15 in the main menu to go to **Menu 15 - NAT Setup**.
2. Enter 2 to display **Menu 15.2 - NAT Server Sets** as shown next.

Figure 189 Menu 15.2 NAT Server Setup

```
            Menu 15.2 - NAT Server Sets
                   1. Server Set 1 (Used for SUA Only)
                   2. Server Set 2
                   3. Server Set 3
                   4. Server Set 4
                   5. Server Set 5
                   6. Server Set 6
                   7. Server Set 7
                   8. Server Set 8
                   9. Server Set 9
                  10. Server Set 10

                    Enter Set Number to Edit:
```

3 Enter 1 to go to **Menu 15.2.1 NAT Server Setup** as follows.

Figure 190 Menu 15.2.1 NAT Server Setup

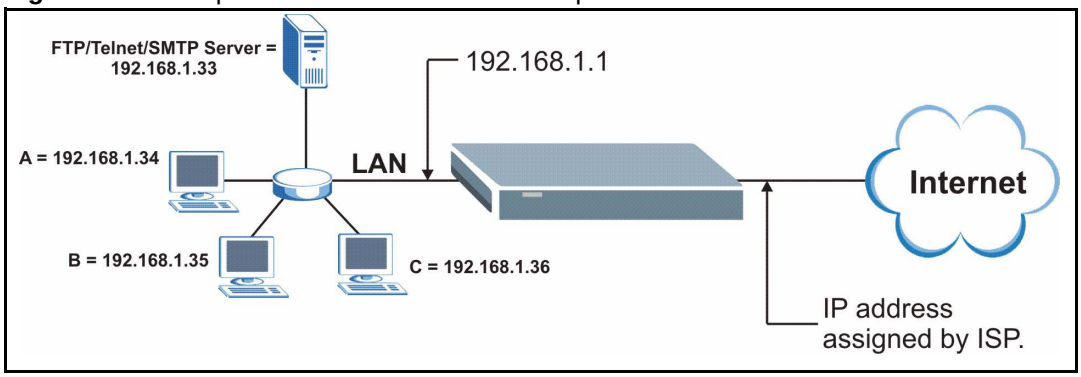
```
            Menu 15.2 - NAT Server Setup
     Rule   Start Port No.   End Port No.   IP Address
    ------------------------------------------------
       1.    Default          Default        0.0.0.0
       2.      21               21           192.168.1.33
       3.      0                0            0.0.0.0
       4.      0                0            0.0.0.0
       5.      0                0            0.0.0.0
       6.      0                0            0.0.0.0
       7.      0                0            0.0.0.0
       8.      0                0            0.0.0.0
       9.      0                0            0.0.0.0
      10.      0                0            0.0.0.0
      11.      0                0            0.0.0.0
      12.      0                0            0.0.0.0

            Press ENTER to Confirm or ESC to Cancel:
```

4 Enter a port number in an unused **Start Port No** field. To forward only one port, enter it again in the **End Port No** field. To specify a range of ports, enter the last port to be forwarded in the **End Port No** field.

5 Enter the inside IP address of the server in the **IP Address** field. In the following figure, you have a computer acting as an FTP, Telnet and SMTP server (ports 21, 23 and 25) at 192.168.1.33.

6 Press [ENTER] at the "`Press ENTER to confirm ...`" prompt to save your configuration after you define all the servers or press [ESC] at any time to cancel.

Figure 191 Multiple Servers Behind NAT Example



34.5 General NAT Examples

The following are some examples of NAT configuration.

34.5.1 Example 1: Internet Access Only

In the following Internet access example, you only need one rule where your ILAs (Inside Local addresses) all map to one dynamic IGA (Inside Global Address) assigned by your ISP.

Figure 192 NAT Example 1

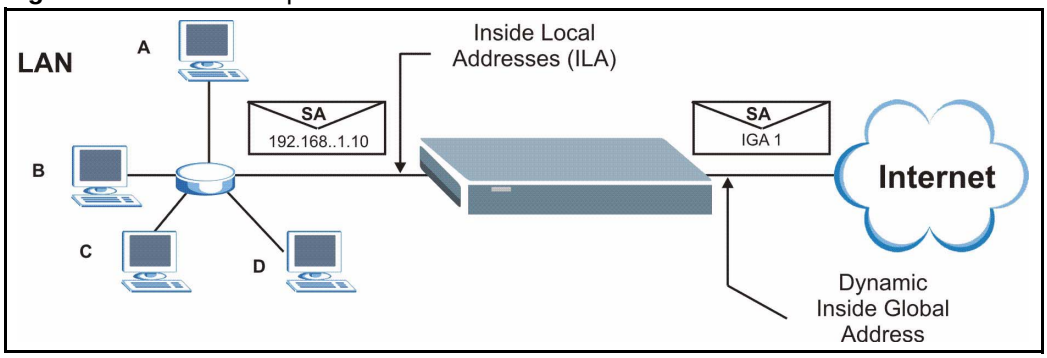


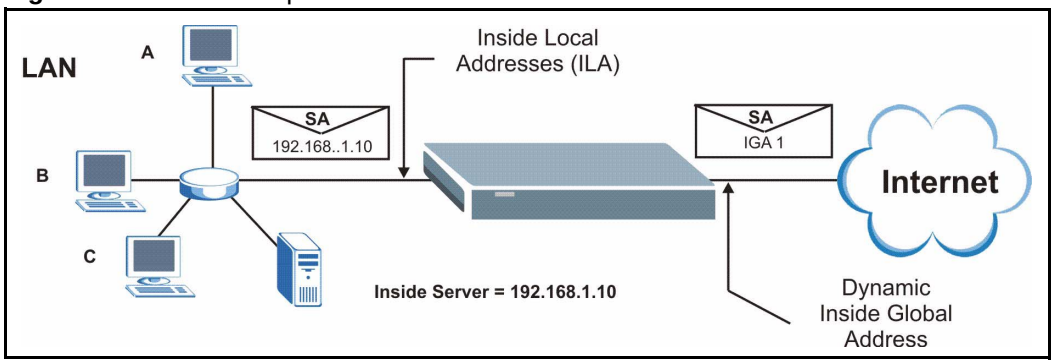
Figure 193 Menu 4 Internet Access & NAT Example

```
                    Menu 4 - Internet Access Setup
ISP's Name= MyISP
Encapsulation= RFC 1483
Multiplexing= LLC-based
VPI #= 8
VCI #= 35
ATM QoS Type= UBR
  Peak Cell Rate (PCR)= 0
  Sustain Cell Rate (SCR)= 0
  Maximum Burst Size (MBS)= 0
My Login= N/A
My Password= N/A
ENET ENCAP Gateway= N/A
IP Address Assignment= Static
  IP Address= 0.0.0.0
Network Address Translation= SUA Only
  Address Mapping Set= N/A

Press ENTER to Confirm or ESC to Cancel:
```

From menu 4, choose the **SUA Only** option from the **Network Address Translation** field. This is the **Many-to-One** mapping discussed in the General NAT Examples section . The **SUA Only** read-only option from the **Network Address Translation** field in menus 4 and 11.3 is specifically pre-configured to handle this case.

34.5.2 Example 2: Internet Access with an Inside Server

Figure 194 NAT Example 2



In this case, you do exactly as above (use the convenient pre-configured **SUA Only** set) and also go to menu 15.2 to specify the Inside Server behind the NAT as shown in the next figure.

Figure 195 Menu 15.2.1 Specifying an Inside Server

```
        Menu 15.2.1 - NAT Server Setup (Used for SUA Only)
 Rule   Start Port No.   End Port No.   IP Address
-------------------------------------------------------
   1.    Default          Default        192.168.1.10
   2.      0                0            0.0.0.0
   3.      0                0            0.0.0.0
   4.      0                0            0.0.0.0
   5.      0                0            0.0.0.0
   6.      0                0            0.0.0.0
   7.      0                0            0.0.0.0
   8.      0                0            0.0.0.0
   9.      0                0            0.0.0.0
  10.      0                0            0.0.0.0
  11.      0                0            0.0.0.0
  12.      0                0            0.0.0.0

          Press ENTER to Confirm or ESC to Cancel:
```

34.5.3 Example 3: Multiple Public IP Addresses With Inside Servers

In this example, there are 3 IGAs from our ISP. There are many departments but two have their own FTP server. All departments share the same router. The example will reserve one IGA for each department with an FTP server and all departments use the other IGA. Map the FTP servers to the first two IGAs and the other LAN traffic to the remaining IGA. Map the third IGA to an inside web server and mail server. Four rules need to be configured, two bi-directional and two unidirectional as follows.

Map the first IGA to the first inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).

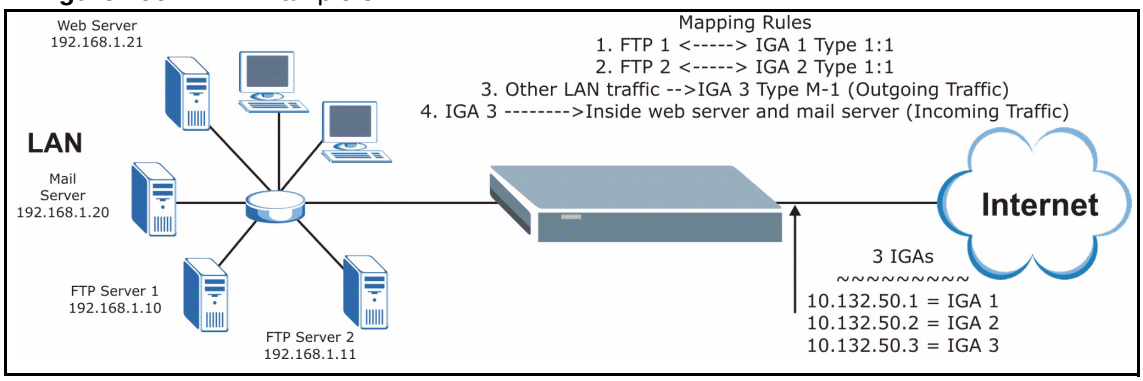
Map the second IGA to our second inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).

Map the other outgoing LAN traffic to IGA3 (**Many : 1** mapping).

You also map your third IGA to the web server and mail server on the LAN. Type **Server** allows you to specify multiple servers, of different types, to other computers behind NAT on the LAN.

The example situation looks somewhat like this:

Figure 196 NAT Example 3



In this case you need to configure Address Mapping Set 1 from **Menu 15.1 - Address Mapping Sets.** Therefore you must choose the **Full Feature** option from the **Network Address Translation** field (in menu 4 or menu 11.3) in Figure 197 .

1. Enter 15 from the main menu.
2. Enter 1 to configure the Address Mapping Sets.
3. Enter 1 to begin configuring this new set. Enter a Set Name, choose the **Edit Action** and then enter 1 for the **Select Rule** field. Press [ENTER] to confirm.
4. Select **Type** as **One-to-One** (direct mapping for packets going both ways), and enter the local **Start IP** as 192.168.1.10 (the IP address of FTP Server 1), the global **Start IP** as 10.132.50.1 (our first IGA). (See Figure 198).
5. Repeat the previous step for rules 2 to 4 as outlined above.

When finished, menu 15.1.1 should look like as shown in Figure 199 .

Figure 197 Example 3: Menu 11.3

```
            Menu 11.3 - Remote Node Network Layer Options
IP Options:                          Bridge Options:
  IP Address Assignment= Static        Ethernet Addr Timeout (min)= 0
  Rem IP Addr: 0.0.0.0
  Rem Subnet Mask= 0.0.0.0
  My WAN Addr= 0.0.0.0
  NAT= Full Feature
    Address Mapping Set= 2
  Metric= 2
  Private= No
  RIP Direction= Both
    Version= RIP-2B
  Multicast= IGMP-v2
  IP Policies=

            Press ENTER to Confirm or ESC to Cancel:
```

The following figures show how to configure the first rule

Figure 198 Example 3: Menu 15.1.1.1

```
            Menu 15.1.1.1 Address Mapping Rule
                 Type= One-to-One
                 Local IP:
                   Start= 192.168.1.10
                   End  = N/A
                 Global IP:
                   Start= 10.132.50.1
                   End  = N/A
                 Server Mapping Set= N/A

             Press ENTER to Confirm or ESC to Cancel:
```

Figure 199 Example 3: Final Menu 15.1.1

```
            Menu 15.1.1 - Address Mapping Rules
Set Name= Example3
Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
---  ---------------  ---------------  ---------------  ---------------  ------
 1. 192.168.1.10                      10.132.50.1                       1-1
 2  192.168.1.11                      10.132.50.2                       1-1
 3. 0.0.0.0           255.255.255.255  10.132.50.3                       M-1
 4.                                    10.132.50.3                       Server
 5.
 6.
 7.
 8.
 9.
10.

            Action= Edit          Select Rule=

            Press ENTER to Confirm or ESC to Cancel:
```

Now configure the IGA3 to map to our web server and mail server on the LAN.

1. Enter 15 from the main menu.
2. Enter 2 in **Menu 15 - NAT Setup**.
3. Enter 1 in **Menu 15.2 - NAT Server Sets** to see the following menu. Configure it as shown.

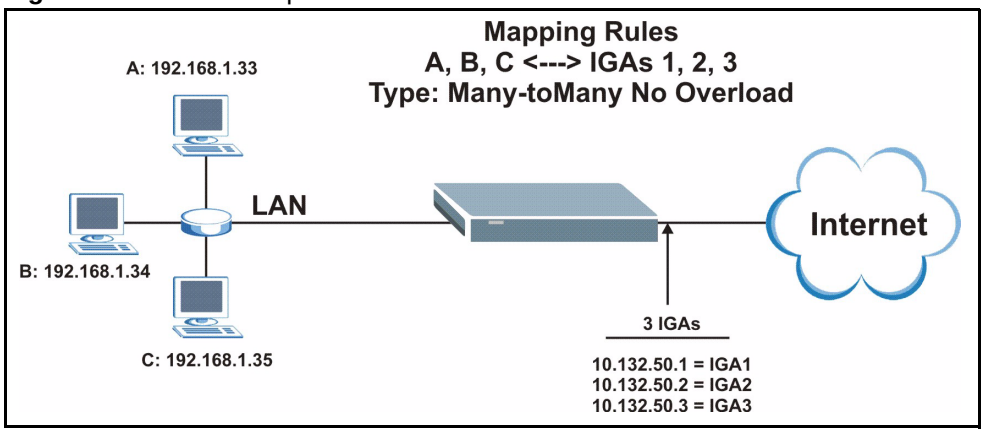
Figure 200 Example 3: Menu 15.2.1

```
          Menu 15.2.1 - NAT Server Setup
Rule   Start Port No.   End Port No.   IP Address
-------------------------------------------------
   1.    Default          Default        0.0.0.0
   2.      80               80           192.168.1.21
   3.      25               25           192.168.1.20
   4.      0                0            0.0.0.0
   5.      0                0            0.0.0.0
   6.      0                0            0.0.0.0
   7.      0                0            0.0.0.0
   8.      0                0            0.0.0.0
   9.      0                0            0.0.0.0
  10.      0                0            0.0.0.0
  11.      0                0            0.0.0.0
  12.      0                0            0.0.0.0

        Press ENTER to Confirm or ESC to Cancel:
```

34.5.4 Example 4: NAT Unfriendly Application Programs

Some applications do not support NAT Mapping using TCP or UDP port address translation. In this case it is better to use **Many-to-Many No Overload** mapping as port numbers do *not* change for **Many-to-Many No Overload** (and **One-to-One**) NAT mapping types. The following figure illustrates this.

Figure 201 NAT Example 4



Other applications such as some gaming programs are NAT unfriendly because they embed addressing information in the data stream. These applications won't work through NAT even when using **One-to-One** and **Many-to-Many No Overload** mapping types.

Follow the steps outlined in example 3 to configure these two menus as follows.

Figure 202 Example 4: Menu 15.1.1.1 Address Mapping Rule

```
              Menu 15.1.1.1 Address Mapping Rule
                   Type= Many-to-Many No Overload
                   Local IP:
                     Start= 192.168.1.10
                     End  = 192.168.1.12
                   Global IP:
                     Start= 10.132.50.1
                     End  = 10.132.50.3
                   Server Mapping Set= N/A

              Press ENTER to Confirm or ESC to Cancel:
```

After you've configured your rule, you should be able to check the settings in menu 15.1.1 as shown next.

Figure 203 Example 4: Menu 15.1.1 Address Mapping Rules

```
             Menu 15.1.1 - Address Mapping Rules
 Set Name= Example4
Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
---  ---------------  ---------------  ---------------  ---------------  ------
 1.  192.168.1.10     192.168.1.12     10.132.50.1      10.132.50.3      M:M NO OV
 2.
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.
                  Action= Edit          Select Rule=

              Press ENTER to Confirm or ESC to Cancel:
```

CHAPTER 35
Enabling the Firewall

This chapter shows you how to get started with the Prestige firewall.

35.1 Remote Management and the Firewall

When SMT menu 24.11 is configured to allow management (see the *Remote Management* chapter) and the firewall is enabled:

- The firewall blocks remote management from the WAN unless you configure a firewall rule to allow it.
- The firewall allows remote management from the LAN.

35.2 Access Methods

The web configurator is, by far, the most comprehensive firewall configuration tool your Prestige has to offer. For this reason, it is recommended that you configure your firewall using the web configurator, see the following chapters for instructions. SMT screens allow you to activate the firewall and view firewall logs.

35.3 Enabling the Firewall

From the main menu enter 21 to go to **Menu 21 - Filter Set and Firewall Configuration** to display the screen shown next**.**

Enter option 2 in this menu to bring up the following screen. Press [SPACE BAR] and then [ENTER] to select **Yes** in the **Active** field to activate the firewall. The firewall must be active to protect against Denial of Service (DoS) attacks. Additional rules may be configured using the web configurator.

Figure 204 Menu 21.2 Firewall Setup

```
        Menu 21.2 - Firewall Setup
The firewall protects against Denial of Service (DOS) attacks when
it is active. The default Policy sets
    1. allow all sessions originating from the LAN to the WAN and
    2. deny all sessions originating from the WAN to the LAN
You may define additional Policy rules or modify existing ones but
please exercise extreme caution in doing so
    Active: Yes
    LAN-to-WAN Set Name: ACL Default Set
    WAN-to-LAN Set Name: ACL Default Set
Please configure the Firewall function through Web Configurator.

         Press ENTER to Confirm or ESC to Cancel:
```

Use the web configurator or the command interpreter to configure the firewall rules

CHAPTER 36
Filter Configuration

This chapter shows you how to create and apply filters.

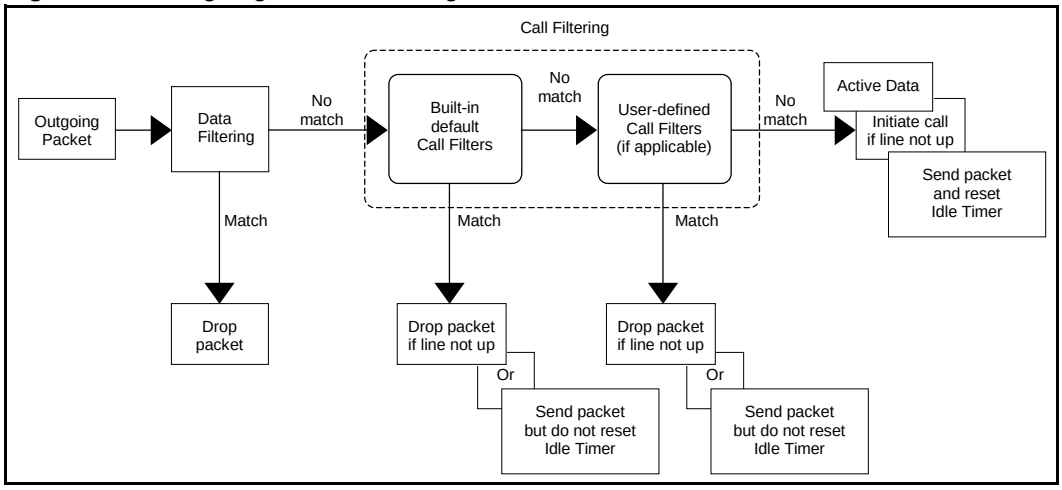
36.1 About Filtering

Your Prestige uses filters to decide whether or not to allow passage of a data packet and/or to make a call. There are two types of filter applications: data filtering and call filtering. Filters are subdivided into device and protocol filters, which are discussed later.

Data filtering screens data to determine if the packet should be allowed to pass. Data filters are divided into incoming and outgoing filters, depending on the direction of the packet relative to a port. Data filtering can be applied on either the WAN side or the Ethernet side. Call filtering is used to determine if a packet should be allowed to trigger a call.

Outgoing packets must undergo data filtering before they encounter call filtering. Call filters are divided into two groups, the built-in call filters and user-defined call filters. Your Prestige has built-in call filters that prevent administrative, for example, RIP packets from triggering calls. These filters are always enabled and not accessible to you. Your Prestige applies the built-in filters first and then the user-defined call filters, if applicable, as shown next.

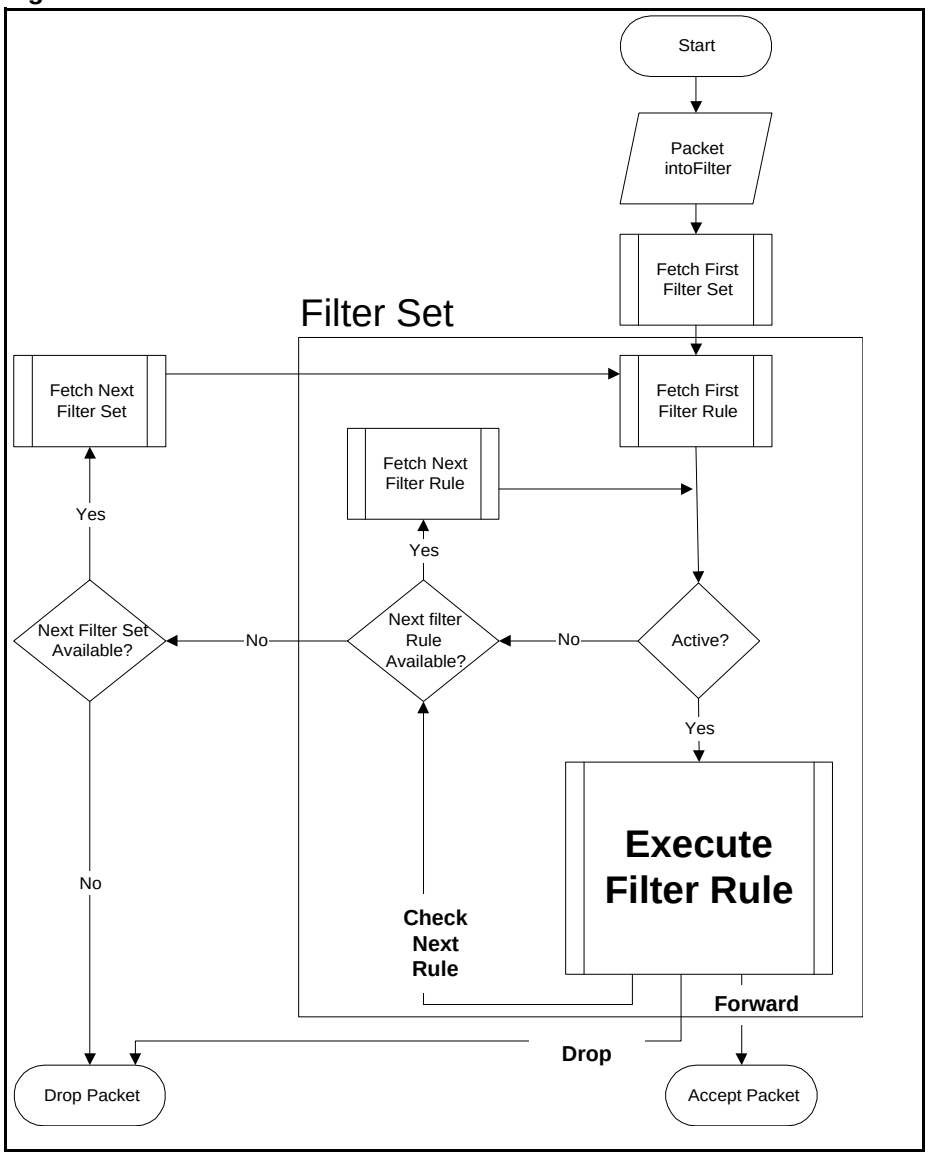
Figure 205 Outgoing Packet Filtering Process



Two sets of factory filter rules have been configured in menu 21 to prevent NetBIOS traffic from triggering calls. A summary of their filter rules is shown in the figures that follow.

The following figure illustrates the logic flow when executing a filter rule.

Figure 206 Filter Rule Process



You can apply up to four filter sets to a particular port to block various types of packets. Because each filter set can have up to six rules, you can have a maximum of 24 rules active for a single port.

For incoming packets, your Prestige applies data filters only. Packets are processed depending on whether a match is found. The following sections describe how to configure filter sets.

36.1.1 The Filter Structure of the Prestige

A filter set consists of one or more filter rules. Usually, you would group related rules, for example, all the rules for NetBIOS, into a single set and give it a descriptive name. You can configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system.

36.2 Configuring a Filter Set for the Prestige

To configure a filter set, follow the steps shown next.

1. Enter 21 in the main menu to display **Menu 21 – Filter and Firewall Setup**.
2. Enter 1 to display **Menu 21.1 – Filter Set Configuration** as shown next.

Figure 207 Menu 21 Filter Set Configuration

```
            Menu 21.1 - Filter Set Configuration
 Filter                                Filter
 Set #        Comments                 Set #        Comments
 ------  -----------------             ------  -----------------
   1      _________________              7      _________________
   2      _________________              8      _________________
   3      _________________              9      _________________
   4      _________________             10      _________________
   5      _________________             11      _________________
   6      _________________             12      _________________

            Enter Filter Set Number to Configure= 0

            Edit Comments= N/A

            Press ENTER to Confirm or ESC to Cancel:
```

3. Type the filter set to configure (no. 1 to 12) and press [ENTER].
4. Type a descriptive name or comment in the **Edit Comments** field and press [ENTER].
5. Press [ENTER] at the message "**Press ENTER to confirm…**" to display **Menu 21.1.1 – Filter Rules Summary** (that is, if you selected filter set 1 in menu 21.1).

Figure 208 NetBIOS_WAN Filter Rules Summary

```
            Menu 21.1.2 - Filter Rules Summary
 # A Type                      Filter Rules                              M m n
 - - ---- ------------------------------------------------------------- -
- -
 1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=137                          N D N
 2 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=138                          N D N
 3 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=139                          N D N
 4 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=137                         N D N
 5 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=138                         N D N
 6 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=139                         N D F

            Enter Filter Rule Number (1-6) to Configure:
```

Figure 209 NetBIOS_LAN Filter Rules Summary

```
             Menu 21.1.3 - Filter Rules Summary
 # A Type                      Filter Rules                              M m n
 - - ---- ------------------------------------------------------------- -
- -
 1 Y IP   Pr=17, SA=0.0.0.0, SP=137, DA=0.0.0.0, DP=53                  N D F
 2 N
 3 N
 4 N
 5 N
 6 N
             Enter Filter Rule Number (1-6) to Configure:
```

Figure 210 IGMP Filter Rules Summary

```
             Menu 21.1.4 - Filter Rules Summary
 # A Type                      Filter Rules                              M m n
 - - ---- ------------------------------------------------------------- -
- -
 1 Y Gen  Off=0, Len=3, Mask=ffffff, Value=01005e                       N D F
 2 N
 3 N
 4 N
 5 N
 6 N

             Enter Filter Rule Number (1-6) to Configure:
```

36.3 Filter Rules Summary Menus

The following tables briefly describe the abbreviations used in menus 21.1.1 and 21.1.2.

Table 125 Abbreviations Used in the Filter Rules Summary Menu

FIELD	DESCRIPTION
#	The filter rule number: 1 to 6.
A	Active: "Y" means the rule is active. "N" means the rule is inactive.
Type	The type of filter rule: "GEN" for Generic, "IP" for TCP/IP.
Filter Rules	These parameters are displayed here.
M	More. "Y" means there are more rules to check which form a rule chain with the present rule. An action cannot be taken until the rule chain is complete. "N" means there are no more rules to check. You can specify an action to be taken for instance, forward the packet, drop the packet or check the next rule. For the latter, the next rule is independent of the rule just checked.

Table 125 Abbreviations Used in the Filter Rules Summary Menu (continued)

FIELD	DESCRIPTION
m	Action Matched. "F" means to forward the packet immediately and skip checking the remaining rules. "D" means to drop the packet. "N" means to check the next rule.
n	Action Not Matched. "F" means to forward the packet immediately and skip checking the remaining rules. "D" means to drop the packet. "N" means to check the next rule.

The protocol dependent filter rules abbreviation are listed as follows:

Table 126 Rule Abbreviations Used

FILTER TYPE	DESCRIPTION
IP	
Pr	Protocol
SA	Source Address
SP	Source Port Number
DA	Destination Address
DP	Destination Port Number
GEN	
Off	Offset
Len	Length

36.4 Configuring a Filter Rule

To configure a filter rule, type its number in **Menu 21.1.x – Filter Rules Summary** and press [ENTER] to open menu 21.1.x.1 for the rule.

There are two types of filter rules: **TCP/IP** and **Generic**. Depending on the type of rule, the parameters for each type will be different. Use [SPACE BAR] to select the type of rule that you want to create in the **Filter Type** field and press [ENTER] to open the respective menu.

To speed up filtering, all rules in a filter set must be of the same class, for instance, protocol filters or generic filters. The class of a filter set is determined by the first rule that you create. When applying the filter sets to a port, separate menu fields are provided for protocol and device filter sets. If you include a protocol filter set in a device filters field or vice versa, the Prestige will warn you and will not allow you to save.

36.4.1 TCP/IP Filter Rule

This section shows you how to configure a TCP/IP filter rule. TCP/IP rules allow you to base the rule on the fields in the IP and the upper layer protocol, for example, UDP and TCP headers.

To configure TCP/IP rules, select TCP/IP Filter Rule from the **Filter Type** field and press [ENTER] to open **Menu 21.1.x.1 – TCP/IP Filter Rule**, as shown next.

Figure 211 Menu 21.1.x.1 TCP/IP Filter Rule

```
                    Menu 21.1.1.1 - TCP/IP Filter Rule

                Filter #: 1,1
                Filter Type= TCP/IP Filter Rule
                Active= No
                IP Protocol= 0     IP Source Route= No
                Destination: IP Addr=
                             IP Mask=
                             Port #=
                             Port # Comp= None
                     Source: IP Addr=
                             IP Mask=
                             Port #=
                             Port # Comp= None
                TCP Estab= N/A
                More= No           Log= None
                Action Matched= Check Next Rule
                Action Not Matched= Check Next Rule

                Press ENTER to Confirm or ESC to Cancel:
```

The following table describes how to configure your TCP/IP filter rule.

Table 127 Menu 21.1.x.1 TCP/IP Filter Rule

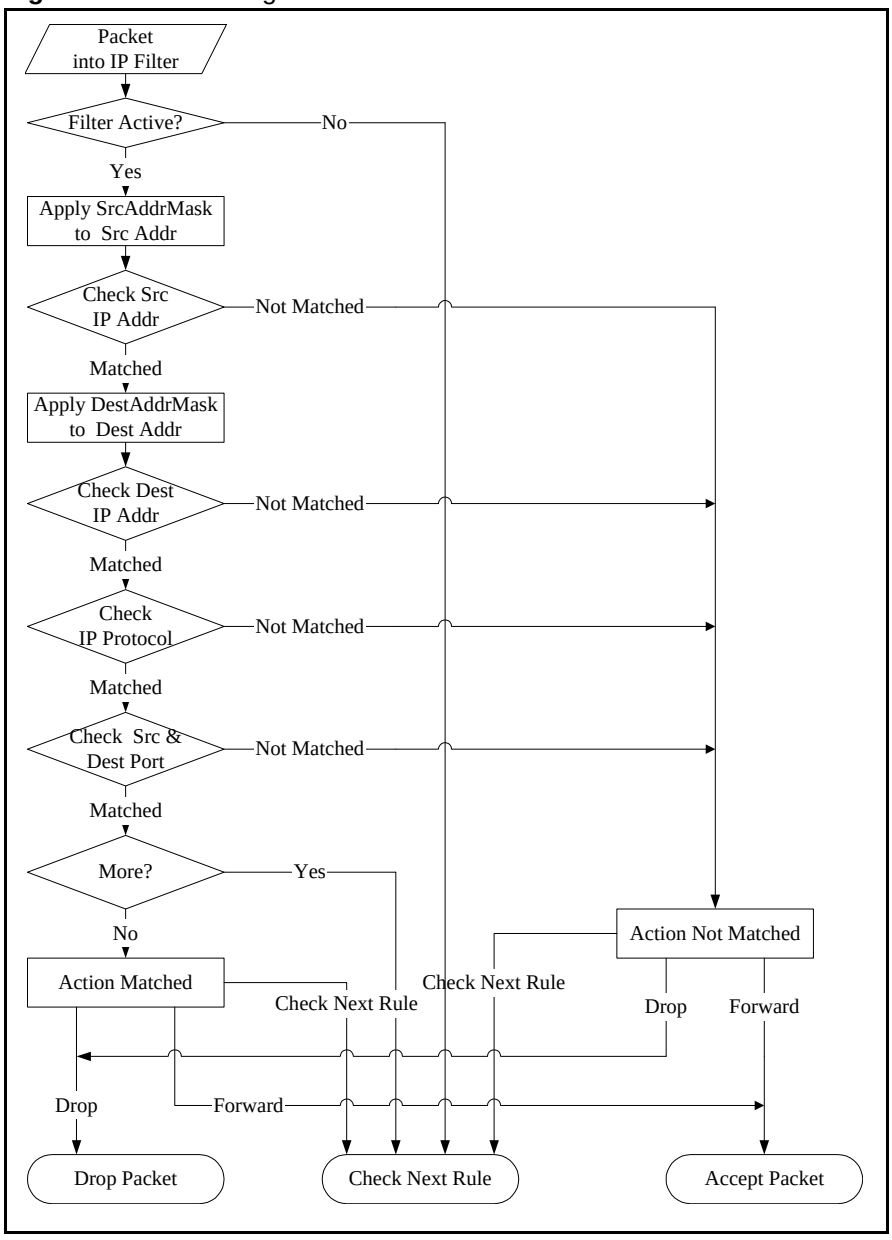
FIELD	DESCRIPTION
Filter #	This is the filter set, filter rule coordinates, for instance, 2, 3 refers to the second filter set and the third filter rule of that set.
Filter Type	Use [SPACE BAR] and then [ENTER] to choose a rule. Parameters displayed for each type will be different. Choices are **TCP/IP Filter Rule** or **Generic Filter Rule**.
Active	Select **Yes** to activate or **No** to deactivate the filter rule.
IP Protocol	This is the upper layer protocol, for example, TCP is 6, UDP is 17 and ICMP is 1. The value must be between 0 and 255. A value of 0 matches ANY protocol.
IP Source Route	IP Source Route is an optional header that dictates the route an IP packet takes from its source to its destination. If **Yes**, the rule applies to any packet with an IP source route. The majority of IP packets do not have source route.
Destination:	
IP Addr	Type the destination IP address of the packet you want to filter. This field is ignored if it is 0.0.0.0.
IP Mask	Type the IP mask to apply to the **Destination: IP Addr** field.

Table 127 Menu 21.1.x.1 TCP/IP Filter Rule (continued)

FIELD	DESCRIPTION
Port #	Type the destination port of the packets you want to filter. The field range is 0 to 65535. A 0 field is ignored.
Port # Comp	Select the comparison to apply to the destination port in the packet against the value given in **Destination: Port #.** Choices are **None**, **Less**, **Greater**, **Equal** or **Not Equal**.
Source:	
IP Addr	Type the source IP Address of the packet you want to filter. A 0.0.0.0 field is ignored.
IP Mask	Type the IP mask to apply to the **Source: IP Addr** field.
Port #	Type the source port of the packets you want to filter. The range of this field is 0 to 65535. A 0 field is ignored.
Port # Comp	Select the comparison to apply to the source port in the packet against the value given in **Source: Port #** field. Choices are **None**, **Less**, **Greater**, **Equal** or **Not Equal**.
TCP Estab	This applies only when the IP Protocol field is 6, TCP. If **Yes**, the rule matches packets that want to establish TCP connection(s) (SYN=1 and ACK=0); else it is ignored.
More	If **Yes**, a matching packet is passed to the next filter rule before an action is taken or else the packet is disposed of according to the action fields. If **More** is **Yes**, then **Action Matched** and **Action Not Matched** will be N/A.
Log	Select the logging option from the following: **None** – No packets will be logged. **Action Matched** – Only packets that match the rule parameters will be logged. **Action Not Matched** – Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.
Action Matched	Select the action for a matching packet. Choices are **Check Next Rule**, **Forward** or **Drop**.
Action Not Matched	Select the action for a packet not matching the rule. Choices are **Check Next Rule**, **Forward** or **Drop**.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

The following figure illustrates the logic flow of an IP filter.

Figure 212 Executing an IP Filter



36.4.2 Generic Filter Rule

This section shows you how to configure a generic filter rule. The purpose of generic rules is to allow you to filter non-IP packets. For IP, it is generally easier to use the IP rules directly.

For generic rules, the Prestige treats a packet as a byte stream as opposed to an IP packet. You specify the portion of the packet to check with the **Offset** (from 0) and the **Length** fields, both in bytes. The Prestige applies the Mask (bit-wise ANDing) to the data portion before comparing the result against the Value to determine a match. The **Mask** and **Value** fields are specified in hexadecimal numbers. Note that it takes two hexadecimal digits to represent a byte, so if the length is 4, the value in either field will take 8 digits, for example, FFFFFFFF.

To configure a generic rule select an empty filter set in menu 21, for example 5. Select **Generic Filter Rule** in the **Filter Type** field and press [ENTER] to open **Menu 21.1.5.1 – Generic Filter Rule**, as shown in the following figure.

Figure 213 Menu 21.1.5.1 Generic Filter Rule

```
            Menu 21.1.5.1 - Generic Filter Rule

            Filter #: 5,1
            Filter Type= Generic Filter Rule
            Active= No
            Offset= 0
            Length= 0
            Mask= N/A
            Value= N/A
            More= No           Log= None
            Action Matched= Check Next Rule
            Action Not Matched= Check Next Rule

            Press ENTER to Confirm or ESC to Cancel:
```

The next table describes the fields in the **Generic Filter Rule** menu.

Table 128 Menu 21.1.5.1 Generic Filter Rule

FIELD	DESCRIPTION
Filter #	This is the filter set, filter rule coordinates, for instance, 2, 3 refers to the second filter set and the third rule of that set.
Filter Type	Press [SPACE BAR] and then [ENTER] to select a type of rule. Parameters displayed below each type will be different. Choices are **Generic Filter Rule** or **TCP/IP Filter Rule**.
Active	Select **Yes** to turn on or **No** to turn off the filter rule.
Offset	Type the starting byte of the data portion in the packet that you want to compare. The range for this field is from 0 to 255.
Length	Type the byte count of the data portion in the packet that you want to compare. The range for this field is 0 to 8.
Mask	Type the mask (in Hexadecimal) to apply to the data portion before comparison.
Value	Type the value (in Hexadecimal) to compare with the data portion.
More	If **Yes**, a matching packet is passed to the next filter rule before an action is taken or else the packet is disposed of according to the action fields. If **More** is **Yes**, then **Action Matched** and **Action Not Matched** will be **N/A**.
Log	Select the logging option from the following: **None** – No packets will be logged. **Action Matched** – Only matching packets and rules will be logged. **Action Not Matched** – Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.
Action Matched	Select the action for a matching packet. Choices are **Check Next Rule**, **Forward** or **Drop**.

Table 128 Menu 21.1.5.1 Generic Filter Rule (continued)

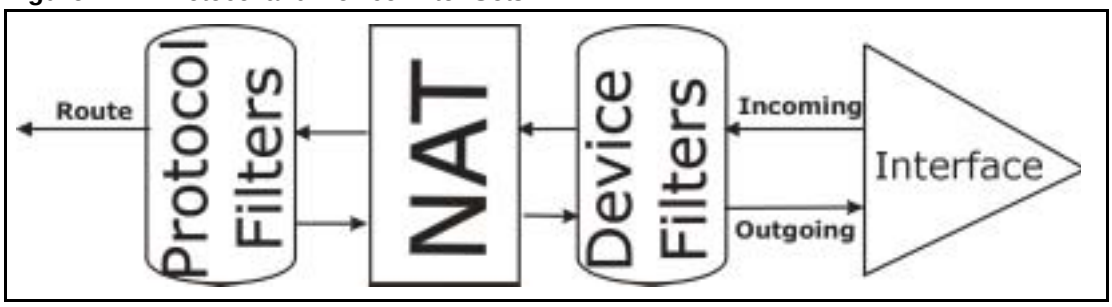
FIELD	DESCRIPTION
Action Not Matched	Select the action for a packet not matching the rule. Choices are **Check Next Rule**, **Forward** or **Drop**.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

36.5 Filter Types and NAT

There are two classes of filter rules, **Generic Filter** Device rules and Protocol Filter (**TCP/IP**) rules. Generic Filter rules act on the raw data from/to LAN and WAN. Protocol Filter rules act on IP packets.

When NAT (Network Address Translation) is enabled, the inside IP address and port number are replaced on a connection-by-connection basis, which makes it impossible to know the exact address and port on the wire. Therefore, the Prestige applies the protocol filters to the "native" IP address and port number before NAT for outgoing packets and after NAT for incoming packets. On the other hand, the generic (or device) filters are applied to the raw packets that appear on the wire. They are applied at the point where the Prestige is receiving and sending the packets; for instance, the interface. The interface can be an Ethernet, or any other hardware port. The following figure illustrates this.

