P-660H/HW/W-T Series

ADSL 2+ Gateway

User's Guide

Version 3.40
6/2005

ZyXEL

Copyright

Copyright © 2005 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

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 residential installation. 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. However, there is no guarantee that interference will not occur in a particular installation

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.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

FCC Caution

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

IMPORTANT NOTE: FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

ZyXEL Communications Corporation declared that Prestige 660HW-T1 is limited in CH1~11 from 2400 to 2483.5 MHz by specified firmware controlled in USA.

Certifications

Go to www.zyxel.com

1. Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.
2. Select the certification you wish to view from this page.

Safety Warnings

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

- To reduce the risk of fire, use only No. 26 AWG (American Wire Gauge) or larger telecommunication line cord.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel can service the device. Please contact your vendor for further information.
- Use ONLY the dedicated power supply for your device. Connect the power cord or power adaptor to the right supply voltage (110V AC in North America or 230V AC in Europe).
- Do NOT use the device if the power supply is damaged as it might cause electrocution.
- If the power supply is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power supply. Contact your local vendor to order a new power supply.
- Place connecting cables carefully so that no one will step on them or stumble over them. Do NOT allow anything to rest on the power cord and do NOT locate the product where anyone can walk on the power cord.
- If you wall mount your device, make sure that no electrical, gas or water pipes will be damaged.
- Do NOT install nor use your device during a thunderstorm. There may be a remote risk of electric shock from lightning.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Make sure to connect the cables to the correct ports.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Do NOT store things on the device.
- Connect ONLY suitable accessories to the device.

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.

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
CORPORATE HEADQUARTERS (WORLDWIDE)	support@zyxel.com.tw	+886-3-578-3942	www.zyxel.com www.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
	sales@zyxel.com.tw	+886-3-578-2439	ftp.zyxel.com ftp.europe.zyxel.com	
CZECH REPUBLIC	info@cz.zyxel.com	+420 241 091 350	www.zyxel.cz	ZyXEL Communications Czech s.r.o. Modranská 621 143 01 Praha 4 - Modrany Ceská Republika
	info@cz.zyxel.com	+420 241 091 359		
DENMARK	support@zyxel.dk	+45 39 55 07 00	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 5 2860 Soeborg Denmark
	sales@zyxel.dk	+45 39 55 07 07		
FINLAND	support@zyxel.fi	+358-9-4780-8411	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland
	sales@zyxel.fi	+358-9-4780 8448		
FRANCE	info@zyxel.fr	+33 (0)4 72 52 97 97	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
		+33 (0)4 72 52 19 20		
GERMANY	support@zyxel.de	+49-2405-6909-0	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
	sales@zyxel.de	+49-2405-6909-99		
NORTH AMERICA	support@zyxel.com	+1-800-255-4101 +1-714-632-0882	www.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
	sales@zyxel.com	+1-714-632-0858	ftp.us.zyxel.com	
NORWAY	support@zyxel.no	+47 22 80 61 80	www.zyxel.no	ZyXEL Communications A/S Nils Hansens vei 13 0667 Oslo Norway
	sales@zyxel.no	+47 22 80 61 81		
SPAIN	support@zyxel.es	+34 902 195 420	www.zyxel.es	ZyXEL Communications Alejandro Villegas 33 1º, 28043 Madrid Spain
	sales@zyxel.es	+34 913 005 345		
SWEDEN	support@zyxel.se	+46 31 744 7700	www.zyxel.se	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden
	sales@zyxel.se	+46 31 744 7701		

METHOD / LOCATION	SUPPORT E-MAIL / SALES E-MAIL	TELEPHONE[A] / FAX	WEB SITE / FTP SITE	REGULAR MAIL
UNITED KINGDOM	support@zyxel.co.uk	+44 (0) 1344 303044 08707 555779 (UK only)	www.zyxel.co.uk	ZyXEL Communications UK Ltd.,11 The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom (UK)
	sales@zyxel.co.uk	+44 (0) 1344 303034	ftp.zyxel.co.uk	

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**

Safety Warnings **5**

ZyXEL Limited Warranty **6**

Customer Support **7**

Table of Contents **10**

List of Figures **24**

List of Tables **32**

Preface **38**

Introduction to DSL **40**

Chapter 1
Getting To Know Your Prestige **42**

1.1 Introducing the Prestige 42
1.2 Features 42
1.2.1 Wireless Features (P-660HW/P-660W) 45
1.3 Applications for the Prestige 46
1.3.1 Protected Internet Access 46
1.3.2 LAN to LAN Application 46
1.4 Front Panel LEDs 46
1.5 Hardware Connection 47

Chapter 2
Introducing the Web Configurator **48**

2.1 Web Configurator Overview 48
2.1.1 Accessing the Web Configurator 48
2.1.2 Resetting the Prestige 49
2.1.2.1 Using the Reset Button 49
2.1.3 Navigating the Web Configurator 50
2.2 Change Login Password 52

Chapter 3
Wizard Setup for Internet Access 54

3.1 Introduction 54
3.1.1 Internet Access Wizard Setup 54

Chapter 4
LAN Setup 62

4.1 LAN Overview 62
4.1.1 LANs, WANs and the Prestige 62
4.1.2 DHCP Setup 63
4.1.2.1 IP Pool Setup 63
4.1.3 DNS Server Address 63
4.1.4 DNS Server Address Assignment 63
4.2 LAN TCP/IP 64
4.2.1 IP Address and Subnet Mask 64
4.2.1.1 Private IP Addresses 65
4.2.2 RIP Setup 65
4.2.3 Multicast 66
4.2.4 Any IP 66
4.2.4.1 How Any IP Works 67
4.3 Configuring LAN 68

Chapter 5
Wireless LAN 70

5.1 Wireless LAN Introduction 70
5.2 Wireless Security Overview 70
5.2.1 Encryption 70
5.2.2 Authentication 70
5.2.3 Restricted Access 71
5.2.4 Hide Prestige Identity 71
5.3 The Main Wireless LAN Screen 71
5.4 Configuring the Wireless Screen 73
5.4.1 WEP Encryption 73
5.5 Configuring MAC Filters 75
5.6 Introduction to WPA 77
5.6.1 WPA-PSK Application Example 77
5.6.2 WPA with RADIUS Application Example 78
5.6.3 Wireless Client WPA Supplicants 79
5.7 Configuring IEEE 802.1x and WPA 79
5.7.1 No Access Allowed or Authentication 80
5.7.2 Authentication Required: 802.1x 80
5.7.3 Authentication Required: WPA 82
5.7.4 Authentication Required: WPA-PSK 84

5.8 Configuring Local User Authentication 85
5.9 Configuring RADIUS 87

Chapter 6
WAN Setup 90

6.1 WAN Overview 90
6.1.1 Encapsulation 90
6.1.1.1 ENET ENCAP 90
6.1.1.2 PPP over Ethernet 90
6.1.1.3 PPPoA 90
6.1.1.4 RFC 1483 91
6.1.2 Multiplexing 91
6.1.2.1 VC-based Multiplexing 91
6.1.2.2 LLC-based Multiplexing 91
6.1.3 VPI and VCI 91
6.1.4 IP Address Assignment 91
6.1.4.1 IP Assignment with PPPoA or PPPoE Encapsulation 91
6.1.4.2 IP Assignment with RFC 1483 Encapsulation 92
6.1.4.3 IP Assignment with ENET ENCAP Encapsulation 92
6.1.5 Nailed-Up Connection (PPP) 92
6.1.6 NAT 92
6.2 Metric 92
6.3 PPPoE Encapsulation 93
6.4 Traffic Shaping 93
6.5 Zero Configuration Internet Access 94
6.6 The Main WAN Screen 95
6.7 Configuring WAN Setup 95
6.8 Traffic Redirect 98
6.9 Configuring WAN Backup 99

Chapter 7
Network Address Translation (NAT) Screens 102

7.1 NAT Overview 102
7.1.1 NAT Definitions 102
7.1.2 What NAT Does 103
7.1.3 How NAT Works 103
7.1.4 NAT Application 104
7.1.5 NAT Mapping Types 105
7.2 SUA (Single User Account) Versus NAT 106
7.3 SUA Server 106
7.3.1 Default Server IP Address 106
7.3.2 Port Forwarding: Services and Port Numbers 106
7.3.3 Configuring Servers Behind SUA (Example) 107

7.4 Selecting the NAT Mode 107
7.5 Configuring SUA Server Set 108
7.6 Configuring Address Mapping Rules 110
7.7 Editing an Address Mapping Rule 111

Chapter 8
Dynamic DNS Setup 114

8.1 Dynamic DNS Overview 114
8.1.1 DYNDNS Wildcard 114
8.2 Configuring Dynamic DNS 114

Chapter 9
Time and Date 116

9.1 Configuring Time and Date 116

Chapter 10
Firewalls 118

10.1 Firewall Overview 118
10.2 Types of Firewalls 118
10.2.1 Packet Filtering Firewalls 118
10.2.2 Application-level Firewalls 119
10.2.3 Stateful Inspection Firewalls 119
10.3 Introduction to ZyXEL's Firewall 119
10.3.1 Denial of Service Attacks 120
10.4 Denial of Service 120
10.4.1 Basics 120
10.4.2 Types of DoS Attacks 121
10.4.2.1 ICMP Vulnerability 123
10.4.2.2 Illegal Commands (NetBIOS and SMTP) 123
10.4.2.3 Traceroute 124
10.5 Stateful Inspection 124
10.5.1 Stateful Inspection Process 125
10.5.2 Stateful Inspection and the Prestige 126
10.5.3 TCP Security 126
10.5.4 UDP/ICMP Security 127
10.5.5 Upper Layer Protocols 127
10.6 Guidelines for Enhancing Security with Your Firewall 127
10.6.1 Security In General 128
10.7 Packet Filtering Vs Firewall 129
10.7.1 Packet Filtering: 129
10.7.1.1 When To Use Filtering 129
10.7.2 Firewall 129
10.7.2.1 When To Use The Firewall 129