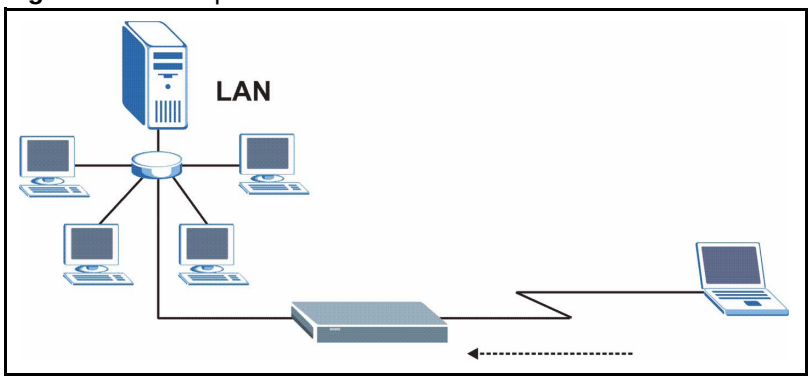
Figure 214 Protocol and Device Filter Sets



36.6 Example Filter

Let's look at an example to block outside users from telnetting into the Prestige.

Figure 215 Sample Telnet Filter



1. Enter 1 in the menu 21 to display **Menu 21.1 — Filter Set Configuration**.
2. Enter the index number of the filter set you want to configure (in this case 6).
3. Type a descriptive name or comment in the **Edit Comments** field (for example, TELNET_WAN) and press [ENTER].
4. Press [ENTER] at the message "`Press [ENTER] to confirm or [ESC] to cancel ...`" to open **Menu 21.1.6 — Filter Rules Summary**.
5. Type 1 to configure the first filter rule. Make the entries in this menu as shown next.

When you press [ENTER] to confirm, the following screen appears. Note that there is only one filter rule in this set.

Figure 216 Menu 21.1.6.1 Sample Filter

```
            Menu 21.1.6.1 - TCP/IP Filter Rule

            Filter #: 6,1
            Filter Type= TCP/IP Filter Rule
            Active= Yes
            IP Protocol= 6      IP Source Route= No
            Destination: IP Addr= 0.0.0.0
            IP Mask= 0.0.0.0
            Port #= 23
            Port # Comp= Equal
                           Source: IP Addr= 0.0.0.0
            IP Mask= 0.0.0.0
            Port #=
            Port # Comp= Equal
            TCP Estab= No
            More= No             Log= None
            Action Matched= Drop
            Action Not Matched= Forward

            Press ENTER to Confirm or ESC to Cancel:
```

After you have created the filter set, you must apply it.

1. Enter 11 in the main menu to display menu 11 and type the remote node number to edit.

2 Go to the **Edit Filter Sets** field, press [SPACE BAR] to choose **Yes** and press [ENTER].

This brings you to menu 11.5. Apply the example filter set (for example, filter set 3) in this menu as shown in the next section.

This shows you that you have configured and activated (**A = Y**) a TCP/IP filter rule (**Type = IP**, **Pr = 6**) for destination telnet ports (**DP = 23**).

M = N means an action can be taken immediately. The action is to drop the packet (**m = D**) if the action is matched and to forward the packet immediately (**n = F**) if the action is not matched no matter whether there are more rules to be checked (there aren't in this example).

Figure 217 Menu 21.1.6.1 Sample Filter Rules Summary

```
             Menu 21.1.6 - Filter Rules Summary
 # A Type                       Filter Rules                              M m n
 - - ---- ------------------------------------------------------------- -
- -
 1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23                           N D F
 2 N
 3 N
 4 N
 5 N
 6 N

             Enter Filter Rule Number (1-6) to Configure: 1
```

36.7 Applying Filters and Factory Defaults

This section shows you where to apply the filter(s) after you design it (them). Sets of factory default filter rules have been configured in menu 21 (but have not been applied) to filter traffic.

Table 129 Filter Sets Table

FILTER SETS	DESCRIPTION
Input Filter Sets:	Apply filters for incoming traffic. You may apply protocol or device filter rules. See earlier in this chapter for information on filters.
Output Filter Sets:	Apply filters for traffic leaving the Prestige. You may apply filter rules for protocol or device filters. See earlier in this section for information on types of filters.
Call Filter Sets:	Apply filters to decide if a packet should be allowed to trigger a call.

36.7.1 Ethernet Traffic

You seldom need to filter Ethernet traffic; however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 3.1 (shown next) and type the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by typing their numbers separated by commas, for example, 3, 4, 6, 11. The factory default filter set, `NetBIOS_LAN`, is inserted in the **protocol filters** field under **Input Filter Sets** in menu 3.1 in order to prevent local NetBIOS messages from triggering calls to the DNS server.

Figure 218 Filtering Ethernet Traffic

```
Menu 3.1 – LAN Port Filter Setup


Input Filter Sets:
protocol filters= 3
device filters=
Output Filter Sets:
protocol filters=
device filters=


Press ENTER to Confirm or ESC to Cancel:
```

36.7.2 Remote Node Filters

Go to menu 11.5 (shown next) and type the number(s) of the filter set(s) as appropriate. You can cascade up to four filter sets by typing their numbers separated by commas. The factory default filter set, `NetBIOS_WAN`, is inserted in the **protocol filters** field under **Call Filter Sets** in menu 11.5 to block local NetBIOS traffic from triggering calls to the ISP.

Figure 219 Filtering Remote Node Traffic

```
Menu 11.5 - Remote Node Filter

          Input Filter Sets:
            protocol filters= 6
            device filters=
          Output Filter Sets:
            protocol filters= 2
            device filters=
          Call Filter Sets:
            Protocol filters=
            Device filters=


Enter here to CONFIRM or ESC to CANCEL:
```

Note that call filter sets are visible when you select PPPoA or PPPoE encapsulation.

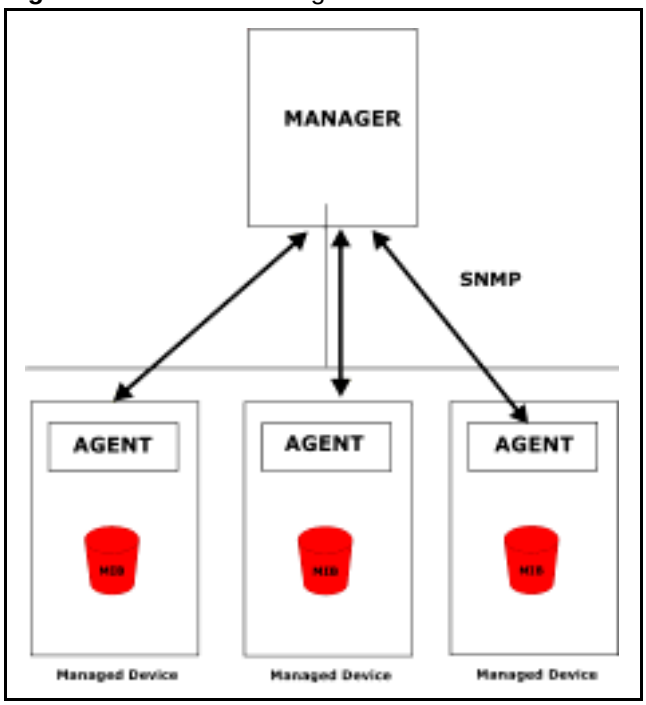
CHAPTER 37
SNMP Configuration

This chapter explains SNMP Configuration menu 22.

37.1 About SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your Prestige supports SNMP agent functionality, which allows a manager station to manage and monitor the Prestige through the network. The Prestige supports SNMP version one (SNMPv1) and version two c (SNMPv2c). The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

Figure 220 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 Prestige). 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 the 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:

- 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.

37.2 Supported MIBs

The Prestige supports RFC-1215 and MIB II as defined in RFC-1213 as well as ZyXEL private MIBs. The focus of the MIBs is to let administrators collect statistic data and monitor status and performance.

37.3 SNMP Configuration

To configure SNMP, select option 22 from the main menu to open **Menu 22 — SNMP Configuration** as shown next. The "community" for Get, Set and Trap fields is SNMP terminology for password.

Figure 221 Menu 22 SNMP Configuration

```
              Menu 22 - SNMP Configuration

              SNMP:
                Get Community= public
                Set Community= public
                Trusted Host= 0.0.0.0
                Trap:
                  Community= public
                  Destination= 0.0.0.0

              Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the SNMP configuration parameters.

Table 130 Menu 22 SNMP Configuration

FIELD	DESCRIPTION
SNMP:	
Get Community	Type the **Get Community**, which is the password for the incoming Get- and GetNext requests from the management station.
Set Community	Type the **Set** community, which is the password for incoming Set requests from the management station.
Trusted Host	If you enter a trusted host, your Prestige will only respond to SNMP messages from this address. A blank (default) field means your Prestige will respond to all SNMP messages it receives, regardless of source.
Trap:	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager.
Destination	Type the IP address of the station to send your SNMP traps to.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

37.4 SNMP Traps

The Prestige will send traps to the SNMP manager when any one of the following events occurs:

Table 131 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
1	coldStart (*defined in RFC-1215*)	A trap is sent after booting (power on).
2	warmStart (*defined in RFC-1215*)	A trap is sent after booting (software reboot).
3	linkDown (*defined in RFC-1215*)	A trap is sent with the port number when any of the links are down. See the following table.
4	linkUp (*defined in RFC-1215*)	A trap is sent with the port number.

Table 131 SNMP Traps (continued)

TRAP #	TRAP NAME	DESCRIPTION
5	authenticationFailure (*defined in RFC-1215*)	A trap is sent to the manager when receiving any SNMP gets or sets requirements with wrong community (password).
6	whyReboot (defined in ZYXEL-MIB)	A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start).
6a	For intentional reboot :	A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (for example, download new files, CI command "sys reboot", etc.).

The port number is its interface index under the interface group.

Table 132 Ports and Permanent Virtual Circuits

PORT	PVC (PERMANENT VIRTUAL CIRCUIT)
1	Ethernet LAN
2	1
3	2
…	…
13	12
14	xDSL

CHAPTER 38
System Security

This chapter describes how to configure the system security on the Prestige.

38.1 System Security

You can configure the system password..

38.1.1 System Password

Enter 23 in the main menu to display **Menu 23 – System Security**.

You should change the default password. If you forget your password you have to restore the default configuration file. Refer to the Changing the System Password section and the Resetting the Prestige section for information.

Figure 222 Menu 23 – System Security

```
            Menu 23 - System Security

                  1. Change Password
                  2. RADIUS Server
                  4. IEEE802.1x

            Enter Menu Selection Number:
```

38.1.2 Configuring External RADIUS Server

From **Menu 23- System Security**, enter 2 to display **Menu 23.2 - System Security-RADIAS Server**.

Figure 223 Menu 23 Systm Security

```
            Menu 23 - System Security

                     1. Change Password
                     2. RADIUS Server
                     4. IEEE802.1x
```

Figure 224 Menu 23.2 System Security: RADIUS Server

```
            Menu 23.2 - System Security - RADIUS Server

                        Authentication Server:
                          Active= No
                          Server Address= 10.11.12.13
                          Port #= 1812
                          Shared Secret= ********
                        Accounting Server:
                          Active= No
                          Server Address= 10.11.12.13
                          Port #= 1813
                          Shared Secret= ********

            Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 133 Menu 23.2 System Security: RADIUS Server

FIELD	DESCRIPTION
Authentication Server	
Active	Press [SPACE BAR] to select **Yes** and press [ENTER] to enable user authentication through an external authentication server.
Server Address	Enter the IP address of the external authentication server in dotted decimal notation.
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 with additional information.
Shared Secret	Specify a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the access points. The key is not sent over the network. This key must be the same on the external authentication server and Prestige.
Accounting Server	
Active	Press [SPACE BAR] to select **Yes** and press [ENTER] to enable user authentication through an external accounting server.
Server Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port	The default port of the RADIUS server for accounting is **1813**. You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Specify a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the access points. The key is not sent over the network. This key must be the same on the external accounting server and Prestige.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

38.1.3 IEEE802.1x

The IEEE802.1x standards outline enhanced security methods for both the authentication of wireless stations and encryption key management.

Follow the steps below to enable EAP authentication on your Prestige.

1 From the main menu, enter 23 to display **Menu23 – System Security**.

Figure 225 Menu 23 System Security

```
            Menu 23 - System Security

                  1. Change Password
                  2. RADIUS Server
                  4. IEEE802.1x


            Enter Menu Selection Number:
```

2 Enter 4 to display **Menu 23.4 – System Security – IEEE802.1x**.

Figure 226 Menu 23.4 System Security: IEEE802.1x

```
            Menu 23.4 - System Security - IEEE802.1x

                  Wireless Port Control= No Authentication Required
                  ReAuthentication Timer (in second)= N/A
                  Idle Timeout (in second)= N/A
                  Key Management Protocol= N/A
                  Dynamic WEP Key Exchange= N/A
                  PSK= N/A
                  WPA Mixed Mode= N/A
                  Data Privacy for Broadcast/Multicast packets= N/A
                  WPA Broadcast/Multicast Key Update Timer= N/A
                  Authentication Databases= N/A


            Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 134 Menu 23.4 System Security : IEEE802.1x

FIELD	DESCRIPTION
Wireless Port Control	Press [SPACE BAR] and select a security mode for the wireless LAN access. Select **No Authentication Required** to allow any wireless stations access to your wired network without entering usernames and passwords. This is the default setting. Selecting **Authentication Required** means wireless stations have to enter usernames and passwords before access to the wired network is allowed. Select **No Access Allowed** to block all wireless stations access to the wired network. The following fields are not available when you select **No Authentication Required** or **No Access Allowed**.
ReAuthentication Timer (in second)	Specify how often a client has to re-enter username and password to stay connected to the wired network. This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. Enter a time interval between 10 and 9999 (in seconds). The default time interval is **1800** seconds (or 30 minutes).
Idle Timeout (in second)	The Prestige automatically disconnects a client from the wired network after a period of inactivity. The client needs to enter the username and password again before access to the wired network is allowed. This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. The default time interval is **3600** seconds (or 1 hour).
Key Management Protocol	Press [SPACE BAR] to select **802.1x**, **WPA** or **WPA-PSK** and press [ENTER].
Dynamic WEP Key Exchange	This field is activated only when you select **Authentication Required** in the **Wireless Port Control** field. Also set the **Authentication Databases** field to **RADIUS Only**. Local user database may not be used. Select **Disable** to allow wireless stations to communicate with the access points without using Dynamic WEP Key Exchange. Select **64-bit WEP** or **128-bit WEP** to enable data encryption. Up to 32 stations can access the Prestige when you configure Dynamic WEP Key Exchange. This field is not available when you set **Key Management Protocol** to **WPA** or **WPA-PSK**.
PSK	Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols) when you select **WPA-PSK** in the **Key Management Protocol** field.
WPA Mixed Mode	Select **Enable** to activate WPA mixed mode. Otherwise, select **Disable** and configure **Group Data Privacy** field.
Data Privacy for Broadcast/ Multicast packets	This field allows you to choose **TKIP** (recommended) or **WEP** for broadcast and multicast ("group") traffic if the **Key Management Protocol** is **WPA** and **WPA Mixed Mode** is disabled. **WEP** is used automatically if you have enabled **WPA Mixed Mode**. All unicast traffic is automatically encrypted by **TKIP** when **WPA** or **WPA-PSK Key Management Protocol** is selected.
WPA Broadcast/ Multicast Key Update Timer	The **WPA Broadcast/Multicast Key Update Timer** is the rate at which the AP (if using **WPA-PSK** key management) or RADIUS server (if using **WPA** key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the **WPA Broadcast/Multicast Key Update Timer** is also supported in WPA-PSK mode. The Prestige default is 1800 seconds (30 minutes).

Table 134 Menu 23.4 System Security : IEEE802.1x (continued)

FIELD	DESCRIPTION
Authentication Databases	The authentication database contains wireless station login information. The local user database is the built-in database on the Prestige. The RADIUS is an external server. Use this field to decide which database the Prestige should use (first) to authenticate a wireless station. Before you specify the priority, make sure you have set up the corresponding database correctly first. When you configure **Key Management Protocol** to **WPA**, the **Authentication Databases** must be **RADIUS Only**. You can only use the **Local User Database** with **802.1x Key Management Protocol**. Select **Local User Database Only** to have the Prestige just check the built-in user database on the Prestige for a wireless station's username and password. Select **RADIUS Only** to have the Prestige just check the user database on the specified RADIUS server for a wireless station's username and password. Select **Local first, then RADIUS** to have the Prestige first check the user database on the Prestige for a wireless station's username and password. If the user name is not found, the Prestige then checks the user database on the specified RADIUS server. Select **RADIUS first, then Local** to have the Prestige first check the user database on the specified RADIUS server for a wireless station's username and password. If the Prestige cannot reach the RADIUS server, the Prestige then checks the local user database on the Prestige. When the user name is not found or password does not match in the RADIUS server, the Prestige will not check the local user database and the authentication fails.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

Once you enable user authentication, you need to specify an external RADIUS server or create local user accounts on the Prestige for authentication.

38.2 Creating User Accounts on the Prestige

By storing user profiles locally, your Prestige is able to authenticate wireless users without interacting with a network RADIUS server.

Follow the steps below to set up user profiles on your Prestige.

1. From the main menu, enter 14 to display **Menu 14 - Dial-in User Setup**.

Figure 227 Menu 14 Dial-in User Setup

```
                          Menu 14 - Dial-in User Setup

1. ________        9. ________        17. ________        25. ________
2. ________       10. ________        18. ________        26. ________
3. ________       11. ________        19. ________        27. ________
4. ________       12. ________        20. ________        28. ________
5. ________       13. ________        21. ________        29. ________
6. ________       14. ________        22. ________        30. ________
7. ________       15. ________        23. ________        31. ________
8. ________       16. ________        24. ________        32. ________

                                  Enter Menu Selection Number:
```

2 Type a number and press [ENTER] to edit the user profile.

Figure 228 Menu 14.1 Edit Dial-in User

```
            Menu 14.1 - Edit Dial-in User

                  User Name= test
                  Active= Yes
                  Password= ********


            Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 135 Menu 14.1 Edit Dial-in User

FIELD	DESCRIPTION
User Name	Enter a username up to 31 alphanumeric characters long for this user profile. This field is case sensitive.
Active	Press [SPACE BAR] to select **Yes** and press [ENTER] to enable the user profile.
Password	Enter a password up to 31 characters long for this user profile.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

CHAPTER 39
System Information and Diagnosis

This chapter covers the information and diagnostic tools in SMT menus 24.1 to 24.4.

39.1 Overview

These tools include updates on system status, port status, log and trace capabilities and upgrades for the system software. This chapter describes how to use these tools in detail.

Type 24 in the main menu to open **Menu 24 – System Maintenance**, as shown in the following figure.

Figure 229 Menu 24 System Maintenance

```
Menu 24 - System Maintenance

1.  System Status
2.  System Information and Console Port Speed
3.  Log and Trace
4.  Diagnostic
5.  Backup Configuration
6.  Restore Configuration
7.  Upload Firmware
8.  Command Interpreter Mode
9.  Call Control
10.  Time and Date Setting
11.  Remote Management

Enter Menu Selection Number:
```

39.2 System Status

The first selection, System Status gives you information on the status and statistics of the ports, as shown next. System Status is a tool that can be used to monitor your Prestige. Specifically, it gives you information on your DSL telephone line status, number of packets sent and received.

To get to System Status, type 24 to go to **Menu 24 — System Maintenance.** From this menu, type 1**. System Status**. There are two commands in **Menu 24.1 — System Maintenance — Status**. Entering 1 resets the counters; [ESC] takes you back to the previous screen.

The following table describes the fields present in **Menu 24.1 — System Maintenance — Status** which are read-only and meant for diagnostic purposes.

Figure 230 Menu 24.1 System Maintenance : Status

```
            Menu 24.1 - System Maintenance - Status          00:36:37
                                                          Sat. Jan. 01, 2000
Node-Lnk Status      TxPkts      RxPkts      Errors  Tx B/s  Rx B/s     Up
Time
 1-PPPoA N/A             0           0           0       0       0     0:00:00
 2       N/A             0           0           0       0       0     0:00:00
 3       N/A             0           0           0       0       0     0:00:00
 4       N/A             0           0           0       0       0     0:00:00
 5       N/A             0           0           0       0       0     0:00:00
 6       N/A             0           0           0       0       0     0:00:00
 7       N/A             0           0           0       0       0     0:00:00
My WAN IP (from ISP): 0.0.0.0
    Ethernet:                                 WAN:
      Status:                 Tx Pkts: 528        Line Status: Down
      Collisions: 0          Rx Pkts: 505       Upstream Speed:     0 kbps
   CPU Load =    2.12%                        Downstream Speed:     0 kbps


                   Press Command:
              COMMANDS: 1-Reset Counters  ESC-Exit
```

The following table describes the fields present in **Menu 24.1 — System Maintenance — Status**.

Table 136 Menu 24.1 System Maintenance : Status

FIELD	DESCRIPTION
Node-Lnk	This is the node index number and link type. Link types are: PPP, ENET, 1483.
Status	This shows the status of the remote node.
TxPkts	The number of transmitted packets to this remote node.
RxPkts	The number of received packets from this remote node.
Errors	The number of error packets on this connection.
Tx B/s	This shows the transmission rate in bytes per second.
Rx B/s	This shows the receiving rate in bytes per second.
Up Time	This is the time this channel has been connected to the current remote node.
My WAN IP (from ISP)	This is the IP address of the ISP remote node.
Ethernet	This shows statistics for the LAN.
Status	This shows the current status of the LAN.
Tx Pkts	This is the number of transmitted packets to the LAN.

Table 136 Menu 24.1 System Maintenance : Status (continued)

FIELD	DESCRIPTION
Rx Pkts	This is the number of received packets from the LAN.
Collision	This is the number of collisions.
WAN	This shows statistics for the WAN.
Line Status	This shows the current status of the xDSL line, which can be Up or Down.
Upstream Speed	This shows the upstream transfer rate in kbps.
Downstream Speed	This shows the downstream transfer rate in kbps.
CPU Load	This specifies the percentage of CPU utilization.

39.3 System Information

To get to the System Information:

1. Enter 24 to display **Menu 24 — System Maintenance**.
2. Enter 2 to display Menu 24.2 — System Information and Console Port Speed.

From this menu you have two choices as shown in the next figure:

Figure 231 Menu 24.2 System Information and Console Port Speed

```
            Menu 24.2 - System Information and Console Port Speed

            1. System Information
            2. Console Port Speed

            Please enter selection:
```

39.3.1 System Information

Enter 1 in menu 24.2 to display the screen shown next.

Figure 232 Menu 24.2.1 System Maintenance: Information

```
                Menu 24.2.1 - System Maintenance - Information

                        Name:
                        Routing: IP
                        ZyNOS F/W Version: V3.40(QR.0)a2 | 3/12/2004
                        ADSL Chipset Vendor: TI AR7 01.01.00.00
                        Standard: Multi-Mode
                        LAN
                          Ethernet Address: 00:a0:c5:78:de:8d
                          IP Address: 192.168.1.1
                          IP Mask: 255.255.255.0
                          DHCP: Server

                Press ESC or RETURN to Exit:
```

The following table describes the fields in this menu.

Table 137 Menu 24.2.1 System Maintenance: Information

FIELD	DESCRIPTION
Name	Displays the system name of your Prestige. This information can be changed in **Menu 1 – General Setup**.
Routing	Refers to the routing protocol used.
ZyNOS F/W Version	Refers to the ZyNOS (ZyXEL Network Operating System) system firmware version. ZyNOS is a registered trademark of ZyXEL Communications Corporation.
ADSL Chipset Vendor	Displays the vendor of the ADSL chipset and DSL version.
Standard	This refers to the operational protocol the Prestige and the DSLAM (Digital Subscriber Line Access Multiplexer) are using.
LAN	
Ethernet Address	Refers to the Ethernet MAC (Media Access Control) of your Prestige.
IP Address	This is the IP address of the Prestige in dotted decimal notation.
IP Mask	This shows the subnet mask of the Prestige.
DHCP	This field shows the DHCP setting (None, Relay or Server) of the Prestige.

39.3.2 Console Port Speed

You can set up different port speeds for the console port through **Menu 24.2.2 – System Maintenance – Console Port Speed**. Your Prestige supports 9600 (default), 19200, 38400, 57600 and 115200 bps. Press [SPACE BAR] and then [ENTER] to select the desired speed in menu 24.2.2, as shown in the following figure.

Figure 233 Menu 24.2.2 System Maintenance : Change Console Port Speed

```
            Menu 24.2.2 – System Maintenance – Change Console Port Speed

                      Console Port Speed: 9600



            Press ENTER to Confirm or ESC to Cancel:
```

Once you change the Prestige console port speed, you must also set the speed parameter for the communication software you are using to connect to the Prestige.

39.4 Log and Trace

There are two logging facilities in the Prestige. The first is the error logs and trace records that are stored locally. The second is the syslog facility for message logging.

39.4.1 Viewing Error Log

The first place you should look for clues when something goes wrong is the error log. Follow the procedures to view the local error/trace log:

1. Type 24 in the main menu to display **Menu 24 – System Maintenance**.
2. From menu 24, type 3 to display **Menu 24.3 – System Maintenance – Log and Trace**.

Figure 234 Menu 24.3 System Maintenance: Log and Trace

```
            Menu 24.3 - System Maintenance - Log and Trace

                   1. View Error Log
                   2. UNIX Syslog


            Please enter selection
```

3. Enter 1 from **Menu 24.3 — System Maintenance — Log and Trace** to display the error log in the system.

After the Prestige finishes displaying the error log, you will have the option to clear it. Samples of typical error and information messages are presented in the next figure.

Figure 235 Sample Error and Information Messages

```
  53 Sat Jan 01 00:00:03 2000 PP01 -WARN  SNMP TRAP 0: cold start
  54 Sat Jan 01 00:00:03 2000 PP01  INFO  main: init completed
  55 Sat Jan 01 00:00:03 2000 PP01  INFO  Starting Connectivity Monitor
  56 Sat Jan 01 00:00:03 2000 PP20  INFO  adjtime task pause 1 day
  57 Sat Jan 01 00:00:03 2000 PP21  INFO  monitoring WAN connectivity
  58 Sat Jan 01 00:03:06 2000 PP19  INFO  SMT Password pass
  59 Sat Jan 01 00:03:06 2000 PP01  INFO  SMT Session Begin
  60 Sat Jan 01 00:23:21 2000 PP01  INFO  SMT Session End
  62 Sat Jan 01 00:23:38 2000 PP19  INFO  SMT Password pass
  63 Sat Jan 01 00:23:38 2000 PP01  INFO  SMT Session Begin
Clear Error Log (y/n):
```

39.4.2 Syslog and Accounting

The Prestige uses the syslog facility to log the CDR (Call Detail Record) and system messages to a syslog server. Syslog and accounting can be configured in **Menu 24.3.2 — System Maintenance — UNIX Syslog**, as shown next.

Figure 236 Menu 24.3.2 System Maintenance: Syslog and Accounting

```
            Menu 24.3.2 - System Maintenance - UNIX Syslog

            UNIX Syslog:
            Active= No
            Syslog IP Address= ?
            Log Facility= Local 1

            Press ENTER to Confirm or ESC to Cancel:
```

You need to configure the UNIX syslog parameters described in the following table to activate syslog then choose what you want to log.

Table 138 Menu 24.3.2 System Maintenance : Syslog and Accounting

PARAMETER	DESCRIPTION
UNIX Syslog:	
Active	Use [SPACE BAR] and then [ENTER] to turn syslog on or off.
Syslog IP Address	Type the IP address of your syslog server.
Log Facility	Use [SPACE BAR] and then [ENTER] to select one of seven different local options. The log facility lets you log the message in different server files. Refer to your UNIX manual.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

The following are examples of the four types of syslog messages sent by the Prestige:

Figure 237 Syslog Example

```
1 - CDR

SdcmdSyslogSend ( SYSLOG_CDR, SYSLOG_INFO, String);

String = board xx line xx channel xx, call xx, str

board = the hardware board ID

line = the WAN ID in a board

Channel = channel ID within the WAN

call = the call reference number which starts from 1 and increments by 1 for each new
call

str = C01 Outgoing Call dev xx ch xx (dev:device No. ch:channel No.)

C01 Incoming Call xxxxBps xxxxx (L2TP, xxxxx = Remote Call ID)

C01 Incoming Call xxxx (= connected speed) xxxxx (= Remote Call ID)

L02 Tunnel Connected (L2TP)

C02 OutCall Connected xxxx (= connected speed) xxxxx (= Remote Call ID)

C02 CLID call refused

L02 Call Terminated

C02 Call Terminated

Jul 19 11:19:27 192.168.102.2 ZYXEL: board 0 line 0 channel 0, call 1, C01 Outgoing
Call dev=2 ch=0 40002
Jul 19 11:19:32 192.168.102.2 ZYXEL: board 0 line 0 channel 0, call 1, C02 OutCall
Connected 64000 40002
Jul 19 11:20:06 192.168.102.2 ZYXEL: board 0 line 0 channel 0, call 1, C02 Call
Terminated

2 - Packet Triggered

SdcmdSyslogSend (SYSLOG_PKTTRI, SYSLOG_NOTICE, String);

String = Packet trigger: Protocol=xx Data=xxxxxxxxxx…..x

Protocol: (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG)

Data: We will send forty-eight Hex characters to the server

Jul 19 11:28:39 192.168.102.2 ZYXEL: Packet Trigger: Protocol=1,
Data=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a6b6c
6d6e6f7071727374
Jul 19 11:28:56 192.168.102.2 ZYXEL: Packet Trigger: Protocol=1,
Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600220008cd40000
020405b4
Jul 19 11:29:06 192.168.102.2 ZYXEL: Packet Trigger: Protocol=1,
Data=450000282401400001f06ac12c0a86614ca849a7b0427001700195b451d1430135004000077600000

3 - Filter Log

SdcmdSyslogSend (SYSLOG_FILLOG, SYSLOG_NOTICE, String);

String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx] S04>R01mD

IP[…] is the packet header and S04>R01mD means filter set 4 (S) and rule 1 (R), match
(m), drop (D).

Src: Source Address

Dst: Destination Address
```

Figure 237 Syslog Example (continued)

```
prot: Protocol (“TCP”, ”UDP”, ”ICMP”)

spo: Source port

dpo: Destination port

Jul 19 14:43:55 192.168.102.2 ZYXEL: IP [Src=202.132.154.123 Dst=255.255.255.255 UDP
spo=0208 dpo=0208]} S03>R01mF
Jul 19 14:44:00 192.168.102.2 ZYXEL: IP [Src=192.168.102.20 Dst=202.132.154.1 UDP
spo=05d4 dpo=0035]} S03>R01mF
Jul 19 14:44:04 192.168.102.2 ZYXEL: IP [Src=192.168.102.20 Dst=202.132.154.1 UDP
spo=05d4 dpo=0035]} S03>R01mF

4 - PPP Log

SdcmdSyslogSend (SYSLOG_PPPLOG, SYSLOG_NOTICE, String);

String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto
Shutdown

Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP / IPXCP

Jul 19 11:42:44 192.168.102.2 ZYXEL: ppp:LCP Closing
Jul 19 11:42:49 192.168.102.2 ZYXEL: ppp:IPCP Closing
Jul 19 11:42:54 192.168.102.2 ZYXEL: ppp:CCP Closing
```

39.5 Diagnostic

The diagnostic facility allows you to test the different aspects of your Prestige to determine if it is working properly. Menu 24.4 allows you to choose among various types of diagnostic tests to evaluate your system, as shown in the following figure.

Follow the procedure next to get to **Diagnostic**:

1. From the main menu, type 24 to open **Menu 24 – System Maintenance**.
2. From this menu, type 4. Diagnostic to open **Menu 24.4 – System Maintenance – Diagnostic**.

Figure 238 Menu 24.4 System Maintenance : Diagnostic

```
            Menu 24.4 - System Maintenance - Diagnostic

xDSL                                    System
  1.  Reset xDSL                          21. Reboot System
                                          22. Command Mode
TCP/IP
  12. Ping Host


              Enter Menu Selection Number:

              Host IP Address= N/A
```

The following table describes the diagnostic tests available in menu 24.4 for and the connections.

Table 139 Menu 24.4 System Maintenance Menu: Diagnostic

FIELD	DESCRIPTION
Reset xDSL	Re-initialize the xDSL link to the telephone company.
Ping Host	Ping the host to see if the links and TCP/IP protocol on both systems are working.
Reboot System	Reboot the Prestige.
Command Mode	Type the mode to test and diagnose your Prestige using specified commands.
Host IP Address	If you typed 12 to Ping Host, now type the address of the computer you want to ping.

CHAPTER 40
Firmware and Configuration File Maintenance

This chapter tells you how to backup and restore your configuration file as well as upload new firmware and configuration files.

40.1 Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the menus such as password, DHCP Setup, TCP/IP Setup, etc. It arrives from ZyXEL with a "rom" filename extension. Once you have customized the Prestige's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the "ras" file) is the system firmware and has a "bin" filename extension. With many FTP and TFTP clients, the filenames are similar to those seen next.

Only use firmware for your Prestige's specific model. Refer to the label on the bottom of your Prestige.

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file " firmware.bin" to the Prestige.

```
ftp> get rom-0 config.cfg
```

This is a sample FTP session saving the current configuration to the computer file "`config.cfg`".

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the Prestige only recognizes "rom-0" and "ras". Be sure you keep unaltered copies of both files for later use.

The following table is a summary. Please note that the internal filename refers to the filename on the Prestige and the external filename refers to the filename not on the Prestige, that is, on your computer, local network or FTP site and so the name (but not the extension) may vary. After uploading new firmware, see the **ZyNOS F/W Version** field in **Menu 24.2.1 – System Maintenance – Information** to confirm that you have uploaded the correct firmware version. The AT command is the command you enter after you press "y" when prompted in the SMT menu to go into debug mode.

Table 140 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	Rom-0	This is the configuration filename on the Prestige. Uploading the rom-0 file replaces the entire ROM file system, including your Prestige configurations, system-related data (including the default password), the error log and the trace log.	*.rom
Firmware	Ras	This is the generic name for the ZyNOS firmware on the Prestige.	*.bin

40.2 Backup Configuration

Option 5 from **Menu 24 – System Maintenance** allows you to backup the current Prestige configuration to your computer. Backup is highly recommended once your Prestige is functioning properly. FTP is the preferred methods for backing up your current configuration to your computer since they are faster. Any serial communications program should work fine; however, you must use Xmodem protocol to perform the download/upload and you don't have to rename the files.

Please note that terms "download" and "upload" are relative to the computer. Download means to transfer from the Prestige to the computer, while upload means from your computer to the Prestige.

40.2.1 Backup Configuration

Follow the instructions as shown in the next screen.

Figure 239 Telnet in Menu 24.5

```
              Menu 24.5 - System Maintenance - Backup Configuration
To transfer the configuration file to your workstation, follow the procedure
below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your Prestige. Then type "root" and SMT
password as requested.
3. Locate the 'rom-0' file.
4. Type 'get rom-0' to back up the current Prestige configuration to
   your workstation.
For details on FTP commands, please consult the documentation of your FTP
client program. For details on backup using TFTP (note that you must remain
in this menu to back up using TFTP), please see your Prestige manual.



              Press ENTER to Exit:
```

40.2.2 Using the FTP Command from the Command Line

1. Launch the FTP client on your computer.
2. Enter "`open`", followed by a space and the IP address of your Prestige.
3. Press [ENTER] when prompted for a username.
4. Enter your password as requested (the default is "1234").
5. Enter "`bin`" to set transfer mode to binary.
6. Use "`get`" to transfer files from the Prestige to the computer, for example, "`get rom-0 config.rom`" transfers the configuration file on the Prestige to your computer and renames it "`config.rom`". See earlier in this chapter for more information on filename conventions.
7. Enter "`quit`" to exit the ftp prompt.

40.2.3 Example of FTP Commands from the Command Line

Figure 240 FTP Session Example

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 16384 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

40.2.4 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 141 General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

40.2.5 TFTP and FTP over WAN Management Limitations

TFTP, FTP and Telnet over WAN will not work when:

- You have disabled Telnet service in menu 24.11.
- You have applied a filter in menu 3.1 (LAN) or in menu 11.5 (WAN) to block Telnet service.
- The IP address in the **Secured Client IP** field in menu 24.11 does not match the client IP. If it does not match, the Prestige will disconnect the Telnet session immediately.
- You have an SMT console session running.

40.2.6 Backup Configuration Using TFTP

The Prestige supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To backup the configuration file, follow the procedure shown next.

1. Use telnet from your computer to connect to the Prestige and log in. Because TFTP does not have any security checks, the Prestige records the IP address of the telnet client and accepts TFTP requests only from this address.
2. Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
3. Enter command "`sys stdio 0`" to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command "`sys stdio 5″` to restore the five-minute SMT timeout (default) when the file transfer is complete.
4. Launch the TFTP client on your computer and connect to the Prestige. Set the transfer mode to binary before starting data transfer.
5. Use the TFTP client (see the example below) to transfer files between the Prestige and the computer. The file name for the configuration file is "`rom-0`" (rom-zero, not capital o).

Note that the telnet connection must be active and the SMT in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use "`get`" to transfer from the Prestige to the computer and "binary" to set binary transfer mode.

40.2.7 TFTP Command Example

The following is an example TFTP command:

```
tftp [-i] host get rom-0 config.rom
```

where "`i`" specifies binary image transfer mode (use this mode when transferring binary files), "`host`" is the Prestige IP address, "`get`" transfers the file source on the Prestige (`rom-0`, name of the configuration file on the Prestige) to the file destination on the computer and renames it config.rom.

40.2.8 GUI-based TFTP Clients

The following table describes some of the fields that you may see in GUI-based TFTP clients.

Table 142 General Commands for GUI-based TFTP Clients

COMMAND	DESCRIPTION
Host	Enter the IP address of the Prestige. 192.168.1.1 is the Prestige's default IP address when shipped.
Send/Fetch	Use "Send" to upload the file to the Prestige and "Fetch" to back up the file on your computer.
Local File	Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer.
Remote File	This is the filename on the Prestige. The filename for the firmware is "ras" and for the configuration file, is "rom-0".
Binary	Transfer the file in binary mode.
Abort	Stop transfer of the file.

Refer to the TFTP and FTP over WAN Management Limitations section to read about configurations that disallow TFTP and FTP over WAN.

40.2.9 Backup Via Console Port

Back up configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

1 Display menu 24.5 and enter "y" at the following screen.

Figure 241 System Maintenance: Backup Configuration

```
            Ready to backup Configuration via Xmodem.
            Do you want to continue (y/n):
```

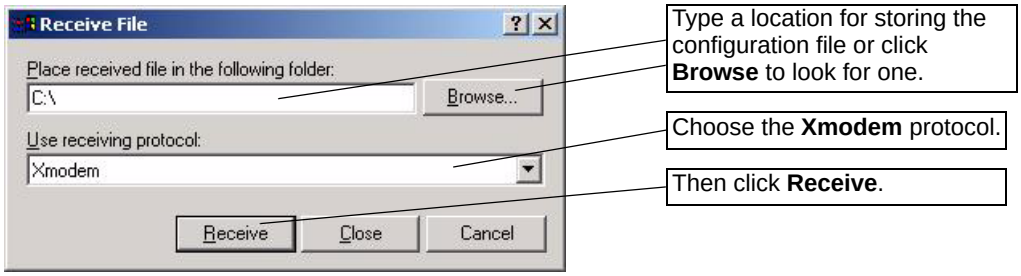
2 The following screen indicates that the Xmodem download has started.

Figure 242 System Maintenance: Starting Xmodem Download Screen

```
            You can enter ctrl-x to terminate operation any
            time.
            Starting XMODEM download...
```

3 Run the HyperTerminal program by clicking **Transfer**, then **Receive File** as shown in the following screen.

Figure 243 Backup Configuration Example



4 After a successful backup you will see the following screen. Press any key to return to the SMT menu.

Figure 244 Successful Backup Confirmation Screen

```
** Backup Configuration completed. OK.
### Hit any key to continue.###
```

40.3 Restore Configuration

This section shows you how to restore a previously saved configuration. Note that this function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

FTP is the preferred method for restoring your current computer configuration to your Prestige since FTP is faster. Please note that you must wait for the system to automatically restart after the file transfer is complete.

Note: Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR Prestige.

40.3.1 Restore Using FTP

For details about backup using (T)FTP please refer to earlier sections on FTP and TFTP file upload in this chapter.

Figure 245 Telnet into Menu 24.6

```
              Menu 24.6 -- System Maintenance - Restore Configuration
To transfer the firmware and configuration file to your workstation, follow
the procedure below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your Prestige. Then type "root" and SMT
password as requested.
3. Type "put backupfilename rom-0" where backupfilename is the name of
   your backup configuration file on your workstation and rom-0 is the
   remote file name on the Prestige. This restores the configuration   to
your Prestige.
4. The system reboots automatically after a successful file transfer

For details on FTP commands, please consult the documentation of your FTP
client program. For details on backup using TFTP (note that you must remain
in this menu to back up using TFTP), please see your Prestige manual.


              Press ENTER to Exit:
```

1. Launch the FTP client on your computer.
2. Enter "`open`", followed by a space and the IP address of your Prestige.
3. Press [ENTER] when prompted for a username.
4. Enter your password as requested (the default is "1234").
5. Enter "`bin`" to set transfer mode to binary.
6. Find the "`rom`" file (on your computer) that you want to restore to your Prestige.
7. Use "`put`" to transfer files from the Prestige to the computer, for example, "`put config.rom rom-0`" transfers the configuration file "`config.rom`" on your computer to the Prestige. See earlier in this chapter for more information on filename conventions.
8. Enter "`quit`" to exit the ftp prompt. The Prestige will automatically restart after a successful restore process.