Chapter 11
Firewall Configuration 132

11.1 Access Methods 132
11.2 Firewall Policies Overview 132
11.3 Rule Logic Overview 133
11.3.1 Rule Checklist 133
11.3.2 Security Ramifications 133
11.3.3 Key Fields For Configuring Rules 134
11.3.3.1 Action 134
11.3.3.2 Service 134
11.3.3.3 Source Address 134
11.3.3.4 Destination Address 134
11.4 Connection Direction 134
11.4.1 LAN to WAN Rules 134
11.4.2 Alerts 135
11.5 Configuring Default Firewall Policy 135
11.6 Rule Summary 136
11.6.1 Configuring Firewall Rules 138
11.7 Customized Services 141
11.8 Configuring A Customized Service 141
11.9 Example Firewall Rule 142
11.10 Predefined Services 146
11.11 Anti-Probing 148
11.12 DoS Thresholds 149
11.12.1 Threshold Values 150
11.12.2 Half-Open Sessions 150
11.12.2.1 TCP Maximum Incomplete and Blocking Time 150
11.12.3 Configuring Firewall Thresholds 151

Chapter 12
Content Filtering 154

12.1 Content Filtering Overview 154
12.2 The Main Content Filter Screen 154
12.3 Configuring Keyword Blocking 155
12.4 Configuring the Schedule 156
12.5 Configuring Trusted Computers 156

Chapter 13
Remote Management Configuration 158

13.1 Remote Management Overview 158
13.1.1 Remote Management Limitations 158
13.1.2 Remote Management and NAT 159
13.1.3 System Timeout 159

13.2 Telnet 159
13.3 FTP 160
13.4 Web 160
13.5 Configuring Remote Management 160

Chapter 14
Universal Plug-and-Play (UPnP) 162

14.1 Introducing Universal Plug and Play 162
14.1.1 How do I know if I'm using UPnP? 162
14.1.2 NAT Traversal 162
14.1.3 Cautions with UPnP 163
14.2 UPnP and ZyXEL 163
14.2.1 Configuring UPnP 163
14.3 Installing UPnP in Windows Example 164
14.4 Using UPnP in Windows XP Example 168

Chapter 15
Logs Screens..... 176

15.1 Logs Overview 176
15.1.1 Alerts and Logs 176
15.2 Configuring Log Settings 176
15.3 Displaying the Logs 178
15.4 SMTP Error Messages 179
15.4.1 Example E-mail Log 180

Chapter 16
Media Bandwidth Management Advanced Setup..... 182

16.1 Media Bandwidth Management Overview 182
16.2 Bandwidth Classes and Filters 182
16.3 Proportional Bandwidth Allocation 183
16.4 Bandwidth Management Usage Examples 183
16.4.1 Application-based Bandwidth Management Example 183
16.4.2 Subnet-based Bandwidth Management Example 183
16.4.3 Application and Subnet-based Bandwidth Management Example 184
16.5 Scheduler 185
16.5.1 Priority-based Scheduler 185
16.5.2 Fairness-based Scheduler 185
16.6 Maximize Bandwidth Usage 185
16.6.1 Reserving Bandwidth for Non-Bandwidth Class Traffic 185
16.6.2 Maximize Bandwidth Usage Example 186
16.7 Bandwidth Borrowing 187
16.7.1 Maximize Bandwidth Usage With Bandwidth Borrowing 187
16.8 The Main Media Bandwidth Management Screen 188

16.9 Configuring Summary 188
16.10 Configuring Class Setup 190
16.10.1 Media Bandwidth Management Class Configuration 190
16.10.2 Media Bandwidth Management Statistics 193
16.11 Bandwidth Monitor 194

Chapter 17
Maintenance 196

17.1 Maintenance Overview 196
17.2 System Status Screen 196
17.2.1 System Statistics 198
17.3 DHCP Table Screen 200
17.4 Any IP Table Screen 201
17.5 Wireless Screen 201
17.5.1 Association List 201
17.6 Diagnostic Screens 202
17.6.1 General Diagnostic 202
17.6.2 DSL Line Diagnostic 203
17.7 Firmware Upgrade 205

Chapter 18
Introducing the SMT 208

18.1 SMT Introduction 208
18.1.1 Procedure for SMT Configuration via Telnet 208
18.1.2 Entering Password 208
18.1.3 Prestige SMT Menus Overview 209
18.2 Navigating the SMT Interface 210
18.2.1 System Management Terminal Interface Summary 211
18.3 Changing the System Password 212

Chapter 19
Menu 1 General Setup 214

19.1 General Setup 214
19.2 Procedure To Configure Menu 1 214
19.2.1 Procedure to Configure Dynamic DNS 215

Chapter 20
Menu 2 WAN Backup Setup 218

20.1 Introduction to WAN Backup Setup 218
20.2 Configuring Dial Backup in Menu 2 218
20.2.1 Traffic Redirect Setup 219

Chapter 21
Menu 3 LAN Setup 222

21.1 LAN Setup 222
21.1.1 General Ethernet Setup 222
21.2 Protocol Dependent Ethernet Setup 223
21.3 TCP/IP Ethernet Setup and DHCP 223

Chapter 22
Wireless LAN Setup 226

22.1 Wireless LAN Overview 226
22.2 Wireless LAN Setup 226
22.2.1 Wireless LAN MAC Address Filter 227

Chapter 23
Internet Access 230

23.1 Internet Access Overview 230
23.2 IP Policies 230
23.3 IP Alias 230
23.4 IP Alias Setup 231
23.5 Route IP Setup 232
23.6 Internet Access Configuration 233

Chapter 24
Remote Node Configuration 236

24.1 Remote Node Setup Overview 236
24.2 Remote Node Setup 236
24.2.1 Remote Node Profile 236
24.2.2 Encapsulation and Multiplexing Scenarios 237
24.2.2.1 Scenario 1: One VC, Multiple Protocols 237
24.2.2.2 Scenario 2: One VC, One Protocol (IP) 237
24.2.2.3 Scenario 3: Multiple VCs 237
24.2.3 Outgoing Authentication Protocol 239
24.3 Remote Node Network Layer Options 240
24.3.1 My WAN Addr Sample IP Addresses 241
24.4 Remote Node Filter 242
24.5 Editing ATM Layer Options 243
24.5.1 VC-based Multiplexing (non-PPP Encapsulation) 243
24.5.2 LLC-based Multiplexing or PPP Encapsulation 243
24.5.3 Advance Setup Options 244

Chapter 25
Static Route Setup 246

25.1 IP Static Route Overview 246

25.2 Configuration 246

Chapter 26
Bridging Setup 250

26.1 Bridging in General 250
26.2 Bridge Ethernet Setup 250
26.2.1 Remote Node Bridging Setup 250
26.2.2 Bridge Static Route Setup 252

Chapter 27
Network Address Translation (NAT) 254

27.1 Using NAT 254
27.1.1 SUA (Single User Account) Versus NAT 254
27.2 Applying NAT 254
27.3 NAT Setup 256
27.3.1 Address Mapping Sets 256
27.3.1.1 SUA Address Mapping Set 257
27.3.1.2 User-Defined Address Mapping Sets 258
27.3.1.3 Ordering Your Rules 259
27.4 Configuring a Server behind NAT 260
27.5 General NAT Examples 261
27.5.1 Example 1: Internet Access Only 262
27.5.2 Example 2: Internet Access with an Inside Server 262
27.5.3 Example 3: Multiple Public IP Addresses With Inside Servers 263
27.5.4 Example 4: NAT Unfriendly Application Programs 267

Chapter 28
Enabling the Firewall 270

28.1 Remote Management and the Firewall 270
28.2 Access Methods 270
28.3 Enabling the Firewall 270

Chapter 29
Filter Configuration 272

29.1 About Filtering 272
29.1.1 The Filter Structure of the Prestige 273
29.2 Configuring a Filter Set for the Prestige 274
29.3 Filter Rules Summary Menus 275
29.4 Configuring a Filter Rule 276
29.4.1 TCP/IP Filter Rule 277
29.4.2 Generic Filter Rule 279
29.5 Filter Types and NAT 281
29.6 Example Filter 281

29.7 Applying Filters and Factory Defaults 283
29.7.1 Ethernet Traffic 284
29.7.2 Remote Node Filters 284

Chapter 30
SNMP Configuration 286

30.1 About SNMP 286
30.2 Supported MIBs 287
30.3 SNMP Configuration 287
30.4 SNMP Traps 288

Chapter 31
System Security 290

31.1 System Security 290
31.1.1 System Password 290
31.1.2 Configuring External RADIUS Server 290
31.1.3 IEEE 802.1x 292
31.2 Creating User Accounts on the Prestige 294

Chapter 32
System Information and Diagnosis 296

32.1 Overview 296
32.2 System Status 296
32.3 System Information 298
32.3.1 System Information 298
32.3.2 Console Port Speed 299
32.4 Log and Trace 300
32.4.1 Viewing Error Log 300
32.4.2 Syslog and Accounting 301
32.5 Diagnostic 303

Chapter 33
Firmware and Configuration File Maintenance 306

33.1 Filename Conventions 306
33.2 Backup Configuration 307
33.2.1 Backup Configuration 307
33.2.2 Using the FTP Command from the Command Line 308
33.2.3 Example of FTP Commands from the Command Line 308
33.2.4 GUI-based FTP Clients 309
33.2.5 TFTP and FTP over WAN Management Limitations 309
33.2.6 Backup Configuration Using TFTP 310
33.2.7 TFTP Command Example 310
33.2.8 GUI-based TFTP Clients 310

33.3 Restore Configuration 311
33.3.1 Restore Using FTP 311
33.3.2 Restore Using FTP Session Example 312
33.4 Uploading Firmware and Configuration Files 313
33.4.1 Firmware File Upload 313
33.4.2 Configuration File Upload 313
33.4.3 FTP File Upload Command from the DOS Prompt Example 314
33.4.4 FTP Session Example of Firmware File Upload 315
33.4.5 TFTP File Upload 315
33.4.6 TFTP Upload Command Example 316

Chapter 34
System Maintenance 318

34.1 Command Interpreter Mode 318
34.2 Call Control Support 319
34.2.1 Budget Management 319
34.3 Time and Date Setting 320
34.3.1 Resetting the Time 322

Chapter 35
Remote Management 324

35.1 Remote Management Overview 324
35.2 Remote Management 324
35.2.1 Remote Management Setup 324
35.2.2 Remote Management Limitations 325
35.3 Remote Management and NAT 326
35.4 System Timeout 326

Chapter 36
IP Policy Routing 328

36.1 IP Policy Routing Overview 328
36.2 Benefits of IP Policy Routing 328
36.3 Routing Policy 328
36.4 IP Routing Policy Setup 329
36.5 Applying an IP Policy 332
36.5.1 Ethernet IP Policies 332
36.6 IP Policy Routing Example 333

Chapter 37
Call Scheduling 338

37.1 Introduction 338

Chapter 38
Troubleshooting 342

38.1 Problems Starting Up the Prestige 342
38.2 Problems with the LAN 342
38.3 Problems with the WAN 343
38.4 Problems Accessing the Prestige 344
38.4.1 Pop-up Windows, JavaScripts and Java Permissions 344
38.4.1.1 Internet Explorer Pop-up Blockers 344
38.4.1.2 JavaScripts 347
38.4.1.3 Java Permissions 349
38.4.2 ActiveX Controls in Internet Explorer 351

Appendix A
Product Specifications 354

Appendix B
Wall-mounting Instructions 358

Appendix C
Setting up Your Computer's IP Address 360

Windows 95/98/Me 360
Windows 2000/NT/XP 363
Macintosh OS 8/9 368
Macintosh OS X 370
Linux 371

Appendix D
IP Subnetting 376

IP Addressing 376
IP Classes 376
Subnet Masks 377
Subnetting 377
Example: Two Subnets 378
Example: Four Subnets 380
Example Eight Subnets 381
Subnetting With Class A and Class B Networks. 382

Appendix E
Boot Commands 384

Appendix F
Command Interpreter 386

Command Syntax 386

Command Usage 386

Appendix G
Firewall Commands 388

Appendix H
NetBIOS Filter Commands 394

Introduction 394
Display NetBIOS Filter Settings 394
NetBIOS Filter Configuration 395

Appendix I
Splitters and Microfilters 398

Connecting a POTS Splitter 398
Telephone Microfilters 398
Prestige With ISDN 399

Appendix J
PPPoE 402

PPPoE in Action 402
Benefits of PPPoE 402
Traditional Dial-up Scenario 402
How PPPoE Works 403
Prestige as a PPPoE Client 403

Appendix K
Log Descriptions 404

Log Commands 418
Log Command Example 419

Appendix L
Wireless LANs 420

Wireless LAN Topologies 420
Channel 422
RTS/CTS 422
Fragmentation Threshold 423
Preamble Type 424
IEEE 802.1x 425
RADIUS 425
Types of Authentication 426
WPA 428
Security Parameters Summary 429

Appendix M
Internal SPTGEN 430

Internal SPTGEN Overview 430
The Configuration Text File Format 430
Internal SPTGEN FTP Download Example 431
Internal SPTGEN FTP Upload Example 432
Command Examples 453

Index 456

List of Figures

Figure 1 Protected Internet Access Applications 46
Figure 2 LAN-to-LAN Application Example 46
Figure 3 Password Screen 49
Figure 4 Change Password at Login 49
Figure 5 Web Configurator: Site Map Screen 50
Figure 6 Password 52
Figure 7 Internet Access Wizard Setup: ISP Parameters 54
Figure 8 Internet Connection with PPPoE 55
Figure 9 Internet Connection with RFC 1483 56
Figure 10 Internet Connection with ENET ENCAP 57
Figure 11 Internet Connection with PPPoA 58
Figure 12 Internet Access Wizard Setup: Third Screen 59
Figure 13 Internet Access Wizard Setup: LAN Configuration 59
Figure 14 Internet Access Wizard Setup: Connection Tests 60
Figure 15 LAN and WAN IP Addresses 62
Figure 16 Any IP Example 67
Figure 17 LAN Setup 68
Figure 18 Wireless LAN 72
Figure 19 Wireless Security Methods 73
Figure 20 Wireless Screen 74
Figure 21 MAC Filter 76
Figure 22 WPA - PSK Authentication 78
Figure 23 WPA with RADIUS Application Example2 79
Figure 24 Wireless LAN: 802.1x/WPA: No Access Allowed 80
Figure 25 Wireless LAN: 802.1x/WPA: No Authentication 80
Figure 26 Wireless LAN: 802.1x/WPA: 802.1xl 81
Figure 27 Wireless LAN: 802.1x/WPA: WPA 83
Figure 28 Wireless LAN: 802.1x/WPA:WPA-PSK 84
Figure 29 Local User Database 86
Figure 30 RADIUS 87
Figure 31 Example of Traffic Shaping 94
Figure 32 WAN 95
Figure 33 WAN Setup (PPPoE) 96
Figure 34 Traffic Redirect Example 99
Figure 35 Traffic Redirect LAN Setup 99
Figure 36 WAN Backup 100
Figure 37 How NAT Works 104
Figure 38 NAT Application With IP Alias 104

Figure 39 Multiple Servers Behind NAT Example 107
Figure 40 NAT Mode 108
Figure 41 Edit SUA/NAT Server Set 109
Figure 42 Address Mapping Rules 110
Figure 43 Edit Address Mapping Rule 112
Figure 44 Dynamic DNS 115
Figure 45 Time and Date 116
Figure 46 Prestige Firewall Application 120
Figure 47 Three-Way Handshake 122
Figure 48 SYN Flood 122
Figure 49 Smurf Attack 123
Figure 50 Stateful Inspection 125
Figure 51 Firewall: Default Policy 135
Figure 52 Firewall: Rule Summary 137
Figure 53 Firewall: Edit Rule 139
Figure 54 Firewall: Customized Services 141
Figure 55 Firewall: Configure Customized Services 142
Figure 56 Firewall Example: Rule Summary 143
Figure 57 Firewall Example: Edit Rule: Destination Address 144
Figure 58 Edit Custom Port Example 144
Figure 59 Firewall Example: Edit Rule: Select Customized Services 145
Figure 60 Firewall Example: Rule Summary: My Service 146
Figure 61 Firewall: Anti Probing 149
Figure 62 Firewall: Threshold 151
Figure 63 Content Filtering 154
Figure 64 Content Filter: Keyword 155
Figure 65 Content Filter: Schedule 156
Figure 66 Content Filter: Trusted 157
Figure 67 Telnet Configuration on a TCP/IP Network 159
Figure 68 Remote Management 160
Figure 69 Configuring UPnP 163
Figure 70 Add/Remove Programs: Windows Setup: Communication 165
Figure 71 Add/Remove Programs: Windows Setup: Communication: Components 165
Figure 72 Network Connections 166
Figure 73 Windows Optional Networking Components Wizard 167
Figure 74 Networking Services 168
Figure 75 Network Connections 169
Figure 76 Internet Connection Properties 170
Figure 77 Internet Connection Properties: Advanced Settings 171
Figure 78 Internet Connection Properties: Advanced Settings: Add 171
Figure 79 System Tray Icon 172
Figure 80 Internet Connection Status 172
Figure 81 Network Connections 173

Figure 82 Network Connections: My Network Places 174
Figure 83 Network Connections: My Network Places: Properties: Example 174
Figure 84 Log Settings 177
Figure 85 View Logs 179
Figure 86 E-mail Log Example 180
Figure 87 Application-based Bandwidth Management Example 183
Figure 88 Subnet-based Bandwidth Management Example 184
Figure 89 Application and Subnet-based Bandwidth Management Example 184
Figure 90 Bandwidth Allotment Example 186
Figure 91 Maximize Bandwidth Usage Example 187
Figure 92 Media Bandwidth Mgnt. 188
Figure 93 Media Bandwidth Management: Summary 189
Figure 94 Media Bandwidth Management: Class Setup 190
Figure 95 Media Bandwidth Management: Class Configuration 191
Figure 96 Media Bandwidth Management Statistics 193
Figure 97 Media Bandwidth Management: Monitor 194
Figure 98 System Status 197
Figure 99 System Status: Show Statistics 199
Figure 100 DHCP Table 200
Figure 101 Any IP Table 201
Figure 102 Association List 202
Figure 103 Diagnostic: General 203
Figure 104 Diagnostic: DSL Line 204
Figure 105 Firmware Upgrade 205
Figure 106 Network Temporarily Disconnected 206
Figure 107 Error Message 206
Figure 108 Login Screen 209
Figure 109 Menu 23.1 Change Password 212
Figure 110 Menu 1 General Setup 215
Figure 111 Menu 1.1 Configure Dynamic DNS 216
Figure 112 Menu 2 WAN Backup Setup 218
Figure 113 Menu 2.1Traffic Redirect Setup 219
Figure 114 Menu 3 LAN Setup 222
Figure 115 Menu 3.1 LAN Port Filter Setup 222
Figure 116 Menu 3.2 TCP/IP and DHCP Ethernet Setup 223
Figure 117 Menu 3.5 - Wireless LAN Setup 226
Figure 118 Menu 3.5.1 WLAN MAC Address Filtering 228
Figure 119 IP Alias Network Example 231
Figure 120 Menu 3.2 TCP/IP and DHCP Setup 231
Figure 121 Menu 3.2.1 IP Alias Setup 232
Figure 122 Menu 1 General Setup 233
Figure 123 Menu 4 Internet Access Setup 233
Figure 124 Menu 11 Remote Node Setup 237