40.3.2 Restore Using FTP Session Example

Figure 246 Restore Using FTP Session Example

```
ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
ftp>quit
```

Refer to the TFTP and FTP over WAN Management Limitations section to read about configurations that disallow TFTP and FTP over WAN.

40.3.3 Restore Via Console Port

Restore configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

1 Display menu 24.6 and enter "y" at the following screen.

Figure 247 System Maintenance: Restore Configuration

```
Ready to restore Configuration via Xmodem.
Do you want to continue (y/n):
```

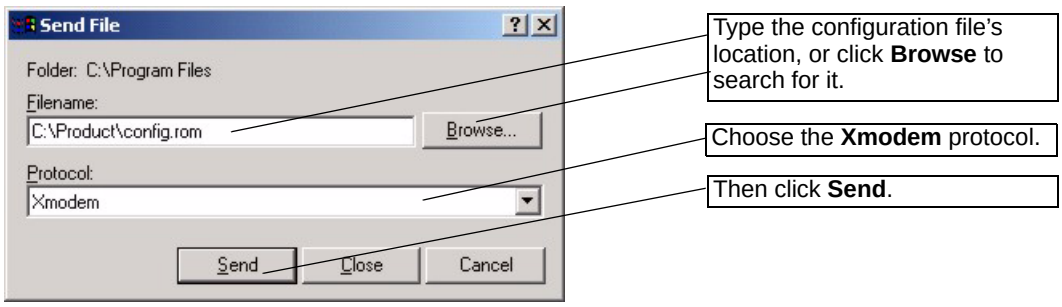
2 The following screen indicates that the Xmodem download has started.

Figure 248 System Maintenance: Starting Xmodem Download Screen

```
Starting XMODEM download (CRC mode) ...CCCCCCCCC
```

3 Run the HyperTerminal program by clicking **Transfer**, then **Send File** as shown in the following screen.

Figure 249 Restore Configuration Example



4 After a successful restoration you will see the following screen. Press any key to restart the Prestige and return to the SMT menu.

Figure 250 Successful Restoration Confirmation Screen

```
            Save to ROM
            Hit any key to start system reboot.
```

40.4 Uploading Firmware and Configuration Files

This section shows you how to upload firmware and configuration files. You can upload configuration files by following the procedure in the Backup Configuration section or by following the instructions in **Menu 24.7.2 – System Maintenance – Upload System Configuration File**.

Note: Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR Prestige.

40.4.1 Firmware File Upload

FTP is the preferred method for uploading the firmware and configuration. To use this feature, your computer must have an FTP client.

When you telnet into the Prestige, you will see the following screens for uploading firmware and the configuration file using FTP.

Figure 251 Telnet Into Menu 24.7.1 Upload System Firmware

```
            Menu 24.7.1 - System Maintenance - Upload System Firmware

To upload the system firmware, follow the procedure below:
  1. Launch the FTP client on your workstation.
  2. Type "open" and the IP address of your system. Then type "root" and
     SMT password as requested.
  3. Type "put firmware filename ras" where "firmwarefilename" is the name
     of your firmware upgrade file on your workstation and "ras" is the
     remote file name on the system.
  4. The system reboots automatically after a successful firmware upload.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP),
please see your manual.

            Press ENTER to Exit:
```

40.4.2 Configuration File Upload

You see the following screen when you telnet into menu 24.7.2.

Figure 252 Telnet Into Menu 24.7.2 System Maintenance

```
Menu 24.7.2 - System Maintenance - Upload System Configuration File

To upload the system configuration file, follow the procedure below:

  1. Launch the FTP client on your workstation.
  2. Type "open" and the IP address of your system. Then type "root" and
     SMT password as requested.
  3. Type "put configuration filename rom-0" where "configurationfilename"
     is the name of your system configuration file on your workstation, which
     will be transferred to the "rom-0" file on the system.
  4. The system reboots automatically after the upload system configuration
     file process is complete.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP),
please see your manual.


              Press ENTER to Exit:
```

To upload the firmware and the configuration file, follow these examples

40.4.3 FTP File Upload Command from the DOS Prompt Example

1. Launch the FTP client on your computer.
2. Enter "`open`", followed by a space and the IP address of your Prestige.
3. Press [ENTER] when prompted for a username.
4. Enter your password as requested (the default is "1234").
5. Enter "`bin`" to set transfer mode to binary.
6. Use "`put`" to transfer files from the computer to the Prestige, for example, "`put firmware.bin ras`" transfers the firmware on your computer (firmware.bin) to the Prestige and renames it "`ras`". Similarly, "`put config.rom rom-0`" transfers the configuration file on your computer (config.rom) to the Prestige and renames it "`rom-0`". Likewise "`get rom-0 config.rom`" transfers the configuration file on the Prestige to your computer and renames it "`config.rom`." See earlier in this chapter for more information on filename conventions.
7. Enter "`quit`" to exit the ftp prompt.

The Prestige automatically restarts after a successful file upload.

40.4.4 FTP Session Example of Firmware File Upload

Figure 253 FTP Session Example of Firmware File Upload

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

More commands (found in GUI-based FTP clients) are listed earlier in this chapter.

Refer to the TFTP and FTP over WAN Management Limitations section to read about configurations that disallow TFTP and FTP over WAN.

40.4.5 TFTP File Upload

The Prestige also supports the uploading of firmware files using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To transfer the firmware and the configuration file, follow the procedure shown next.

1. Use telnet from your computer to connect to the Prestige and log in. Because TFTP does not have any security checks, the Prestige records the IP address of the telnet client and accepts TFTP requests only from this address.
2. Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
3. Enter the command "`sys stdio 0`" to disable the console timeout, so the TFTP transfer will not be interrupted. Enter "`sys stdio 5`" to restore the five-minute console timeout (default) when the file transfer is complete.
4. Launch the TFTP client on your computer and connect to the Prestige. Set the transfer mode to binary before starting data transfer.
5. Use the TFTP client (see the example below) to transfer files between the Prestige and the computer. The file name for the firmware is "`ras`".

Note that the telnet connection must be active and the Prestige in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use "`get`" to transfer from the Prestige to the computer, "`put`" the other way around, and "`binary`" to set binary transfer mode.

40.4.6 TFTP Upload Command Example

The following is an example TFTP command:

```
tftp [-i] host put firmware.bin ras
```

where "i" specifies binary image transfer mode (use this mode when transferring binary files), "host" is the Prestige's IP address and "put" transfers the file source on the computer (firmware.bin – name of the firmware on the computer) to the file destination on the remote host (ras - name of the firmware on the Prestige).

Commands that you may see in GUI-based TFTP clients are listed earlier in this chapter.

40.4.7 Uploading Via Console Port

FTP or TFTP are the preferred methods for uploading firmware to your Prestige. However, in the event of your network being down, uploading files is only possible with a direct connection to your Prestige via the console port. Uploading files via the console port under normal conditions is not recommended since FTP or TFTP is faster. Any serial communications program should work fine; however, you must use the Xmodem protocol to perform the download/upload.

40.4.8 Uploading Firmware File Via Console Port

1. Select 1 from Menu 24.7 – System Maintenance – Upload Firmware to display Menu 24.7.1 - System Maintenance - Upload System Firmware, and then follow the instructions as shown in the following screen.

Figure 254 Menu 24.7.1 As Seen Using the Console Port

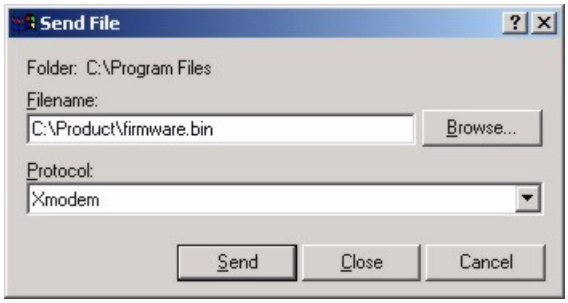
```
Menu 24.7.1 - System Maintenance - Upload System Firmware

To upload system firmware:
1. Enter "y" at the prompt below to go into debug mode.
2. Enter "atur" after "Enter Debug Mode" message.
3. Wait for "Starting XMODEM upload" message before activating
Xmodem upload on your terminal.
4. After successful firmware upload, enter "atgo" to restart
the router.

Warning: Proceeding with the upload will erase the current
system       firmware.

        Do You Wish To Proceed:(Y/N)
```

2. After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

40.4.9 Example Xmodem Firmware Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

Figure 255 Example Xmodem Upload



After the firmware upload process has completed, the Prestige will automatically restart.

40.4.10 Uploading Configuration File Via Console Port

1. Select 2 from Menu 24.7 – System Maintenance – Upload Firmware to display Menu 24.7.2 - System Maintenance - Upload System Configuration File. Follow the instructions as shown in the next screen.

Figure 256 Menu 24.7.2 As Seen Using the Console Port

```
            Menu 24.7.2 - System Maintenance - Upload System Configuration
            File

            To upload system configuration file:
            1. Enter "y" at the prompt below to go into debug mode.
            2. Enter "atlc" after "Enter Debug Mode" message.
            3. Wait for "Starting XMODEM upload" message before activating
               Xmodem upload on your terminal.
            4. After successful firmware upload, enter "atgo" to restart
               the system.

            Warning:
            1. Proceeding with the upload will erase the current
            configuration file.
            2. The system's console port speed (Menu 24.2.2) may change
            when it is restarted; please adjust your terminal's speed
            accordingly. The password may change (menu 23), also.
            3. When uploading the DEFAULT configuration file, the console
            port speed will be reset to 9600 bps and the password to
            "1234".

                      Do You Wish To Proceed:(Y/N)
```

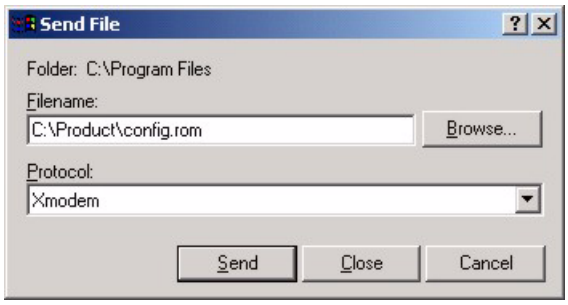
2. After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

3 Enter "atgo" to restart the Prestige.

40.4.11 Example Xmodem Configuration Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

Figure 257 Example Xmodem Upload



After the configuration upload process has completed, restart the Prestige by entering "atgo".

CHAPTER 41
System Maintenance

This chapter leads you through SMT menus 24.8 to 24.10.

41.1 Command Interpreter Mode

The Command Interpreter (CI) is a part of the main system firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. Enter the CI from the SMT by selecting menu 24.8. See the included disk or the zyxel.com web site for more detailed information on CI commands. Enter 8 from **Menu 24 — System Maintenance**. A list of valid commands can be found by typing `help` or `?` at the command prompt. Type "`exit`" to return to the SMT main menu when finished.

Figure 258 Command Mode in Menu 24

```
                Menu 24 - System Maintenance

                   1.  System Status
                   2.  System Information and Console Port Speed
                   3.  Log and Trace
                   4.  Diagnostic
                   5.  Backup Configuration
                   6.  Restore Configuration
                   7.  Upload Firmware
                   8.  Command Interpreter Mode
                   9.  Call Control
                   10. Time and Date Setting
                   11. Remote Management

             Enter Menu Selection Number:
```

Figure 259 Valid Commands

```
Copyright (c) 1994 - 2003 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys             exit            ether           wan
wlan            ip              ipsec           bridge
lan             radius          8021x
ras>
```

41.2 Call Control Support

Call Control Support is only applicable when **Encapsulation** is set to **PPPoE** in menu 4 or menu 11.1.

The budget management function allows you to set a limit on the total outgoing call time of the Prestige within certain times. When the total outgoing call time exceeds the limit, the current call will be dropped and any future outgoing calls will be blocked.

To access the call control menu, select option 9 in menu 24 to go to **Menu 24.9 — System Maintenance — Call Control**, as shown in the next table.

Figure 260 Menu 24.9 System Maintenance: Call Control

```
Menu 24.9 - System Maintenance - Call Control

1. Budget Management

Enter Menu Selection Number:
```

41.2.1 Budget Management

Menu 24.9.1 shows the budget management statistics for outgoing calls. Enter 1 from **Menu 24.9 — System Maintenance — Call Control** to bring up the following menu.

Figure 261 Menu 24.9.1 System Maintenance: Budget Management

```
            Menu 24.9.1 - System Maintenance - Budget Management


Remote Node        Connection Time/Total Budget  Elapsed Time/Total Period
1.MyIsp            No Budget                     No Budget
2.--------         ---                           ---
3.--------         ---                           ---
4.--------         ---                           ---
5.--------         ---                           ---
6.--------         ---                           ---
7.--------         ---                           ---
8.--------         ---                           ---



            Reset Node (0 to update screen):
```

The total budget is the time limit on the accumulated time for outgoing calls to a remote node. When this limit is reached, the call will be dropped and further outgoing calls to that remote node will be blocked. After each period, the total budget is reset. The default for the total budget is 0 minutes and the period is 0 hours, meaning no budget control. You can reset the accumulated connection time in this menu by entering the index of a remote node. Enter 0 to update the screen. The budget and the reset period can be configured in menu 11.1 for the remote node when PPPoE encapsulation is selected.

Table 143 Menu 24.9.1 System Maintenance : Budget Management

FIELD	DESCRIPTION
Remote Node	Enter the index number of the remote node you want to reset (just one in this case)
Connection Time/Total Budget	This is the total connection time that has gone by (within the allocated budget that you set in menu 11.1.
Elapsed Time/Total Period	The period is the time cycle in hours that the allocation budget is reset (see menu 11.1.) The elapsed time is the time used up within this period.
Enter "0" to update the screen or press [ESC] to return to the previous screen.	

41.3 Time and Date Setting

The Prestige keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server when you turn on your Prestige. Menu 24.10 allows you to update the time and date settings of your Prestige. The real time is then displayed in the Prestige error logs and firewall logs.

Select menu 24 in the main menu to open **Menu 24 System Maintenance**, as shown next.

Figure 262 Menu 24 System Maintenance

```
            Menu 24 - System Maintenance

                        1.  System Status
                        2.  System Information and Console Port Speed
                        3.  Log and Trace
                        4.  Diagnostic
                        5.  Backup Configuration
                        6.  Restore Configuration
                        7.  Upload Firmware
                        8.  Command Interpreter Mode
                        9.  Call Control
                        10. Time and Date Setting
                        11. Remote Management

            Enter Menu Selection Number:
```

Then enter 10 to go to **Menu 24.10 System Maintenance Time and Date Setting** to update the time and date settings of your Prestige as shown in the following screen.

Figure 263 Menu 24.10 System Maintenance: Time and Date Setting

```
            Menu 24.10 - System Maintenance - Time and Date Setting
     Use Time Server when Bootup= None
     Time Server Address= N/A
     Current Time:                          00 : 51 : 24
     New Time (hh:mm:ss):                   00 : 51 : 19
     Current Date:                          2000 - 01 - 01
     New Date (yyyy-mm-dd):                 2000 - 01 - 01
     Time Zone= GMT
     Daylight Saving= No
     Start Date (mm-dd):                          01 - 00
     End Date (mm-dd):                            01 - 00

            Press ENTER to Confirm or ESC to Cancel:
```

Table 144 Menu 24.10 System Maintenance: Time and Date Setting

FIELD	DESCRIPTION
Use Time Server when Bootup	Enter the time service protocol that your time server sends when you turn on the Prestige. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main differences between them are the format. **Daytime (RFC 867)** format is day/month/year/time zone of the server. **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**. The default, enter the time manually.
Time Server Address	Enter the IP address or domain name of your time server. Check with your ISP/ network administrator if you are unsure of this information.

Table 144 Menu 24.10 System Maintenance: Time and Date Setting (continued)

FIELD	DESCRIPTION
Current Time	This field displays an updated time only when you reenter this menu.
New Time	Enter the new time in hour, minute and second format.
Current Date	This field displays an updated date only when you re-enter this menu.
New Date	Enter the new date in year, month and day format.
Time Zone	Press [SPACE BAR] and then [ENTER] to set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Saving	If you use daylight savings time, then choose **Yes**.
Start Date	If using daylight savings time, enter the month and day that it starts on.
End Date	If using daylight savings time, enter the month and day that it ends on
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

41.3.1 Resetting the Time

- The Prestige resets the time in three instances:
- On leaving menu 24.10 after making changes.
- When the Prestige starts up, if there is a timeserver configured in menu 24.10.
- 24-hour intervals after starting.

CHAPTER 42
Remote Management

This chapter covers remote management (SMT menu 24.11).

42.1 Remote Management Overview

Remote management allows you to determine which services/protocols can access which Prestige interface (if any) from which computers.

When you configure remote management to allow management from the WAN, you still need to configure a firewall rule to allow access. See the firewall chapters for details on configuring firewall rules.

42.2 Remote Management

To disable remote management of a service, select **Disable** in the corresponding **Server Access** field.

Enter 11 from menu 24 to display **Menu 24.11 — Remote Management Control**.

42.2.1 Remote Management Setup

You may manage your Prestige from a remote location via:

the Internet (**WAN only**), the **LAN only**, **All** (LAN and WAN) or **Disable** (neither).

- WAN only (Internet)
- ALL (LAN and WAN)
- LAN only
- Disable (Neither)

If you enable remote management of a service, but have applied a filter to block the service, then you will not be able to remotely manage the Prestige using the service.

Enter 11, from menu 24, to display **Menu 24.11 — Remote Management Control** (shown next).

Figure 264 Menu 24.11 Remote Management Control

```
            Menu 24.11 - Remote Management Control

TELNET Server:
  Server Port = 23                  Server Access = LAN only
  Secured Client IP = 0.0.0.0
FTP Server:
  Server Port = 21                  Server Access = LAN only
  Secured Client IP = 0.0.0.0
Web Server:
  Server Port = 80                  Server Access = LAN only
  Secured Client IP = 0.0.0.0

            Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 145 Menu 24.11 Remote Management Control

FIELD	DESCRIPTION
Telnet Server FTP Server Web Server	Each of these read-only labels denotes a service or protocol.
Port	This field shows the port number for the service or protocol. You may change the port number if needed, but you must use the same port number to access the Prestige.
Access	Select the access interface (if any) by pressing the [SPACE BAR]. Choices are: **LAN only**, **WAN only**, **All** or **Disable**. The default is **LAN only**.
Secured Client IP	The default 0.0.0.0 allows any client to use this service or protocol to access the Prestige. Enter an IP address to restrict access to a client with a matching IP address.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

42.2.2 Remote Management Limitations

Remote management over LAN or WAN will not work when:

- A filter in menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
- You have disabled that service in menu 24.11.
- The IP address in the **Secured Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the Prestige will disconnect the session immediately.
- There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.
- There is a firewall rule that blocks it.

42.3 Remote Management and NAT

When NAT is enabled:

- Use the Prestige's WAN IP address when configuring from the WAN.
- Use the Prestige's LAN IP address when configuring from the LAN.

42.4 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The Prestige automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when it is continuously updating the status in menu 24.1 or when `sys stdio` has been changed on the command line.

CHAPTER 43
IP Policy Routing

This chapter covers setting and applying policies used for IP routing.

43.1 IP Policy Routing Overview

Traditionally, routing is based on the destination address only and the IAD takes the shortest path to forward a packet. IP Routing Policy (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing.

43.2 Benefits of IP Policy Routing

Source-Based Routing – Network administrators can use policy-based routing to direct traffic from different users through different connections.

Quality of Service (QoS) – Organizations can differentiate traffic by setting the precedence or TOS (Type of Service) values in the IP header at the periphery of the network to enable the backbone to prioritize traffic.

Cost Savings – IPPR allows organizations to distribute interactive traffic on high-bandwidth, high-cost paths while using low-cost paths for batch traffic.

Load Sharing – Network administrators can use IPPR to distribute traffic among multiple paths.

43.3 Routing Policy

Individual routing policies are used as part of the overall IPPR process. A policy defines the matching criteria and the action to take when a packet meets the criteria. The action is taken only when all the criteria are met. The criteria includes the source address and port, IP protocol (ICMP, UDP, TCP, etc.), destination address and port, TOS and precedence (fields in the IP header) and length. The inclusion of length criterion is to differentiate between interactive and bulk traffic. Interactive applications, for example, telnet, tend to have short packets, while bulk traffic, for example, file transfer, tends to have large packets.

The actions that can be taken include:

- routing the packet to a different gateway (and hence the outgoing interface).
- setting the TOS and precedence fields in the IP header.

IPPR follows the existing packet filtering facility of RAS in style and in implementation. The policies are divided into sets, where related policies are grouped together. A user defines the policies before applying them to an interface or a remote node, in the same fashion as the filters. There are 12 policy sets with six policies in each set.

43.4 IP Routing Policy Setup

Menu 25 shows all the policies defined.

Figure 265 Menu 25 IP Routing Policy Setup

```
                Menu 25 - IP Routing Policy Setup

Policy                                Policy
Set #         Name                    Set #         Name
------  -----------------             ------  -----------------
  1      ________________               7      ________________
  2      ________________               8      ________________
  3      ________________               9      ________________
  4      ________________              10      ________________
  5      ________________              11      ________________
  6      ________________              12      ________________

            Enter Policy Set Number to Configure= 0

            Edit Name= N/A

            Press ENTER to Confirm or ESC to Cancel:
```

To setup a routing policy, perform the following procedures:

1. Type 25 in the main menu to open **Menu 25 – IP Routing Policy Setup**.
2. Type the index of the policy set you want to configure to open **Menu 25.1 – IP Routing Policy Setup**.

Menu 25.1 shows the summary of a policy set, including the criteria and the action of a single policy, and whether a policy is active or not. Each policy contains two lines. The former part is the criteria of the incoming packet and the latter is the action. Between these two parts, separator "|" means the action is taken on criteria matched and separator "=" means the action is taken on criteria not matched.

Figure 266 Menu 25.1 IP Routing Policy Setup

```
            Menu 25.1 - IP Routing Policy Setup

# A                          Criteria/Action
- - ------------------------------------------------------------------------
1 Y SA=1.1.1.1-1.1.1.1,DA=2.2.2.2-2.2.2.5
    SP=20-25,DP=20-25,P=6,T=NM,PR=0              |GW=192.168.1.1,T=MT,PR=0
2 N ____________________________________________________________________________
    ____________________________________________________________________________
3 N ____________________________________________________________________________
    ____________________________________________________________________________
4 N ____________________________________________________________________________
    ____________________________________________________________________________
5 N ____________________________________________________________________________
    ____________________________________________________________________________
6 N ____________________________________________________________________________
    ____________________________________________________________________________

            Enter Policy Rule Number (1-6) to Configure:
```

Table 146 Menu 25.1 IP Routing Policy Setup

ABBREVIATION		MEANING
Criterion	SA	Source IP Address
	SP	Source Port
	DA	Destination IP Address
	DP	Destination Port
	P	IP layer 4 protocol number (TCP=6, UDP=17…)
	T	Type of service of incoming packet
	PR	Precedence of incoming packet
Action	GW	Gateway IP address
	T	Outgoing Type of service
	P	Outgoing Precedence
Service	NM	Normal
	MD	Minimum Delay
	MT	Maximum Throughput
	MR	Maximum Reliability
	MC	Minimum Cost

Type a number from 1 to 6 to display **Menu 25.1.1 – IP Routing Policy** (see the next figure). This menu allows you to configure a policy rule.

Figure 267 Menu 25.1.1 IP Routing Policy

```
            Menu 25.1.1 - IP Routing Policy

  Policy Set Name= test
  Active= No
  Criteria:
    IP Protocol    = 0
    Type of Service= Don't Care           Packet length= 0
    Precedence     = Don't Care             Len Comp= N/A
    Source:
      addr start= 0.0.0.0                 end= N/A
      port start= N/A                     end= N/A
    Destination:
      addr start= 0.0.0.0                 end= N/A
      port start= N/A                     end= N/A
  Action= Matched
    Gateway addr   = 0.0.0.0              Log= No
    Type of Service= No Change
    Precedence     = No Change

            Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 147 Menu 25.1.1 IP Routing Policy

FIELD	DESCRIPTION
Policy Set Name	This is the policy set name assigned in **Menu 25 – IP Routing Policy Setup**.
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** to activate or No to deactivate the policy. Inactive policies are displayed with a minus sign "-" in SMT menu 25.
Criteria	
IP Protocol	IP layer 4 protocol, for example, **UDP**, **TCP**, **ICMP**, etc.
Type of Service	Prioritize incoming network traffic by choosing from **Don't Care**, **Normal**, **Min Delay**, **Max Thruput, Min Cost** or **Max Reliable**.
Precedence	Precedence value of the incoming packet. Press [SPACE BAR] and then [ENTER] to select a value from **0** to **7** or **Don't Care**.
Packet Length	Type the length of incoming packets (in bytes). The operators in the **Len Comp** (next field) apply to packets of this length.
Len Comp	Press [SPACE BAR] and then [ENTER] to choose from **Equal**, **Not Equal**, **Less**, **Greater**, **Less or Equal** or **Greater or Equal**.
Source:	
addr start / end	Source IP address range from start to end.
port start / end	Source port number range from start to end; applicable only for TCP/UDP.
Destination:	
addr start / end	Destination IP address range from start to end.
port start / end	Destination port number range from start to end; applicable only for TCP/UDP.
Action	Specifies whether action should be taken on criteria **Matched** or **Not Matched**.

Table 147 Menu 25.1.1 IP Routing Policy (continued)

FIELD	DESCRIPTION
Gateway addr	Defines the outgoing gateway address. The gateway must be on the same subnet as the Prestige if it is on the LAN, otherwise, the gateway must be the IP address of a remote node. The default gateway is specified as 0.0.0.0.
Type of Service	Set the new TOS value of the outgoing packet. Prioritize incoming network traffic by choosing **No Change**, **Normal**, **Min Delay**, **Max Thruput**, **Max Reliable** or **Min Cost**.
Precedence	Set the new outgoing packet precedence value. Values are **0** to **7** or **No Change**.
Log	Press [SPACE BAR] and then [ENTER] to select **Yes** to make an entry in the system log when a policy is executed.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

43.5 Applying an IP Policy

This section shows you where to apply the IP policies after you design them.

43.5.1 Ethernet IP Policies

From **Menu 3 — Ethernet Setup**, type 2 to go to **Menu 3.2 — TCP/IP and DHCP Ethernet Setup**.

You can choose up to four IP policy sets (from 12) by typing their numbers separated by commas, for example, 2, 4, 7, 9.

Figure 268 Menu 3.2 TCP/IP and DHCP Ethernet Setup

```
            Menu 3.2 - TCP/IP and DHCP Setup
                    DHCP Setup
                      DHCP= Server
                      Client IP Pool Starting Address= 192.168.1.33
                      Size of Client IP Pool= 32
                      Primary DNS Server= 0.0.0.0
                      Secondary DNS Server= 0.0.0.0
                      Remote DHCP Server= N/A
                    TCP/IP Setup:
                      IP Address= 192.168.1.1
                      IP Subnet Mask= 255.255.255.0
                      RIP Direction= Both
                        Version= RIP-1
                      Multicast= None
                      IP Policies=
                      Edit IP Alias= No
            Press ENTER to Confirm or ESC to Cancel:
```

Go to menu 11.3 (shown next) and type the number(s) of the IP Routing Policy set(s) as appropriate. You can cascade up to four policy sets by typing their numbers separated by commas.

Figure 269 Menu 11.3 Remote Node Network Layer Options

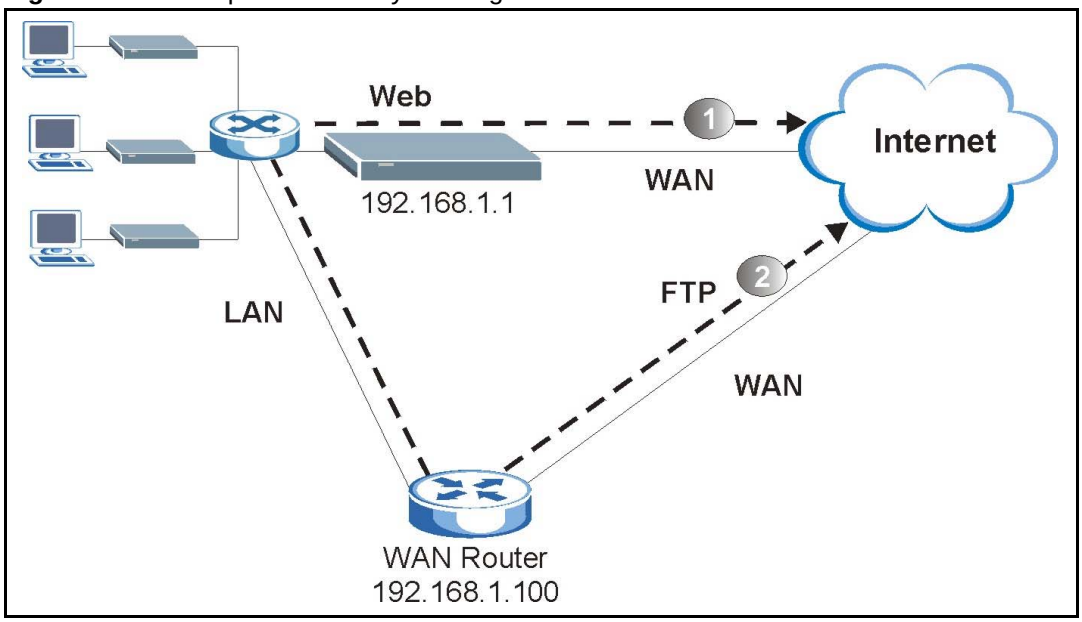
```
            Menu 11.3 - Remote Node Network Layer Options

IP Options:                         Bridge Options:
  IP Address Assignment= Static       Ethernet Addr Timeout (min)= 0
  Rem IP Addr: 0.0.0.0
  Rem Subnet Mask= 0.0.0.0
  My WAN Addr= 0.0.0.0
  NAT= Full Feature
    Address Mapping Set= 2
  Metric= 2
  Private= No
  RIP Direction= Both
    Version= RIP-2B
  Multicast= IGMP-v2
  IP Policies=


            Press ENTER to Confirm or ESC to Cancel:
```

43.6 IP Policy Routing Example

If a network has both Internet and remote node connections, you can route Web packets to the Internet using one policy and route FTP packets to a remote network using another policy. See the next figure.

Route 1 represents the default IP route and route 2 represents the configured IP route.

Figure 270 Example of IP Policy Routing



To force packets coming from clients with IP addresses of 192.168.1.33 to 192.168.1.64 to be routed to the Internet via the WAN port of the Prestige, follow the steps as shown next.

1. Create a routing policy set in menu 25.
2. Create a rule for this set in **Menu 25.1.1 — IP Routing Policy** as shown next.

Figure 271 IP Routing Policy Example

```
                Menu 25.1.1 - IP Routing Policy

        Policy Set Name= set1            Packet length= 10
        Active= Yes                        Len Comp= N/A
        Criteria:
          IP Protocol    = 6             end= 192.168.1.64
          Type of Service= Don't Care    end= N/A
          Precedence     = Don't Care    end= N/A
          Source:                        end= 80
            addr start= 192.168.1.2      Log= No
         port start= 0
          Destination:
         addr start= 0.0.0.0
         port start= 80
        Action= Matched
      Gateway addr  = 192.168.1.1
          Type of Service= No Change
          Precedence     = No Change


           Press ENTER to Confirm or ESC to Cancel:
```

1. Check **Menu 25.1 — IP Routing Policy Setup** to see if the rule is added correctly.
2. Create another policy set in menu 25.

3 Create a rule in menu 25.1 for this set to route packets from any host (`IP=0.0.0.0` means any host) with protocol TCP and port FTP access through another gateway (192.168.1.100).

Figure 272 IP Routing Policy Example

```
            Menu 25.1.1 - IP Routing Policy

          Policy Set Name= set2          Packet length= 10
          Active= Yes                      Len Comp= N/A
          Criteria:
            IP Protocol    = 6           end= N/A
            Type of Service= Don't Care  end= N/A
            Precedence     = Don't Care  end= N/A
            Source:                      end= 21
              addr start= 0.0.0.0        Log= No
           port start= 0
            Destination:
          addr start= 0.0.0.0
          port start= 20
          Action= Matched
       Gateway addr =192.168.1.100
            Type of Service= No Change
            Precedence     = No Change



            Press ENTER to Confirm or ESC to Cancel:
```

4 Check **Menu 25.1 — IP Routing Policy Setup** to see if the rule is added correctly.

5 Apply both policy sets in menu 3.2 as shown next.

Figure 273 Applying IP Policies Example

```
            Menu 3.2 - TCP/IP and DHCP Ethernet Setup

                 DHCP Setup
                   DHCP= Server
                   Client IP Pool Starting Address= 192.168.1.33
                   Size of Client IP Pool= 64
                   Primary DNS Server= 0.0.0.0
                   Secondary DNS Server= 0.0.0.0
                   Remote DHCP Server= N/A
                 TCP/IP Setup:
                   IP Address= 192.168.1.1
                   IP Subnet Mask= 255.255.255.0
                   RIP Direction= Both
                     Version= RIP-1
                   Multicast= None
                   IP Policies= 1,2
                   Edit IP Alias= No


            Press ENTER to Confirm or ESC to Cancel:
```

CHAPTER 44
Call Scheduling

Call scheduling (applicable for PPPoA or PPPoE encapsulation only) allows you to dictate when a remote node should be called and for how long.

44.1 Introduction

The call scheduling feature allows the Prestige to manage a remote node and dictate when a remote node should be called and for how long. This feature is similar to the scheduler in a videocassette recorder (you can specify a time period for the VCR to record). You can apply up to 4 schedule sets in **Menu 11.1 — Remote Node Profile**. From the main menu, enter 26 to access **Menu 26 — Schedule Setup** as shown next.

Figure 274 Menu 26 Schedule Setup

```
            Menu 26 - Schedule Setup

Schedule                              Schedule
Set #           Name                  Set #           Name
------  ------------------            ------  ------------------
  1      ________________               7      ________________
  2      ________________               8      ________________
  3      ________________               9      ________________
  4      ________________              10      ________________
  5      ________________              11      ________________
  6      ________________              12      ________________

           Enter Schedule Set Number to Configure= 0

           Edit Name= N/A

           Press ENTER to Confirm or ESC to Cancel:
```

Lower numbered sets take precedence over higher numbered sets thereby avoiding scheduling conflicts. For example, if sets 1, 2 ,3 and 4 in are applied in the remote node then set 1 will take precedence over set 2, 3 and 4 as the Prestige, by default, applies the lowest numbered set first. Set 2 will take precedence over set 3 and 4, and so on.

You can design up to 12 schedule sets but you can only apply up to four schedule sets for a remote node.

To delete a schedule set, enter the set number and press **[SPACE BAR]** and then **[ENTER]** (or delete) in the **Edit Name** field.

To setup a schedule set, select the schedule set you want to setup from menu 26 (1-12) and press [ENTER] to see **Menu 26.1 — Schedule Set Setup** as shown next.

Figure 275 Menu 26.1 Schedule Set Setup

```
              Menu 26.1 Schedule Set Setup

                 Active= Yes
                 Start Date(yyyy-mm-dd)= 2000 - 01 - 01
                 How Often= Once
                 Once:
                   Date(yyyy-mm-dd)= 2000 - 01 - 01
                 Weekdays:
                   Sunday= N/A
                   Monday= N/A
                   Tuesday= N/A
                   Wednesday= N/A
                   Thursday= N/A
                   Friday= N/A
                   Saturday= N/A
                 Start Time(hh:mm)= 00 : 00
                 Duration(hh:mm)= 00 : 00
                 Action= Forced On

              Press ENTER to Confirm or ESC to Cancel:
```

If a connection has been already established, your Prestige will not drop it. Once the connection is dropped manually or it times out, then that remote node can't be triggered up until the end of the **Duration**.

Table 148 Menu 26.1 Schedule Set Setup

FIELD	DESCRIPTION
Active	Press [SPACE BAR] to select **Yes** or **No**. Choose **Yes** and press [ENTER] to activate the schedule set.
Start Date	Enter the start date when you wish the set to take effect in year -month-date format. Valid dates are from the present to 2036-February-5.
How Often	Should this schedule set recur weekly or be used just once only? Press the [SPACE BAR] and then [ENTER] to select **Once** or **Weekly**. Both these options are mutually exclusive. If **Once** is selected, then all weekday settings are **N/A**. When **Once** is selected, the schedule rule deletes automatically after the scheduled time elapses.
Once: Date	If you selected **Once** in the **How Often** field above, then enter the date the set should activate here in year-month-date format.
Weekday: Day	If you selected **Weekly** in the **How Often** field above, then select the day(s) when the set should activate (and recur) by going to that day(s) and pressing [SPACE BAR] to select **Yes**, then press [ENTER].
Start Time	Enter the start time when you wish the schedule set to take effect in hour-minute format.
Duration	Enter the maximum length of time this connection is allowed in hour-minute format.

Table 148 Menu 26.1 Schedule Set Setup (continued)

FIELD	DESCRIPTION
Action	**Forced On** means that the connection is maintained whether or not there is a demand call on the line and will persist for the time period specified in the **Duration** field. **Forced Down** means that the connection is blocked whether or not there is a demand call on the line. **Enable Dial-On-Demand** means that this schedule permits a demand call on the line. **Disable Dial-On-Demand** means that this schedule prevents a demand call on the line.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

Once your schedule sets are configured, you must then apply them to the desired remote node(s). Enter 11 from the **Main Menu** and then enter the target remote node index. Using [SPACE BAR], select **PPPoE** or **PPPoA** in the **Encapsulation** field and then press [ENTER] to make the schedule sets field available as shown next.

Figure 276 Applying Schedule Set(s) to a Remote Node (PPPoE)

```
            Menu 11.1 - Remote Node Profile
Rem Node Name= MyISP                  Route= IP
Active= Yes                           Bridge= No
Encapsulation= PPPoA                  Edit IP/Bridge= No
Multiplexing= LLC-based               Edit ATM Options= No
Service Name= N/A                     Edit Advance Options= N/A
Incoming:                             Telco Option:
  Rem Login=                            Allocated Budget(min)= 0
  Rem Password= ********                Period(hr)= 0
Outgoing:                               Schedule Sets=
  My Login= ChangeMe                    Nailed-Up Connection= No
  My Password= ********               Session Options:
  Authen= CHAP/PAP                      Edit Filter Sets= No
                                        Idle Timeout(sec)= 0
            Press ENTER to Confirm or ESC to Cancel:
```

You can apply up to four schedule sets, separated by commas, for one remote node. Change the schedule set numbers to your preference(s).

CHAPTER 45
VPN/IPSec Setup

This chapter introduces the VPN SMT menus.

45.1 VPN/IPSec Overview

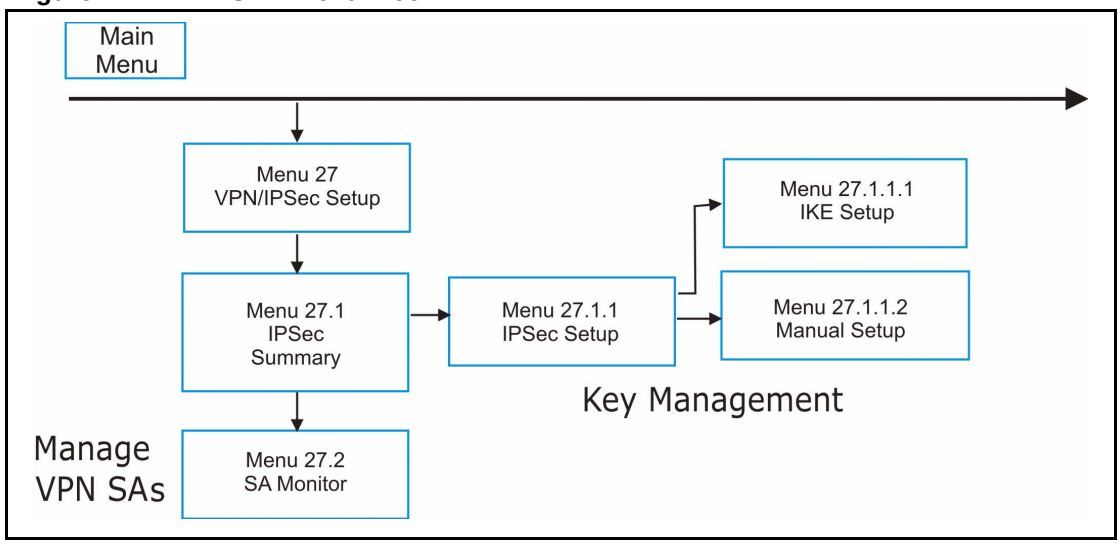
The VPN/IPSec main SMT menu has these main submenus:

Define VPN policies in menu 27.1 submenus, including security policies, endpoint IP addresses, peer IPSec router IP address and key management.

Menu 27.2 - SA Monitor allows you to manage (refresh or disconnect) your SA connections.

This is an overview of the VPN menu tree.

Figure 277 VPN SMT Menu Tree



From the main menu, enter 27 to display the first VPN menu (shown next).

Figure 278 Menu 27 VPN/IPSec Setup

```
              Menu 27 - VPN/IPSec Setup

                     1. IPSec Summary
                     2. SA Monitor


              Enter Menu Selection Number:
```

45.2 IPSec Summary Screen

Type 1 in menu 27 and then press [ENTER] to display **Menu 27.1 IPSec Summary**. This is a summary read-only menu of your IPSec rules (tunnels). Edit or create an IPSec rule by selecting an index number and then configuring the associated submenus.

Figure 279 Menu 27.1 IPSec Summary

```
              Menu 27.1 – IPSec Summary

#     Name     A   Local Addr Start    - Addr End / Mask  Encap    IPSec Algorithm
      Key Mgt      Remote Addr Start   - Addr End / Mask           Secure GW Addr
-     ------   -   -----------------   ---------------    ------   ------------------
001   Taiwan   Y   192.168.1.35        192.168.1.38       Tunnel   ESP AES MD5
      IKE          172.16.2.40         172.16.2.46                 193.81.13.2
002   zw50     N   1.1.1.1             1.1.1.1            Tunnel   AH SHA1
      IKE          4.4.4.4             255.255.0.0                 zw50test.zyxel.
003   China    N   192.168.1.40        192.168.1.42       Tunnel   ESP DES MD5
      IKE          N/A                 N/A                         0.0.0.0
004

005


      Select Command= None             Select Rule= N/A
              Press ENTER to Confirm or ESC to Cancel:
```

Table 149 Menu 27.1 IPSec Summary

FIELD	DESCRIPTION
#	This is the VPN policy index number.
Name	This field displays the unique identification name for this VPN rule. The name may be up to 32 characters long but only 10 characters will be displayed here.

Table 149 Menu 27.1 IPSec Summary (continued)

FIELD	DESCRIPTION
A	**Y** signifies that this VPN rule is active.
Local Addr Start	When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Single**, this is a static IP address on the LAN behind your Prestige. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Range**, this is the beginning (static) IP address, in a range of computers on the LAN behind your Prestige. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **SUBNET**, this is a static IP address on the LAN behind your Prestige.
Addr End / Mask	When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Single**, this is the same (static) IP address as in the **Local Addr Start** field. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Range**, this is the end (static) IP address, in a range of computers on the LAN behind your Prestige. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **SUBNET**, this is a subnet mask on the LAN behind your Prestige.
Encap	This field displays **Tunnel** mode or **Transport** mode. See earlier for a discussion of these. You need to finish configuring the VPN policy in menu 27.1.1.1 or 27.1.1.2 if **???** is displayed.
IPSec Algorithm	This field displays the security protocols used for an SA. **ESP** provides confidentiality and integrity of data by encrypting the data and encapsulating it into IP packets. Encryption methods include 56-bit **DES** and 168-bit **3DES**. **NULL** denotes a tunnel without encryption.168-bit **3DES** and 128-bit **AES**. **NULL** denotes a tunnel without encryption. **AH** (Authentication Header) provides strong integrity and authentication by adding authentication information to IP packets. This authentication information is calculated using header and payload data in the IP packet. This provides an additional level of security. **AH** choices are **MD5** (default - 128 bits) and **SHA -1**(160 bits)**.** Both **AH** and **ESP** increase the Prestige's processing requirements and communications latency (delay). You need to finish configuring the VPN policy in menu 27.1.1.1 or 27.1.1.2 if **???** is displayed.
Key Mgt	This field displays the SA's type of key management, (**IKE** or **Manual**).
Remote Addr Start	When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Single**, this is a static IP address on the network behind the remote IPSec router. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Range**, this is the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **SUBNET**, this is a static IP address on the network behind the remote IPSec router. This field displays **N/A** when you configure the **Secure Gateway Address** field in SMT 27.1.1 to 0.0.0.0.
Addr End / Mask	When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Single**, this is the same (static) IP address as in the **Remote Addr Start** field. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **Range**, this is the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Addr Type** field in **Menu 27.1.1 IPSec Setup** is configured to **SUBNET**, this is a subnet mask on the network behind the remote IPSec router. This field displays **N/A** when you configure the **Secure Gateway Address** field in SMT 27.1.1 to 0.0.0.0.

Table 149 Menu 27.1 IPSec Summary (continued)

FIELD	DESCRIPTION
Secure GW Addr	This is the WAN IP address or the domain name (up to the first 15 characters are displayed) of the IPSec router with which you are making the VPN connection. This field displays **0.0.0.0** when you configure the **Secure Gateway Address** field in SMT 27.1.1 to 0.0.0.0.
Select Command	Press [SPACE BAR] to choose from **None**, **Edit**, **Delete**, **Go To Rule**, **Next Page** or **Previous Page** and then press [ENTER]. You must select a rule in the next field when you choose the **Edit**, Delete or **Go To** commands. Select **None** and then press [ENTER] to go to the "Press ENTER to Confirm…" prompt. Use **Edit** to create or edit a rule. Use **Delete** to remove a rule. To edit or delete a rule, first make sure you are on the correct page. When a VPN rule is deleted, subsequent rules do not move up in the page list. Use **Go To Rule** to view the page where your desired rule is listed. Select **Next Page** or **Previous Page** to view the next or previous page of rules (respectively).
Select Rule	Type the VPN rule index number you wish to edit or delete and then press [ENTER].
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

45.3 IPSec Setup

Select **Edit** in the **Select Command** field; type the index number of a rule in the **Select Rule** field and press [ENTER] to edit the VPN using the menu shown next.

Note: You must also configure menu 27.1.1.1 or menu 27.1.1.2 to fully configure and use a VPN.

Figure 280 Menu 27.1.1 IPSec Setup

```
             Menu 27.1.1 – IPSec Setup

             Index= 1         Name= Taiwan
Active= Yes       Keep Alive= No    Nat Traversal= No
Local ID type= IP             Content:
My IP Addr= 0.0.0.0
Peer ID type= IP              Content:
Secure Gateway Address= zw50test.zyxel.com.tw
Protocol= 0       DNS Server= 0.0.0.0
Local:             Addr Type= SINGLE
               IP Addr Start= 1.1.1.1        End/Subnet Mask= N/A
                  Port Start= 0              End= N/A
Remote:            Addr Type= SUBNET
               IP Addr Start= 4.4.4.4        End/Subnet Mask= 255.255.0.0
                  Port Start= 0              End= N/A
Enable Replay Detection = No
Key Management= IKE
Edit Key Management Setup= No

              Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 150 Menu 27.1.1 IPSec Setup

FIELD	DESCRIPTION
Index	This is the VPN rule index number you selected in the previous menu.
Name	Enter a unique identification name for this VPN rule. The name may be up to 32 characters long but only 10 characters will be displayed in **Menu 27.1 - IPSec Summary**.
Active	Press [SPACE BAR] to choose either **Yes** or **No**. Choose **Yes** and press [ENTER] to activate the VPN tunnel. This field determines whether a VPN rule is applied before a packet leaves the firewall.
Keep Alive	Press [SPACE BAR] to choose either **Yes** or **No**. Choose **Yes** and press [ENTER] to have the Prestige automatically re-initiate the SA after the SA lifetime times out, even if there is no traffic. The remote IPSec router must also have keep alive enabled in order for this feature to work.

Table 150 Menu 27.1.1 IPSec Setup (continued)

FIELD	DESCRIPTION
Nat Traversal	Press [SPACE BAR] to choose either **Yes** or **No**. Choose **Yes** and press [ENTER] to enable NAT traversal. NAT traversal allows you to set up a VPN connection when there are NAT routers between the two IPSec routers. The remote IPSec router must also have NAT traversal enabled. You can use NAT traversal with **ESP** protocol using **Transport** or **Tunnel** mode, but not with **AH** protocol nor with **Manual** key management. In order for an IPSec router behind a NAT router to receive an initiating IPSec packet, set the NAT router to forward UDP port 500 to the IPSec router behind the NAT router.
Local ID type	Press [SPACE BAR] to choose **IP**, **DNS**, or **E-mail** and press [ENTER]. Select **IP** to identify this Prestige by its IP address. Select **DNS** to identify this Prestige by a domain name. Select **E-mail** to identify this Prestige by an e-mail address.
Content	When you select **IP** in the **Local ID Type** field, type the IP address of your computer or leave the field blank to have the Prestige automatically use its own IP address. When you select **DNS** in the **Local ID Type** field, type a domain name (up to 31 characters) by which to identify this Prestige. When you select **E-mail** in the **Local ID Type** field, type an e-mail address (up to 31 characters) by which to identify this Prestige. The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address.
My IP Addr	Enter the IP address of your Prestige. The Prestige uses its current WAN IP address (static or dynamic) in setting up the VPN tunnel if you leave this field as 0.0.0.0. The VPN tunnel has to be rebuilt if this IP address changes.
Peer ID type	Press [SPACE BAR] to choose **IP**, **DNS**, or **E-mail** and press [ENTER]. Select **IP** to identify the remote IPSec router by its IP address. Select **DNS** to identify the remote IPSec router by a domain name. Select **E-mail** to identify the remote IPSec router by an e-mail address.
Content	When you select **IP** in the **Peer ID Type** field, type the IP address of the computer with which you will make the VPN connection or leave the field blank to have the Prestige automatically use the address in the **Secure Gateway Address** field. When you select **DNS** in the **Peer ID Type** field, type a domain name (up to 31 characters) by which to identify the remote IPSec router. When you select **E-mail** in the **Peer ID Type** field, type an e-mail address (up to 31 characters) by which to identify the remote IPSec router. The domain name or e-mail address that you use in the **Content** field is used for identification purposes only and does not need to be a real domain name or e-mail address. The domain name also does not have to match the remote router's IP address or what you configure in the **Secure Gateway Address** field below.
Secure Gateway Address	Type the IP address or the domain name (up to 31 characters) of the IPSec router with which you're making the VPN connection. Set this field to 0.0.0.0 if the remote IPSec router has a dynamic WAN IP address (the **Key Management** field must be set to **IKE**, see later).
Protocol	Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol.

Table 150 Menu 27.1.1 IPSec Setup (continued)

FIELD	DESCRIPTION
DNS Server	If there is a private DNS server that services the VPN, type its IP address here. The Prestige assigns this additional DNS server to the Prestige's DHCP clients that have IP addresses in this IPSec rule's range of local addresses. A DNS server allows clients on the VPN to find other computers and servers on the VPN by their (private) domain names.
Local	Local IP addresses must be static and correspond to the remote IPSec router's configured remote IP addresses. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Addr Type	Press [SPACE BAR] to choose **SINGLE**, **RANGE**, or **SUBNET** and press [ENTER]. Select **SINGLE** with a single IP address. Select **RANGE** for a specific range of IP addresses. Select **SUBNET** to specify IP addresses on a network by their subnet mask.
IP Addr Start	When the **Addr Type** field is configured to **Single**, enter a static IP address on the LAN behind your Prestige. When the **Addr Type** field is configured to **Range**, enter the beginning (static) IP address, in a range of computers on your LAN behind your Prestige. When the **Addr Type** is configured to **SUBNET**, this is a (static) IP address on the LAN behind your Prestige.
End/Subnet Mask	When the **Addr Type** field is configured to **Single**, this field is **N/A**. When the **Addr Type** field is configured to **Range**, enter the end (static) IP address, in a range of computers on the LAN behind your Prestige. When the **Addr Type** field is configured to **SUBNET**, this is a subnet mask on the LAN behind your Prestige.
Port Start	0 is the default and signifies any port. Type a port number from 0 to 65535. You cannot create a VPN tunnel if you try to connect using a port number that does not match this port number or range of port numbers. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3
End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. This field is **N/A** when 0 is configured in the **Port Start** field.
Remote	Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. The remote fields are **N/A** when the **Secure Gateway Address** field is configured to 0.0.0.0. Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.
Addr Type	Press [SPACE BAR] to choose **SINGLE**, **RANGE**, or **SUBNET** and press [ENTER]. Select **SINGLE** with a single IP address. Use **RANGE** for a specific range of IP addresses. Use **SUBNET** to specify IP addresses on a network by their subnet mask.

Table 150 Menu 27.1.1 IPSec Setup (continued)

FIELD	DESCRIPTION
IP Addr Start	When the **Addr Type** field is configured to **Single**, enter a static IP address on the network behind the remote IPSec router. When the **Addr Type** field is configured to **Range**, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Addr Type** field is configured to **SUBNET**, enter a static IP address on the network behind the remote IPSec router. This field displays **N/A** when you configure the **Secure Gateway Address** field to 0.0.0.0.
End/Subnet Mask	When the **Addr Type** field is configured to **Single**, this field is **N/A**. When the **Addr Type** field is configured to **Range**, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the **Addr Type** field is configured to **SUBNET**, enter a subnet mask on the network behind the remote IPSec router. This field displays **N/A** when you configure the **Secure Gateway Address** field to 0.0.0.0.
Port Start	0 is the default and signifies any port. Type a port number from 0 to 65535. Someone behind the remote IPSec router cannot create a VPN tunnel when attempting to connect using a port number that does not match this port number or range of port numbers. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. This field is **N/A** when 0 is configured in the **Port Start** field.
Enable Replay Detection	As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DoS) attacks The IPSec receiver can detect and reject old or duplicate packets to protect against replay attacks. Enable replay detection by setting this field to **Yes**. Press [SPACE BAR] to select **Yes** or **No**. Choose **Yes** and press [ENTER] to enable replay detection.
Key Management	Press [SPACE BAR] to choose either **IKE** or **Manual** and then press [ENTER]. **Manual** is useful for troubleshooting if you have problems using **IKE** key management.
Edit Key Management Setup	Press [SPACE BAR] to change the default **No** to **Yes** and then press [ENTER] to go to a key management menu for configuring your key management setup (described later). If you set the **Key Management** field to **IKE**, this will take you to **Menu 27.1.1.1 – IKE Setup**. If you set the **Key Management** field to **Manual**, this will take you to **Menu 27.1.1.2 – Manual Setup**.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

45.4 IKE Setup

To edit this menu, the **Key Management** field in **Menu 27.1.1 – IPSec Setup** must be set to **IKE**. Move the cursor to the **Edit Key Management Setup** field in **Menu 27.1.1 – IPSec Setup**; press [SPACE BAR] to select **Yes** and then press [ENTER] to display **Menu 27.1.1.1 – IKE Setup**.

Figure 281 Menu 27.1.1.1KE Setup

```
            Menu 27.1.1.1 - IKE Setup
                      Phase 1
                        Negotiation Mode= Main
                        Pre-Shared Key=
                        Encryption Algorithm = AES
                        Authentication Algorithm = SHA1
                        SA Life Time (Seconds)= 28800
                        Key Group= DH1
                      Phase 2
                        Active Protocol  = ESP
                        Encryption Algorithm  = AES
                        Authentication Algorithm  = MD5
                        SA Life Time (Seconds)= 28800
                        Encapsulation  = Tunnel
                        Perfect Forward Secrecy (PFS)= None
            Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 151 Menu 27.1.1.1 IKE Setup

FIELD	DESCRIPTION
Phase 1	
Negotiation Mode	Press [SPACE BAR] to choose from **Main** or **Aggressive** and then press [ENTER]. See earlier for a discussion of these modes. Multiple SAs connecting through a secure gateway must have the same negotiation mode.
Pre-Shared Key	Prestige gateways authenticate an IKE VPN session by matching pre-shared keys. Pre-shared keys are best for small networks with fewer than ten nodes. Enter your pre-shared key here. Enter up to 31 characters. Any character may be used, including spaces, but trailing spaces are truncated. Both ends of the VPN tunnel must use the same pre-shared key. You will receive a "PYLD_MALFORMED" (payload malformed) packet if the same pre-shared key is not used on both ends.
Encryption Algorithm	The Prestige and the remote IPSec router generate an encryption key from the Diffie-Hellman key exchange. Prestige **DES** encryption algorithm uses a 56-bit key. Triple DES (**3DES**), is a variation on DES that uses a 168-bit key. As a result, **3DES** is more secure than **DES**. It also requires more processing power, resulting in slightly increased latency and decreased throughput. This implementation of **AES** uses a 128-bit key. **AES** is faster than **3DES**. Press [SPACE BAR] to choose from **DES**, **3DES** or **AES** and then press [ENTER].
Authentication Algorithm	**MD5** (Message Digest 5) and **SHA1** (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The **SHA1** algorithm is generally considered stronger than **MD5**, but is slightly slower. Press [SPACE BAR] to choose from **SHA1** or **MD5** and then press [ENTER].
SA Life Time (Seconds)	Define the length of time before an IKE Security Association automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days). A short **SA Life Time** increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.

Table 151 Menu 27.1.1.1 IKE Setup (continued)

FIELD	DESCRIPTION
Key Group	You must choose a key group for phase 1 IKE setup. **DH1** (default) refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number.
Phase 2	
Active Protocol	Press [SPACE BAR] to choose from **ESP** or **AH** and then press [ENTER]. See earlier for a discussion of these protocols.
Encryption Algorithm	Press [SPACE BAR] to choose from **NULL**, **DES**, **3DES** or **AES** and then press [ENTER]. Select **NULL** to set up a tunnel without encryption.
Authentication Algorithm	Press [SPACE BAR] to choose from **SHA1** or **MD5** and then press [ENTER].
SA Life Time (Seconds)	Define the length of time before an IPSec Security Association automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days).
Encapsulation	Press [SPACE BAR] to choose from **Tunnel** mode or **Transport** mode and then press [ENTER]. See earlier for a discussion of these.
Perfect Forward Secrecy (PFS)	Perfect Forward Secrecy (PFS) is disabled (**None**) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure. Press [SPACE BAR] and choose from **DH1** or **DH2** to enable PFS. **DH1** refers to Diffie-Hellman Group 1 a 768 bit random number. **DH2** refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number (more secure, yet slower).
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

45.5 Manual Setup

You only configure **Menu 27.1.1.2 – Manual Setup** when you select **Manual** in the **Key Management** field in **Menu 27.1.1 – IPSec Setup**. Manual key management is useful if you have problems with **IKE** key management.

45.5.1 Active Protocol

This field is a combination of mode and security protocols used for the VPN. See the Web Configurator part on VPN for more information on these parameters.

Table 152 Active Protocol: Encapsulation and Security Protocol

MODE	SECURITY PROTOCOL
Tunnel	ESP
Transport	AH

45.5.2 Security Parameter Index (SPI)

To edit this menu, move the cursor to the **Edit Manual Setup** field in **Menu 27.1.1 – IPSec Setup** press [SPACE BAR] to select **Yes** and then press [ENTER] to go to **Menu 27.1.1.2 – Manual Setup**.

Figure 282 Menu 27.1.1.2 Manual Setup

```
              Menu 27.1.1.2 – Manual Setup

              Active Protocol= ESP Tunnel
              ESP Setup
                SPI (Decimal)= 0
                Encryption Algorithm= DES
                  Key1= ?
                  Key2= N/A
                  Key3= N/A
                Authentication Algorithm= MD5
                  Key= ?

              AH Setup
                SPI (Decimal)= N/A
                Authentication Algorithm= N/A
                  Key= N/A

              Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 153 Menu 27.1.1.2 Manual Setup

FIELD	DESCRIPTION
Active Protocol	Press [SPACE BAR] to choose from **ESP Tunnel**, **ESP Transport**, **AH Tunnel** or **AH Transport** and then press [ENTER]. Choosing an **ESP** combination causes the **AH Setup** fields to be non-applicable (**N/A**)
ESP Setup	The **ESP Setup** fields are **N/A** if you chose an **AH Active Protocol**.
SPI (Decimal)	The **SPI** must be unique and from one to four integers ("0" to "9").
Encryption Algorithm	Press [SPACE BAR] to choose from **NULL**, **DES**, **3DES** or **AES** and then press [ENTER]. Fill in the **Key1** field below when you choose **DES** and fill in fields **Key1** to **Key3** when you choose **3DES**. Select **NULL** to set up a tunnel without encryption. When you select **NULL**, you do not enter any encryption keys.
Key1	Enter a unique eight-character key. Any character may be used, including spaces, but trailing spaces are truncated. Fill in the **Key1** field when you choose **DES** and fill in fields **Key1** to **Key3** when you choose **3DES**.
Key2	Enter a unique eight-character key. It can be comprised of any character including spaces (but trailing spaces are truncated).
Key3	Enter a unique eight-character key. It can be comprised of any character including spaces (but trailing spaces are truncated).
Authentication Algorithm	Press [SPACE BAR] to choose from **MD5** or **SHA1** and then press [ENTER].
Key	Enter the authentication key to be used by IPSec if applicable. The key must be unique. Enter 16 characters for **MD5** authentication and 20 characters for **SHA-1** authentication. Any character may be used, including spaces, but trailing spaces are truncated.
AH Setup	The **AH Setup** fields are **N/A** if you chose an **ESP Active Protocol**.
SPI (Decimal)	The **SPI** must be from one to four unique decimal characters ("0" to "9") long.

Table 153 Menu 27.1.1.2 Manual Setup (continued)

FIELD	DESCRIPTION
Authentication Algorithm	Press [SPACE BAR] to choose from **MD5** or **SHA1** and then press [ENTER].
Key	Enter the authentication key to be used by IPSec if applicable. The key must be unique. Enter 16 characters for **MD5** authentication and 20 characters for **SHA-1** authentication. Any character may be used, including spaces, but trailing spaces are truncated.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

CHAPTER 46
SA Monitor

This chapter teaches you how to manage your SAs by using the SA Monitor in SMT menu 27.2.

46.1 SA Monitor Overview

A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This menu (shown next) displays active VPN connections.

Note: When there is outbound traffic but no inbound traffic, the SA times out automatically after two minutes. A tunnel with no outbound or inbound traffic is "idle" and does not timeout until the SA lifetime period expires. See the Web configurator part on keep alive to have the Prestige renegotiate an IPSec SA when the SA lifetime expires, even if there is no traffic.

46.2 Using SA Monitor

Use the **Refresh** function to display active VPN connections.

Use the **Disconnect** function to cut off active connections.

Type 2 in **Menu 27 - VPN/IPSec Setup**, and then press [ENTER] to go to **Menu 27.2 - SA Monitor**.

Figure 283 Menu 27.2 SA Monitor

```
      Menu 27.2 - SA Monitor

 #    Name                                 Encap.     IPSec ALgorithm
---   -------------------------------    ---------    ----------------
001   Taiwan : 3.3.3.1 – 3.3.3.3.100      Tunnel       ESP DES MD5
002
003
004
005
006
007
008
009
010


      Select Command= Refresh
      Select Connection= N/A
      Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 154 Menu 27.2 SA Monitor

FIELD	DESCRIPTION
#	This is the security association index number.
Name	This field displays the identification name for this VPN policy. This name is unique for each connection where the secure gateway IP address is a public static IP address. When the secure gateway IP address is 0.0.0.0 (as discussed in the last chapter), there may be different connections using this same VPN rule. In this case, the name is followed by the remote IP address as configured in **Menu 27.1.1. – IPSec Setup**. Individual connections using the same VPN rule may be terminated without affecting other connections using the same rule.
Encap.	This field displays **Tunnel** mode or **Transport** mode. See previous for discussion.
IPSec Algorithm	This field displays the security protocols used for an SA. **ESP** provides confidentiality and integrity of data by encrypting the data and encapsulating it into IP packets. Encryption methods include 56-bit **DES** and 168-bit **3DES**. **NULL** denotes a tunnel without encryption. An incoming SA may have an **AH** in addition to **ESP**. The Authentication Header provides strong integrity and authentication by adding authentication information to IP packets. This authentication information is calculated using header and payload data in the IP packet. This provides an additional level of security. **AH** choices are **MD5** (default - 128 bits) and **SHA -1**(160 bits). Both **AH** and **ESP** increase Prestige processing requirements and communications latency (delay).

Table 154 Menu 27.2 SA Monitor (continued)

FIELD	DESCRIPTION
Select Command	Press [SPACE BAR] to choose from **Refresh**, **Disconnect**, **None**, **Next Page**, or **Previous Page** and then press [ENTER]. You must select a connection in the next field when you choose the **Disconnect** command. **Refresh** displays current active VPN connections. **None** allows you to jump to the "Press ENTER to Confirm…" prompt. Select **Next Page** or **Previous Page** to view the next or previous page of rules (respectively).
Select Connection	Type the VPN connection index number that you want to disconnect and then press [ENTER].
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

CHAPTER 47
Internal SPTGEN

47.1 Internal SPTGEN Overview

Internal SPTGEN (System Parameter Table Generator) is a configuration text file useful for efficient configuration of multiple Prestiges. Internal SPTGEN lets you configure, save and upload multiple menus at the same time using just one configuration text file – eliminating the need to navigate and configure individual SMT menus for each Prestige.

47.2 The Configuration Text File Format

All Internal SPTGEN text files conform to the following format:

```
<field identification number = field name = parameter values
allowed = input>,
```

where <input> is your input conforming to <parameter values allowed>.

The figure shown next is an example of an Internal SPTGEN text file.

Figure 284 Configuration Text File Format: Column Descriptions

```
/ Menu 1 General Setup
 10000000 = Configured                <0(No)| 1(Yes)>       = 1
 10000001 = System Name               <Str>                 = Prestige
 10000002 = Location                  <Str>                 =
 10000003 = Contact Person's Name     <Str>                 =
 10000004 = Route IP                  <0(No)| 1(Yes)>       = 1
 10000005 = Route IPX                <0(No)| 1(Yes)>      = 0
 10000006 = Bridge                   <0(No)| 1(Yes)>      = 0
```

Note: DO NOT alter or delete any field except parameters in the Input column.

For more text file examples, refer to the Example Internal SPTGEN Screens appendix.

47.2.1 Internal SPTGEN File Modification - Important Points to Remember

Each parameter you enter must be preceded by one "="sign and one space.

Some parameters are dependent on others. For example, if you disable the **Configured** field in menu 1 (see Figure 284), then you disable every field in this menu.

If you enter a parameter that is invalid in the **Input** column, the Prestige will not save the configuration and the command line will display the **Field Identification Number**. Figure 285 , shown next, is an example of what the Prestige displays if you enter a value other than "0" or "1" in the **Input** column of **Field Identification Number** 1000000 (refer to Figure 284).

Figure 285 Invalid Parameter Entered: Command Line Example

```
field value is not legal error:-1
ROM-t is not saved, error Line ID:10000000
reboot to get the original configuration
Bootbase Version: V2.02 | 2/22/2001 13:33:11
RAM: Size = 8192 Kbytes
FLASH: Intel 8M *2
```

The Prestige will display the following if you enter parameter(s) that *are* valid.

Figure 286 Valid Parameter Entered: Command Line Example

```
Please wait for the system to write SPT text file(ROM-t)...
Bootbase Version: V2.02 | 2/22/2001 13:33:11
RAM: Size = 8192 Kbytes
FLASH: Intel 8M *2
```

47.3 Internal SPTGEN FTP Download Example

1. Launch your FTP application.
2. Enter "`bin`". The command "`bin`" sets the transfer mode to binary.
3. Get "`rom-t`" file. The command "`get`" transfers files from the Prestige to your computer. The name "`rom-t`" is the configuration filename on the Prestige.
4. Edit the "`rom-t`" file using a text editor (do not use a word processor). You must leave this FTP screen to edit.

Figure 287 Internal SPTGEN FTP Download Example

```
c:\ftp 192.168.1.1
220 PPP FTP version 1.0 ready at Sat Jan 1 03:22:12 2000
User (192.168.1.1:(none)):
331 Enter PASS command
Password:
230 Logged in
ftp>bin
200 Type I OK
ftp> get rom-t
ftp>bye
c:\edit rom-t
(edit the rom-t text file by a text editor and save it)
```

Note: You can rename your "`rom-t`" file when you save it to your computer but it must be named "`rom-t`" when you upload it to your Prestige.

47.4 Internal SPTGEN FTP Upload Example

1. Launch your FTP application.
2. Enter "`bin`". The command "`bin`" sets the transfer mode to binary.
3. Upload your "`rom-t`" file from your computer to the Prestige using the "`put`" command. computer to the Prestige.
4. Exit this FTP application.

Figure 288 Internal SPTGEN FTP Upload Example

```
c:\ftp 192.168.1.1
220 PPP FTP version 1.0 ready at Sat Jan 1 03:22:12 2000
User (192.168.1.1:(none)):
331 Enter PASS command
Password:
230 Logged in
ftp>bin
200 Type I OK
ftp> put rom-t
ftp>bye
```

CHAPTER 48
Troubleshooting

This chapter covers potential problems and the corresponding remedies.

48.1 Problems Starting Up the Prestige

Table 155 Troubleshooting the Start-Up of Your Prestige

PROBLEM	CORRECTIVE ACTION
None of the LEDs turn on when I turn on the Prestige.	Make sure that the Prestige's power adaptor is connected to the Prestige and plugged in to an appropriate power source. Check that the Prestige and the power source are both turned on. Turn the Prestige off and on. If the error persists, you may have a hardware problem. In this case, you should contact your vendor.

48.2 Problems with the LAN LED

Table 156 Troubleshooting the LAN LED

PROBLEM	CORRECTIVE ACTION
The LAN LEDs do not turn on.	Check your Ethernet cable connections and type (refer to the *Quick Start Guide* for details). Check for faulty Ethernet cables.
	Make sure your computer's Ethernet card is working properly.

48.3 Problems with the DSL LED

Table 157 Troubleshooting the DSL LED

PROBLEM	CORRECTIVE ACTION
The DSL LED is off.	Check the telephone wire and connections between the Prestige DSL port and the wall jack.
	Make sure that the telephone company has checked your phone line and set it up for DSL service.
	Reset your ADSL line to reinitialize your link to the DSLAM. For details, refer to the Maintenance chapter (web configurator) or the System Information and Diagnosis chapter (SMT).

48.4 Problems with the LAN Interface

Table 158 Troubleshooting the LAN Interface

PROBLEM	CORRECTIVE ACTION
I cannot access the Prestige from the LAN.	If the 10M/100M LEDs on the front panel are both off, refer to the Problems with the LAN LED section. Make sure that the IP address and the subnet mask of the Prestige and your computer(s) are on the same subnet.
I cannot ping any computer on the LAN.	If the 10M/100M LEDs on the front panel are both off, refer to the Problems with the LAN LED section. Make sure that the IP address and the subnet mask of the Prestige and the computers are on the same subnet.

48.5 Problems with the WAN Interface

Table 159 Troubleshooting the WAN Interface

PROBLEM	CORRECTIVE ACTION
I cannot get a WAN IP address from the ISP.	The ISP provides the WAN IP address after authenticating you. Authentication may be through the user name and password, the MAC address or the host name. The username and password apply to PPPoE and PPPoA encapsulation only. Make sure that you have entered the correct **Service Type**, **User Name** and **Password** (be sure to use the correct casing). Refer to the WAN Setup chapter (web configurator) or the Internet Access chapter (SMT).

48.6 Problems with Internet Access

Table 160 Troubleshooting Internet Access

PROBLEM	CORRECTIVE ACTION
I cannot access the Internet.	Make sure the Prestige is turned on and connected to the network. If the DSL LED is off, refer to the Problems with the DSL LED section. Verify your WAN settings. Refer to the chapter on WAN setup (web configurator) or the section on Internet Access (SMT). Make sure you entered the correct user name and password. If you use PPPoE pass through, make sure that bridge is turned on. See the Menu 1 General Setup chapter for details. For wireless stations, check that both the Prestige and wireless station(s) are using the same ESSID, channel, WEP keys (if WEP encryption is activated) and authentication method.
Internet connection disconnects.	Check the schedule rules. Refer to the Call Scheduling chapter (SMT). If you use PPPoA or PPPoE encapsulation, check the idle time-out setting. Refer to the WAN Setup chapter (web configurator) or the Remote Node Configuration chapter (SMT). Contact your ISP.

48.7 Problems with the Password

Table 161 Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
I cannot access the Prestige.	The username is "admin". The default password is "1234". The **Password** and **Username** fields are case-sensitive. Make sure that you enter the correct password and username using the proper casing. If you have changed the password and have now forgotten it, you will need to upload the default configuration file (Refer to the Resetting the Prestige section in the Introducing the Web Configurator chapter). This restores all of the factory defaults including the password.

48.8 Problems with the Web Configurator

Table 162 Troubleshooting the Web Configurator

PROBLEM	CORRECTIVE ACTION
I cannot access the web configurator.	Refer to the *Quick Start Guide* for hardware connections. Make sure that there is not an SMT console session running. Check that you have enabled web service access. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on remote management for details. For WAN access, you must configure remote management to allow server access from the Wan (or all). You must also configure a firewall rule to allow access from the WAN. Refer to the chapters on remote management and firewall for details. Your computer's and the Prestige's IP addresses must be on the same subnet for LAN access. If you changed the Prestige's LAN IP address, then enter the new one as the URL. Remove any filters in SMT menu 3.1 (LAN) or menu 11.5 (WAN) that block web service. See also the Problems with Remote Management section.

48.9 Problems with Remote Management

Table 163 Troubleshooting Remote Management

PROBLEM	CORRECTIVE ACTION
I cannot remotely manage the Prestige from the LAN or WAN.	Refer to the Remote Management Limitations section in the Remote Management Configuration chapter for scenarios when remote management may not be possible.
	Use the Prestige's WAN IP address when configuring from the WAN. Use the Prestige's LAN IP address when configuring from the LAN.
	Refer to for instructions on checking your LAN connection.
	Refer to the Problems with the LAN Interface section for instructions on checking your WAN connection.
	See also the Problems with the Web Configurator section.

Appendix A
Pin Assignments

Cable Pin Assignments

In a serial communications connection, generally a computer is DTE (Data Terminal Equipment) and a modem is DCE (Data Circuit-terminating Equipment). The Prestige is DCE when you connect a computer to the console port. The Prestige is DTE when you connect a modem to the dial backup port.

Figure 289 Console/Dial Backup Port Pin Layouts [3]

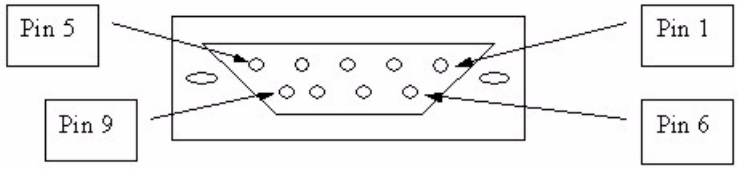
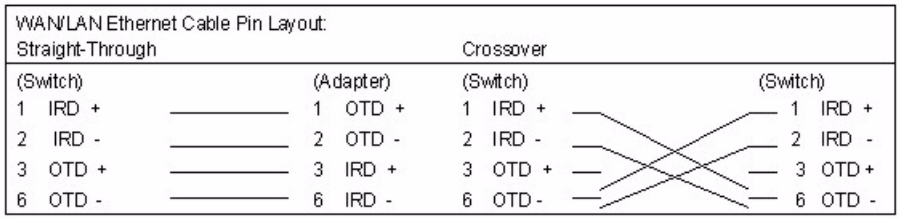


Table 164 Console/Dial Backup Port Pin Assignments

CONSOLE PORT RS – 232 (FEMALE) DB-9F	DIAL BACKUP RS – 232 (MALE) DB-9M
Pin 1 = NON Pin 2 = DCE-TXD Pin 3 = DCE –RXD Pin 4 = DCE –DSR Pin 5 = GND Pin 6 = DCE –DTR Pin 7 = DCE –CTS Pin 8 = DCE –RTS PIN 9 = NON	Pin 1 = NON Pin 2 = DTE-RXD Pin 3 = DTE-TXD Pin 4 = DTE-DTR Pin 5 = GND Pin 6 = DTE-DSR Pin 7 = DTE-RTS Pin 8 = DTE-CTS PIN 9 = NON.
The CON/AUX port also has these pin assignments. The CON/AUX switch changes the setting in the firmware only and does not change the CON/AUX port's pin assignments.	Prestiges with a CON/AUX port also have a 9-pin adaptor for the console cable with these pin assignments on the male end.

3. Products without flow control only use pins 2,3 and 5.

Figure 290 Ethernet Cable Pin Assignments



Appendix B
Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

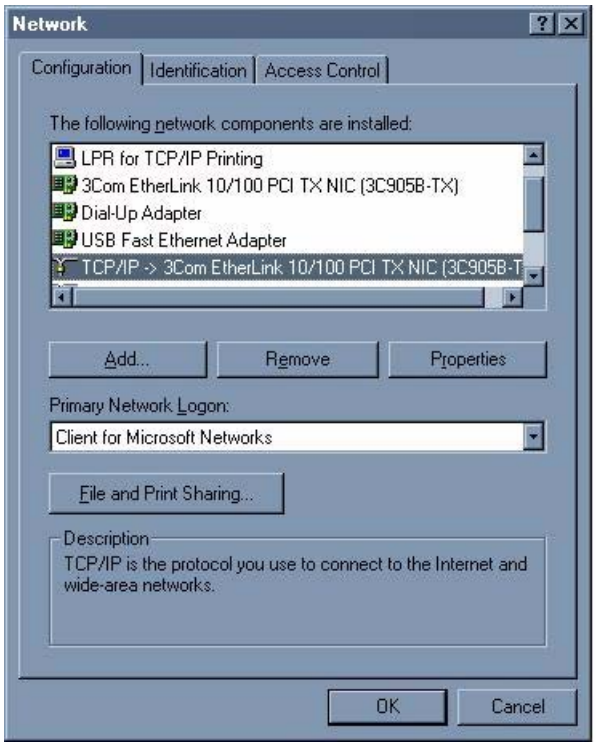
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the Prestige's LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window

Figure 291 WIndows 95/98/Me: Network: Configuration



Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

1. In the **Network** window, click **Add**.
2. Select **Adapter** and then click **Add**.
3. Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

1. In the **Network** window, click **Add**.
2. Select **Protocol** and then click **Add**.
3. Select **Microsoft** from the list of **manufacturers**.
4. Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

1. Click **Add**.
2. Select **Client** and then click **Add**.

3 Select **Microsoft** from the list of manufacturers.

4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.

5 Restart your computer so the changes you made take effect.

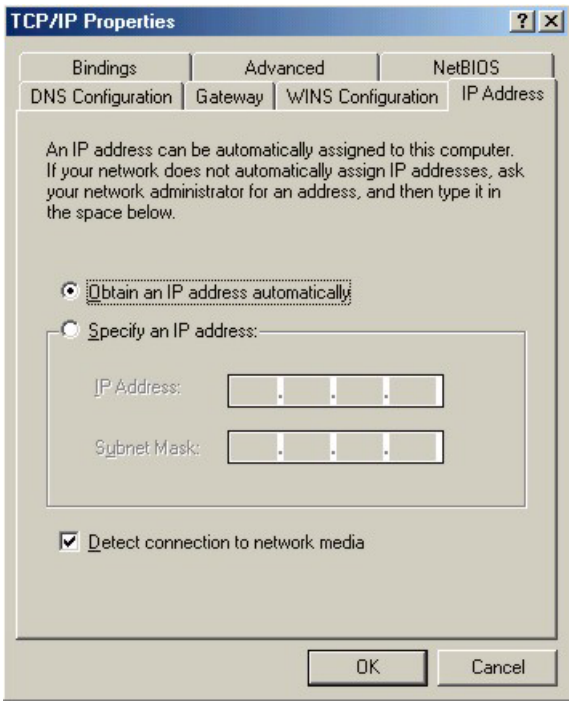
Configuring

1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**

2 Click the **IP Address** tab.

- If your IP address is dynamic, select **Obtain an IP address automatically**.
- If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

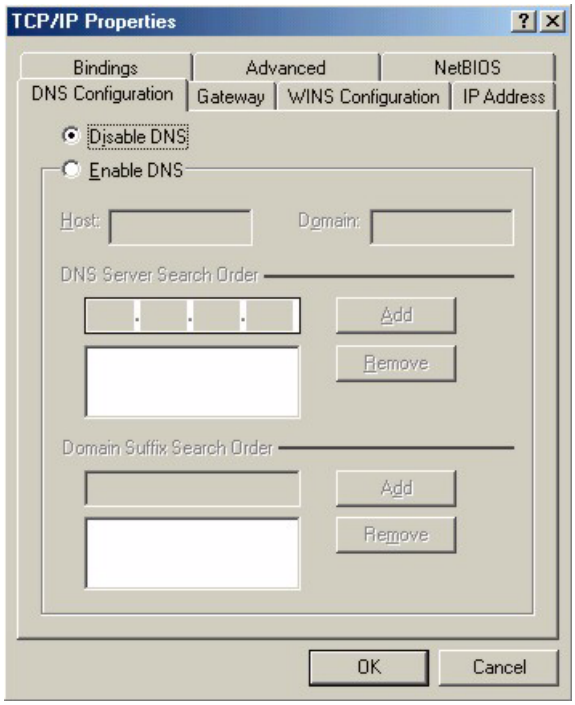
Figure 292 Windows 95/98/Me: TCP/IP Properties: IP Address



3 Click the **DNS** Configuration tab.

- If you do not know your DNS information, select **Disable DNS**.
- If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

Figure 293 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



4 Click the **Gateway** tab.

- If you do not know your gateway's IP address, remove previously installed gateways.
- If you have a gateway IP address, type it in the **New gateway field** and click **Add**.

5 Click **OK** to save and close the **TCP/IP Properties** window.

6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.

7 Turn on your Prestige and restart your computer when prompted.

Verifying Settings

1 Click **Start** and then **Run**.

2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.