Figure 125 Menu 11.1 Remote Node Profile 238
Figure 126 Menu 11.3 Remote Node Network Layer Options 240
Figure 127 Sample IP Addresses for a TCP/IP LAN-to-LAN Connection 242
Figure 128 Menu 11.5 Remote Node Filter (RFC 1483 or ENET Encapsulation) 242
Figure 129 Menu 11.5 Remote Node Filter (PPPoA or PPPoE Encapsulation) 243
Figure 130 Menu 11.6 for VC-based Multiplexing 243
Figure 131 Menu 11.6 for LLC-based Multiplexing or PPP Encapsulation 244
Figure 132 Menu 11.1 Remote Node Profile 244
Figure 133 Menu 11.8 Advance Setup Options 245
Figure 134 Sample Static Routing Topology 246
Figure 135 Menu 12 Static Route Setup 247
Figure 136 Menu 12.1 IP Static Route Setup 247
Figure 137 Menu12.1.1 Edit IP Static Route 247
Figure 138 Menu 11.1 Remote Node Profile 251
Figure 139 Menu 11.3 Remote Node Network Layer Options 251
Figure 140 Menu 12.3.1 Edit Bridge Static Route 252
Figure 141 Menu 4 Applying NAT for Internet Access 255
Figure 142 Applying NAT in Menus 4 & 11.3 255
Figure 143 Menu 15 NAT Setup 256
Figure 144 Menu 15.1 Address Mapping Sets 257
Figure 145 Menu 15.1.255 SUA Address Mapping Rules 257
Figure 146 Menu 15.1.1 First Set 258
Figure 147 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set 259
Figure 148 Menu 15.2 NAT Server Setup 260
Figure 149 Menu 15.2.1 NAT Server Setup 261
Figure 150 Multiple Servers Behind NAT Example 261
Figure 151 NAT Example 1 262
Figure 152 Menu 4 Internet Access & NAT Example 262
Figure 153 NAT Example 2 263
Figure 154 Menu 15.2.1 Specifying an Inside Server 263
Figure 155 NAT Example 3 264
Figure 156 Example 3: Menu 11.3 265
Figure 157 Example 3: Menu 15.1.1.1 265
Figure 158 Example 3: Final Menu 15.1.1 266
Figure 159 Example 3: Menu 15.2.1 266
Figure 160 NAT Example 4 267
Figure 161 Example 4: Menu 15.1.1.1 Address Mapping Rule 267
Figure 162 Example 4: Menu 15.1.1 Address Mapping Rules 268
Figure 163 Menu 21.2 Firewall Setup 271
Figure 164 Outgoing Packet Filtering Process 272
Figure 165 Filter Rule Process 273
Figure 166 Menu 21 Filter Set Configuration 274
Figure 167 NetBIOS_WAN Filter Rules Summary 274

Figure 168 NetBIOS_LAN Filter Rules Summary 275
Figure 169 IGMP Filter Rules Summary 275
Figure 170 Menu 21.1.x.1 TCP/IP Filter Rule 277
Figure 171 Executing an IP Filter 279
Figure 172 Menu 21.1.5.1 Generic Filter Rule 280
Figure 173 Protocol and Device Filter Sets 281
Figure 174 Sample Telnet Filter 282
Figure 175 Menu 21.1.6.1 Sample Filter 282
Figure 176 Menu 21.1.6.1 Sample Filter Rules Summary 283
Figure 177 Filtering Ethernet Traffic 284
Figure 178 Filtering Remote Node Traffic 284
Figure 179 SNMP Management Model 286
Figure 180 Menu 22 SNMP Configuration 288
Figure 181 Menu 23 – System Security 290
Figure 182 Menu 23.2 System Security: RADIUS Server 291
Figure 183 Menu 23 System Security 292
Figure 184 Menu 23.4 System Security: IEEE 802.1x 292
Figure 185 Menu 14 Dial-in User Setup 295
Figure 186 Menu 14.1 Edit Dial-in User 295
Figure 187 Menu 24 System Maintenance 296
Figure 188 Menu 24.1 System Maintenance : Status 297
Figure 189 Menu 24.2 System Information and Console Port Speed 298
Figure 190 Menu 24.2.1 System Maintenance: Information 299
Figure 191 Menu 24.2.2 System Maintenance : Change Console Port Speed 300
Figure 192 Menu 24.3 System Maintenance: Log and Trace 300
Figure 193 Sample Error and Information Messages 301
Figure 194 Menu 24.3.2 System Maintenance: Syslog and Accounting 301
Figure 195 Syslog Example 302
Figure 196 Menu 24.4 System Maintenance : Diagnostic 303
Figure 197 Telnet in Menu 24.5 308
Figure 198 FTP Session Example 309
Figure 199 Telnet into Menu 24.6 312
Figure 200 Restore Using FTP Session Example 312
Figure 201 Telnet Into Menu 24.7.1 Upload System Firmware 313
Figure 202 Telnet Into Menu 24.7.2 System Maintenance 314
Figure 203 FTP Session Example of Firmware File Upload 315
Figure 204 Command Mode in Menu 24 318
Figure 205 Valid Commands 318
Figure 206 Menu 24.9 System Maintenance: Call Control 319
Figure 207 Menu 24.9.1 System Maintenance: Budget Management 320
Figure 208 Menu 24 System Maintenance 321
Figure 209 Menu 24.10 System Maintenance: Time and Date Setting 321
Figure 210 Menu 24.11 Remote Management Control 325

Figure 211 Menu 25 IP Routing Policy Setup 329
Figure 212 Menu 25.1 IP Routing Policy Setup 330
Figure 213 Menu 25.1.1 IP Routing Policy 331
Figure 214 Menu 3.2 TCP/IP and DHCP Ethernet Setup 333
Figure 215 Menu 11.3 Remote Node Network Layer Options 333
Figure 216 Example of IP Policy Routing 334
Figure 217 IP Routing Policy Example 335
Figure 218 IP Routing Policy Example 336
Figure 219 Applying IP Policies Example 336
Figure 220 Menu 26 Schedule Setup 338
Figure 221 Menu 26.1 Schedule Set Setup 339
Figure 222 Applying Schedule Set(s) to a Remote Node (PPPoE) 340
Figure 223 Pop-up Blocker 345
Figure 224 Internet Options 345
Figure 225 Internet Options 346
Figure 226 Pop-up Blocker Settings 347
Figure 227 Internet Options 348
Figure 228 Security Settings - Java Scripting 349
Figure 229 Security Settings - Java 350
Figure 230 Java (Sun) 351
Figure 231 Internet Options Security 352
Figure 232 Security Setting ActiveX Controls 353
Figure 233 WIndows 95/98/Me: Network: Configuration 361
Figure 234 Windows 95/98/Me: TCP/IP Properties: IP Address 362
Figure 235 Windows 95/98/Me: TCP/IP Properties: DNS Configuration 363
Figure 236 Windows XP: Start Menu 364
Figure 237 Windows XP: Control Panel 364
Figure 238 Windows XP: Control Panel: Network Connections: Properties 365
Figure 239 Windows XP: Local Area Connection Properties 365
Figure 240 Windows XP: Internet Protocol (TCP/IP) Properties 366
Figure 241 Windows XP: Advanced TCP/IP Properties 367
Figure 242 Windows XP: Internet Protocol (TCP/IP) Properties 368
Figure 243 Macintosh OS 8/9: Apple Menu 369
Figure 244 Macintosh OS 8/9: TCP/IP 369
Figure 245 Macintosh OS X: Apple Menu 370
Figure 246 Macintosh OS X: Network 371
Figure 247 Red Hat 9.0: KDE: Network Configuration: Devices 372
Figure 248 Red Hat 9.0: KDE: Ethernet Device: General 372
Figure 249 Red Hat 9.0: KDE: Network Configuration: DNS 373
Figure 250 **Red Hat 9.0: KDE: Network Configuration: Activate** 373
Figure 251 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0 374
Figure 252 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0 374
Figure 253 Red Hat 9.0: DNS Settings in resolv.conf 374

Figure 254 Red Hat 9.0: Restart Ethernet Card 375
Figure 255 Red Hat 9.0: Checking TCP/IP Properties 375
Figure 256 Option to Enter Debug Mode 384
Figure 257 Boot Module Commands 385
Figure 258 Connecting a POTS Splitter 398
Figure 259 Connecting a Microfilter 399
Figure 260 Prestige with ISDN 399
Figure 261 Single-Computer per Router Hardware Configuration 403
Figure 262 Prestige as a PPPoE Client 403
Figure 263 Displaying Log Categories Example 418
Figure 264 Displaying Log Parameters Example 418
Figure 265 Peer-to-Peer Communication in an Ad-hoc Network 420
Figure 266 Basic Service Set 421
Figure 267 Infrastructure WLAN 422
Figure 268 RTS/CTS 423
Figure 269 Configuration Text File Format: Column Descriptions 430
Figure 270 Invalid Parameter Entered: Command Line Example 431
Figure 271 Valid Parameter Entered: Command Line Example 431
Figure 272 Internal SPTGEN FTP Download Example 432
Figure 273 Internal SPTGEN FTP Upload Example 432

List of Tables

Table 1 ADSL Standards 42
Table 2 Front Panel LEDs 47
Table 3 Web Configurator Screens Summary 50
Table 4 Password 53
Table 5 Internet Access Wizard Setup: ISP Parameters 55
Table 6 Internet Connection with PPPoE 56
Table 7 Internet Connection with RFC 1483 56
Table 8 Internet Connection with ENET ENCAP 57
Table 9 Internet Connection with PPPoA 58
Table 10 Internet Access Wizard Setup: LAN Configuration 60
Table 11 LAN Setup 68
Table 12 Wireless LAN 72
Table 13 Wireless LAN 74
Table 14 MAC Filter 76
Table 15 Wireless LAN: 802.1x/WPA: No Access/Authentication 80
Table 16 Wireless LAN: 802.1x/WPA: 802.1x 81
Table 17 Wireless LAN: 802.1x/WPA: WPA 83
Table 18 Wireless LAN: 802.1x/WPA: WPA-PSK 84
Table 19 Local User Database 86
Table 20 RADIUS 87
Table 21 WAN 95
Table 22 WAN Setup 96
Table 23 WAN Backup 100
Table 24 NAT Definitions 102
Table 25 NAT Mapping Types 105
Table 26 Services and Port Numbers 106
Table 27 NAT Mode 108
Table 28 Edit SUA/NAT Server Set 109
Table 29 Address Mapping Rules 110
Table 30 Edit Address Mapping Rule 112
Table 31 Dynamic DNS 115
Table 32 Time and Date 117
Table 33 Common IP Ports 121
Table 34 ICMP Commands That Trigger Alerts 123
Table 35 Legal NetBIOS Commands 123
Table 36 Legal SMTP Commands 124
Table 37 Firewall: Default Policy 135
Table 38 Rule Summary 137

Table 39 Firewall: Edit Rule 140
Table 40 Customized Services 141
Table 41 Firewall: Configure Customized Services 142
Table 42 Predefined Services 146
Table 43 Firewall: Anti Probing 149
Table 44 Firewall: Threshold 152
Table 45 154
Table 46 Content Filter: Keyword 155
Table 47 Content Filter: Schedule 156
Table 48 Content Filter: Trusted 157
Table 49 Remote Management 160
Table 50 Configuring UPnP 164
Table 51 Log Settings 177
Table 52 View Logs 179
Table 53 SMTP Error Messages 179
Table 54 Application and Subnet-based Bandwidth Management Example 184
Table 55 Media Bandwidth Mgnt. 188
Table 56 Media Bandwidth Management: Summary 189
Table 57 Media Bandwidth Management: Class Setup 190
Table 58 Media Bandwidth Management: Class Configuration 191
Table 59 Services and Port Numbers 192
Table 60 Media Bandwidth Management Statistics 193
Table 61 Media Bandwidth Management: Monitor 194
Table 62 System Status 197
Table 63 System Status: Show Statistics 199
Table 64 DHCP Table 200
Table 65 Any IP Table 201
Table 66 Association List 202
Table 67 Diagnostic: General 203
Table 68 Diagnostic: DSL Line 204
Table 69 Firmware Upgrade 205
Table 70 SMT Menus Overview 209
Table 71 Navigating the SMT Interface 210
Table 72 SMT Main Menu 211
Table 73 Main Menu Summary 211
Table 74 Menu 1 General Setup 215
Table 75 Menu 1.1 Configure Dynamic DNS 216
Table 76 Menu 2 WAN Backup Setup 218
Table 77 Menu 2.1Traffic Redirect Setup 219
Table 78 DHCP Ethernet Setup 224
Table 79 TCP/IP Ethernet Setup 224
Table 80 Menu 3.5 - Wireless LAN Setup 226
Table 81 Menu 3.5.1 WLAN MAC Address Filtering 228

Table 82 Menu 3.2.1 IP Alias Setup 232
Table 83 Menu 4 Internet Access Setup 234
Table 84 Menu 11.1 Remote Node Profile 238
Table 85 Menu 11.3 Remote Node Network Layer Options 240
Table 86 Menu 11.8 Advance Setup Options 245
Table 87 Menu12.1.1 Edit IP Static Route 248
Table 88 Remote Node Network Layer Options: Bridge Fields 251
Table 89 Menu 12.3.1 Edit Bridge Static Route 252
Table 90 Applying NAT in Menus 4 & 11.3 256
Table 91 SUA Address Mapping Rules 257
Table 92 Menu 15.1.1 First Set 259
Table 93 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set 260
Table 94 Abbreviations Used in the Filter Rules Summary Menu 275
Table 95 Rule Abbreviations Used 276
Table 96 Menu 21.1.x.1 TCP/IP Filter Rule 277
Table 97 Menu 21.1.5.1 Generic Filter Rule 280
Table 98 Filter Sets Table 283
Table 99 Menu 22 SNMP Configuration 288
Table 100 SNMP Traps 288
Table 101 Ports and Permanent Virtual Circuits 289
Table 102 Menu 23.2 System Security: RADIUS Server 291
Table 103 Menu 23.4 System Security: IEEE 802.1x 293
Table 104 Menu 14.1 Edit Dial-in User 295
Table 105 Menu 24.1 System Maintenance: Status 297
Table 106 Menu 24.2.1 System Maintenance: Information 299
Table 107 Menu 24.3.2 System Maintenance : Syslog and Accounting 301
Table 108 Menu 24.4 System Maintenance Menu: Diagnostic 304
Table 109 Filename Conventions 307
Table 110 General Commands for GUI-based FTP Clients 309
Table 111 General Commands for GUI-based TFTP Clients 311
Table 112 Menu 24.9.1 System Maintenance: Budget Management 320
Table 113 Menu 24.10 System Maintenance: Time and Date Setting 321
Table 114 Menu 24.11 Remote Management Control 325
Table 115 Menu 25.1 IP Routing Policy Setup 330
Table 116 Menu 25.1.1 IP Routing Policy 331
Table 117 Menu 26.1 Schedule Set Setup 339
Table 118 Troubleshooting Starting Up Your Prestige 342
Table 119 Troubleshooting the LAN 342
Table 120 Troubleshooting the WAN 343
Table 121 Troubleshooting Accessing the Prestige 344
Table 122 Device 354
Table 123 Firmware 355
Table 124 Classes of IP Addresses 376

Table 125 Allowed IP Address Range By Class 377
Table 126 "Natural" Masks 377
Table 127 Alternative Subnet Mask Notation 378
Table 128 Two Subnets Example 378
Table 129 Subnet 1 379
Table 130 Subnet 2 379
Table 131 Subnet 1 380
Table 132 Subnet 2 380
Table 133 Subnet 3 380
Table 134 Subnet 4 381
Table 135 Eight Subnets 381
Table 136 Class C Subnet Planning 381
Table 137 Class B Subnet Planning 382
Table 138 Firewall Commands 388
Table 139 NetBIOS Filter Default Settings 395
Table 140 System Maintenance Logs 404
Table 141 System Error Logs 405
Table 142 Access Control Logs 405
Table 143 TCP Reset Logs 406
Table 144 Packet Filter Logs 406
Table 145 ICMP Logs 407
Table 146 CDR Logs 407
Table 147 PPP Logs 407
Table 148 UPnP Logs 408
Table 149 Content Filtering Logs 408
Table 150 Attack Logs 409
Table 151 IPSec Logs 410
Table 152 IKE Logs 410
Table 153 PKI Logs 413
Table 154 Certificate Path Verification Failure Reason Codes 414
Table 155 802.1X Logs 415
Table 156 ACL Setting Notes 416
Table 157 ICMP Notes 416
Table 158 Syslog Logs 417
Table 159 RFC-2408 ISAKMP Payload Types 417
Table 160 IEEE 802.11g 424
Table 161 Comparison of EAP Authentication Types 428
Table 162 Wireless Security Relational Matrix 429
Table 163 Abbreviations Used in the Example Internal SPTGEN Screens Table 432
Table 164 Menu 1 General Setup (SMT Menu 1) 433
Table 165 Menu 3 (SMT Menu 3) 433
Table 166 Menu 4 Internet Access Setup (SMT Menu 4) 436
Table 167 Menu 12 (SMT Menu 12) 438

Table 168 Menu 15 SUA Server Setup (SMT Menu 15) 442
Table 169 Menu 21.1 Filter Set #1 (SMT Menu 21.1) 444
Table 170 Menu 21.1 Filer Set #2, (SMT Menu 21.1) 447
Table 171 Menu 23 System Menus (SMT Menu 23) 452
Table 172 Menu 24.11 Remote Management Control (SMT Menu 24.11) 453
Table 173 Command Examples 453

Preface

Congratulations on your purchase of the P-660H/HW/W T series ADSL 2+ gateway. P-660W and P-660HW come with biult-in IEEE 802.11g wireless capability allowing wireless connectivity. P-660H and P-660HW have a 4-port switch that allows you to connect up to 4 computers to the Prestige without purchasing a switch/hub.

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.

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.

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 P-600H/HW/W T series may be referred to as the "Prestige" in this User's Guide.
- Application graphics and screen shoots shown are for the P-660W model unless otherwise specified.

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.

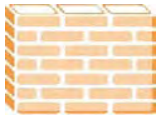
- ZyXEL Glossary and Web Site

  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.

Graphics Icons Key

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

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

The Prestige is an ADSL2+ gateway that allows super-fast, secure Internet access over analog (POTS) or digital (ISDN) telephone lines (depending on your model).

In the Prestige product name, "H" denotes an integrated 4-port switch (hub) and "W" denotes an included wireless LAN card that provides wireless connectivity.

Models ending in "1", for example P-660W-T1, 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 Services Digital Network). 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 DSL RJ-11 (ADSL over POTS models) or RJ-45 (ADSL over ISDN models) connects to your ADSL-enabled telephone line. The Prestige is 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.

1.2 Features

The following sections describe the features of the Prestige.

Note: See the product specifications in the appendix for detailed features and standards support.

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 the ADSL service you subscribed to, distance from your ISP, line quality, etc.

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.

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.

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 (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. The Prestige also includes PPPoE idle time-out (the PPPoE connection terminates after a period of no traffic that you configure) and PPPoE Dial-on-Demand (the PPPoE connection is brought up only when an Internet access request is made).

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).

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.

DHCP

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.