3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

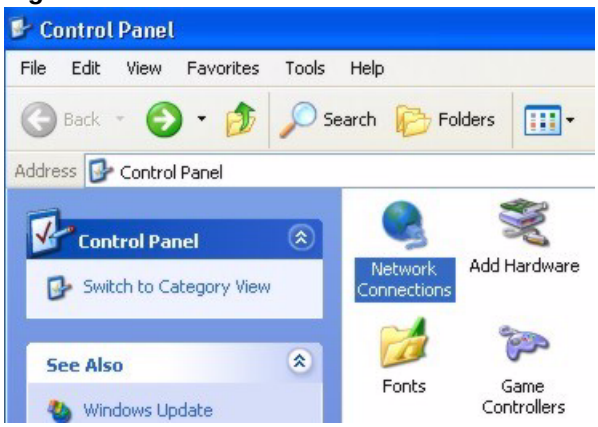
Windows 2000/NT/XP

1 For Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.

Figure 294 Windows XP: Start Menu

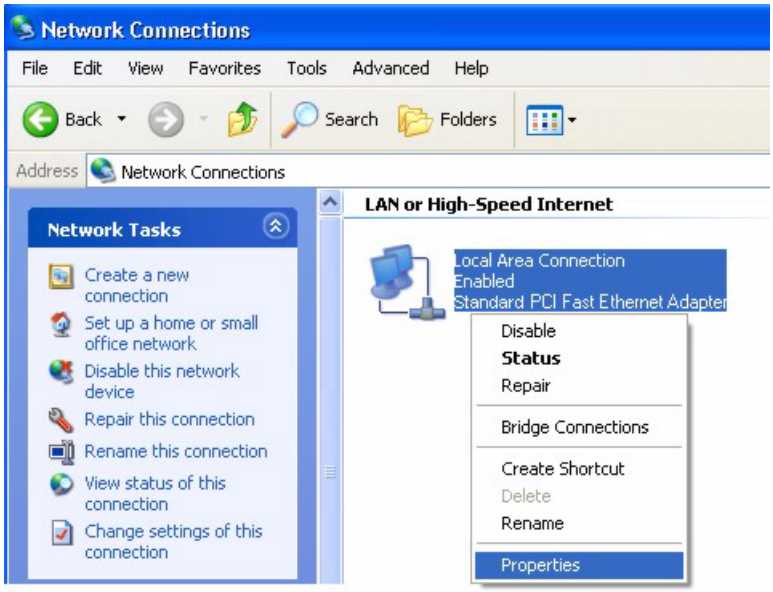
2 For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.

Figure 295 Windows XP: Control Panel



3 Right-click **Local Area Connection** and then click **Properties**.

Figure 296 Windows XP: Control Panel: Network Connections: Properties



4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and click **Properties**.

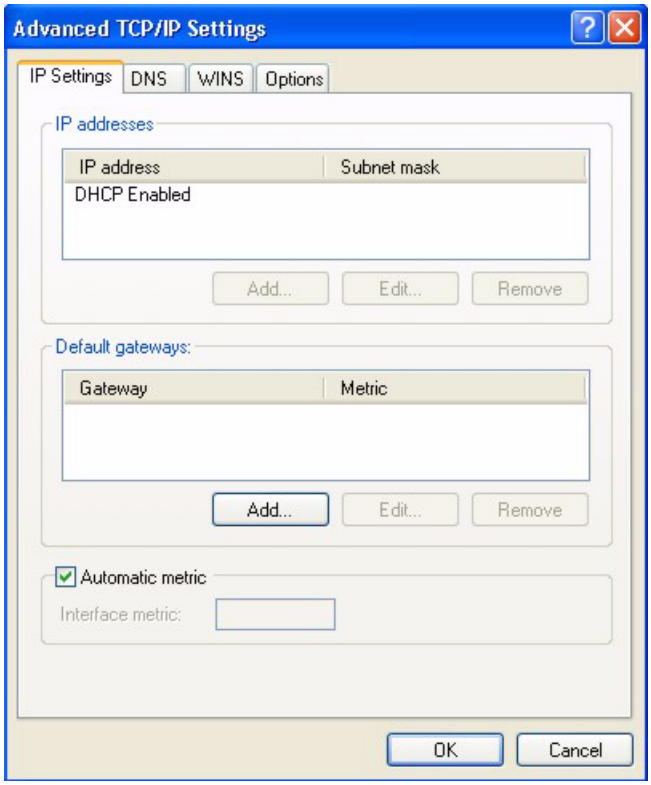
Figure 297 Windows XP: Local Area Connection Properties

5 The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.

- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields. Click **Advanced**.

Figure 298 Windows XP: Advanced TCP/IP Settings



6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Setting**s tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

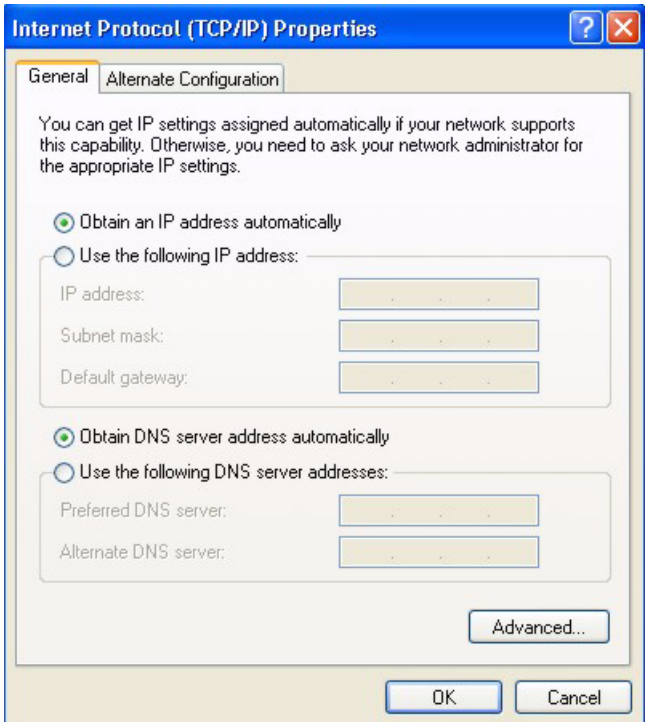
- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

7 In the **Internet Protocol TCP/IP Properties** window (the **General tab** in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

  If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 299 Windows XP: Internet Protocol (TCP/IP) Properties



8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **OK** to close the **Local Area Connection Properties** window.

10 Turn on your Prestige and restart your computer (if prompted).

Verifying Settings

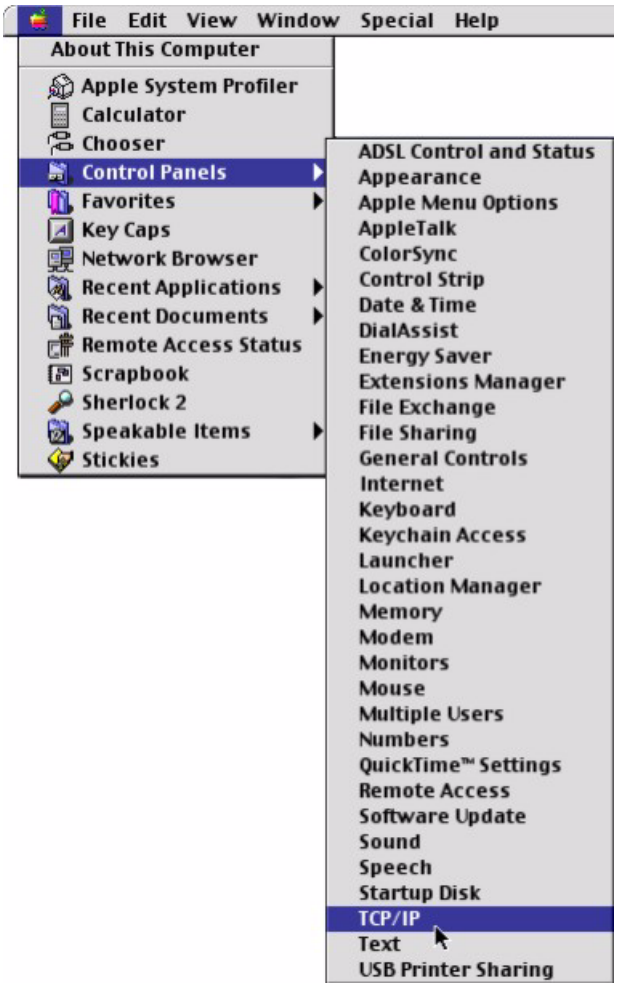
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

2 In the **Command Prompt** window, type "`ipconfig`" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

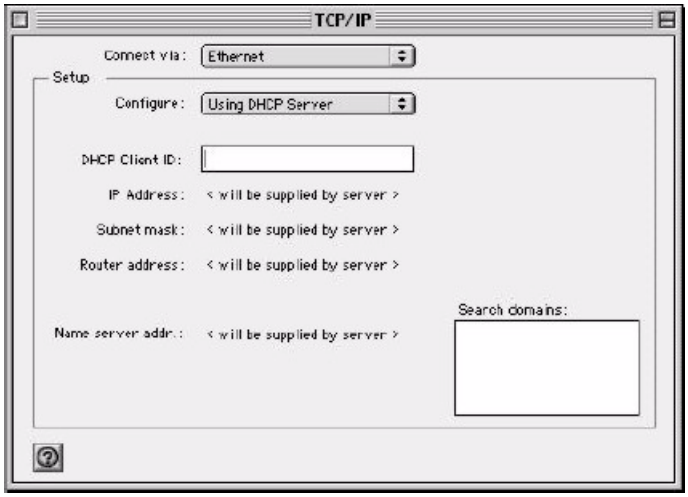
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 300 Macintosh OS 8/9: Apple Menu



2 Select **Ethernet built-in** from the **Connect via** list.

Figure 301 Macintosh OS 8/9: TCP/IP



3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your Prestige in the **Router address** box.

5 Close the **TCP/IP Control Panel**.

6 Click **Save** if prompted, to save changes to your configuration.

7 Turn on your Prestige and restart your computer (if prompted).

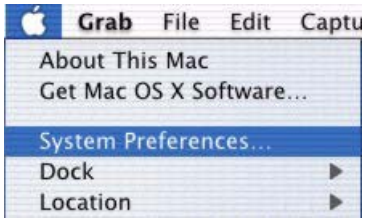
Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

Macintosh OS X

1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 302 Macintosh OS X: Apple Menu

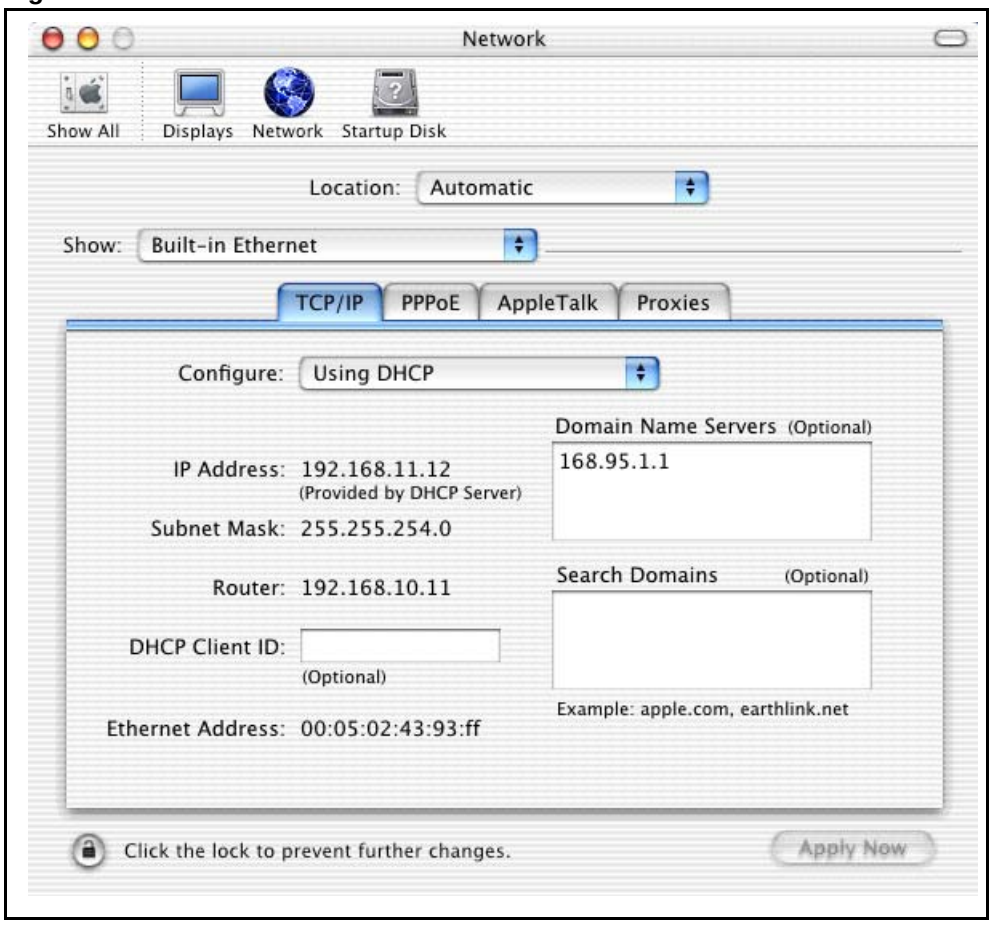


2 Click **Network** in the icon bar.

- Select **Automatic** from the **Location** list.
- Select **Built-in Ethernet** from the **Show** list.
- Click the **TCP/IP** tab.

3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

Figure 303 Macintosh OS X: Network



4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your Prestige in the **Router address** box.

5 Click **Apply Now** and close the window.

6 Turn on your Prestige and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

Appendix C
IP Subnetting

IP Addressing

Routers "route" based on the network number. The router that delivers the data packet to the correct destination host uses the host ID.

IP Classes

An IP address is made up of four octets (eight bits), written in dotted decimal notation, for example, 192.168.1.1. IP addresses are categorized into different classes. The class of an address depends on the value of its first octet.

- Class "A" addresses have a 0 in the left most bit. In a class "A" address the first octet is the network number and the remaining three octets make up the host ID.
- Class "B" addresses have a 1 in the left most bit and a 0 in the next left most bit. In a class "B" address the first two octets make up the network number and the two remaining octets make up the host ID.
- Class "C" addresses begin (starting from the left) with 1 1 0. In a class "C" address the first three octets make up the network number and the last octet is the host ID.
- Class "D" addresses begin with 1 1 1 0. Class "D" addresses are used for multicasting. (There is also a class "E" address. It is reserved for future use.)

Table 165 Classes of IP Addresses

IP ADDRESS:		OCTET 1	OCTET 2	OCTET 3	OCTET 4
Class A	0	Network number	Host ID	Host ID	Host ID
Class B	10	Network number	Network number	Host ID	Host ID
Class C	110	Network number	Network number	Network number	Host ID

Note: Host IDs of all zeros or all ones are not allowed.

Therefore:

A class "C" network (8 host bits) can have 2^8 –2 or 254 hosts.

A class "B" address (16 host bits) can have 2^{16} –2 or 65534 hosts.

A class "A" address (24 host bits) can have 2^{24} –2 hosts (approximately 16 million hosts).

Since the first octet of a class "A" IP address must contain a "0", the first octet of a class "A" address can have a value of 0 to 127.

Similarly the first octet of a class "B" must begin with "10", therefore the first octet of a class "B" address has a valid range of 128 to 191. The first octet of a class "C" address begins with "110", and therefore has a range of 192 to 223.

Table 166 Allowed IP Address Range By Class

CLASS	ALLOWED RANGE OF FIRST OCTET (BINARY)	ALLOWED RANGE OF FIRST OCTET (DECIMAL)
Class A	**0**0000000 to **0**1111111	0 to 127
Class B	**10**000000 to **10**111111	128 to 191
Class C	**110**00000 to **110**11111	192 to 223
Class D	**1110**0000 to **1110**1111	224 to 239

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). A subnet mask has 32 is a "1" then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is "0" then the corresponding bit in the IP address is part of the host ID.

Subnet masks are expressed in dotted decimal notation just as IP addresses are. The "natural" masks for class A, B and C IP addresses are as follows.

Table 167 "Natural" Masks

CLASS	NATURAL MASK
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Subnetting

With subnetting, the class arrangement of an IP address is ignored. For example, a class C address no longer has to have 24 bits of network number and 8 bits of host ID. With subnetting, some of the host ID bits are converted into network number bits. By convention, subnet masks always consist of a continuous sequence of ones beginning from the left most bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with mask 255.255.255.128.

The following table shows all possible subnet masks for a class "C" address using both notations.

Table 168 Alternative Subnet Mask Notation

SUBNET MASK IP ADDRESS	SUBNET MASK "1" BITS	LAST OCTET BIT VALUE
255.255.255.0	/24	0000 0000
255.255.255.128	/25	1000 0000
255.255.255.192	/26	1100 0000
255.255.255.224	/27	1110 0000
255.255.255.240	/28	1111 0000
255.255.255.248	/29	1111 1000
255.255.255.252	/30	1111 1100

The first mask shown is the class "C" natural mask. Normally if no mask is specified it is understood that the natural mask is being used.

Example: Two Subnets

As an example, you have a class "C" address 192.168.1.0 with subnet mask of 255.255.255.0.

Table 169 Two Subnets Example

	NETWORK NUMBER	HOST ID
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask	255.255.255.	0
Subnet Mask (Binary)	11111111.11111111.11111111.	00000000

The first three octets of the address make up the network number (class "C"). You want to have two separate networks.

Divide the network 192.168.1.0 into two separate subnets by converting one of the host ID bits of the IP address to a network number bit. The "borrowed" host ID bit can be either "0" or "1" thus giving two subnets; 192.168.1.0 with mask 255.255.255.128 and 192.168.1.128 with mask 255.255.255.128.

Note: In the following charts, shaded/bold last octet bit values indicate host ID bits "borrowed" to form network ID bits. The number of "borrowed" host ID bits determines the number of subnets you can have. The remaining number of host ID bits (after "borrowing") determines the number of hosts you can have on each subnet.

Table 170 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**0**0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	**1**0000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 171 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**1**0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	**1**0000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

The remaining 7 bits determine the number of hosts each subnet can have. Host IDs of all zeros represent the subnet itself and host IDs of all ones are the broadcast address for that subnet, so the actual number of hosts available on each subnet in the example above is $2^7 - 2$ or 126 hosts for each subnet.

192.168.1.0 with mask 255.255.255.128 is the subnet itself, and 192.168.1.127 with mask 255.255.255.128 is the directed broadcast address for the first subnet. Therefore, the lowest IP address that can be assigned to an actual host for the first subnet is 192.168.1.1 and the highest is 192.168.1.126. Similarly the host ID range for the second subnet is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The above example illustrated using a 25-bit subnet mask to divide a class "C" address space into two subnets. Similarly to divide a class "C" address into four subnets, you need to "borrow" two host ID bits to give four possible combinations of 00, 01, 10 and 11. The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192. Each subnet contains 6 host ID bits, giving 2^6-2 or 62 hosts for each subnet (all 0's is the subnet itself, all 1's is the broadcast address on the subnet).

Table 172 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 173 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 174 Subnet 3

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 175 Subnet 4

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example Eight Subnets

Similarly use a 27-bit mask to create 8 subnets (001, 010, 011, 100, 101, 110).

The following table shows class C IP address last octet values for each subnet.

Table 176 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	223	254	255

The following table is a summary for class "C" subnet planning.

Table 177 Class C Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

Subnetting With Class A and Class B Networks.

For class "A" and class "B" addresses the subnet mask also determines which bits are part of the network number and which are part of the host ID.

A class "B" address has two host ID octets available for subnetting and a class "A" address has three host ID octets (see Table 165) available for subnetting.

The following table is a summary for class "B" subnet planning.

Table 178 Class B Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Appendix D PPPoE

PPPoE in Action

An ADSL modem bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your computer to an ATM PVC (Permanent Virtual Circuit) which connects to a DSL Access Concentrator where the PPP session terminates (see Figure 304). One PVC can support any number of PPP sessions from your LAN. PPPoE provides access control and billing functionality in a manner similar to dial-up services using PPP.

Benefits of PPPoE

PPPoE offers the following benefits:

It provides you with a familiar dial-up networking (DUN) user interface.

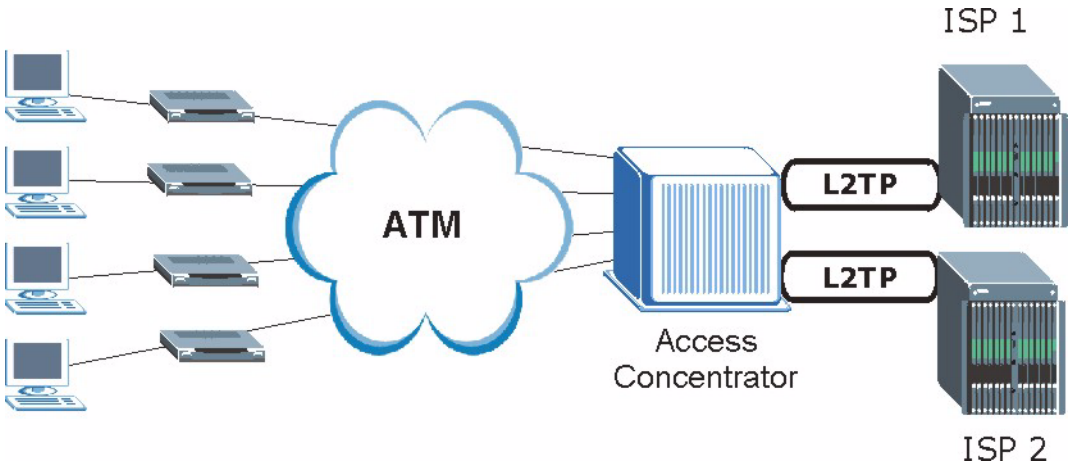
It lessens the burden on the carriers of provisioning virtual circuits all the way to the ISP on multiple switches for thousands of users. For GSTN (PSTN and ISDN), the switching fabric is already in place.

It allows the ISP to use the existing dial-up model to authenticate and (optionally) to provide differentiated services.

Traditional Dial-up Scenario

The following diagram depicts a typical hardware configuration where the computers use traditional dial-up networking.

Figure 304 Single-Computer per Router Hardware Configuration



How PPPoE Works

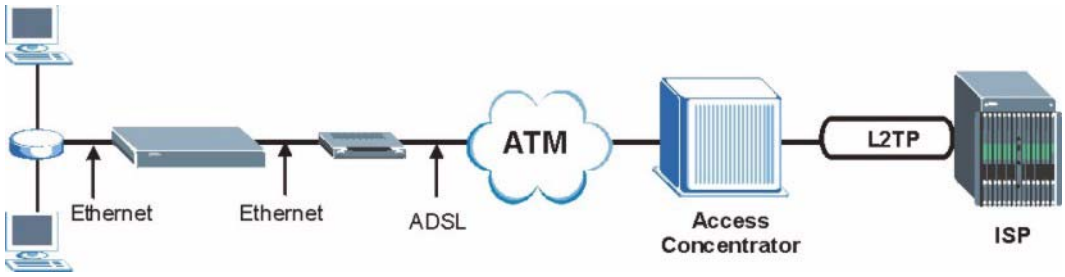
The PPPoE driver makes the Ethernet appear as a serial link to the computer and the computer runs PPP over it, while the modem bridges the Ethernet frames to the Access Concentrator (AC). Between the AC and an ISP, the AC is acting as a L2TP (Layer 2 Tunneling Protocol) LAC (L2TP Access Concentrator) and tunnels the PPP frames to the ISP. The L2TP tunnel is capable of carrying multiple PPP sessions.

With PPPoE, the VC (Virtual Circuit) is equivalent to the dial-up connection and is between the modem and the AC, as opposed to all the way to the ISP. However, the PPP negotiation is between the computer and the ISP.

Prestige as a PPPoE Client

When using the Prestige as a PPPoE client, the computers on the LAN see only Ethernet and are not aware of PPPoE. This alleviates the administrator from having to manage the PPPoE clients on the individual computers.

Figure 305 Prestige as a PPPoE Client



Appendix E
Wireless LAN and IEEE 802.11

A wireless LAN (WLAN) provides a flexible data communications system that you can use to access various services (navigating the Internet, E-mail, printer services, etc.) without the use of a cabled connection. In effect a wireless LAN environment provides you the freedom to stay connected to the network while roaming around in the coverage area.

Benefits of a Wireless LAN

Wireless LAN offers the following benefits:

It provides you with access to network services in areas otherwise hard or expensive to wire, such as historical buildings, buildings with asbestos materials and classrooms.

It provides healthcare workers like doctors and nurses access to a complete patient's profile on a handheld or notebook computer upon entering a patient's room.

It allows flexible workgroups a lower total cost of ownership for workspaces that are frequently reconfigured.

It allows conference room users access to the network as they move from meeting to meeting, getting up-to-date access to information and the ability to communicate decisions while "on the go".

It provides campus-wide networking mobility, allowing enterprises the roaming capability to set up easy-to-use wireless networks that cover the entire campus transparently.

IEEE 802.11

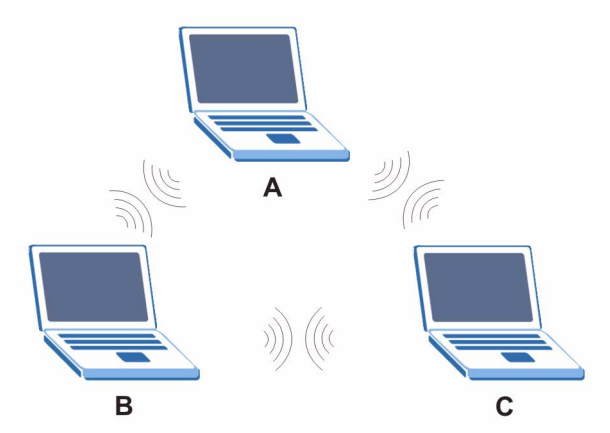
The 1997 completion of the IEEE 802.11 standard for wireless LANs (WLANs) was a first important step in the evolutionary development of wireless networking technologies. The standard was developed to maximize interoperability between differing brands of wireless LANs as well as to introduce a variety of performance improvements and benefits.

The IEEE 802.11 specifies three different transmission methods for the PHY, the layer responsible for transferring data between nodes. Two of the methods use spread spectrum RF signals, Direct Sequence Spread Spectrum (DSSS) and Frequency-Hopping Spread Spectrum (FHSS), in the 2.4 to 2.4825 GHz unlicensed ISM (Industrial, Scientific and Medical) band. The third method is infrared technology, using very high frequencies, just below visible light in the electromagnetic spectrum to carry data.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless nodes or stations (STA), which is called a Basic Service Set (BSS). In the most basic form, a wireless LAN connects a set of computers with wireless adapters. Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an Ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an Ad-hoc wireless LAN.

Figure 306 Peer-to-Peer Communication in an Ad-hoc Network

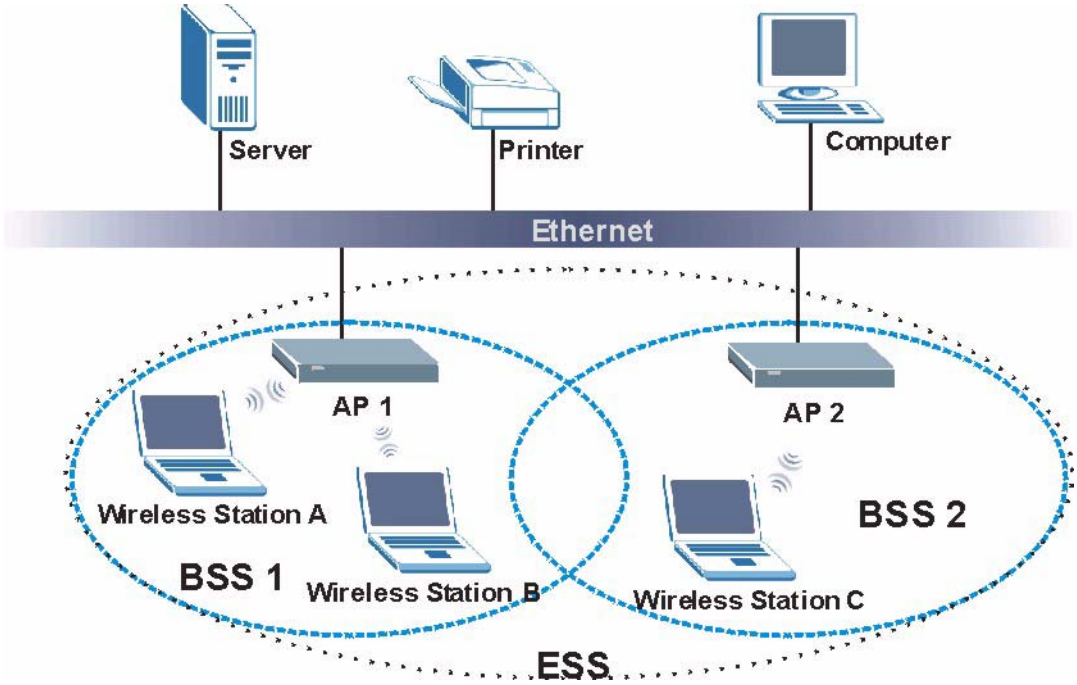


Infrastructure Wireless LAN Configuration

For Infrastructure WLANs, multiple Access Points (APs) link the WLAN to the wired network and allow users to efficiently share network resources. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood. Multiple Access Points can provide wireless coverage for an entire building or campus. All communications between stations or between a station and a wired network client go through the Access Point.

The Extended Service Set (ESS) shown in the next figure consists of a series of overlapping BSSs (each containing an Access Point) connected together by means of a Distribution System (DS). Although the DS could be any type of network, it is almost invariably an Ethernet LAN. Mobile nodes can roam between Access Points and seamless campus-wide coverage is possible.

Figure 307 ESS Provides Campus-Wide Coverage



Appendix F
Wireless LAN With IEEE 802.1x

As wireless networks become popular for both portable computing and corporate networks, security is now a priority.

Security Flaws with IEEE 802.11

Wireless networks based on the original IEEE 802.11 have a poor reputation for safety. The IEEE 802.11b wireless access standard, first published in 1999, was based on the MAC address. As the MAC address is sent across the wireless link in clear text, it is easy to spoof and fake. Even the WEP (Wire Equivalent Privacy) data encryption is unreliable as it can be easily decrypted with current computer speed

Deployment Issues with IEEE 802.11

User account management has become a network administrator's nightmare in a corporate environment, as the IEEE 802.11b standard does not provide any central user account management. User access control is done through manual modification of the MAC address table on the access point. Although WEP data encryption offers a form of data security, you have to reset the WEP key on the clients each time you change your WEP key on the access point.

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices.

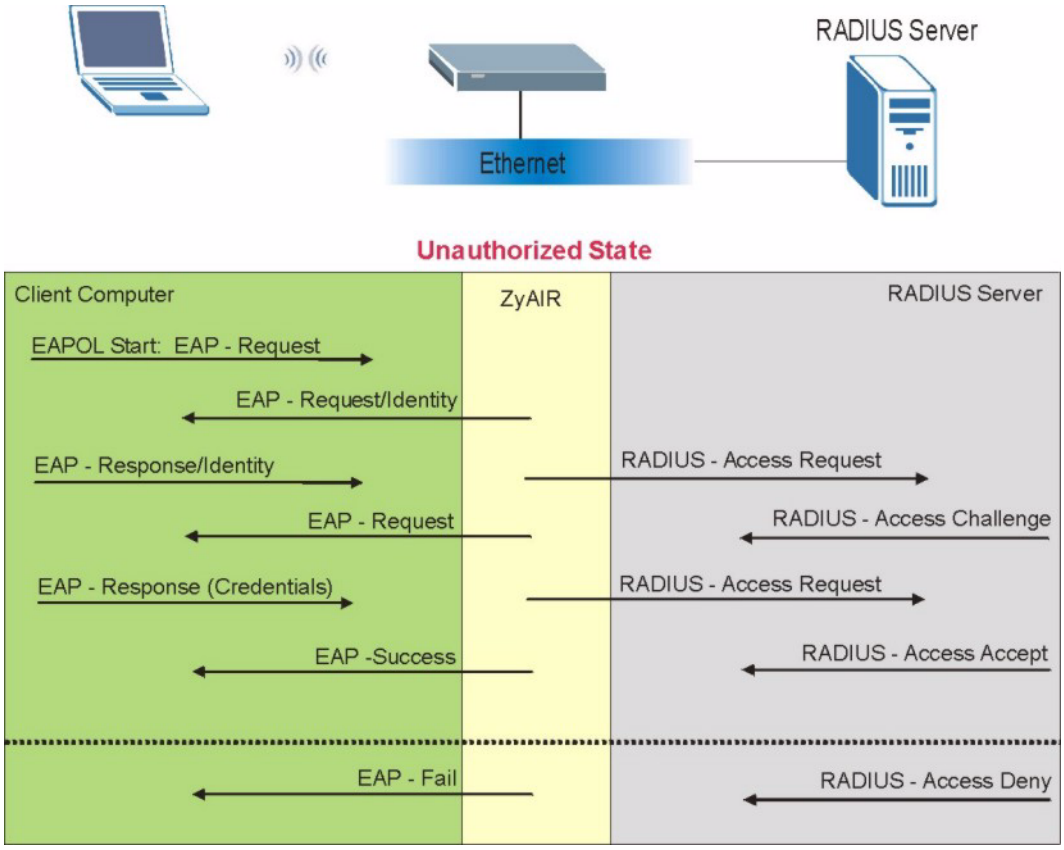
Advantages of the IEEE 802.1x

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

RADIUS Server Authentication Sequence

The following figure depicts a typical wireless network with a remote RADIUS server for user authentication using EAPOL (EAP Over LAN).

Figure 308 Sequences for EAP MD5–Challenge Authentication



Appendix G
Types of EAP Authentication

This appendix discusses three popular EAP authentication types: **EAP-MD5**, **EAP-TLS** and **EAP-TTLS**. The type of authentication you use depends on the RADIUS server or the AP. Consult your network administrator for more information.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless station. The wireless station 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless stations for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE802.1x.

Table 179 Comparison of EAP Authentication Types

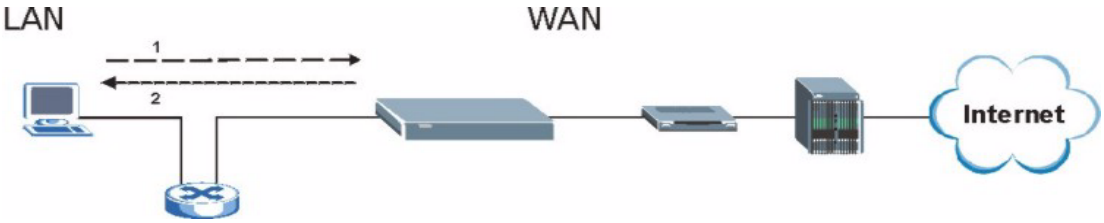
	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

Appendix H Triangle Route

The Ideal Setup

When the firewall is on, your Prestige acts as a secure gateway between your LAN and the Internet. In an ideal network topology, all incoming and outgoing network traffic passes through the Prestige to protect your LAN against attacks.

Figure 309 Ideal Setup



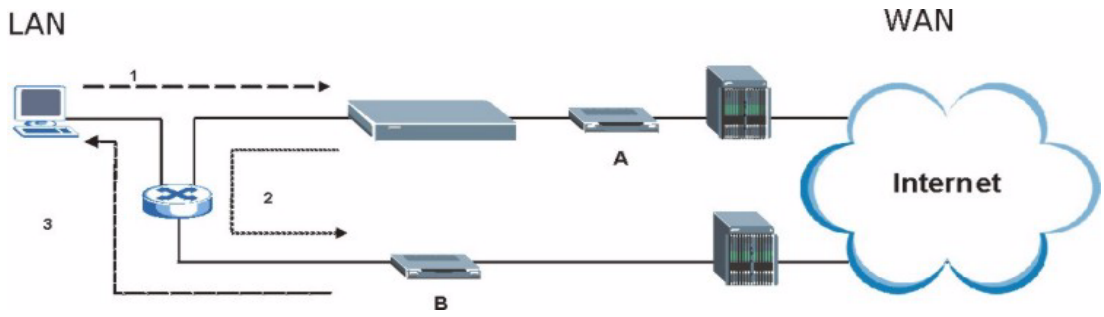
The "Triangle Route" Problem

A traffic route is a path for sending or receiving data packets between two Ethernet devices. Some companies have more than one alternate route to one or more ISPs. If the LAN and ISP(s) are in the same subnet, the "triangle route" problem may occur. The steps below describe the "triangle route" problem.

1. A computer on the LAN initiates a connection by sending out a SYN packet to a receiving server on the WAN.
2. The Prestige reroutes the SYN packet through Gateway **B** on the LAN to the WAN.
3. The reply from the WAN goes directly to the computer on the LAN without going through the Prestige.

As a result, the Prestige resets the connection, as the connection has not been acknowledged.

Figure 310 "Triangle Route" Problem



The "Triangle Route" Solutions

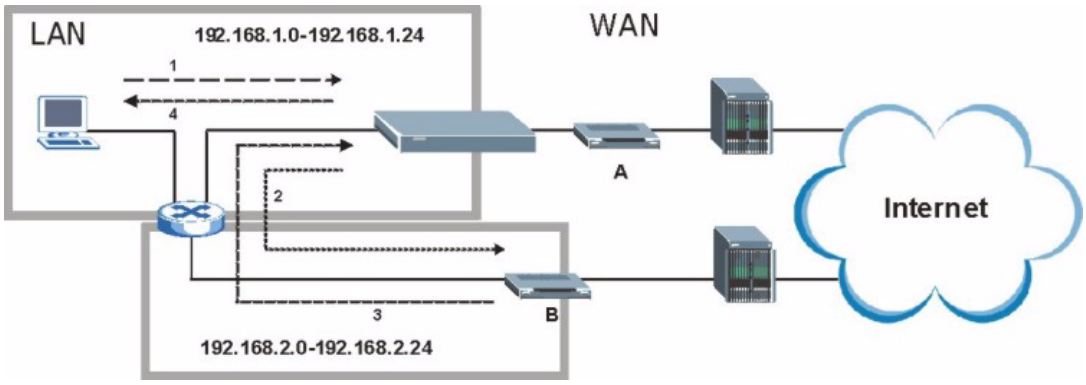
This section presents you two solutions to the "triangle route" problem.

IP Aliasing

IP alias allows you to partition your network into logical sections over the same Ethernet interface. Your Prestige supports up to three logical LAN interfaces with the Prestige being the gateway for each logical network. By putting your LAN and Gateway **B** in different subnets, all returning network traffic must pass through the Prestige to your LAN. The following steps describe such a scenario.

1. A computer on the LAN initiates a connection by sending a SYN packet to a receiving server on the WAN.
2. The Prestige reroutes the packet to Gateway B, which is in Subnet 2.
3. The reply from WAN goes through the Prestige to the computer on the LAN in Subnet 1.

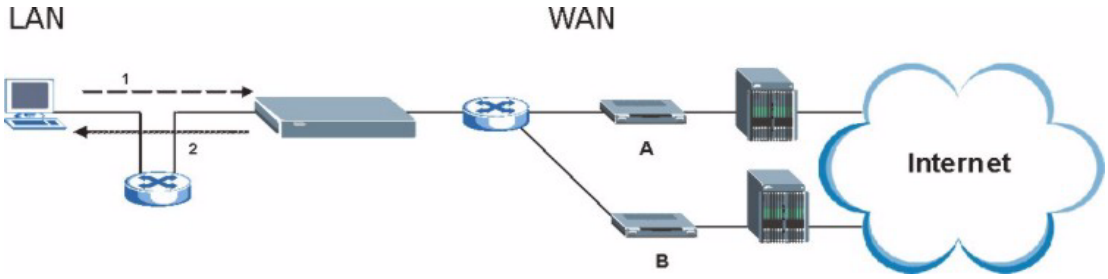
Figure 311 IP Alias



Gateways on the WAN Side

A second solution to the "triangle route" problem is to put all of your network gateways on the WAN side as the following figure shows. This ensures that all incoming network traffic passes through your Prestige to your LAN. Therefore your LAN is protected.

Figure 312 Gateways on the WAN Side



Appendix I myZyXEL.com

Introduction

myZyXEL.com is ZyXEL's online services center where you can register your ZyXEL device. You can also generate an activation key and service set key that may be needed to use device-specific feature(s).

A Note on myZyXEL.com Numbers

You need the following (unique) numbers to install and activate device-specific feature(s).

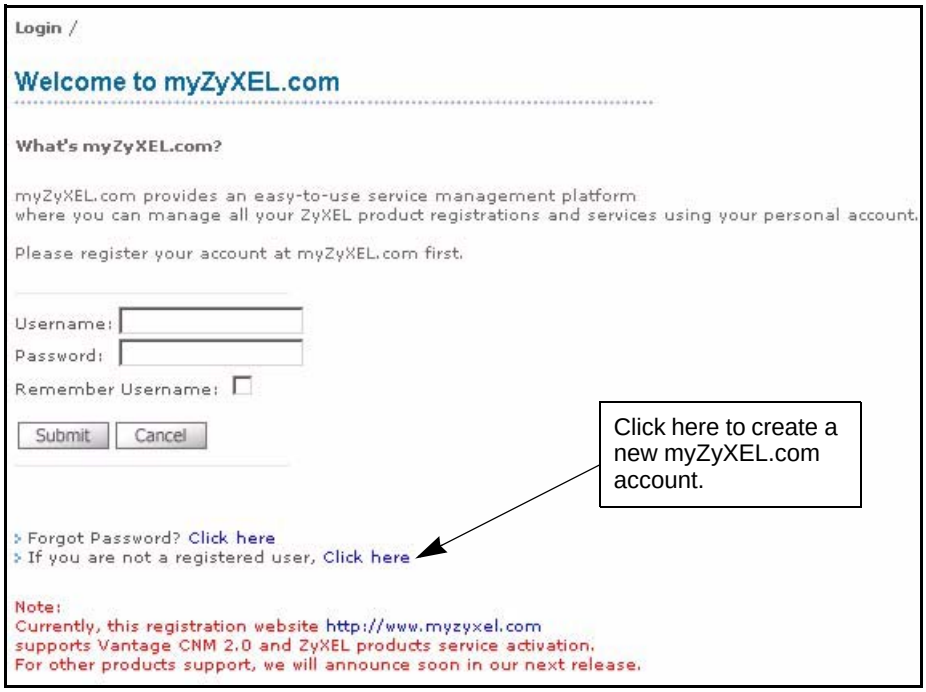
Table 180 myZyXEL.com Numbers

TYPES	DESCRIPTION
Serial Number	You need the serial number to register your ZyXEL device. Locate the serial number on your ZyXEL device.
Authentication Code	This is the MAC address of your ZyXEL device. You need this number to register your ZyXEL device at myZyXEL.com. Locate the MAC address on your ZyXEL device.

myZyXEL.com Account Login

1. Go to myZeXEL.com using your web browser.
2. Create a new account (if you don't have one already) with a user name and password by filling in an account registration form at myZyXEL.com.