Packet Filters

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

Housing

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

4-Port Switch (P-660H/P-660HW)

A combination of switch and router makes your Prestige a cost-effective and viable network solution. You can connect up to four computers to the Prestige without the cost of a hub. Use a hub to add more than four computers to your LAN.

1.2.1 Wireless Features (P-660HW/P-660W)

Wireless LAN

The Prestige supports the IEEE 802.11g standard, which is fully compatible with the IEEE 802.11b standard, meaning that you can have both IEEE 802.11b and IEEE 802.11g wireless clients in the same wireless network.

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.

Wi-Fi Protected Access

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

Antenna

The Prestige is equipped with one 2dBi fixed antenna to provide clear radio signal between the wireless stations and the access points.

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.

1.3 Applications for the Prestige

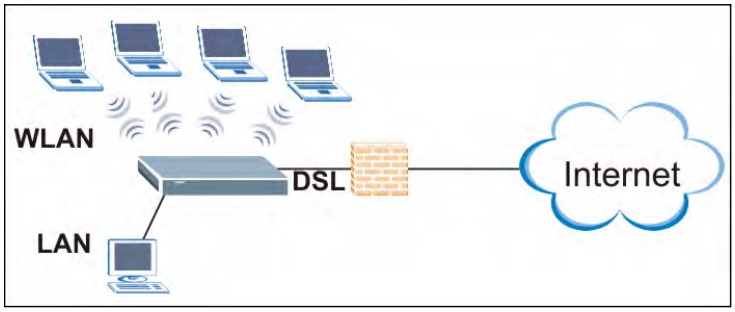
Here are some example uses for which the Prestige is well suited. Application graphics shown are for the P-660W.

1.3.1 Protected Internet Access

The Prestige is the ideal high-speed Internet access solution. It is compatible with all major ADSL DSLAM (Digital Subscriber Line Access Multiplexer) providers and supports the ADSL standards as shown in Table 1 on page 42. In addition, the Prestige allows wireless clients access to your network resources.

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.

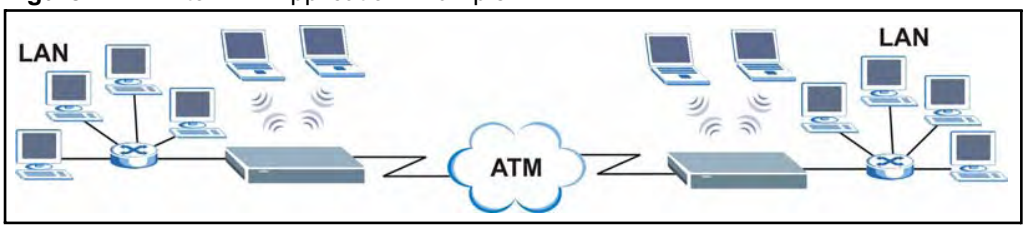
Figure 1 Protected Internet Access Applications



1.3.2 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 example is shown as follows.

Figure 2 LAN-to-LAN Application Example



1.4 Front Panel LEDs

The following figure shows the front panel LEDs.

The following table describes the LEDs.

Table 2 Front Panel LEDs

LED	COLOR	STATUS	DESCRIPTION
PWR/SYS	Green	On	The Prestige is receiving power and functioning properly.
		Blinking	The Prestige is rebooting or performing diagnostics.
	Red	On	Power to the Prestige is too low.
		Off	The system is not ready or has malfunctioned.
LAN	Green	On	The Prestige has a successful 10Mb Ethernet connection.
		Blinking	The Prestige is sending/receiving data.
	Amber	On	The Prestige has a successful 100Mb Ethernet connection.
		Blinking	The Prestige is sending/receiving data.
		Off	The LAN is not connected.
WLAN (P-660HW/ P-660W)	Green	On	The Prestige is ready, but is not sending/receiving data through the wireless LAN.
		Blinking	The Prestige is sending/receiving data through the wireless LAN.
		Off	The wireless LAN is not ready or has failed.
DSL/PPP	Green	Fast Blinking	The Prestige is sending/receiving non-PPP data.
		Slow Blinking	The Prestige is initializing the DSL line.
		On	The system is ready, but is not sending/receiving non-PPP data.
	Amber	On	The connection to the PPPoE server is up.
		Blinking	The Prestige is sending/receiving PPP data.
		Off	The DSL link is down.

1.5 Hardware Connection

Refer to the Quick Start Guide for information on hardware connection.

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. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

See the chapter on troubleshooting if you need to make sure these functions are allowed in Internet Explorer.

2.1.1 Accessing the 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. A window displays as shown.The **Password** field already contains the default password "1234". Click **Login** to proceed to a screen asking you to change your password or click **Cancel** to revert to the default password.

Figure 3 Password Screen

6 It is highly recommended you change the default password! Enter a new password between 1 and 30 characters, 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.

Note: If you do not change the password at least once, the following screen appears every time you log in.

Figure 4 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 Web Configurator

The following summarizes how to navigate the web configurator from the **SITE MAP** screen. We use the Prestige 660W-T1 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 5 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	Connection Setup	Use these screens for initial configuration including general setup, ISP parameters for Internet Access and WAN IP/DNS Server/MAC address assignment.
	Media Bandwidth Mgnt	Use these screens to limit bandwidth usage by application.
Advanced Setup		
Password		Use this screen to change your password.
LAN		Use this screen to configure LAN DHCP and TCP/IP settings.

Table 3 Web Configurator Screens Summary (continued)

LINK	SUB-LINK	FUNCTION
Wireless LAN (P-660W / P-660HW only)	Wireless	Use this screen to configure the wireless LAN settings.
	MAC Filter	Use this screen to change MAC filter settings on the Prestige.
	802.1x/WPA	Use this screen to configure WLAN authentication and security settings.
	Local User Database	Use this screen to set up built-in user profiles for wireless station authentication.
	RADIUS	Use this screen to specify the external RADIUS server for wireless station authentication.
WAN	WAN Setup	Use this screen to change the Prestige's WAN remote node settings.
	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.
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 assign bandwidth limits 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.

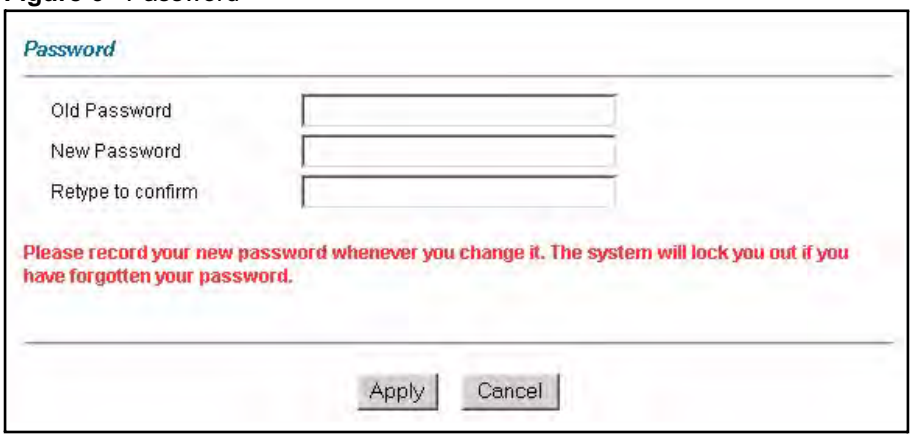
Table 3 Web Configurator Screens Summary (continued)

LINK	SUB-LINK	FUNCTION
DHCP Table		This screen displays DHCP (Dynamic Host Configuration Protocol) related information and is READ-ONLY.
Any IP Table		Use this screen to view the IP and MAC addresses of LAN computers communicating with the Prestige.
Wireless LAN (P-660W / P-660HW only)	Association List	This screen displays the MAC address(es) of the wireless stations that are currently associating with the Prestige.
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 **Logout** to exit the web configurator.

2.2 Change Login Password

It is highly recommended that you periodically change the password for accessing the Prestige. If you didn't change the default one after you logged in or you want to change to a new password again, then click **Password** in the **Site Map** screen to display the screen as shown next.

Figure 6 Password



The following table describes the fields in this screen.

Table 4 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 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

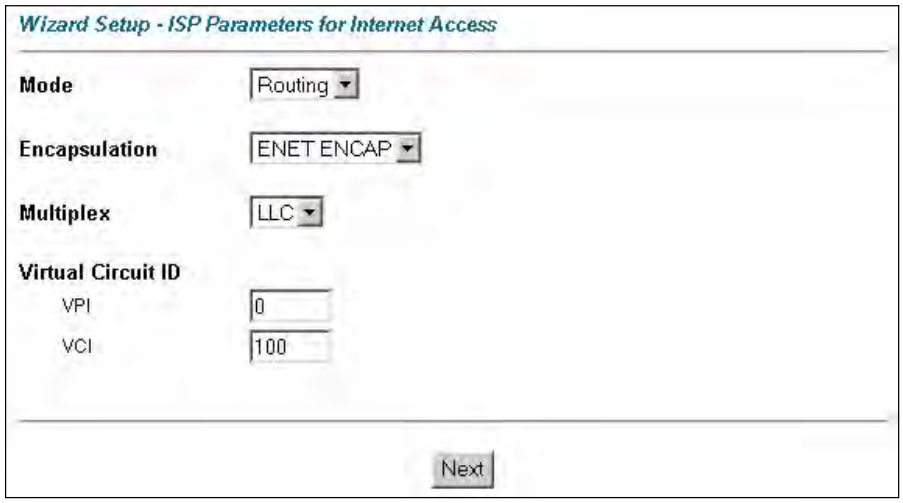
Use the Wizard Setup screens to configure your system for Internet access with the information given to you by your ISP.

Note: See the advanced menu chapters for background information on these fields.