Figure 313 myZyXEL.com Login Screen

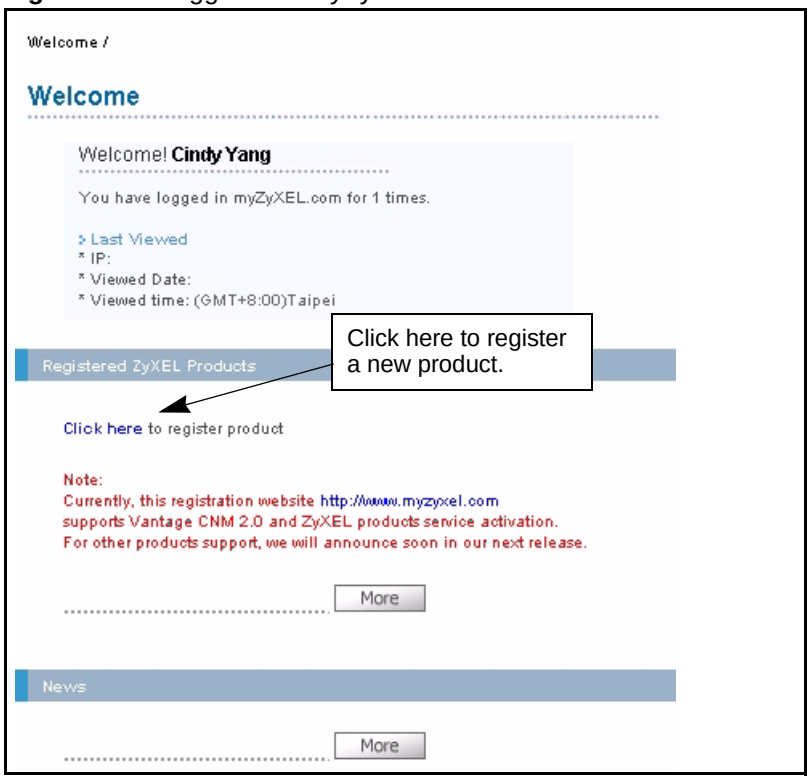


Note: You are automatically logged out of your myZyXEL.com account after five minutes of inactivity. Simply log back into your myZyXEL.com account if this happens to you.

Registering Your ZyXEL Device

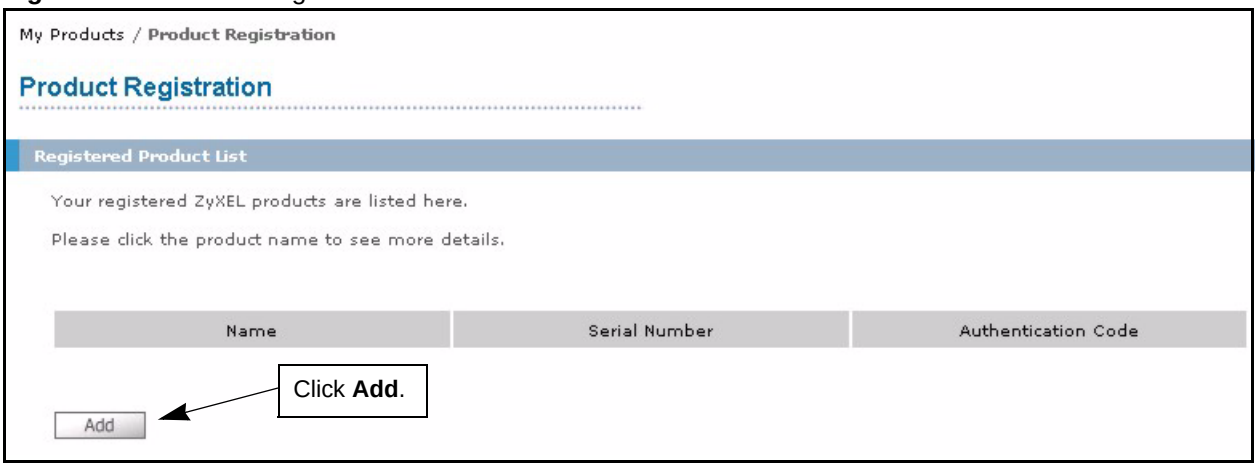
1 After you have created a myZyXEL.com account, log in and register your ZyXEL device by clicking the hyperlink as shown in the next screen.

Figure 314 Logged Into myZyXEL.com



2 Click **Add** in the next screen.

Figure 315 Product Registration



3 The **Add New Product** screen displays. Enter the produce serial number in the **Serial Number** field.

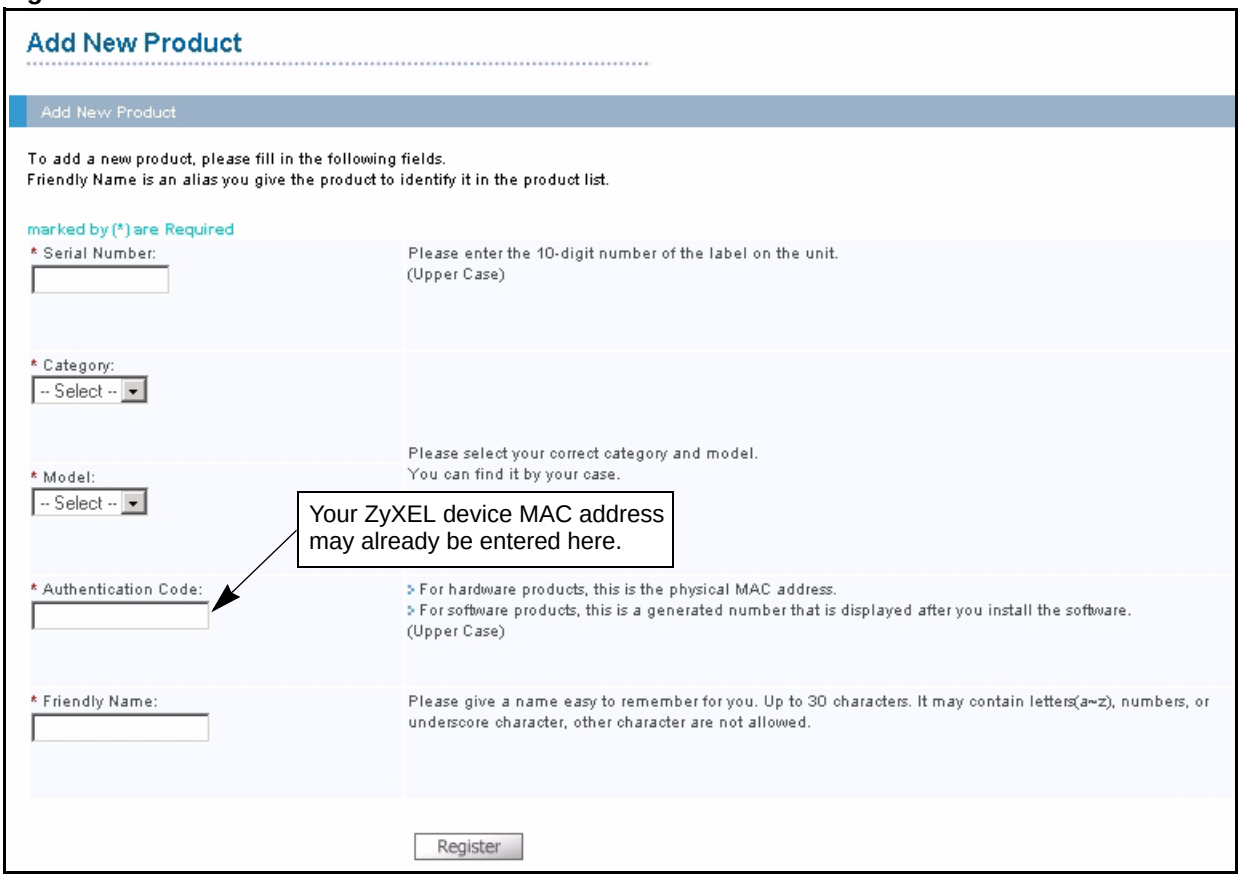
4 Your device category and model number automicatically display in the **Category** and **Model** fields respectively. Otherwise, select the correct ones from the drop-down list boxes.

5 Enter the device MAC address in the **Authentication Code** field.

6 Enter a descriptive name in the **Friendly Name** field for identification purposes.

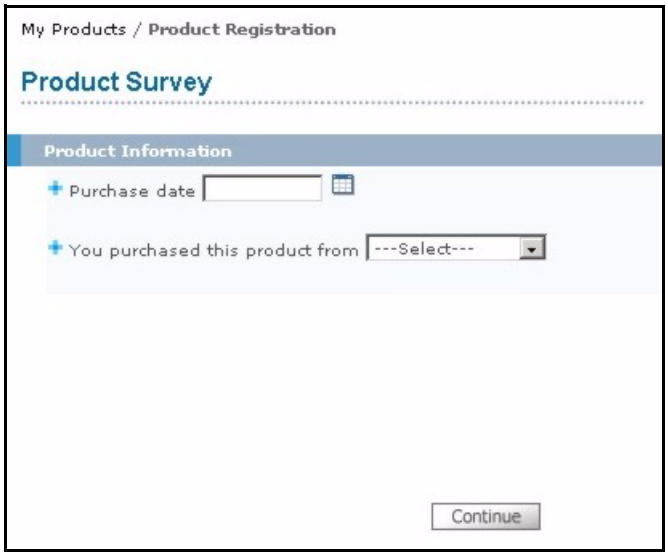
7 Click **Register**.

Figure 316 Add New Product



8 Specify the purchase information and click **Continue**.

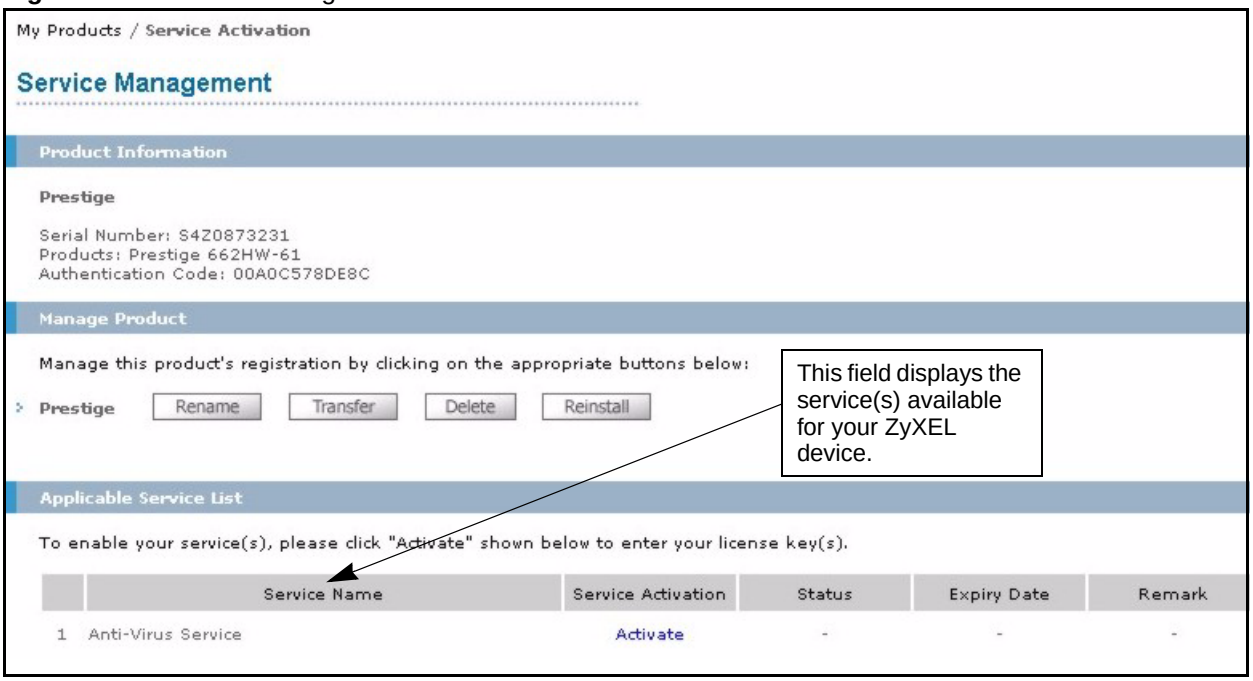
Figure 317 Product Survey



9 Click **Continue** again.

10 After you have registered your ZyXEL device, you can view its registration details in the screen shown next.

Figure 318 Service Management

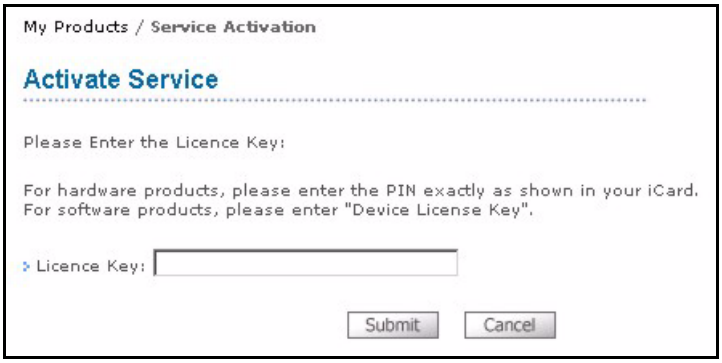


Activating a Service

The product is now registered but the related service(s) is *not* activated. You need to activate the service(s) before you can use it on your ZyXEL device.

1. Display the **Service Management** screen (see Figure 318) for your registered ZyXEL device (click **My Product** and the link for your ZyXEL device) .
2. Click **Activate** for the corresponding service to display the next screen.

Figure 319 Service Activation: Entering Licence Key



3. Enter the license key exactly as displayed on the iCard that you have purchased or that comes with your ZyXEL device. Click **Submit**.
4. A screen displays indicating that you have successfully activated a service.

Congratulations! You have successfully registered your ZyXEL device and activated a service at myZyXEL.com.

Note: You must then activate the service(s) on your ZyXEL device via its web configurator to start using the service(s).

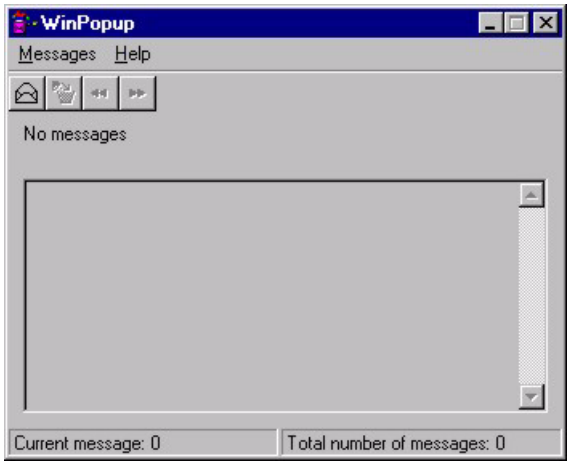
Appendix J
Windows 98/Me Requirements for Anti-Virus Packet Scan Message Display

With the anti-virus packet scan, when a virus is detected, an alert message is displayed on Miscrosoft Windows-based operation systems only.

For Windows 98/Me, you must open the **WinPopup** window in order to view real-time alert messages.

Click **Start**, **Run** and enter "winpopup" in the field provided and click **OK**. The **WinPopup** window displays as shown.

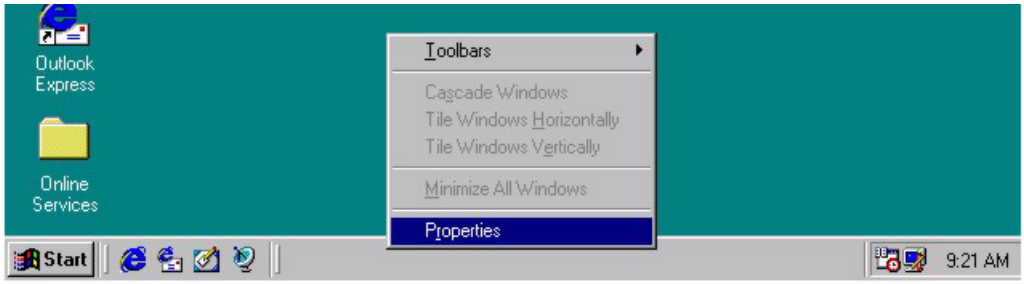
Figure 320 Windows 98: WinPopup



If you want to display the WinPopup window at startup, follow the steps below for Windows 98 (steps are similar for Windows Me).

1 Right-click on the program task bar and click **Properties**.

Figure 321 WIndows 98: Program Task Bar

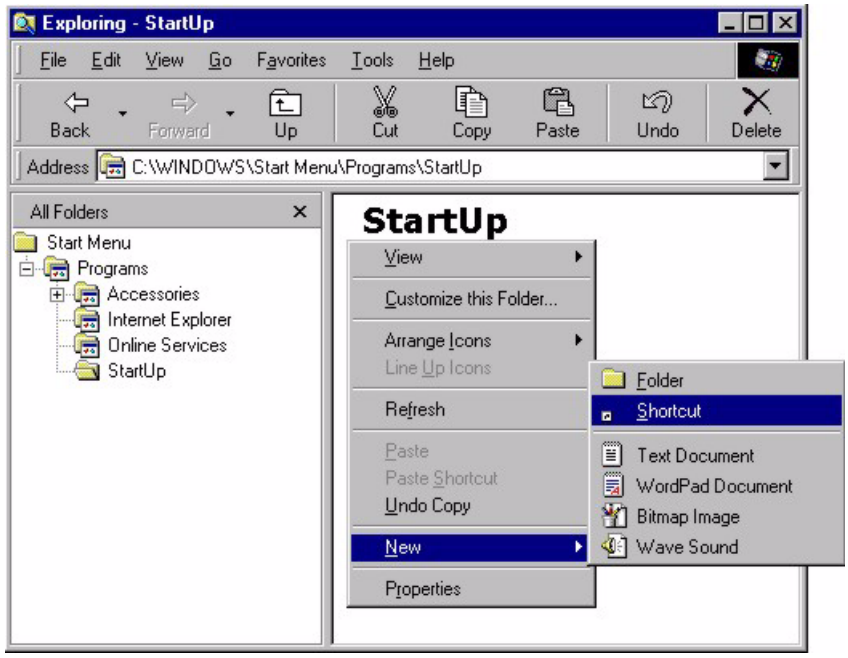


2 Click the **Start Menu Programs** tab and click **Advanced ...**.

Figure 322 Windows 98: Task Bar Properties

3 Double-click **Programs** and click **StartUp**.

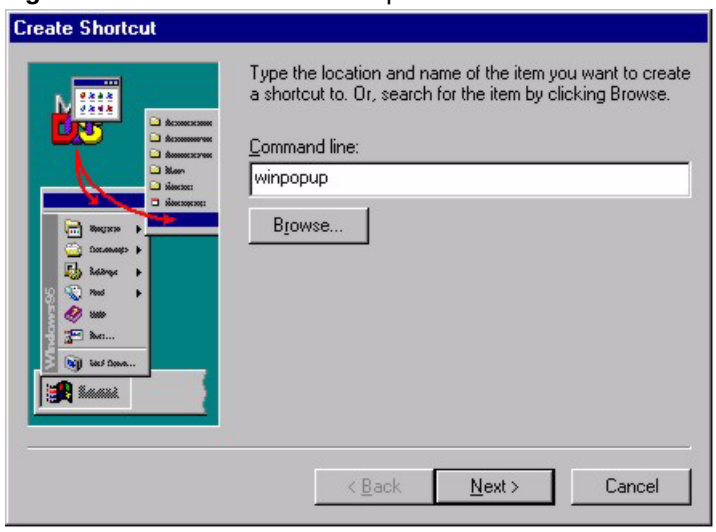
Figure 323 Windows 98: StartUp



4 Right-click in the **StartUp** pane and click **New**, **Shortcut**.

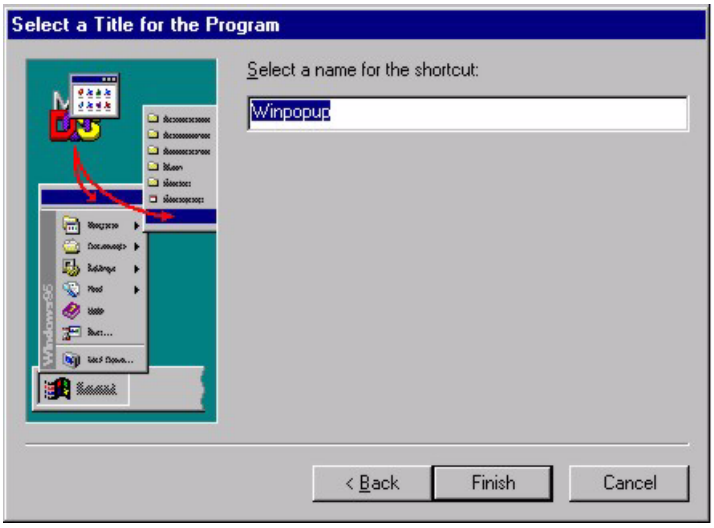
5 A **Create Shortcut** window displays. Enter "winpopup" in the **Command line** field and click **Next**.

Figure 324 Windows 98: Startup: Create Shortcut



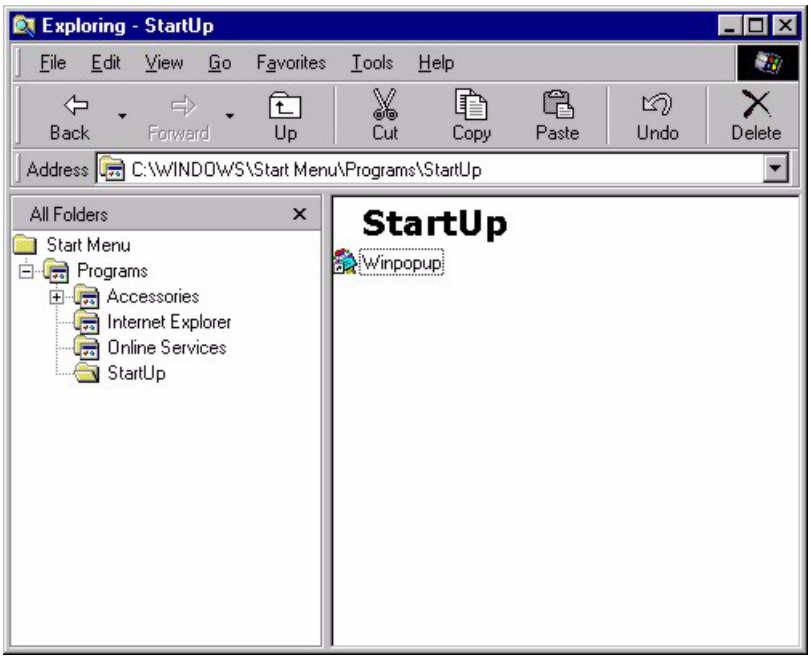
6 Accept the default or specify a name for the shortcut and click **Finish**.

Figure 325 Windows 98: Startup: Select a Title for the Program



7 A shortcut is created in the **StartUp** pane. Restart the computer when prompted.

Figure 326 Windows 98: Startup: Shortcut



Note: The WinPopup window displays after the computer finishes the startup process

Appendix K
Example Internal SPTGEN Screens

This appendix covers Prestige Internal SPTGEN screens.

Table 181 Abbreviations Used in the Example Internal SPTGEN Screens Table

ABBREVIATION	MEANING
FIN	Field Identification Number (not seen in SMT screens)
FN	Field Name
PVA	Parameter Values Allowed
INPUT	An example of what you may enter
*	Applies to the Prestige.

The following are Internal SPTGEN screens associated with the SMT screens of your Prestige.

Example Internal SPTGEN Screens Table

Table 182 Menu 1 General Setup (SMT Menu 1)

/ Menu 1 General Setup (SMT Menu 1)			
FIN	FN	PVA	INPUT
10000000 =	Configured	<0(No) | 1(Yes)>	= 0
10000001 =	System Name	<Str>	= Prestige
10000002 =	Location	<Str>	=
10000003 =	Contact Person's Name	<Str>	=
10000004 =	Route IP	<0(No) | 1(Yes)>	= 1
10000006 =	Bridge	<0(No) | 1(Yes)>	= 0

Table 183 Menu 3 (SMT Menu 1)

/ Menu 3.1 General Ethernet Setup (SMT menu 3.1)			
FIN	FN	PVA	INPUT
30100001 =	Input Protocol filters Set 1		= 2
30100002 =	Input Protocol filters Set 2		= 256
30100003 =	Input Protocol filters Set 3		= 256
30100004 =	Input Protocol filters Set 4		= 256
30100005 =	Input device filters Set 1		= 256
30100006 =	Input device filters Set 2		= 256
30100007 =	Input device filters Set 3		= 256

Table 183 Menu 3 (SMT Menu 1)

30100008 =	Input device filters Set 4		= 256
30100009 =	Output protocol filters Set 1		= 256
30100010 =	Output protocol filters Set 2		= 256
30100011 =	Output protocol filters Set 3		= 256
30100012 =	Output protocol filters Set 4		= 256
30100013 =	Output device filters Set 1		= 256
30100014 =	Output device filters Set 2		= 256
30100015 =	Output device filters Set 3		= 256
30100016 =	Output device filters Set 4		= 256
/ Menu 3.2 TCP/IP and DHCP Ethernet Setup (SMT Menu 3.2)			
FIN	FN	PVA	INPUT
30200001 =	DHCP	<0(None) | 1(Server) | 2(Relay)>	= 0
30200002 =	Client IP Pool Starting Address		= 192.168.1.33
30200003 =	Size of Client IP Pool		= 32
30200004 =	Primary DNS Server		= 0.0.0.0
30200005 =	Secondary DNS Server		= 0.0.0.0
30200006 =	Remote DHCP Server		= 0.0.0.0
30200008 =	IP Address		= 172.21.2.200
30200009 =	IP Subnet Mask		= 16
30200010 =	RIP Direction	<0(None) | 1(Both) | 2(In Only) | 3(Out Only)>	= 0
30200011 =	Version	<0(Rip-1) | 1(Rip-2B) |2(Rip-2M)>	= 0
30200012 =	Multicast	<0(IGMP-v2) | 1(IGMP-v1) | 2(None)>	= 2
30200013 =	IP Policies Set 1 (1~12)		= 256
30200014 =	IP Policies Set 2 (1~12)		= 256
30200015 =	IP Policies Set 3 (1~12)		= 256
30200016 =	IP Policies Set 4 (1~12)		= 256
/ Menu 3.2.1 IP Alias Setup (SMT Menu 3.2.1)			
FIN	FN	PVA	INPUT
30201001 =	IP Alias 1	<0(No) | 1(Yes)>	= 0
30201002 =	IP Address		= 0.0.0.0
30201003 =	IP Subnet Mask		= 0

Table 183 Menu 3 (SMT Menu 1)

30201004 =	RIP Direction	<0(None) | 1(Both) | 2(In Only) | 3(Out Only)>	= 0
30201005 =	Version	<0(Rip-1) | 1(Rip-2B) |2(Rip-2M)>	= 0
30201006 =	IP Alias #1 Incoming protocol filters Set 1		= 256
30201007 =	IP Alias #1 Incoming protocol filters Set 2		= 256
30201008 =	IP Alias #1 Incoming protocol filters Set 3		= 256
30201009 =	IP Alias #1 Incoming protocol filters Set 4		= 256
30201010 =	IP Alias #1 Outgoing protocol filters Set 1		= 256
30201011 =	IP Alias #1 Outgoing protocol filters Set 2		= 256
30201012 =	IP Alias #1 Outgoing protocol filters Set 3		= 256
30201013 =	IP Alias #1 Outgoing protocol filters Set 4		= 256
30201014 =	IP Alias 2 <0(No) | 1(Yes)>		= 0
30201015 =	IP Address		= 0.0.0.0
30201016 =	IP Subnet Mask		= 0
30201017 =	RIP Direction	<0(None) | 1(Both) | 2(In Only) | 3(Out Only)>	= 0
30201018 =	Version	<0(Rip-1) | 1(Rip-2B) |2(Rip-2M)>	= 0
30201019 =	IP Alias #2 Incoming protocol filters Set 1		= 256
30201020 =	IP Alias #2 Incoming protocol filters Set 2		= 256
30201021 =	IP Alias #2 Incoming protocol filters Set 3		= 256
30201022 =	IP Alias #2 Incoming protocol filters Set 4		= 256
30201023 =	IP Alias #2 Outgoing protocol filters Set 1		= 256
30201024 =	IP Alias #2 Outgoing protocol filters Set 2		= 256
30201025 =	IP Alias #2 Outgoing protocol filters Set 3		= 256

Table 183 Menu 3 (SMT Menu 1)

30201026 =	IP Alias #2 Outgoing protocol filters Set 4		= 256
*/ Menu 3.5 Wireless LAN Setup (SMT Menu 3.5)			
30500001 =	ESSID		Wireless
30500002 =	Hide ESSID	<0(No) | 1(Yes)>	= 0
30500003 =	Channel ID	<1|2|3|4|5|6|7|8|9|10|11|12|13>	= 1
30500004 =	RTS Threshold	<0 ~ 2432>	= 2432
30500005 =	FRAG. Threshold	<256 ~ 2432>	= 2432
30500006 =	WEP	<0(DISABLE) | 1(64-bit WEP) | 2(128-bit WEP)>	= 0
30500007 =	Default Key	<1|2|3|4>	= 0
30500008 =	WEP Key1		=
30500009 =	WEP Key2		=
30500010 =	WEP Key3		=
30500011 =	WEP Key4		=
*/ MENU 3.5.1 WLAN MAC ADDRESS FILTER (SMT MENU 3.5.1)			
30501001 =	Mac Filter Active	<0(No) | 1(Yes)>	= 0
30501002 =	Filter Action	<0(Allow) | 1(Deny)>	= 0
30501003 =	Address 1		= 00:00:00:00:00:00
30501004 =	Address 2		= 00:00:00:00:00:00
30501005 =	Address 3		= 00:00:00:00:00:00
Continued	…		…
30501034 =	Address 32		= 00:00:00:00:00:00

Table 184 Menu 4 Internet Access Setup (SMT Menu 4)

/ Menu 4 Internet Access Setup (SMT Menu 4)			
FIN	FN	PVA	INPUT
40000000 =	Configured	<0(No) | 1(Yes)>	= 1
40000001 =	ISP	<0(No) | 1(Yes)>	= 1
40000002 =	Active	<0(No) | 1(Yes)>	= 1
40000003 =	ISP's Name		= ChangeMe
40000004 =	Encapsulation	<2(PPPOE) | 3(RFC 1483)| 4(PPPoA)| 5(ENET ENCAP)>	= 2
40000005 =	Multiplexing	<1(LLC-based) | 2(VC-based)	= 1
40000006 =	VPI #		= 0
40000007 =	VCI #		= 35
40000008 =	Service Name	<Str>	= any
40000009 =	My Login	<Str>	= test@pqa
40000010 =	My Password	<Str>	= 1234
40000011 =	Single User Account	<0(No) | 1(Yes)>	= 1
40000012 =	IP Address Assignment	<0(Static)|1(Dynamic)>	= 1
40000013 =	IP Address		= 0.0.0.0
40000014 =	Remote IP address		= 0.0.0.0
40000015 =	Remote IP subnet mask		= 0
40000016 =	ISP incoming protocol filter set 1		= 6
40000017 =	ISP incoming protocol filter set 2		= 256
40000018 =	ISP incoming protocol filter set 3		= 256
40000019 =	ISP incoming protocol filter set 4		= 256
40000020 =	ISP outgoing protocol filter set 1		= 256
40000021 =	ISP outgoing protocol filter set 2		= 256
40000022 =	ISP outgoing protocol filter set 3		= 256
40000023 =	ISP outgoing protocol filter set 4		= 256
40000024 =	ISP PPPoE idle timeout		= 0
40000025 =	Route IP	<0(No) | 1(Yes)>	= 1
40000026 =	Bridge	<0(No) | 1(Yes)>	= 0

Table 184 Menu 4 Internet Access Setup (SMT Menu 4)

40000027 =	ATM QoS Type	<0(CBR) | (1 (UBR)>	= 1
40000028 =	Peak Cell Rate (PCR)		= 0
40000029 =	Sustain Cell Rate (SCR)		= 0
40000030 =	Maximum Burst Size(MBS)		= 0
40000031=	RIP Direction	<0(None) | 1(Both) | 2(In Only) | 3(Out Only)>	= 0
40000032=	RIP Version	<0(Rip-1) | 1(Rip-2B) |2(Rip-2M)>	= 0
40000033=	Nailed-up Connection	<0(No) |1(Yes)>	= 0

Table 185 Menu 12(SMT Menu 12)

/ Menu 12.1.1 IP Static Route Setup (SMT Menu 12.1.1)			
FIN	FN	PVA	INPUT
120101001 =	IP Static Route set #1, Name	<Str>	=
120101002 =	IP Static Route set #1, Active	<0(No) |1(Yes)>	= 0
120101003 =	IP Static Route set #1, Destination IP address		= 0.0.0.0
120101004 =	IP Static Route set #1, Destination IP subnetmask		= 0
120101005 =	IP Static Route set #1, Gateway		= 0.0.0.0
120101006 =	IP Static Route set #1, Metric		= 0
120101007 =	IP Static Route set #1, Private	<0(No) |1(Yes)>	= 0
/ Menu 12.1.2 IP Static Route Setup (SMT Menu 12.1.2)			
FIN	FN	PVA	INPUT
120102001 =	IP Static Route set #2, Name		=
120102002 =	IP Static Route set #2, Active	<0(No) |1(Yes)>	= 0
120102003 =	IP Static Route set #2, Destination IP address		= 0.0.0.0
120102004 =	IP Static Route set #2, Destination IP subnetmask		= 0
120102005 =	IP Static Route set #2, Gateway		= 0.0.0.0
120102006 =	IP Static Route set #2, Metric		= 0
120102007 =	IP Static Route set #2, Private	<0(No) |1(Yes)>	= 0
/ Menu 12.1.3 IP Static Route Setup (SMT Menu 12.1.3)			
FIN	FN	PVA	INPUT
120103001 =	IP Static Route set #3, Name	<Str>	=

Table 185 Menu 12(SMT Menu 12) (continued)

120103002 =	IP Static Route set #3, Active	<0(No) |1(Yes)>	= 0
120103003 =	IP Static Route set #3, Destination IP address		= 0.0.0.0
120103004 =	IP Static Route set #3, Destination IP subnetmask		= 0
120103005 =	IP Static Route set #3, Gateway		= 0.0.0.0
120103006 =	IP Static Route set #3, Metric		= 0
120103007 =	IP Static Route set #3, Private	<0(No) |1(Yes)>	= 0
/ Menu 12.1.4 IP Static Route Setup (SMT Menu 12.1.4)			
FIN	FN	PVA	INPUT
120104001 =	IP Static Route set #4, Name	<Str>	=
120104002 =	IP Static Route set #4, Active	<0(No) |1(Yes)>	= 0
120104003 =	IP Static Route set #4, Destination IP address		= 0.0.0.0
120104004 =	IP Static Route set #4, Destination IP subnetmask		= 0
120104005 =	IP Static Route set #4, Gateway		= 0.0.0.0
120104006 =	IP Static Route set #4, Metric		= 0
120104007 =	IP Static Route set #4, Private	<0(No) |1(Yes)>	= 0
/ Menu 12.1.5 IP Static Route Setup (SMT Menu 12.1.5)			
FIN	FN	PVA	INPUT
120105001 =	IP Static Route set #5, Name	<Str>	=
120105002 =	IP Static Route set #5, Active	<0(No) |1(Yes)>	= 0
120105003 =	IP Static Route set #5, Destination IP address		= 0.0.0.0
120105004 =	IP Static Route set #5, Destination IP subnetmask		= 0
120105005 =	IP Static Route set #5, Gateway		= 0.0.0.0
120105006 =	IP Static Route set #5, Metric		= 0
120105007 =	IP Static Route set #5, Private	<0(No) |1(Yes)>	= 0
/ Menu 12.1.6 IP Static Route Setup (SMT Menu 12.1.6)			
FIN	FN	PVA	INPUT
120106001 =	IP Static Route set #6, Name	<Str>	=
120106002 =	IP Static Route set #6, Active	<0(No) |1(Yes)>	= 0
120106003 =	IP Static Route set #6, Destination IP address		= 0.0.0.0
120106004 =	IP Static Route set #6, Destination IP subnetmask		= 0
120106005 =	IP Static Route set #6, Gateway		= 0.0.0.0
120106006 =	IP Static Route set #6, Metric		= 0
120106007 =	IP Static Route set #6, Private	<0(No) |1(Yes)>	= 0
/ Menu 12.1.7 IP Static Route Setup (SMT Menu 12.1.7)			

Table 185 Menu 12(SMT Menu 12) (continued)

FIN	FN	PVA	INPUT
120107001 =	IP Static Route set #7, Name	<Str>	=
120107002 =	IP Static Route set #7, Active	<0(No) |1(Yes)>	= 0
120107003 =	IP Static Route set #7, Destination IP address		= 0.0.0.0
120107004 =	IP Static Route set #7, Destination IP subnetmask		= 0
120107005 =	IP Static Route set #7, Gateway		= 0.0.0.0
120107006 =	IP Static Route set #7, Metric		= 0
120107007 =	IP Static Route set #7, Private	<0(No) |1(Yes)>	= 0
/ Menu 12.1.8 IP Static Route Setup (SMT Menu 12.1.8)			
FIN	FN	PVA	INPUT
120108001 =	IP Static Route set #8, Name	<Str>	=
120108002 =	IP Static Route set #8, Active	<0(No) |1(Yes)>	= 0
120108003 =	IP Static Route set #8, Destination IP address		= 0.0.0.0
120108004 =	IP Static Route set #8, Destination IP subnetmask		= 0
120108005 =	IP Static Route set #8, Gateway		= 0.0.0.0
120108006 =	IP Static Route set #8, Metric		= 0
120108007 =	IP Static Route set #8, Private	<0(No) |1(Yes)>	= 0
*/ Menu 12.1.9 IP Static Route Setup (SMT Menu 12.1.9)			
FIN	FN	PVA	INPUT
120109001 =	IP Static Route set #9, Name	<Str>	=
120109002 =	IP Static Route set #9, Active	<0(No) |1(Yes)>	= 0
120109003 =	IP Static Route set #9, Destination IP address		= 0.0.0.0
120109004 =	IP Static Route set #9, Destination IP subnetmask		= 0
120109005 =	IP Static Route set #9, Gateway		= 0.0.0.0
120109006 =	IP Static Route set #9, Metric		= 0
120109007 =	IP Static Route set #9, Private	<0(No) |1(Yes)>	= 0
*/ Menu 12.1.10 IP Static Route Setup (SMT Menu 12.1.10)			
FIN	FN	PVA	INPUT
120110001 =	IP Static Route set #10, Name		=
120110002 =	IP Static Route set #10, Active	<0(No) |1(Yes)>	= 0
120110003 =	IP Static Route set #10, Destination IP address		= 0.0.0.0
120110004 =	IP Static Route set #10, Destination IP subnetmask		= 0
120110005 =	IP Static Route set #10, Gateway		= 0.0.0.0
120110006 =	IP Static Route set #10, Metric		= 0

Table 185 Menu 12(SMT Menu 12) (continued)

120110007 =	IP Static Route set #10, Private	<0(No) |1(Yes)>	= 0
*/ Menu 12.1.11 IP Static Route Setup (SMT Menu 12.1.11)			
FIN	FN	PVA	INPUT
120111001 =	IP Static Route set #11, Name	<Str>	=
120111002 =	IP Static Route set #11, Active	<0(No) |1(Yes)>	= 0
120111003 =	IP Static Route set #11, Destination IP address		= 0.0.0.0
120111004 =	IP Static Route set #11, Destination IP subnetmask		= 0
120111005 =	IP Static Route set #11, Gateway		= 0.0.0.0
120111006 =	IP Static Route set #11, Metric		= 0
120111007 =	IP Static Route set #11, Private	<0(No) |1(Yes)>	= 0
*/ Menu 12.1.12 IP Static Route Setup (SMT Menu 12.1.12)			
FIN	FN	PVA	INPUT
120112001 =	IP Static Route set #12, Name	<Str>	=
120112002 =	IP Static Route set #12, Active	<0(No) |1(Yes)>	= 0
120112003 =	IP Static Route set #12, Destination IP address		= 0.0.0.0
120112004 =	IP Static Route set #12, Destination IP subnetmask		= 0
120112005 =	IP Static Route set #12, Gateway		= 0.0.0.0
120112006 =	IP Static Route set #12, Metric		= 0
120112007 =	IP Static Route set #12, Private	<0(No) |1(Yes)>	= 0
*/ Menu 12.1.13 IP Static Route Setup (SMT Menu 12.1.13)			
FIN	FN	PVA	INPUT
120113001 =	IP Static Route set #13, Name	<Str>	=
120113002 =	IP Static Route set #13, Active	<0(No) |1(Yes)>	= 0
120113003 =	IP Static Route set #13, Destination IP address		= 0.0.0.0
120113004 =	IP Static Route set #13, Destination IP subnetmask		= 0
120113005 =	IP Static Route set #13, Gateway		= 0.0.0.0
120113006 =	IP Static Route set #13, Metric		= 0
120113007 =	IP Static Route set #13, Private	<0(No) |1(Yes)>	= 0
*/ Menu 12.1.14 IP Static Route Setup (SMT Menu 12.1. 14)			
FIN	FN	PVA	INPUT
120114001 =	IP Static Route set #14, Name	<Str>	=
120114002 =	IP Static Route set #14, Active	<0(No) |1(Yes)>	= 0
120114003 =	IP Static Route set #14, Destination IP address		= 0.0.0.0