3.1.1 Internet Access Wizard Setup

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

Figure 7 Internet Access Wizard Setup: ISP Parameters



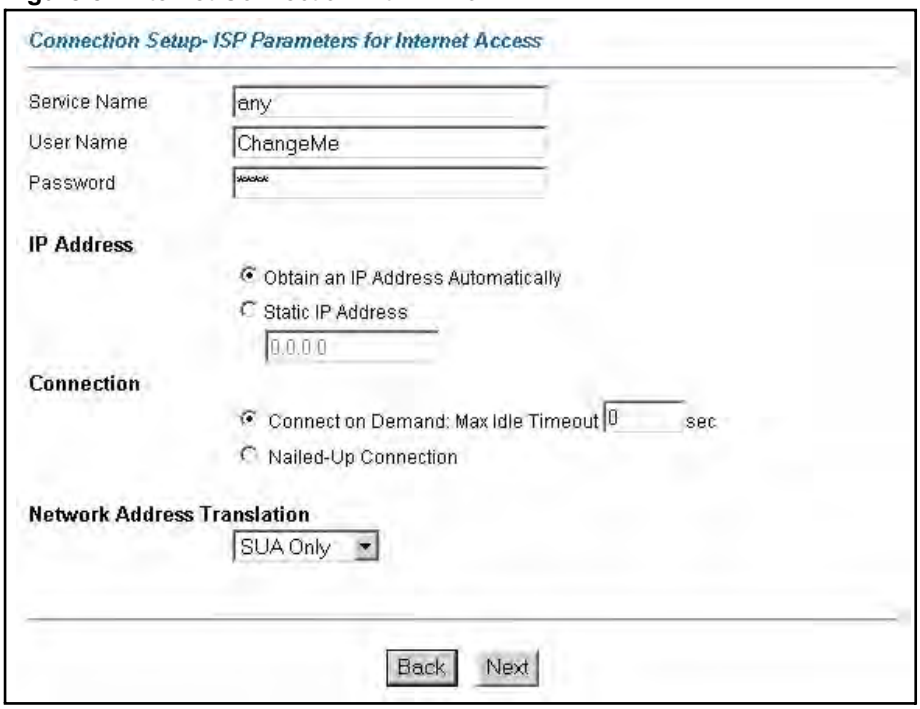
The following table describes the fields in this screen.

Table 5 Internet Access Wizard Setup: ISP Parameters

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.

2 The next 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

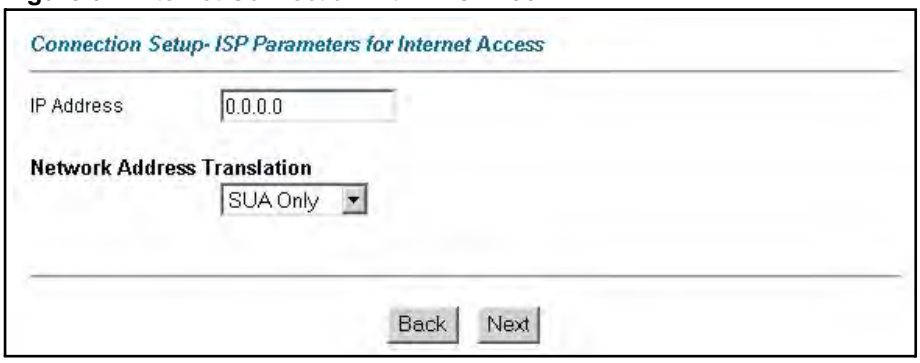


The following table describes the fields in this screen.

Table 6 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.

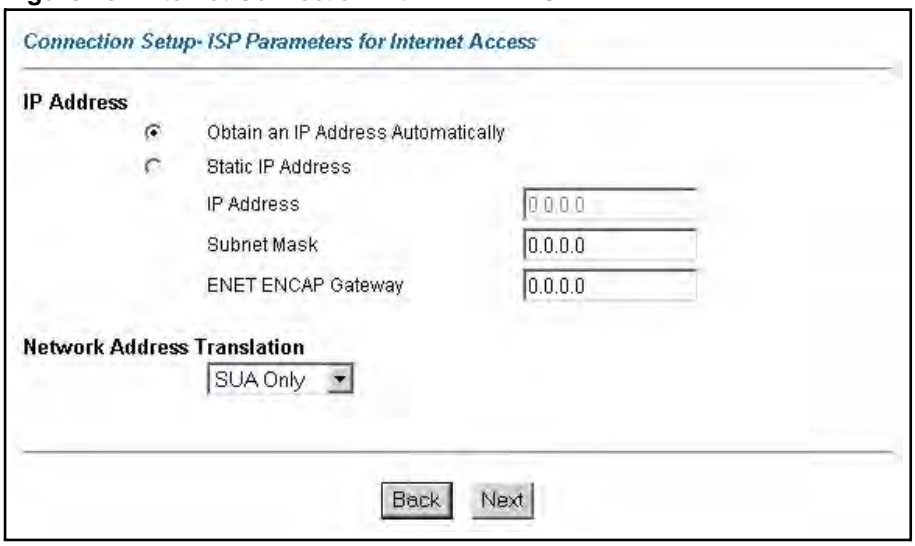
Table 7 Internet Connection with RFC 1483

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-down list box. Refer to the NAT chapter for more details.

Table 7 Internet Connection with RFC 1483 (continued)

LABEL	DESCRIPTION
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

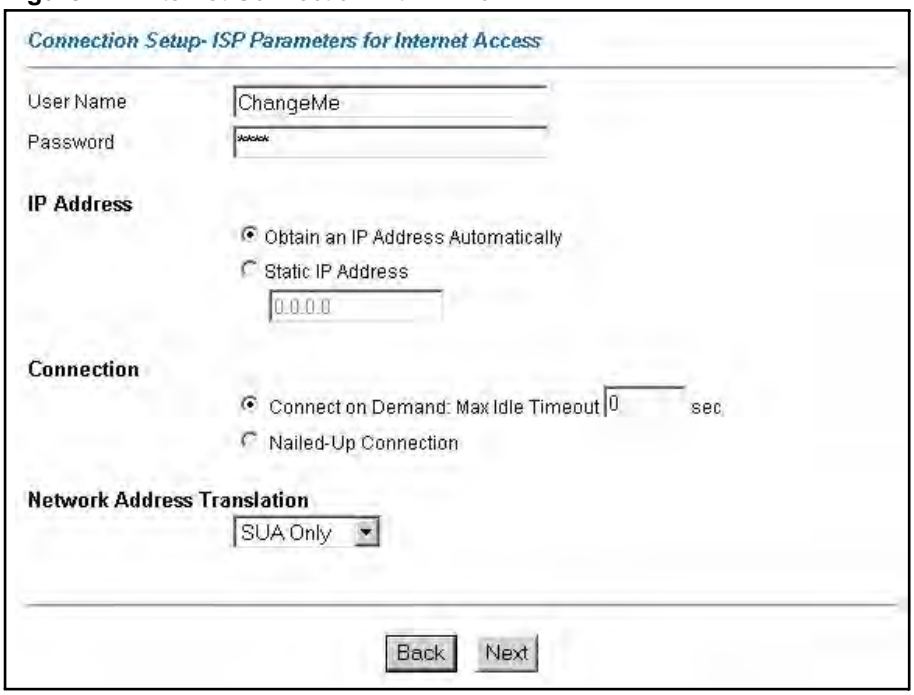


The following table describes the fields in this screen.

Table 8 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 appendices 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



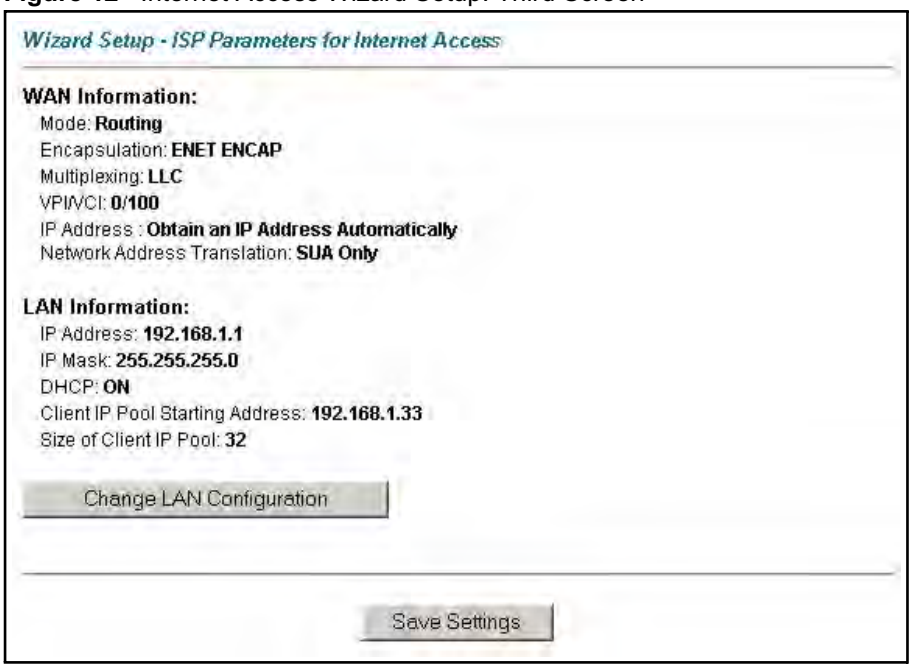
The following table describes the fields in this screen.

Table 9 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 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.