Table 185 Menu 12(SMT Menu 12) (continued)

120114004 =	IP Static Route set #14, Destination IP subnetmask		= 0
120114005 =	IP Static Route set #14, Gateway		= 0.0.0.0
120114006 =	IP Static Route set #14, Metric		= 0
120114007 =	IP Static Route set #14, Private	<0(No) |1(Yes)>	= 0
*/ Menu 12.1.15 IP Static Route Setup (SMT Menu 12.1. 15)			
FIN	FN	PVA	INPUT
120115001 =	IP Static Route set #15, Name	<Str>	=
120115002 =	IP Static Route set #15, Active	<0(No) |1(Yes)>	= 0
120115003 =	IP Static Route set #15, Destination IP address		= 0.0.0.0
120115004 =	IP Static Route set #15, Destination IP subnetmask		= 0
120115005 =	IP Static Route set #15, Gateway		= 0.0.0.0
120115006 =	IP Static Route set #15, Metric		= 0
120115007 =	IP Static Route set #15, Private	<0(No) |1(Yes)>	= 0
*/ Menu 12.1.16 IP Static Route Setup (SMT Menu 12.1. 16)			
FIN	FN	PVA	INPUT
120116001 =	IP Static Route set #16, Name	<Str>	=
120116002 =	IP Static Route set #16, Active	<0(No) |1(Yes)>	= 0
120116003 =	IP Static Route set #16, Destination IP address		= 0.0.0.0
120116004 =	IP Static Route set #16, Destination IP subnetmask		= 0
120116005 =	IP Static Route set #16, Gateway		= 0.0.0.0
120116006 =	IP Static Route set #16, Metric		= 0
120116007 =	IP Static Route set #16, Private	<0(No) |1(Yes)>	= 0

Table 186 Menu 15 SUA Server Setup (SMT Menu 15)

/ Menu 15 SUA Server Setup (SMT Menu 15)			
FIN	FN	PVA	INPUT
150000001 =	SUA Server IP address for default port		= 0.0.0.0
150000002 =	SUA Server #2 Active	<0(No) | 1(Yes)>	= 0
150000003 =	SUA Server #2 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000004 =	SUA Server #2 Port Start		= 0
150000005 =	SUA Server #2 Port End		= 0
150000006 =	SUA Server #2 Local IP address		= 0.0.0.0

Table 186 Menu 15 SUA Server Setup (SMT Menu 15) (continued)

150000007 =	SUA Server #3 Active	<0(No) | 1(Yes)>	= 0
150000008 =	SUA Server #3 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000009 =	SUA Server #3 Port Start		= 0
150000010 =	SUA Server #3 Port End		= 0
150000011 =	SUA Server #3 Local IP address		= 0.0.0.0
150000012 =	SUA Server #4 Active	<0(No) | 1(Yes)>	= 0
150000013 =	SUA Server #4 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000014 =	SUA Server #4 Port Start		= 0
150000015 =	SUA Server #4 Port End		= 0
150000016 =	SUA Server #4 Local IP address		= 0.0.0.0
150000017 =	SUA Server #5 Active	<0(No) | 1(Yes)>	= 0
150000018 =	SUA Server #5 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000019 =	SUA Server #5 Port Start		= 0
150000020 =	SUA Server #5 Port End		= 0
150000021 =	SUA Server #5 Local IP address		= 0.0.0.0
150000022 =	SUA Server #6 Active	<0(No) | 1(Yes)> = 0	= 0
150000023 =	SUA Server #6 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000024 =	SUA Server #6 Port Start		= 0
150000025 =	SUA Server #6 Port End		= 0
150000026 =	SUA Server #6 Local IP address		= 0.0.0.0
150000027 =	SUA Server #7 Active	<0(No) | 1(Yes)>	= 0
150000028 =	SUA Server #7 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0.0.0.0
150000029 =	SUA Server #7 Port Start		= 0
150000030 =	SUA Server #7 Port End		= 0
150000031 =	SUA Server #7 Local IP address		= 0.0.0.0
150000032 =	SUA Server #8 Active	<0(No) | 1(Yes)>	= 0
150000033 =	SUA Server #8 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000034 =	SUA Server #8 Port Start		= 0
150000035 =	SUA Server #8 Port End		= 0
150000036 =	SUA Server #8 Local IP address		= 0.0.0.0
150000037 =	SUA Server #9 Active	<0(No) | 1(Yes)>	= 0
150000038 =	SUA Server #9 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000039 =	SUA Server #9 Port Start		= 0
150000040 =	SUA Server #9 Port End		= 0

Table 186 Menu 15 SUA Server Setup (SMT Menu 15) (continued)

150000041 =	SUA Server #9 Local IP address		= 0.0.0.0
150000042	= SUA Server #10 Active	<0(No) | 1(Yes)>	= 0
150000043 =	SUA Server #10 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000044 =	SUA Server #10 Port Start		= 0
150000045 =	SUA Server #10 Port End		= 0
150000046 =	SUA Server #10 Local IP address		= 0.0.0.0
150000047 =	SUA Server #11 Active	<0(No) | 1(Yes)>	= 0
150000048 =	SUA Server #11 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000049 =	SUA Server #11 Port Start		= 0
150000050 =	SUA Server #11 Port End		= 0
150000051 =	SUA Server #11 Local IP address		= 0.0.0.0
150000052 =	SUA Server #12 Active	<0(No) | 1(Yes)>	= 0
150000053 =	SUA Server #12 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000054 =	SUA Server #12 Port Start		= 0
150000055 =	SUA Server #12 Port End		= 0
150000056 =	SUA Server #12 Local IP address		= 0.0.0.0
/ Menu 21 Filter set #1 (SMT Menu 21)			
FIN	FN	PVA	INPUT
210100001 =	Filter Set 1, Name	<Str>	=

Table 187 Menu 21.1 Filter Set #1 (SMT Menu 21.1)

/ Menu 21.1.1.1 Filter set #1, rule #1 (SMT Menu 21.1.1.1)			
FIN	FN	PVA	INPUT
210101001 =	IP Filter Set 1,Rule 1 Type	<2(TCP/IP)>	= 2
210101002 =	IP Filter Set 1,Rule 1 Active	<0(No)|1(Yes)>	= 1
210101003 =	IP Filter Set 1,Rule 1 Protocol		= 6
210101004 =	IP Filter Set 1,Rule 1 Dest IP address		= 0.0.0.0
210101005 =	IP Filter Set 1,Rule 1 Dest Subnet Mask		= 0
210101006 =	IP Filter Set 1,Rule 1 Dest Port		= 137
210101007 =	IP Filter Set 1,Rule 1 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210101008 =	IP Filter Set 1,Rule 1 Src IP address		= 0.0.0.0
210101009 =	IP Filter Set 1,Rule 1 Src Subnet Mask		= 0
210101010 =	IP Filter Set 1,Rule 1 Src Port		= 0

Table 187 Menu 21.1 Filter Set #1 (SMT Menu 21.1) (continued)

210101011 =	IP Filter Set 1,Rule 1 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210101013 =	IP Filter Set 1,Rule 1 Act Match	<1(check next)|2(forward)|3(drop)>	= 3
210101014 =	IP Filter Set 1,Rule 1 Act Not Match	<1(check next)|2(forward)|3(drop)>	= 1
/ Menu 21.1.1.2 set #1, rule #2 (SMT Menu 21.1.1.2)			
FIN	FN	PVA	INPUT
210102001 =	IP Filter Set 1,Rule 2 Type	<2(TCP/IP)>	= 2
210102002 =	IP Filter Set 1,Rule 2 Active	<0(No)|1(Yes)>	= 1
210102003 =	IP Filter Set 1,Rule 2 Protocol		= 6
210102004 =	IP Filter Set 1,Rule 2 Dest IP address		= 0.0.0.0
210102005 =	IP Filter Set 1,Rule 2 Dest Subnet Mask		= 0
210102006 =	IP Filter Set 1,Rule 2 Dest Port		= 138
210102007 =	IP Filter Set 1,Rule 2 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210102008 =	IP Filter Set 1,Rule 2 Src IP address		= 0.0.0.0
210102009 =	IP Filter Set 1,Rule 2 Src Subnet Mask		= 0
210102010 =	IP Filter Set 1,Rule 2 Src Port		= 0
210102011 =	IP Filter Set 1,Rule 2 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210102013 =	IP Filter Set 1,Rule 2 Act Match	<1(check next)|2(forward)|3(drop)>	= 3
210102014 =	IP Filter Set 1,Rule 2 Act Not Match	<1(check next)|2(forward)|3(drop)>	= 1
/ Menu 21.1.1.3 set #1, rule #3 (SMT Menu 21.1.1.3)			
FIN	FN	PVA	INPUT
210103001 =	IP Filter Set 1,Rule 3 Type	<2(TCP/IP)>	= 2
210103002 =	IP Filter Set 1,Rule 3 Active	<0(No)|1(Yes)>	= 1
210103003 =	IP Filter Set 1,Rule 3 Protocol		= 6
210103004 =	IP Filter Set 1,Rule 3 Dest IP address		= 0.0.0.0
210103005 =	IP Filter Set 1,Rule 3 Dest Subnet Mask		= 0
210103006 =	IP Filter Set 1,Rule 3 Dest Port		= 139

Table 187 Menu 21.1 Filter Set #1 (SMT Menu 21.1) (continued)

210103007 =	IP Filter Set 1,Rule 3 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210103008 =	IP Filter Set 1,Rule 3 Src IP address		= 0.0.0.0
210103009 =	IP Filter Set 1,Rule 3 Src Subnet Mask		= 0
210103010 =	IP Filter Set 1,Rule 3 Src Port		= 0
210103011 =	IP Filter Set 1,Rule 3 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210103013 =	IP Filter Set 1,Rule 3 Act Match	<1(check next)|2(forward)|3(drop)	= 3
210103014 =	IP Filter Set 1,Rule 3 Act Not Match	<1(check next)|2(forward)|3(drop)	= 1
/ Menu 21.1.1.4 set #1, rule #4 (SMT Menu 21.1.1.4)			
FIN	FN	PVA	INPUT
210104001 =	IP Filter Set 1,Rule 4 Type	<2(TCP/IP)>	= 2
210104002 =	IP Filter Set 1,Rule 4 Active	<0(No)|1(Yes)>	= 1
210104003 =	IP Filter Set 1,Rule 4 Protocol		= 17
210104004 =	IP Filter Set 1,Rule 4 Dest IP address		= 0.0.0.0
210104005 =	IP Filter Set 1,Rule 4 Dest Subnet Mask		= 0
210104006 =	IP Filter Set 1,Rule 4 Dest Port		= 137
210104007 =	IP Filter Set 1,Rule 4 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210104008 =	IP Filter Set 1,Rule 4 Src IP address		= 0.0.0.0
210104009 =	IP Filter Set 1,Rule 4 Src Subnet Mask		= 0
210104010 =	IP Filter Set 1,Rule 4 Src Port		= 0
210104011 =	IP Filter Set 1,Rule 4 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210104013 =	IP Filter Set 1,Rule 4 Act Match	<1(check next)|2(forward) |3(drop)	= 3
210104014 =	IP Filter Set 1,Rule 4 Act Not Match	<1(check next)|2(forward)|3(drop)	= 1
/ Menu 21.1.1.5 set #1, rule #5 (SMT Menu 21.1.1.5)			
FIN	FN	PVA	INPUT
210105001 =	IP Filter Set 1,Rule 5 Type	<2(TCP/IP)>	= 2

Table 187 Menu 21.1 Filter Set #1 (SMT Menu 21.1) (continued)

210105002 =	IP Filter Set 1,Rule 5 Active	<0(No)|1(Yes)>	= 1
210105003 =	IP Filter Set 1,Rule 5 Protocol		= 17
210105004 =	IP Filter Set 1,Rule 5 Dest IP address		= 0.0.0.0
210105005 =	IP Filter Set 1,Rule 5 Dest Subnet Mask		= 0
210105006 =	IP Filter Set 1,Rule 5 Dest Port		= 138
210105007 =	IP Filter Set 1,Rule 5 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210105008 =	IP Filter Set 1,Rule 5 Src IP Address		= 0.0.0.0
210105009 =	IP Filter Set 1,Rule 5 Src Subnet Mask		= 0
210105010 =	IP Filter Set 1,Rule 5 Src Port		= 0
210105011 =	IP Filter Set 1,Rule 5 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210105013 =	IP Filter Set 1,Rule 5 Act Match	<1(check next)|2(forward)|3(drop)>	= 3
210105014 =	IP Filter Set 1,Rule 5 Act Not Match	<1(Check Next)|2(Forward)|3(Drop)>	= 1
/ Menu 21.1.1.6 set #1, rule #6 (SMT Menu 21.1.1.6)			
FIN	FN	PVA	INPUT
210106001 =	IP Filter Set 1,Rule 6 Type	<2(TCP/IP)>	= 2
210106002 =	IP Filter Set 1,Rule 6 Active	<0(No)|1(Yes)>	= 1
210106003 =	IP Filter Set 1,Rule 6 Protocol		= 17
210106004 =	IP Filter Set 1,Rule 6 Dest IP address		= 0.0.0.0
210106005 =	IP Filter Set 1,Rule 6 Dest Subnet Mask		= 0
210106006 =	IP Filter Set 1,Rule 6 Dest Port		= 139
210106007 =	IP Filter Set 1,Rule 6 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210106008 =	IP Filter Set 1,Rule 6 Src IP address		= 0.0.0.0
210106009 =	IP Filter Set 1,Rule 6 Src Subnet Mask		= 0
210106010 =	IP Filter Set 1,Rule 6 Src Port		= 0
210106011 =	IP Filter Set 1,Rule 6 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0

Table 187 Menu 21.1 Filter Set #1 (SMT Menu 21.1) (continued)

210106013 =	IP Filter Set 1,Rule 6 Act Match	<1(check next)|2(forward)|3(drop)>	= 3
210106014 =	IP Filter Set 1,Rule 6 Act Not Match	<1(check next)|2(forward)|3(drop)>	= 2

Table 188 Menu 21.1 Filer Set #2, (SMT Menu 21.1)

/ Menu 21.1 filter set #2, (SMT Menu 21.1)			
FIN	FN	PVA	INPUT
210200001 =	Filter Set 2, Nam	<Str>	= NetBIOS_WAN
/ Menu 21.1.2.1 Filter set #2, rule #1 (SMT Menu 21.1.2.1)			
FIN	FN	PVA	INPUT
210201001 =	IP Filter Set 2, Rule 1 Type	<0(none)|2(TCP/IP)>	= 2
210201002 =	IP Filter Set 2, Rule 1 Active	<0(No)|1(Yes)>	= 1
210201003 =	IP Filter Set 2, Rule 1 Protocol		= 6
210201004 =	IP Filter Set 2, Rule 1 Dest IP address		= 0.0.0.0
210201005 =	IP Filter Set 2, Rule 1 Dest Subnet Mask		= 0
210201006 =	IP Filter Set 2, Rule 1 Dest Port		= 137
210201007 =	IP Filter Set 2, Rule 1 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210201008 =	IP Filter Set 2, Rule 1 Src IP address		= 0.0.0.0
210201009 =	IP Filter Set 2, Rule 1 Src Subnet Mask		= 0
210201010 =	IP Filter Set 2, Rule 1 Src Port		= 0
210201011 =	IP Filter Set 2, Rule 1 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210201013 =	IP Filter Set 2, Rule 1 Act Match	<1(check next)|2(forward)|3(drop)>	= 3
210201014 =	IP Filter Set 2, Rule 1 Act Not Match	<1(check next)|2(forward)|3(drop)>	= 1
/ Menu 21.1.2.2 Filter set #2, rule #2 (SMT Menu 21.1.2.2)			
FIN	FN	PVA	INPUT

Table 188 Menu 21.1 Filer Set #2, (SMT Menu 21.1) (continued)

210202001 =	IP Filter Set 2, Rule 2 Type	<0(none)|2(TCP/IP)>	= 2
210202002 =	IP Filter Set 2, Rule 2 Active	<0(No)|1(Yes)>	= 1
210202003 =	IP Filter Set 2, Rule 2 Protocol		= 6
210202004 =	IP Filter Set 2, Rule 2 Dest IP address		= 0.0.0.0
210202005 =	IP Filter Set 2, Rule 2 Dest Subnet Mask		= 0
210202006 =	IP Filter Set 2, Rule 2 Dest Port		= 138
210202007 =	IP Filter Set 2, Rule 2 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210202008 =	IP Filter Set 2, Rule 2 Src IP address		= 0.0.0.0
210202009 =	IP Filter Set 2, Rule 2 Src Subnet Mask		= 0
210202010 =	IP Filter Set 2,Rule 2 Src Port		= 0
210202011 =	IP Filter Set 2, Rule 2 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210202013 =	IP Filter Set 2, Rule 2 Act Match	<1(check next)|2(forward)|3(drop)>	= 3
210202014 =	IP Filter Set 2, Rule 2 Act Not Match	<1(check next)|2(forward)|3(drop)>	= 1
/ Menu 21.1.2.3 Filter set #2, rule #3 (SMT Menu 21.1.2.3)			
FIN	FN	PVA	INPUT
210203001 =	IP Filter Set 2, Rule 3 Type	<0(none)|2(TCP/IP)>	= 2
210203002 =	IP Filter Set 2, Rule 3 Active	<0(No)|1(Yes)>	= 1
210203003 =	IP Filter Set 2, Rule 3 Protocol		= 6
210203004 =	IP Filter Set 2, Rule 3 Dest IP address		= 0.0.0.0
210203005 =	IP Filter Set 2, Rule 3 Dest Subnet Mask		= 0
210203006 =	IP Filter Set 2, Rule 3 Dest Port		= 139
210203007 =	IP Filter Set 2, Rule 3 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210203008 =	IP Filter Set 2, Rule 3 Src IP address		= 0.0.0.0
210203009 =	IP Filter Set 2,Rule 3 Src Subnet Mask		= 0
210203010 =	IP Filter Set 2, Rule 3 Src Port		= 0

Table 188 Menu 21.1 Filer Set #2, (SMT Menu 21.1) (continued)

210203011 =	IP Filter Set 2, Rule 3 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210203013 =	IP Filter Set 2, Rule 3 Act Match	<1(check next)|2(forward)|3(drop)>	= 3
210203014 =	IP Filter Set 2,Rule 3 Act Not Match	<1(check next)|2(forward)|3(drop)>	= 1
/ Menu 21.1.2.4 Filter set #2, rule #4 (SMT Menu 21.1.2.4)			
FIN	FN	PVA	INPUT
210204001 =	IP Filter Set 2, Rule 4 Type	<0(none)|2(TCP/IP)>	= 2
210204002 =	IP Filter Set 2, Rule 4 Active		<0(No)|1(Yes)> = 1
210204003 =	IP Filter Set 2, Rule 4 Protocol		= 17
210204004 =	IP Filter Set 2, Rule 4 Dest IP address		= 0.0.0.0
210204005 =	IP Filter Set 2, Rule 4 Dest Subnet Mask		= 0
210204006 =	IP Filter Set 2, Rule 4 Dest Port		= 137
210204007 =	IP Filter Set 2, Rule 4 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210204008 =	IP Filter Set 2, Rule 4 Src IP address		= 0.0.0.0
210204009 =	IP Filter Set 2, Rule 4 Src Subnet Mask		= 0
210204010 =	IP Filter Set 2, Rule 4 Src Port		= 0
210204011 =	IP Filter Set 2, Rule 4 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210204013 =	IP Filter Set 2, Rule 4 Act Match	<1(check next)|2(forward)|3(drop)>	= 3
210204014 =	IP Filter Set 2, Rule 4 Act Not Match	<1(check next)|2(forward)|3(drop)>	= 1
/ Menu 21.1.2.5 Filter set #2, rule #5 (SMT Menu 21.1.2.5)			
FIN	FN	PVA	INPUT
210205001 =	IP Filter Set 2, Rule 5 Type	<0(none)|2(TCP/IP)>	= 2
210205002 =	IP Filter Set 2, Rule 5 Active	<0(No)|1(Yes)>	= 1
210205003 =	IP Filter Set 2,Rule 5 Protocol		= 17

Table 188 Menu 21.1 Filer Set #2, (SMT Menu 21.1) (continued)

210205004 =	IP Filter Set 2, Rule 5 Dest IP address		= 0.0.0.0
210205005 =	IP Filter Set 2, Rule 5 Dest Subnet Mask		= 0
210205006 =	IP Filter Set 2, Rule 5 Dest Port		= 138
210205007 =	IP Filter Set 2, Rule 5 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210205008 =	IP Filter Set 2, Rule 5 Src IP address		= 0.0.0.0
210205009 =	IP Filter Set 2, Rule 5 Src Subnet Mask		= 0
210205010 =	IP Filter Set 2, Rule 5 Src Port		= 0
210205011 =	IP Filter Set 2, Rule 5 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210205013 =	IP Filter Set 2, Rule 5 Act Match	<1(check next)|2(forward)|3(drop)>	= 3
210205014 =	IP Filter Set 2, Rule 5 Act Not Match	<1(check next)|2(forward)|3(drop)>	= 1
/ Menu 21.1.2.6 Filter set #2, rule #6 (SMT Menu 21.1.2.5)			
FIN	FN	PVA	INPUT
210206001 =	IP Filter Set 2, Rule 6 Type	<0(none)|2(TCP/IP)>	= 2
210206002 =	IP Filter Set 2, Rule 6 Active	<0(No)|1(Yes)>	= 1
210206003 =	IP Filter Set 2, Rule 6 Protocol		= 17
210206004 =	IP Filter Set 2, Rule 6 Dest IP address		= 0.0.0.0
210206005 =	IP Filter Set 2, Rule 6 Dest Subnet Mask		= 0
210206006 =	IP Filter Set 2, Rule 6 Dest Port		= 139
210206007 =	IP Filter Set 2, Rule 6 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210206008 =	IP Filter Set 2, Rule 6 Src IP address		= 0.0.0.0
210206009 =	IP Filter Set 2, Rule 6 Src Subnet Mask		= 0
210206010 =	IP Filter Set 2, Rule 6 Src Port		= 0
210206011 =	IP Filter Set 2, Rule 6 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0

Table 188 Menu 21.1 Filer Set #2, (SMT Menu 21.1) (continued)

210206013 =	IP Filter Set 2,Rule 6 Act Match	<1(check next)|2(forward)|3(drop)>	= 3
210206014 =	IP Filter Set 2,Rule 6 Act Not Match	<1(check next)|2(forward)|3(drop)>	= 2
*/ Menu 23.1 System Password Setup (SMT Menu 23.1)			
FIN	FN	PVA	INPUT
230000000 =	System Password		= 1234
*/ Menu 23.2 System security: radius server (SMT Menu 23.2)			
FIN	FN	PVA	INPUT
230200001 =	Authentication Server Configured	<0(No) | 1(Yes)>	= 1
230200002 =	Authentication Server Active	<0(No) | 1(Yes)>	= 1
230200003 =	Authentication Server IP Address		= 192.168.1.32
230200004 =	Authentication Server Port		= 1822
230200005 =	Authentication Server Shared Secret		= 111111111111111 111111111111111
230200006 =	Accounting Server Configured	<0(No) | 1(Yes)>	= 1
230200007 =	Accounting Server Active	<0(No) | 1(Yes)>	= 1
230200008 =	Accounting Server IP Address		= 192.168.1.44
230200009 =	Accounting Server Port		= 1823
230200010 =	Accounting Server Shared Secret		= 1234
*/ Menu 23.4 System security: IEEE802.1x (SMT Menu 23.4)			
FIN	FN	PVA	INPUT
230400002 =	ReAuthentication Timer (in second)		= 555
230400003 =	Idle Timeout (in second)		= 999
230400004 =	Authentication Databases	<0(Local User Database Only) |1(RADIUS Only) |2(Local,RADIUS) |3(RADIUS,Local)>	= 1
/ Menu 24.11 Remote Management Control (SMT Menu 24.11)			
FIN	FN	PVA	INPUT
241100001 =	TELNET Server Port		= 23
241100002 =	TELNET Server Access	<0(all)|1(none)|2(Lan)|3(Wan)>	= 0
241100003 =	TELNET Server Secured IP address		= 0.0.0.0
241100004 =	FTP Server Port		= 21

Table 188 Menu 21.1 Filer Set #2, (SMT Menu 21.1) (continued)

241100005 =	FTP Server Access	<0(all)|1(none)|2(Lan)|3(Wan)>	= 0
241100006 =	FTP Server Secured IP address		= 0.0.0.0
241100007 =	WEB Server Port		= 80
241100008 =	WEB Server Access	<0(all)|1(none)|2(Lan) |3(Wan)>	= 0
241100009 =	WEB Server Secured IP address		= 0.0.0.0

Command Examples

The following are example Internal SPTGEN screens associated with the Prestige's command interpreter commands.

Table 189 ci command (for annex a): wan adsl opencmd

/ci command (for annex a): wan adsl opencmd			
FIN	FN	PVA	INPUT
990000001 =	ADSL OPMD	<0(glite)|1(t1.413)|2(gdmt)|3(multimode)>	= 3
/ci command (for annex B): wan adsl opencmd			
FIN	FN	PVA	INPUT
990000001 =	ADSL OPMD	<0(etsi)|1(normal)|2(gdmt)|3(multimode)>	= 3

Appendix L Command Interpreter

The following describes how to use the command interpreter. Enter 24 in the main menu to bring up the system maintenance menu. Enter 8 to go to **Menu 24.8 - Command Interpreter Mode**. See the included disk or zyxel.com for more detailed information on these commands.

Note: Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.

Command Syntax

- The command keywords are in `courier new` font.
- Enter the command keywords exactly as shown, do not abbreviate.
- The required fields in a command are enclosed in angle brackets <>.
- The optional fields in a command are enclosed in square brackets `[]`.
- The `|` symbol means or.

  For example,

  sys filter netbios config <type> <on|off>

  means that you must specify the type of netbios filter and whether to turn it on or off.

Command Usage

A list of valid commands can be found by typing `help` or `?` at the command prompt. Always type the full command. Type `exit` to return to the SMT main menu when finished.

Appendix M Firewall Commands

Sys Firewall Commands

The following describes the firewall commands. See Appendix L for information on the command structure. Each of these commands must be preceded by `sys firewall` when you use them. For example, type `sys firewall active yes` to turn on the firewall.

Table 190 Sys Firewall Commands

Command		Description
`acl`	`disp`	Displays ACLs or a specific ACL set # and rule #.
`active`	`<yes|no>`	Active firewall or deactivate firewall Enables/disables the firewall.
`cnt`		
	`disp`	Displays the firewall log type and count.
	`clear`	Clears the firewall log count.
`pktdump`		Dumps the last 64 bytes of packets that the firewall has dropped.
`dynamicrule`	`display`	Displays the firewall's dynamic rules.
`tcprst`		
	`rst`	Turns TCP reset sending on/off.
	`rst113`	Turns TCP reset sending for port 113 on/off.
	`display`	Displays the TCP reset sending settings.
`icmp`		This rule is not in use.
`dos`		
	`smtp`	Enables/disables the SMTP DoS defender.
	`display`	Displays the SMTP DoS defender setting.
	`ignore`	Sets if the firewall will ignore DoS attacks on the LAN/WAN.
`ignore`		
	`dos`	Sets if the firewall will ignore DoS attacks on the LAN/WAN.
	`triangle`	Sets if the firewall will ignore triangle route packets on the LAN/WAN.

Appendix N
NetBIOS Filter Commands

The following describes the NetBIOS packet filter commands. See Appendix L for information on the command structure.

Introduction

NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN.

For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls.

You can configure NetBIOS filters to do the following :

- Allow or disallow the sending of NetBIOS packets from the LAN to the WAN and from the WAN to the LAN.
- Allow or disallow the sending of NetBIOS packets from the LAN to the DMZ and from the DMZ to the LAN.
- Allow or disallow the sending of NetBIOS packets from the WAN to the DMZ and from the DMZ to the WAN.
- Allow or disallow the sending of NetBIOS packets through VPN connections.
- Allow or disallow NetBIOS packets to initiate calls.

Display NetBIOS Filter Settings

Syntax: `sys filter netbios disp`

This command gives a read-only list of the current NetBIOS filter modes for The Prestige.

NetBIOS Display Filter Settings Command Example

```
=========== NetBIOS Filter Status ===========
        Between LAN and WAN: Block
        Between LAN and DMZ: Block
        Between WAN and DMZ: Block
        IPSec Packets: Forward
        Trigger Dial: Disabled
```

The filter types and their default settings are as follows.

Table 191 NetBIOS Filter Default Settings

NAME	DESCRIPTION	EXAMPLE
Between LAN and WAN	This field displays whether NetBIOS packets are blocked or forwarded between the LAN and the WAN.	Block
Between LAN and DMZ	This field displays whether NetBIOS packets are blocked or forwarded between the LAN and the DMZ.	Block
Between WAN and DMZ	This field displays whether NetBIOS packets are blocked or forwarded between the WAN and the DMZ.	Block
IPSec Packets	This field displays whether NetBIOS packets sent through a VPN connection are blocked or forwarded.	Forward
Trigger dial	This field displays whether NetBIOS packets are allowed to initiate calls. Disabled means that NetBIOS packets are blocked from initiating calls.	Disabled

NetBIOS Filter Configuration

```
Syntax:sys filter netbios config <type> <on|off>
```

where

`<type>  =`	Identify which NetBIOS filter (numbered 0-3) to configure. 0 = Between LAN and WAN 1 = Between LAN and DMZ 2 = Between WAN and DMZ 3 = IPSec packet pass through 4 = Trigger Dial
`<on|off>  =`	For type 0 and 1, use on to enable the filter and block NetBIOS packets. Use off to disable the filter and forward NetBIOS packets. For type 3, use on to block NetBIOS packets from being sent through a VPN connection. Use off to allow NetBIOS packets to be sent through a VPN connection. For type 4, use on to allow NetBIOS packets to initiate dial backup calls. Use off to block NetBIOS packets from initiating dial backup calls.

Example commands

`sys filter netbios config 0 on`	This command blocks LAN to WAN and WAN to LAN NetBIOS packets.
`sys filter netbios config 1 off`	This command forwards LAN to DMZ and DMZ to LAN NetBIOS packets.

`sys filter netbios config 3 on`	This command blocks IPSec NetBIOS packets.
`sys filter netbios config 4 off`	This command stops NetBIOS commands from initiating calls.

Appendix O Brute-Force Password Guessing Protection

The following describes the commands for enabling, disabling and configuring the brute-force password guessing protection mechanism for the password. See Appendix L for information on the command structure.

Table 192 Brute-Force Password Guessing Protection Commands

COMMAND	DESCRIPTION
sys pwderrtm	This command displays the brute-force guessing password protection settings.
sys pwderrtm 0	This command turns off the password's protection from brute-force guessing. The brute-force password guessing protection is turned off by default.
sys pwderrtm N	This command sets the password protection to block all access attempts for N (a number from 1 to 60) minutes after the third time an incorrect password is entered.

Example

```
sys pwderrtm 5
```

This command sets the password protection to block all access attempts for five minutes after the third time an incorrect password is entered.

Appendix P
Boot Commands

The BootModule AT commands execute from within the router's bootup software, when debug mode is selected before the main router firmware is started. When you start up your Prestige, you are given a choice to go into debug mode by pressing a key at the prompt shown in the following screen. In debug mode you have access to a series of boot module commands, for example ATUR (for uploading firmware) and ATLC (for uploading the configuration file). These are already discussed in the **Firmware and Configuration File Maintenance** chapter.

Figure 327 Option to Enter Debug Mode

```
Bootbase Version: V1.02 | 08/08/2001 15:40:50
RAM: Size = 16384 Kbytes
DRAM Post: Testing:  16384K OK
FLASH: Intel 16M
RAS Version: V3.50(WB.0)b3 | 08/08/2001 16:21:27
Press any key to enter debug mode within 3
seconds.
.............................................
```

Enter ATHE to view all available Prestige boot module commands as shown in the next screen. ATBAx allows you to change the console port speed. The x denotes the number preceding the colon to give the console port speed following the colon in the list of numbers that follows; for example ATBA3 will give a console port speed of 9.6 Kbps. ATSE displays the seed that is used to generate a password to turn on the debug flag in the firmware. The ATSH command shows product related information such as boot module version, vendor name, product model, RAS code revision, etc. ATGO allows you to continue booting the system. Most other commands aid in advanced troubleshooting and should only be used by qualified engineers.

Figure 328 Boot Module Commands

```
AT            just answer OK
ATHE          print help
ATBAx        change baudrate. 1:38.4k, 2:19.2k, 3:9.6k 4:57.6k
5:115.2k
ATENx,(y)     set BootExtension Debug Flag (y=password)
ATSE          show the seed of password generator
ATTI(h,m,s)   change system time to hour:min:sec or show
current time
ATDA(y,m,d)   change system date to year/month/day or show
current date
ATDS          dump RAS stack
ATDT          dump Boot Module Common Area
ATDUx,y       dump memory contents from address x for length y
ATRBx         display the  8-bit value of address x
ATRWx         display the 16-bit value of address x
ATRLx         display the 32-bit value of address x
ATGO(x)       run program at addr x or boot router
ATGR          boot router
ATGT          run Hardware Test Program
ATRTw,x,y(,z) RAM test level w, from address x to y (z
iterations)
ATSH          dump manufacturer related data in ROM
ATDOx,y       download from address x for length y to PC via
XMODEM
ATTD          download router configuration to PC via XMODEM
ATUR          upload router firmware to flash ROM
ATLC          upload router configuration file to flash ROM
ATXSx         xmodem select: x=0: CRC mode(default); x=1:
checksum mode
ATSR          system reboot
```

Appendix Q Log Descriptions

This appendix provides descriptions of example log messages.

Table 193 System Maintenance Logs

LOG MESSAGE	DESCRIPTION
`Time calibration is successful`	The router has adjusted its time based on information from the time server.
`Time calibration failed`	The router failed to get information from the time server.
`WAN interface gets IP: %s`	A WAN interface got a new IP address from the DHCP, PPPoE, PPTP or dial-up server.
`DHCP client IP expired`	A DHCP client's IP address has expired.
`DHCP server assigns %s`	The DHCP server assigned an IP address to a client.
`Successful SMT login`	Someone has logged on to the router's SMT interface.
`SMT login failed`	Someone has failed to log on to the router's SMT interface.
`Successful WEB login`	Someone has logged on to the router's web configurator interface.
`WEB login failed`	Someone has failed to log on to the router's web configurator interface.
`Successful TELNET login`	Someone has logged on to the router via telnet.
`TELNET login failed`	Someone has failed to log on to the router via telnet.
`Successful FTP login`	Someone has logged on to the router via ftp.
`FTP login failed`	Someone has failed to log on to the router via ftp.
`NAT Session Table is Full!`	The maximum number of NAT session table entries has been exceeded and the table is full.
`Starting Connectivity Monitor`	Starting Connectivity Monitor.
`Time initialized by Daytime Server`	The router got the time and date from the Daytime server.
`Time initialized by Time server`	The router got the time and date from the time server.
`Time initialized by NTP server`	The router got the time and date from the NTP server.
`Connect to Daytime server fail`	The router was not able to connect to the Daytime server.
`Connect to Time server fail`	The router was not able to connect to the Time server.
`Connect to NTP server fail`	The router was not able to connect to the NTP server.
`Too large ICMP packet has been dropped`	The router dropped an ICMP packet that was too large.
`SMT Session Begin`	An SMT management session has started.
`SMT Session End`	An SMT management session has ended.

Table 193 System Maintenance Logs (continued)

LOG MESSAGE	DESCRIPTION
`Configuration Change: PC = 0x%x, Task ID = 0x%x`	The router is saving configuration changes.
`Successful SSH login`	Someone has logged on to the router's SSH server.
`SSH login failed`	Someone has failed to log on to the router's SSH server.
`Successful HTTPS login`	Someone has logged on to the router's web configurator interface using HTTPS protocol.
`HTTPS login failed`	Someone has failed to log on to the router's web configurator interface using HTTPS protocol.

Table 194 System Error Logs

LOG MESSAGE	DESCRIPTION
`%s exceeds the max. number of session per host!`	This attempt to create a NAT session exceeds the maximum number of NAT session table entries allowed to be created per host.
`setNetBIOSFilter: calloc error`	The router failed to allocate memory for the NetBIOS filter settings.
`readNetBIOSFilter: calloc error`	The router failed to allocate memory for the NetBIOS filter settings.
`WAN connection is down.`	A WAN connection is down. You cannot access the network through this interface.

Table 195 Access Control Logs

LOG MESSAGE	DESCRIPTION
`Firewall default policy: [ TCP | UDP | IGMP | ESP | GRE | OSPF ] <Packet Direction>`	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched the default policy and was blocked or forwarded according to the default policy's setting.
`Firewall rule [NOT] match:[ TCP | UDP | IGMP | ESP | GRE | OSPF ] <Packet Direction>, <rule:%d>`	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched (or did not match) a configured firewall rule (denoted by its number) and was blocked or forwarded according to the rule.
`Triangle route packet forwarded: [ TCP | UDP | IGMP | ESP | GRE | OSPF ]`	The firewall allowed a triangle route session to pass through.
`Packet without a NAT table entry blocked: [ TCP | UDP | IGMP | ESP | GRE | OSPF ]`	The router blocked a packet that didn't have a corresponding NAT table entry.
`Router sent blocked web site message: TCP`	The router sent a message to notify a user that the router blocked access to a web site that the user requested.

Table 196 TCP Reset Logs

LOG MESSAGE	DESCRIPTION
`Under SYN flood attack, sent TCP RST`	The router sent a TCP reset packet when a host was under a SYN flood attack (the TCP incomplete count is per destination host.)
`Exceed TCP MAX incomplete, sent TCP RST`	The router sent a TCP reset packet when the number of TCP incomplete connections exceeded the user configured threshold. (the TCP incomplete count is per destination host.) Note: Refer to **TCP Maximum Incomplete** in the **Firewall Attack Alerts** screen.
`Peer TCP state out of order, sent TCP RST`	The router sent a TCP reset packet when a TCP connection state was out of order.Note: The firewall refers to RFC793 Figure 6 to check the TCP state.
`Firewall session time out, sent TCP RST`	The router sent a TCP reset packet when a dynamic firewall session timed out.Default timeout values:ICMP idle timeout (s): 60UDP idle timeout (s): 60TCP connection (three way handshaking) timeout (s): 30TCP FIN-wait timeout (s): 60TCP idle (established) timeout (s): 3600
`Exceed MAX incomplete, sent TCP RST`	The router sent a TCP reset packet when the number of incomplete connections (TCP and UDP) exceeded the user-configured threshold. (Incomplete count is for all TCP and UDP connections through the firewall.)Note: When the number of incomplete connections (TCP + UDP) > "Maximum Incomplete High", the router sends TCP RST packets for TCP connections and destroys TOS (firewall dynamic sessions) until incomplete connections < "Maximum Incomplete Low".
`Access block, sent TCP RST`	The router sends a TCP RST packet and generates this log if you turn on the firewall TCP reset mechanism (via CI command: "sys firewall tcprst").

Table 197 Packet Filter Logs

LOG MESSAGE	DESCRIPTION
`[ TCP | UDP | ICMP | IGMP | Generic ] packet filter matched (set: %d, rule: %d)`	Attempted access matched a configured filter rule (denoted by its set and rule number) and was blocked or forwarded according to the rule.

Table 198 ICMP Logs

LOG MESSAGE	DESCRIPTION
`Firewall default policy: ICMP <Packet Direction>, <type:%d>, <code:%d>`	ICMP access matched the default policy and was blocked or forwarded according to the user's setting. For type and code details, see Table 208.
`Firewall rule [NOT] match: ICMP <Packet Direction>, <rule:%d>, <type:%d>, <code:%d>`	ICMP access matched (or didn't match) a firewall rule (denoted by its number) and was blocked or forwarded according to the rule. For type and code details, see Table 208.

Table 198 ICMP Logs (continued)

LOG MESSAGE	DESCRIPTION
`Triangle route packet forwarded: ICMP`	The firewall allowed a triangle route session to pass through.
`Packet without a NAT table entry blocked: ICMP`	The router blocked a packet that didn't have a corresponding NAT table entry.
`Unsupported/out-of-order ICMP: ICMP`	The firewall does not support this kind of ICMP packets or the ICMP packets are out of order.
`Router reply ICMP packet: ICMP`	The router sent an ICMP reply packet to the sender.

Table 199 CDR Logs

LOG MESSAGE	DESCRIPTION
`board %d line %d channel %d, call %d, %s C01 Outgoing Call dev=%x ch=%x %s`	The router received the setup requirements for a call. "call" is the reference (count) number of the call. "dev" is the device type (3 is for dial-up, 6 is for PPPoE, 10 is for PPTP). "channel" or "ch" is the call channel ID.For example,"board 0 line 0 channel 0, call 3, C01 Outgoing Call dev=6 ch=0 "Means the router has dialed to the PPPoE server 3 times.
`board %d line %d channel %d, call %d, %s C02 OutCall Connected %d %s`	The PPPoE, PPTP or dial-up call is connected.
`board %d line %d channel %d, call %d, %s C02 Call Terminated`	The PPPoE, PPTP or dial-up call was disconnected.

Table 200 PPP Logs

LOG MESSAGE	DESCRIPTION
`ppp:LCP Starting`	The PPP connection's Link Control Protocol stage has started.
`ppp:LCP Opening`	The PPP connection's Link Control Protocol stage is opening.
`ppp:CHAP Opening`	The PPP connection's Challenge Handshake Authentication Protocol stage is opening.
`ppp:IPCP Starting`	The PPP connection's Internet Protocol Control Protocol stage is starting.
`ppp:IPCP Opening`	The PPP connection's Internet Protocol Control Protocol stage is opening.
`ppp:LCP Closing`	The PPP connection's Link Control Protocol stage is closing.
`ppp:IPCP Closing`	The PPP connection's Internet Protocol Control Protocol stage is closing.

Table 201 UPnP Logs

LOG MESSAGE	DESCRIPTION
UPnP pass through Firewall	UPnP packets can pass through the firewall.

Table 202 Content Filtering Logs

LOG MESSAGE	DESCRIPTION
%s: Keyword blocking	The content of a requested web page matched a user defined keyword.
%s: Not in trusted web list	The web site is not in a trusted domain, and the router blocks all traffic except trusted domain sites.
%s: Forbidden Web site	The web site is in the forbidden web site list.
%s: Contains ActiveX	The web site contains ActiveX.
%s: Contains Java applet	The web site contains a Java applet.
%s: Contains cookie	The web site contains a cookie.
%s: Proxy mode detected	The router detected proxy mode in the packet.
%s	The content filter server responded that the web site is in the blocked category list, but it did not return the category type.
%s: %s	The content filter server responded that the web site is in the blocked category list, and returned the category type.
%s(cache hit)	The system detected that the web site is in the blocked list from the local cache, but does not know the category type.
%s :%s(cache hit)	The system detected that the web site is in blocked list from the local cache, and knows the category type.
%s: Trusted Web site	The web site is in a trusted domain.
%s	When the content filter is not on according to the time schedule or you didn't select the "Block Matched Web Site" checkbox, the system forwards the web content.
Waiting content filter server timeout	The external content filtering server did not respond within the timeout period.
DNS resolving failed	The Prestige cannot get the IP address of the external content filtering via DNS query.
Creating socket failed	The Prestige cannot issue a query because TCP/IP socket creation failed, port:port number.
Connecting to content filter server fail	The connection to the external content filtering server failed.
License key is invalid	The external content filtering license key is invalid.

Table 203 Attack Logs

LOG MESSAGE	DESCRIPTION
`attack [ TCP | UDP | IGMP | ESP | GRE | OSPF ]`	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF attack.
`attack ICMP (type:%d, code:%d)`	The firewall detected an ICMP attack. For type and code details, see Table 208.
`land [ TCP | UDP | IGMP | ESP | GRE | OSPF ]`	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF land attack.
`land ICMP (type:%d, code:%d)`	The firewall detected an ICMP land attack. For type and code details, see Table 208.
`ip spoofing - WAN [ TCP | UDP | IGMP | ESP | GRE | OSPF ]`	The firewall detected an IP spoofing attack on the WAN port.
`ip spoofing - WAN ICMP (type:%d, code:%d)`	The firewall detected an ICMP IP spoofing attack on the WAN port. For type and code details, see Table 208.
`icmp echo : ICMP (type:%d, code:%d)`	The firewall detected an ICMP echo attack. For type and code details, see Table 208.
`syn flood TCP`	The firewall detected a TCP syn flood attack.
`ports scan TCP`	The firewall detected a TCP port scan attack.
`teardrop TCP`	The firewall detected a TCP teardrop attack.
`teardrop UDP`	The firewall detected an UDP teardrop attack.
`teardrop ICMP (type:%d, code:%d)`	The firewall detected an ICMP teardrop attack. For type and code details, see Table 208.
`illegal command TCP`	The firewall detected a TCP illegal command attack.
`NetBIOS TCP`	The firewall detected a TCP NetBIOS attack.
`ip spoofing - no routing entry [ TCP | UDP | IGMP | ESP | GRE | OSPF ]`	The firewall classified a packet with no source routing entry as an IP spoofing attack.
`ip spoofing - no routing entry ICMP (type:%d, code:%d)`	The firewall classified an ICMP packet with no source routing entry as an IP spoofing attack.
`vulnerability ICMP (type:%d, code:%d)`	The firewall detected an ICMP vulnerability attack. For type and code details, see Table 208.
`traceroute ICMP (type:%d, code:%d)`	The firewall detected an ICMP traceroute attack. For type and code details, see Table 208.

Table 204 IPSec Logs

LOG MESSAGE	DESCRIPTION
Discard REPLAY packet	The router received and discarded a packet with an incorrect sequence number.
Inbound packet authentication failed	The router received a packet that has been altered. A third party may have altered or tampered with the packet.
Receive IPSec packet, but no corresponding tunnel exists	The router dropped an inbound packet for which SPI could not find a corresponding phase 2 SA.
Rule <%d> idle time out, disconnect	The router dropped a connection that had outbound traffic and no inbound traffic for a certain time period. You can use the "ipsec timer chk_conn" CI command to set the time period. The default value is 2 minutes.
WAN IP changed to <IP>	The router dropped all connections with the "MyIP" configured as "0.0.0.0" when the WAN IP address changed.

Table 205 IKE Logs

LOG MESSAGE	DESCRIPTION
Active connection allowed exceeded	The IKE process for a new connection failed because the limit of simultaneous phase 2 SAs has been reached.
Start Phase 2: Quick Mode	Phase 2 Quick Mode has started.
Verifying Remote ID failed:	The connection failed during IKE phase 2 because the router and the peer's Local/Remote Addresses don't match.
Verifying Local ID failed:	The connection failed during IKE phase 2 because the router and the peer's Local/Remote Addresses don't match.
IKE Packet Retransmit	The router retransmitted the last packet sent because there was no response from the peer.
Failed to send IKE Packet	An Ethernet error stopped the router from sending IKE packets.
Too many errors! Deleting SA	An SA was deleted because there were too many errors.
Phase 1 IKE SA process done	The phase 1 IKE SA process has been completed.
Duplicate requests with the same cookie	The router received multiple requests from the same peer while still processing the first IKE packet from the peer.
IKE Negotiation is in process	The router has already started negotiating with the peer for the connection, but the IKE process has not finished yet.
No proposal chosen	Phase 1 or phase 2 parameters don't match. Please check all protocols / settings. Ex. One device being configured for 3DES and the other being configured for DES causes the connection to fail.
Local / remote IPs of incoming request conflict with rule <%d>	The security gateway is set to "0.0.0.0" and the router used the peer's "Local Address" as the router's "Remote Address". This information conflicted with static rule #d; thus the connection is not allowed.

Table 205 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
Cannot resolve Secure Gateway Addr for rule <%d>	The router couldn't resolve the IP address from the domain name that was used for the secure gateway address.
Peer ID: <peer id> <My remote type> -<My local type>	The displayed ID information did not match between the two ends of the connection.
vs. My Remote <My remote> -<My remote>	The displayed ID information did not match between the two ends of the connection.
vs. My Local <My local>-<My local>	The displayed ID information did not match between the two ends of the connection.
Send <packet>	A packet was sent.
Recv <packet>	IKE uses ISAKMP to transmit data. Each ISAKMP packet contains many different types of payloads. All of them show in the LOG. Refer to RFC2408 – ISAKMP for a list of all ISAKMP payload types.
Recv <Main or Aggressive> Mode request from <IP>	The router received an IKE negotiation request from the peer address specified.
Send <Main or Aggressive> Mode request to <IP>	The router started negotiation with the peer.
Invalid IP <Peer local> / <Peer local>	The peer's "Local IP Address" is invalid.
Remote IP <Remote IP> / <Remote IP> conflicts	The security gateway is set to "0.0.0.0" and the router used the peer's "Local Address" as the router's "Remote Address". This information conflicted with static rule #d; thus the connection is not allowed.
Phase 1 ID type mismatch	This router's "Peer ID Type" is different from the peer IPSec router's "Local ID Type".
Phase 1 ID content mismatch	This router's "Peer ID Content" is different from the peer IPSec router's "Local ID Content".
No known phase 1 ID type found	The router could not find a known phase 1 ID in the connection attempt.
ID type mismatch. Local / Peer: <Local ID type/Peer ID type>	The phase 1 ID types do not match.
ID content mismatch	The phase 1 ID contents do not match.
Configured Peer ID Content: <Configured Peer ID Content>	The phase 1 ID contents do not match and the configured "Peer ID Content" is displayed.
Incoming ID Content: <Incoming Peer ID Content>	The phase 1 ID contents do not match and the incoming packet's ID content is displayed.
Unsupported local ID Type: <%d>	The phase 1 ID type is not supported by the router.
Build Phase 1 ID	The router has started to build the phase 1 ID.
Adjust TCP MSS to %d	The router automatically changed the TCP Maximum Segment Size value after establishing a tunnel.
Rule <%d> input idle time out, disconnect	The tunnel for the listed rule was dropped because there was no inbound traffic within the idle timeout period.
XAUTH succeed! Username: <Username>	The router used extended authentication to authenticate the listed username.

Table 205 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
XAUTH fail! Username: <Username>	The router was not able to use extended authentication to authenticate the listed username.
Rule[%d] Phase 1 negotiation mode mismatch	The listed rule's IKE phase 1 negotiation mode did not match between the router and the peer.
Rule [%d] Phase 1 encryption algorithm mismatch	The listed rule's IKE phase 1 encryption algorithm did not match between the router and the peer.
Rule [%d] Phase 1 authentication algorithm mismatch	The listed rule's IKE phase 1 authentication algorithm did not match between the router and the peer.
Rule [%d] Phase 1 authentication method mismatch	The listed rule's IKE phase 1 authentication method did not match between the router and the peer.
Rule [%d] Phase 1 key group mismatch	The listed rule's IKE phase 1 key group did not match between the router and the peer.
Rule [%d] Phase 2 protocol mismatch	The listed rule's IKE phase 2 protocol did not match between the router and the peer.
Rule [%d] Phase 2 encryption algorithm mismatch	The listed rule's IKE phase 2 encryption algorithm did not match between the router and the peer.
Rule [%d] Phase 2 authentication algorithm mismatch	The listed rule's IKE phase 2 authentication algorithm did not match between the router and the peer.
Rule [%d] Phase 2 encapsulation mismatch	The listed rule's IKE phase 2 encapsulation did not match between the router and the peer.
Rule [%d]> Phase 2 pfs mismatch	The listed rule's IKE phase 2 perfect forward secret (pfs) setting did not match between the router and the peer.
Rule [%d] Phase 1 ID mismatch	The listed rule's IKE phase 1 ID did not match between the router and the peer.
Rule [%d] Phase 1 hash mismatch	The listed rule's IKE phase 1 hash did not match between the router and the peer.
Rule [%d] Phase 1 preshared key mismatch	The listed rule's IKE phase 1 pre-shared key did not match between the router and the peer.
Rule [%d] Tunnel built successfully	The listed rule's IPSec tunnel has been built successfully.
Rule [%d] Peer's public key not found	The listed rule's IKE phase 1 peer's public key was not found.
Rule [%d] Verify peer's signature failed	The listed rule's IKE phase 1verification of the peer's signature failed.
Rule [%d] Sending IKE request	IKE sent an IKE request for the listed rule.
Rule [%d] Receiving IKE request	IKE received an IKE request for the listed rule.
Swap rule to rule [%d]	The router changed to using the listed rule.
Rule [%d] Phase 1 key length mismatch	The listed rule's IKE phase 1 key length (with the AES encryption algorithm) did not match between the router and the peer.
Rule [%d] phase 1 mismatch	The listed rule's IKE phase 1 did not match between the router and the peer.

Table 205 IKE Logs (continued)

LOG MESSAGE	DESCRIPTION
`Rule [%d] phase 2 mismatch`	The listed rule's IKE phase 2 did not match between the router and the peer.
`Rule [%d] Phase 2 key length mismatch`	The listed rule's IKE phase 2 key lengths (with the AES encryption algorithm) did not match between the router and the peer.

Table 206 802.1X Logs

LOG MESSAGE	DESCRIPTION
`Local User Database accepts user.`	A user was authenticated by the local user database.
`Local User Database reports user credential error.`	A user was not authenticated by the local user database because of an incorrect user password.
`Local User Database does not find user`s credential.`	A user was not authenticated by the local user database because the user is not listed in the local user database.
`RADIUS accepts user.`	A user was authenticated by the RADIUS Server.
`RADIUS rejects user. Pls check RADIUS Server.`	A user was not authenticated by the RADIUS Server. Please check the RADIUS Server.
`Local User Database does not support authentication method.`	The local user database only supports the EAP-MD5 method. A user tried to use another authentication method and was not authenticated.
`User logout because of session timeout expired.`	The router logged out a user whose session expired.
`User logout because of user deassociation.`	The router logged out a user who ended the session.
`User logout because of no authentication response from user.`	The router logged out a user from which there was no authentication response.
`User logout because of idle timeout expired.`	The router logged out a user whose idle timeout period expired.
`User logout because of user request.`	A user logged out.
`Local User Database does not support authentication mothed.`	A user tried to use an authentication method that the local user database does not support (it only supports EAP-MD5).
`No response from RADIUS. Pls check RADIUS Server.`	There is no response message from the RADIUS server, please check the RADIUS server.
`Use Local User Database to authenticate user.`	The local user database is operating as the authentication server.
`Use RADIUS to authenticate user.`	The RADIUS server is operating as the authentication server.
`No Server to authenticate user.`	There is no authentication server to authenticate a user.
`Local User Database does not find user`s credential.`	A user was not authenticated by the local user database because the user is not listed in the local user database.

Table 207 ACL Setting Notes

PACKET DIRECTION	DIRECTION	DESCRIPTION
(L to W)	LAN to WAN	ACL set for packets traveling from the LAN to the WAN.
(W to L)	WAN to LAN	ACL set for packets traveling from the WAN to the LAN.
(D to L)	DMZ to LAN	ACL set for packets traveling from the DMZ to the LAN.
(D to W)	DMZ to WAN	ACL set for packets traveling from the DMZ to the WAN.
(W to D)	WAN to DMZ	ACL set for packets traveling from the WAN to the DMZ.
(L to D)	LAN to DMZ	ACL set for packets traveling from the LAN to the DMZ.
(L to L/Prestige)	LAN to LAN/ Prestige	ACL set for packets traveling from the LAN to the LAN or the Prestige.
(W to W/Prestige)	WAN to WAN/ Prestige	ACL set for packets traveling from the WAN to the WAN or the Prestige.
(D to D/Prestige)	DMZ to DMZ/ Prestige	ACL set for packets traveling from the DMZ to the DM or the Prestige.

Table 208 ICMP Notes

TYPE	CODE	DESCRIPTION
0		Echo Reply
	0	Echo reply message
3		Destination Unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)
	5	Source route failed
4		Source Quench
	0	A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host
8		Echo
	0	Echo message

Table 208 ICMP Notes (continued)

TYPE	CODE	DESCRIPTION
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp Reply
	0	Timestamp reply message
15		Information Request
	0	Information request message
16		Information Reply
	0	Information reply message

Table 209 Syslog Logs

LOG MESSAGE	DESCRIPTION
<Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>" devID="<mac address last three numbers>" cat="<category>	"This message is sent by the system ("RAS" displays as the system name if you haven't configured one) when the router generates a syslog. The facility is defined in the web MAIN MENU->LOGS->Log Settings page. The severity is the log's syslog class. The definition of messages and notes are defined in the various log charts throughout this appendix. The "devID" is the last three characters of the MAC address of the router's LAN port. The "cat" is the same as the category in the router's logs.

The following table shows RFC-2408 ISAKMP payload types that the log displays. Please refer to the RFC for detailed information on each type.

Table 210 RFC-2408 ISAKMP Payload Types

LOG DISPLAY	PAYLOAD TYPE
SA	Security Association
PROP	Proposal
TRANS	Transform
KE	Key Exchange
ID	Identification
CER	Certificate
CER_REQ	Certificate Request
HASH	Hash

Table 210 RFC-2408 ISAKMP Payload Types (continued)

LOG DISPLAY	PAYLOAD TYPE
SIG	Signature
NONCE	Nonce
NOTFY	Notification
DEL	Delete
VID	Vendor ID

Log Commands

Go to the command interpreter interface (Appendix L explains how to access and use the commands).

Configuring What You Want the Prestige to Log

1. Use the sys logs load command to load the log setting buffer that allows you to configure which logs the Prestige is to record.
2. Use sys logs category to view a list of the log categories.

Figure 329 Displaying Log Categories Example

```
Copyright (c) 1994 - 2004 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys             exit            device          ether
wan             poe             aux             config
wlan            ip              ipsec           ppp
bridge          hdap            bm              lan
radius          8021x
ras>
```

3. Use sys logs category followed by a log category to display the parameters that are available for the category.

Figure 330 Displaying Log Parameters Example

```
ras> sys logs category access
Usage: [0:none/1:log/2:alert/3:both]
ras>
```

4. Use sys logs category followed by a log category and a parameter to decide what to record.

Use 0 to not record logs for that category, 1 to record only logs for that category, 2 to record only alerts for that category, and 3 to record both logs and alerts for that category. Not every parameter is available with every category.

5 Use the sys logs save command to store the settings in the Prestige (you must do this in order to record logs).

Displaying Logs

- Use the sys logs display command to show all of the logs in the Prestige's log.
- Use the sys logs category display command to show the log settings for all of the log categories.
- Use the sys logs display [log category] command to show the logs in an individual Prestige log category.
- Use the sys logs clear command to erase all of the Prestige's logs.

Log Command Example

This example shows how to set the Prestige to record the access logs and alerts and then view the results.

Figure 331 Log Command Example

```
ras> sys logs load
ras> sys logs category access 3
ras> sys logs save
ras> sys logs display access
#  .time                source                 destination            notes

    message
  7|01/01/2000 09:40:13 |192.168.1.1:3         |192.168.1.33:1        |ACCESS FO
RWARD
    Router reply ICMP packet: ICMP(type:3, code:1)
  8|01/01/2000 09:40:07 |192.168.1.1:3         |192.168.1.33:1        |ACCESS FO
RWARD
    Router reply ICMP packet: ICMP(type:3, code:1)
  9|01/01/2000 09:40:04 |192.168.1.1:3         |192.168.1.33:1        |ACCESS FO
RWARD
    Router reply ICMP packet: ICMP(type:3, code:1)
 10|01/01/2000 09:40:04 |192.168.1.33:1199     |207.69.188.186:110    |ACCESS FO
RWARD
    Firewall default policy: TCP (L to W)
 11|01/01/2000 09:40:04 |192.168.1.1:53        |192.168.1.33:1200     |ACCESS FO
RWARD
    none: UDP
```

Index

A

Access methods **360**
Address Assignment **79**
Address mapping **136**
Address Resolution Protocol (ARP) **82**
Ad-hoc Configuration **483**
ADSL, what is it? **42**
ADSLstandards **44**
AH **214**
AH (Authentication Header) **436**
AH Protocol **218**
alert message **500**
Alternative Subnet Mask Notation **474**
antenna **46**
Anti-virus
  Online update **208**
  Registration **208**
Anti-virus packet scan
  Configuration **207**
anti-virus packet scan **46**, **500**
  packet types **46**
  Windows 98/Me requirements **500**
Anti-virus scan
  packet types **206**
Any IP **45**, **81**
  How it works **82**
  note **82**
Any IP Setup **84**
Any IP table **289**
AP (access point) **90**
applicaions
  Internet access **51**
Application-level Firewalls **144**
AT command **308**, **310**, **397**
ATM Adaptation Layer 5 (AAL5) **60**
ATM layer options **333**
Attack Alert **176**, **178**
Attack Types **149**
Authentication **328**, **329**
Authentication Code **494**
Authentication databases **104**
authentication databases **384**
Authentication Header **218**
Authentication protocol **329**
auto-Crossover **48**
auto-negotiation **48**
Available Services **189**

B

Backup **397**
Backup Typ **119**
Bandwidth Borrowing **275**
bandwidth budget **270**
bandwidth capacity **270**
Bandwidth Class **270**
bandwidth class **270**
Bandwidth Filter **270**
bandwidth filter **270**
Bandwidth Management **270**
Bandwidth Management Statistics **282**
Bandwidth Manager Class Configuration **279**
Bandwidth Manager Class Setup **278**
Bandwidth Manager Monitor **283**
Bandwidth Manager Summary **277**
Basic Service Set **483**
Blocking Time **177**, **178**
Boot sector virus **204**
Borrow bandwidth from parent class **280**
Bridging **329**, **340**
  Ether Address **342**
  Ethernet **340**
  Ethernet Addr Timeout **341**
  Remote Node **340**
  Static Route Setup **342**
bridging **303**
Brute-force Attack, **148**
BSS **483**
Budget Management **413**, **414**
BW Budget **280**

C

CA **488**
CAC **184**
call back delay **311**
Call filtering **362**
Call filters
  Built-in **362**
  User-defined **362**
Call Scheduling **430**
  Maximum Number of Schedule Sets **430**
  PPPoE **432**
  Precedence **430**
  Precedence Example **430**
CBR (Continuous Bit Rate) **116**
CDR **392**
CDR (Call Detail Record) **391**
CE regulations **46**
Certificate Authority **488**
change password at login **55**
Channel **90**
  Interference **90**
Channel ID **317**
CHAP **328**
Class Name **280**
Collision **388**
Command Interpreter Mode **412**
Community **377**
compact **50**
compact guide **54**
Computer Name **302**
Computer virus **204**
Computer virus infection and prevention **205**
Computer virus types **204**
Conditions that prevent TFTP and FTP from working over WAN **399**
Configuration **69**, **288**
configuration file **396**
configuration of multiple Prestiges **450**
Console Port **458**
  Configuration File Upload **409**
  File Backup **401**
  File Upload **408**
  Restoring Files **404**
console session **457**
Content Access Control
  activation **185**
  Administrator Login **202**
  Application **184**
  configuration steps **184**
  Content Filtering Service **186**
  create user groups **185**
  Customize services **188**
  Diagnose **197**
  diagnose sequence **198**
  Idle Timeout **185**
  log out **201**
  online status **200**
  test web site access privileges **197**
  Time Left **200**
  Time schedule **186**
  Unlimited time schedule **187**
  User Account **198**
  user accoutns **184**
  User groups **185**
  user groups **184**
  User Login **201**
  User Profile **198**
  Web Site Filters **191**
  web site test sequence **197**
  WLAN application **184**
Content Access Control (CAC) **184**
Content Filtering **180**
  Categories **180**
  Schedule **181**
  Tursted computers **182**
  URL keyword blocking **180**
Content filtering **180**
content filtering **45**, **191**
Copyright **2**
Cost Of Transmission **331**, **338**
Country Code **389**
CPU Load **388**
CTS (Clear to Send) **91**
Custom Ports
  Creating/Editing **168**
Customer Support **5**
Customized Services **168**
Customized services **168**

D

Data Confidentiality **213**
Data encryption **93**
Data Filtering **362**
Data Integrity **213**
Data Origin Authentication **213**
data privacy **383**
default LAN IP address **54**
default user name and password **54**
DeMilitarized Zone (DMZ) **48**
Denial of Service **145**, **146**, **177**, **360**
Destination Address **161**

Device Filter rules 371
device model number 293
Device rule 371
DH 233
DHCP 49, 69, 79, 80, 140, 288, 314, 389
DHCP client 49
DHCP relay 49
DHCP server 49, 288, 314
DHCP table 288
diagnostic 290
Diagnostic Tools 386
DIAL BACKUP 458
dial timeout 310
Diffie-Hellman Key Groups 233
Direct Sequence Spread Spectrum 482
Distribution System 483
Distribution System (DS) 100
DMZ 86
DNS 314
DNS Server
  For VPN Host 223
DNS server 440
Domain Name 79, 132
domain name 302
Domain Name System 79
DoS 146
  Basics 146
  Types 147
DoS (Denial of Service) 45, 48, 86
DoS attacks, types of 147
drop timeout 311
DS 483
DSL (Digital Subscriber Line) 42
DSL line, reinitialize 292
DSL, What Is It? 42
DSLAM (Digital Subscriber Line Access Multiplexer) 51
DSSS 482
DTR 124, 310
Dynamic DNS 48, 140, 303
dynamic DNS 48, 303
Dynamic Host Configuration Protocol 49
Dynamic Secure Gateway Address 220
Dynamic WEP key exchange 104
dynamic WEP key exchange 383
DYNDNS Wildcard 140

E

EAP 92, 97, 98
EAP Authentication 488
  MD5 488
  TLS 488
  TTLS 488
EAP authentication 382
EAP Authentication Sequence 98
ECHO 132
E-mail
  Log Example 268
E-mail virus 204
embedded help 56
Encapsulated Routing Link Protocol (ENET ENCAP) 60
Encapsulation 49, 60, 214, 324, 327
  ENET ENCAP 60
  PPP over Ethernet 60
  PPPoA 60
  RFC 1483 61
encapsulation 49
Encapsulation Security Payload 218
Encryption 99, 212
Error Log 390
ESP 214
ESP Protocol 218
ESS 91, 483
ESS ID 91
ESSID (Extended Service Set Identification) 94
Example Internal SPTGEN Screens 504
Extended Service Set 483
Extended Service Set (ESS) 91
Extensible Authentication Protocol 92

F

Factory LAN Defaults 80
Fairness-based Scheduler 273
faulty Ethernet cables 454
FCC 3
FHSS 482
File infector 204
Filename Conventions 396
filename conventions 397
Filter 312, 362
  Applying Filters 373
  Ethernet Traffic 374
  Ethernet traffic 374
  Filter Rules 365

Filter structure **363**
Generic Filter Rule **369**
Remote Node **332**
Remote Node Filter **332**
Remote Node Filters **374**
Sample **372**
SUA **371**
TCP/IP Filter Rule **367**
Filter Log **392**
Filter Rule Process **363**
Filter Rule Setup **366**
Filter Set
Class **366**
Filtering **362**, **366**
Filtering Process
Outgoing Packets **362**
Finger **132**
Firewall
Access Methods **158**, **360**
Address Type **167**
Alerts **162**
Anti-Probing **175**
Attack alerts **176**
Connection Direction **161**
Creating/Editing Rules **165**
Custom Ports **168**
Enabling **162**
Firewall Vs Filters **155**
Guidelines For Enhancing Security **154**
Introduction **145**
LAN to WAN Rules **161**
Policies **158**
Remote Management **360**
Rule Checklist **159**
Rule Logic **159**
Rule Security Ramifications **160**
Services **173**
SMT menus **360**
Types **144**
When To Use **156**
firmware **293**, **396**
upgrade **293**
upload **293**
upload error **294**
Fragment Threshold **317**
Fragmentation Threshold **92**
Fragmentation threshold **92**
Frame Relay **51**
Frequency-Hopping Spread Spectrum **482**
FTP **132**, **246**, **419**
Restrictions **419**
FTP File Transfer **405**
FTP Restrictions **246**, **399**
FTP Server **355**

G

Gateway **338**
Gateway Node **342**
General Setup **302**
Generic filter **371**
Graphical User Interface (GUI) **45**

H

Half-Open Sessions **177**
hardware problem **454**
Hidden Menus **298**
Hidden node **91**
Hop Count **331**, **338**
Host **76**
Host IDs **472**
How Prestige virus scan works **206**
HTTP **132**, **144**, **146**, **147**, **440**, **441**
HTTP (Hypertext Transfer Protocol) **293**
HyperTerminal **409**, **410**
HyperTerminal program **401**, **404**

I

IANA **64**
IANA (Internet Assigned Number Authority) **168**
IBSS **483**
ICMP echo **149**
ID Type and Content **224**
Idle timeout **329**
IEEE 802.11 **482**
Deployment Issues **486**
Security Flaws **486**
IEEE 802.11g **46**
IEEE 802.11i **47**
IEEE 802.1x **486**
Additional requirements **90**
Advantages **486**
IEEE802.1x **382**
IGMP **81**
IGMP support **331**
IKE Phases **231**
Independent Basic Service Set **483**
Infrastructure Configuration **483**
initialization vector (IV) **99**

Inside Header **215**
Install UPnP **252**
  Windows Me **252**
  Windows XP **254**
Interactive Applications **422**
Internal SPTGEN **450**
  FTP Upload Example **452**
  Points to Remember **451**
  Text File **450**
Internal SPTGEN Screens **504**
Internal SPTGEN screens **504**
Internet Access **45**, **51**, **320**, **323**, **324**
Internet access **60**, **320**
Internet Access Setup **344**, **455**
Internet access wizard setup **61**
Internet Assigned Numbers AuthoritySee IANA **64**
Internet Control Message Protocol (ICMP) **148**, **175**
Internet Key Exchange **231**
Internet Protocol Security **212**
IP Address **62**, **80**, **132**, **288**, **314**, **338**, **342**, **368**, **389**, **394**, **424**
IP Address Assignment **63**
  ENET ENCAP **63**
  PPPoA or PPPoE **63**
  RFC 1483 **63**
IP Addressing **472**
IP alias **49**, **320**
IP Alias Setup **321**
IP Classes **472**
IP Filter **369**
  Logic Flow **368**
IP mask **367**
IP Packet **369**
IP Policies **426**
IP policy **320**
IP policy routing **422**
IP Policy Routing (IPPR) **49**, **320**
  Applying an IP Policy **426**
  Ethernet IP Policies **426**
  Gateway **426**
IP Pool Setup **69**
IP Ports **440**, **441**
IP Protocol **425**
IP protocol **422**
IP protocol type **173**
IP Routing Policy (IPPR) **422**
  Benefits **422**
  Cost Savings **422**
  Criteria **422**
  Load Sharing **422**
  Setup **423**
IP Spoofing **147**, **150**
IP Static Route **336**
IP Static Route Setup **337**
IPSec **212**
IPSec Algorithm **436**
IPSec algorithm **447**
IPSec Algorithms **214**, **218**
IPSec and NAT **215**
IPSec Architecture **213**
IPSec rule **435**
ISDN (Integrated Synchronous Digital System) **44**

K

Keep Alive **222**
Key Fields For Configuring Rules **160**
Key management protocol **383**

L

LAN **387**, **388**
LAN Setup **78**, **112**
LAN TCP/IP **80**
LAN to WAN Rules **161**
LAND **147**, **148**
LEDs **454**
Limitations of the Prestige packet scan **206**
Link type **387**
LLC-based Multiplexing **334**
Local Network
  Rule Summary **164**
Local User Database **384**
Local user database **108**
Log and Trace **390**
Log Facility **391**
Logging Option **368**, **370**
Logical networks **320**
Login **328**
Logs **264**

M

MAC (Media Access Control) **288**
MAC (Media Access Control) address. **95**
MAC address **342**

MAC Address Filter 317
MAC address filter 317
  Filter action 318
MAC Address Filter Action 96, 318
MAC Address Filtering 95
MAC filter 95
Macro virus 204
Main Menu 298
maintenance 284
management idle timeout period 55, 495
Management Information Base (MIB) 377
Manually Update Virus Information 209
Maximize Bandwidth Usage 273
Maximum Burst Size (MBS) 113, 116
Max-incomplete High 177
Max-incomplete Low 177
MBSSee Maximum Burst Size 324
MD5 488
MD5 (Message Digest 5) 442
MDI/MDI-X 48
Media Access Control 340
Media Bandwidth Management 47
Message Digest Algorithm 5 488
Message Integrity Check (MIC) 99
Message Logging 390
Metric 112, 122, 331, 338
MSDU (MAC Service Data Unit) 317
Multicast 81, 331
Multiplexing 49, 61, 324, 327
multiplexing 49, 61
  LLC-based 61
  VC-based 61
Multiprotocol Encapsulation 61
My IP Address 219
My WAN Address 330
myZyXEL.com 494
  device registration 495
  Login Screen 495
  Product Registration 496
  service activation 498
myZyXEL.com Account 494

N

Nailed-Up Connection 64
NAT 63, 132, 133, 371
  Address mapping rule 137
  Application 130
  Applying NAT in the SMT Menus 344
  Configuring 346
  Definitions 128
  Examples 352
  How it works 129
  Mapping Types 130
  Non NAT Friendly Application Programs 358
  Ordering Rules 349
  What it does 129
  What NAT does 129
NAT (Network Address Translation) 128
NAT mode 134
NAT Traversal 222, 250
NAT traversal 439
navigating the web configurator 56
Negotiation Mode 232, 442
NetBIOS commands 149
Network Address Translation 324
Network Address Translation (NAT) 47, 122, 344
Network Management 49, 132
Network Topology With RADIUS Server Example 487
NNTP 132

O

One-Minute High 177
Operating frequency 317
Outside Header 215

P

Packet
  Error 387
  Received 388
  Transmitted 387
Packet Filtering 155
Packet filtering
  When to use 155
Packet Filtering Firewalls 144
Packet Triggered 392
Packets 387
Pairwise Master Key (PMK) 99
PAP 329
Parental Control 184
Password 76, 296, 299, 328, 377
password 296, 456
Pattern file 204
Peak Cell Rate (PCR) 113, 116
Perfect Forward Secrecy 233
Perfect Forward Secrecy (PFS) 443

PFS 233
Ping 394
Ping of Death 48, 147
Point to Point Protocol over ATM Adaptation Layer 5 (AAL5) 60
Point-to-Point 42
Point-to-Point Tunneling Protocol 133
policy-based routing 422
POP3 132, 146, 147
Port Numbers 132
power 454
PPP (Point-to-Point Protocol) 97
PPP Encapsulation 334
PPP Log 393
PPP session over Ethernet (PPP over Ethernet, RFC 2516) 60
PPPoA 327
PPPoE 113, 480
  Benefits 113
PPPoE (Point-to-Point Protocol over Ethernet) 47, 113
PPPoE pass-through 335
PPTP 133
Precedence 422, 425
Pre-defined Web Content Categories 193
Pre-Shared Key 226, 383, 442
  Format 100
Prestige anti-virus packet scan 205
Prestige model 396
Prestige models 44
Prestige Wireless Security Levels 93
Priority 280
Priority-based Scheduler 273
Private 331, 338
Proportional Bandwidth Allocation 271
Protocol 367
Protocol filter 371
Protocol Filter Rules 371
protocol type 189
PSK 383
PVC (Permanent Virtual Circuit) 60

Q

Quality of Service 422
Quick Start Guide 40

R

Radio frequency 94
RADIUS 92, 97
  Configuring 109
  Shared Secret Key 98
RADIUS Message Types 97
RADIUS Messages 97
RADIUS server 380
RAS 389, 423
Rate
  Receiving 387
  Transmission 387
real-time alert message 500
real-time application 270
reinitialize the ADSL line 292
Related Documentation 40
Remote Authentication Dial-In User Service 92
Remote DHCP Server 314
Remote Management
  Firewall 360
remote management 457
Remote Management and NAT 247
Remote Management Limitations 246, 419
Remote Management Setup 418
Remote Node 326, 387
  Remote Node Profile 328
  Remote Node Setup 326
Remote node 326
Remote Node Index Number 387
Required fields 298
Reset button, the 55
resetting the Prestige 55
Restore Configuration 402
retry count 310
retry interval 310
RF (Radio Frequency) 46
RF signals 482
RFC 1483 61
RFC 1631 128
RFC-1483 327
RFC-2364 327, 328
RFC2516 47
RIP 315, 331
RIPSee Routing Information Protocol 80
romfile 396
Root Class 278
Routing 320
Routing Information Protocol 80
  Direction 80
  Version 80

Routing Policy **422**
RTS (Request To Send) **91**
RTS (Request To Send) threshold **94**
RTS Threshold **91**, **92**, **317**
RTS(Request To Send) **317**
Rule Summary **164**
Rules **161**
  Checklist **159**
  Key Fields **160**
  LAN to WAN **161**
  Logic **159**
  Predefined Services **173**
  Summary **164**

S

SA **212**, **440**
SA life time **442**
SA lifetime **446**
SA Monitor **446**
SA monitor **446**
Sample IP Addresses **331**
Saving the State **150**
Scanning engine **204**
Schedule Sets
  Duration **431**
Scheduler **272**
SCRSee Sustain Cell Rate **324**
Secure Gateway Address **219**, **439**
Security Association **212**, **446**
Security In General **154**
Security Parameter Index **236**
Security Parameter Index (SPI) **443**
Security Parameters **101**
security protocols **436**
Security Ramifications **160**
Serial Number **494**
Server **131**, **346**, **348**, **350**, **351**, **353**, **354**, **355**, **415**
Server behind NAT **350**
Service **4**, **160**
Service Type **169**, **455**
Services **132**
setup a schedule **431**
Shared secret **110**, **381**
Signature **204**
Signature-based **204**
Signature-based virus scan **204**
Single User Account (SUA) **51**
SMT Menu Overview **297**
SMTP **132**
SMTP Error Messages **267**
Smurf **148**, **149**
SNMP **132**, **133**
  Community **378**
  Configuration **377**
  Get **377**
  GetNext **377**
  Manager **376**
  MIBs **377**
  Set **377**
  Trap **377**
  Trusted Host **378**
SOHO (Small Office/Home Office) **51**
Source Address **160**, **167**
Source-Based Routing **422**
SPI **236**, **443**, **444**
SPTGEN (System Parameter Table Generator) **450**
SPTGEN Screens **504**
startup **501**
Stateful Inspection **45**, **144**, **145**, **150**, **151**
  Prestige **152**
  Process **151**
Static DHCP **84**
Static route **336**
Static Routing Topology **336**
SUA **131**, **133**
SUA (Single User Account) **122**, **131**, **344**
SUA server **132**, **134**
  Default server set **132**
SUA vs NAT **131**
SUA/NAT Server Set **135**
Sub-class Layers **278**
Subnet Mask **62**, **80**, **167**, **315**, **330**, **338**, **389**
Subnet Masks **473**
Subnetting **473**
Supporting Disk **40**
Sustain Cell Rate (SCR) **116**
Sustained Cell Rate (SCR) **113**
SYN Flood **147**, **148**
SYN flooding **48**
SYN-ACK **148**
Syntax Conventions **41**
Syslog **173**, **391**
Syslog IP Address **391**
Syslog Server **391**
System
  Console Port Speed **389**
  Diagnostic **393**
  Log and Trace **390**
  Syslog and Accounting **391**
  System Information **388**

System Status 386
System Information 388
System Information & Diagnosis 386
System Maintenance 267, 386, 388, 397, 400, 407, 408, 412, 413, 415
System Management Terminal 297
System password 380
System Security 380
System Status 387
System Timeout 247, 420

T

task bar properties 501
TCP Maximum Incomplete 177, 178
TCP Security 152
TCP/IP 146, 147, 247, 371, 394
Teardrop 147
Telnet 247, 296
Telnet Configuration 247
Temporal Key Integrity Protocol (TKIP) 99
Text File Format 450
TFTP
  Restrictions 419
TFTP File Transfer 407
TFTP Restrictions 246, 399
The DeMilitarized Zone (DMZ) 86
Three-Way Handshake 148
Threshold Values 177
Time and Date Setting 414, 415
Time Zone 416
Timeout 307
TKIP 99
TLS 488
TOS (Type of Service) 422
Trace Records 390
Traceroute 150
Traffic Redirect 117, 118
  Setup 307
Traffic redirect 117
traffic redirect 47
Traffic shaping 113
Transmission Rates 45
Transport Layer Security 488
Transport Mode 215
Triangle 490
Triangle Route Solutions 491
Triple DES (3DES) 442
TTLS 488
Tunnel Mode 215
Tunneled Transport Layer Service 488
Type of Service 422, 424, 425, 426

U

UBR (Unspecified Bit Rate) 116
UDP/ICMP Security 153
Universal Plug and Play 250
  Application 250
  Security issues 250
Universal Plug and Play (UPnP) 47
Universal Plug and Play Forum 251
UNIX Syslog 390, 391
UNIX syslog parameters 391
Update Schedule 209
Update the virus scan 210
Upload Firmware 405
UPnP 250
Upper Layer Protocols 152, 153
URL keyword blocking 191
User Authentication 99
User Name 141
User Profiles 108
user profiles 384

V

VBR (Variable Bit Rate) 116
VC-based Multiplexing 327
Virtual Channel Identifier (VCI) 61
virtual circuit (VC) 61
Virtual Path Identifier (VPI) 61
Virtual Private Network 212
Virus attack 204
Virus life cycle 205
Voice-over-IP (VoIP) 270
VPI & VCI 61
VPN 212
VPN Applications 213
VPN/IPSec 434

W

WAN (Wide Area Network) **112**
WAN backup **118**
  Advanced configuration **121**
  Authentication type **122**
WAN Setup **306**
WAN to LAN Rules **161**
Web Configurator **54**, **56**, **145**, **154**, **160**, **361**
web configurator screen summary **56**
web service **457**
Web Site Filters **191**
WEP
  Default Key **317**
WEP (Wired Equivalent Privacy) **47**, **95**, **317**
WEP Encryption **317**
WEP encryption **93**
Wi-Fi Protected Access **99**
Wi-Fi Protected Access (WPA) **47**
WinPopup window **500**
Wireless Client WPA Supplicants **102**
Wireless LAN **316**, **482**
  Benefits **482**
  Configuring **93**
Wireless LAN MAC Address Filtering **47**
Wireless LAN Setup **316**
Wireless port control **103**, **383**
Wireless security **92**
Wizard Setup **73**
WLAN **482**
  Interference **90**
  Security parameters **101**
Worm **204**
WPA **99**, **383**
  Supplicants **102**
  with RADIUS Application Example **100**
WPA Mixed Mode **383**
WPA -Pre-Shared Key **99**
WPA with RADIUS Application **100**
WPA-PSK **99**
WPA-PSK Application **100**

X

Xmodem
  File Upload **409**
XMODEM protocol **397**

Z

Zero Configuration Internet Access **45**
Zero configuration Internet access **114**
ZyNOS **397**
ZyNOS (ZyXEL Network Operating System) **396**
ZyNOS F/W Version **397**
ZyXEL Limited Warranty
  Note **4**
ZyXEL_s Firewall
  Introduction **145**
ZyXEL's online services center **494**