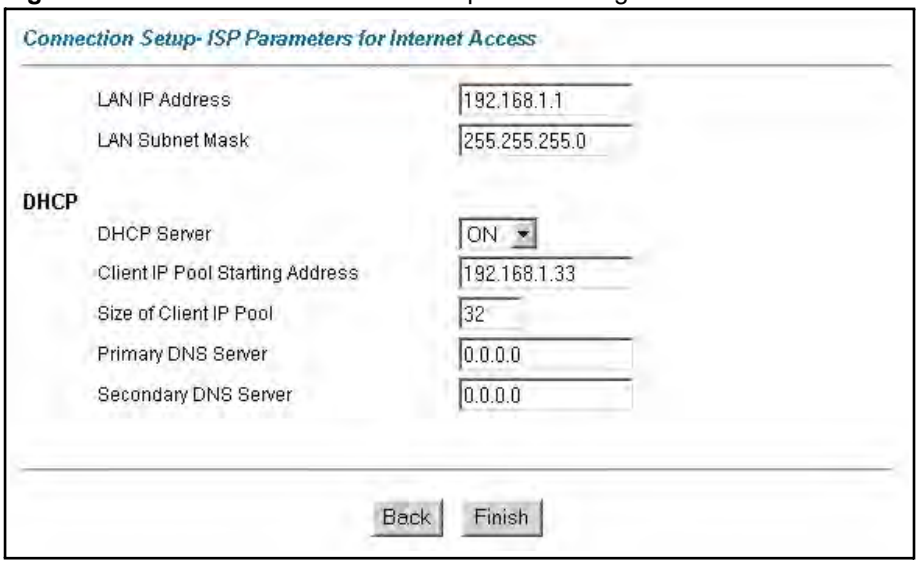
3 Verify the settings in the screen shown next. To change the LAN information on the Prestige, click **Change LAN Configurations**. Otherwise click **Save Settings** to save the configuration and skip to the section 3.13.

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



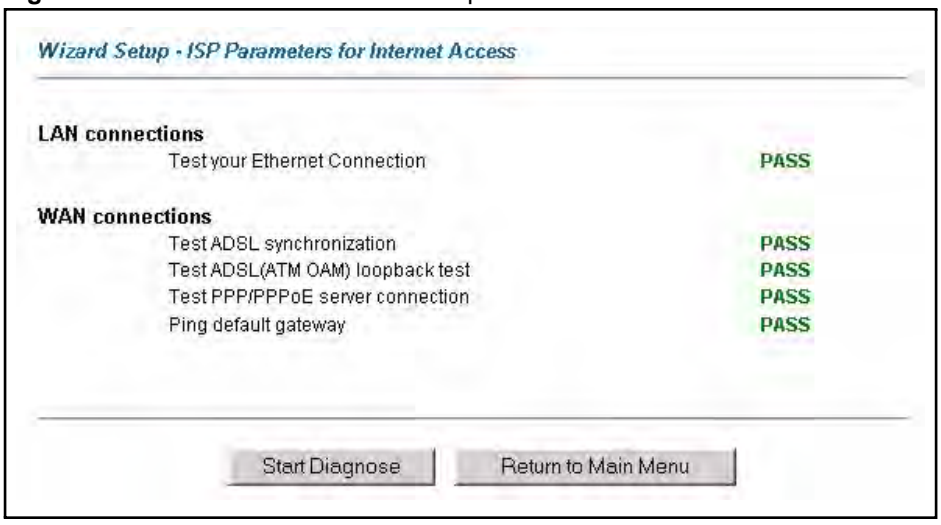
The following table describes the fields in this screen.

Table 10 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.

4 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



5 Launch your web browser and navigate to www.zyxel.com. Internet access is just the beginning. Refer to the rest of this 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
LAN Setup

This chapter describes how to configure LAN settings.

4.1 LAN Overview

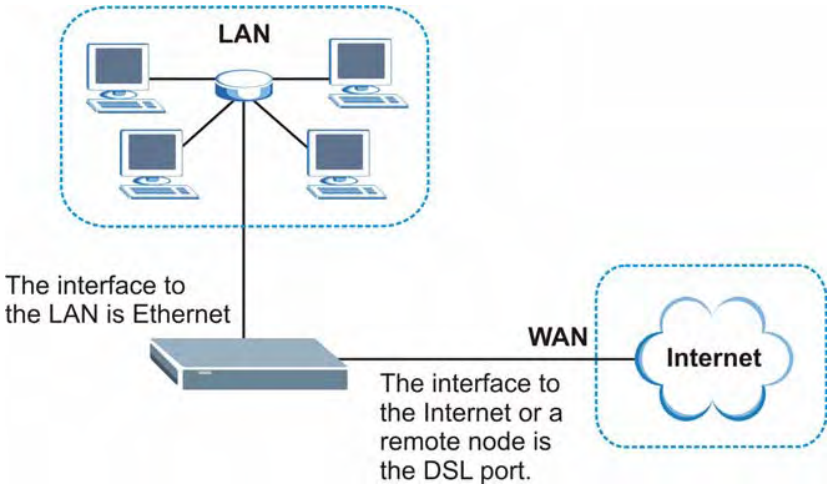
A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building. The LAN screens can help you configure a LAN DHCP server and manage IP addresses.

See Section 4.3 on page 68 to configure the **LAN** screens.

4.1.1 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 15 LAN and WAN IP Addresses



4.1.2 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.

4.1.2.1 IP Pool Setup

The Prestige is pre-configured with a pool of IP addresses for the DHCP clients (DHCP Pool). See the product specifications in the appendices. Do not assign static IP addresses from the DHCP pool to your LAN computers.

4.1.3 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.

4.1.4 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 the **LAN Setup** screen.
- The Prestige acts as a DNS proxy when the **Primary** and **Secondary DNS Server** fields are left blank in the **LAN Setup** screen.

4.2 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.

4.2.1 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.

4.2.1.1 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.*

4.2.2 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.

4.2.3 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.

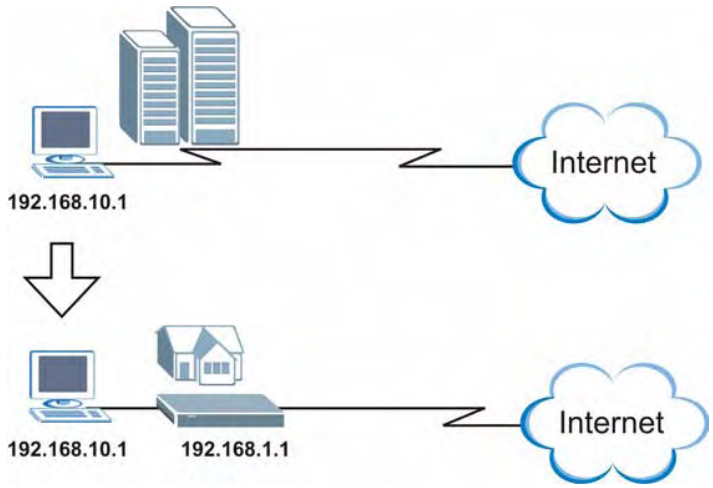
4.2.4 Any IP

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 16 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.

4.2.4.1 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.

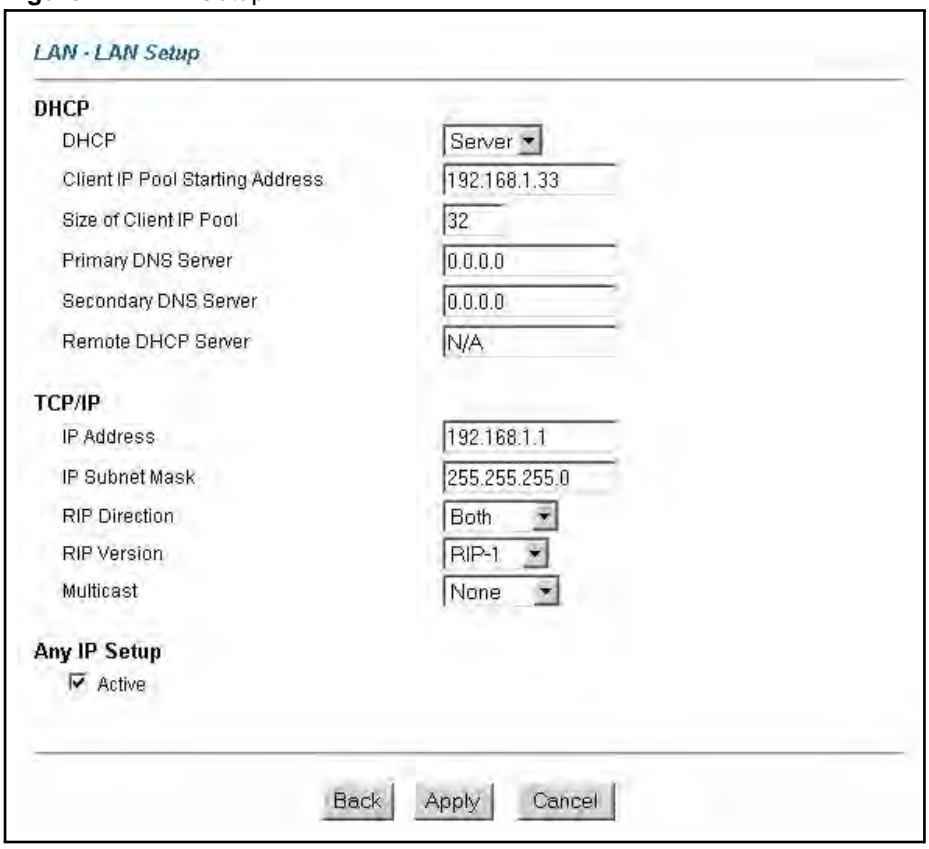
1. When a computer (which is in a different subnet) first attempts to access the Internet, it sends packets to its default gateway (which is not the Prestige) by looking at the MAC address in its ARP table.
2. When the computer cannot locate the default gateway, an ARP request is broadcast on the LAN.
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.

4.3 Configuring LAN

Click **LAN** to open the **LAN Setup** screen. See Section 4.1 on page 62 for background information.

Figure 17 LAN Setup



The following table describes the fields in this screen.

Table 11 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.

Table 11 LAN Setup (continued)

LABEL	DESCRIPTION
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** check box 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.

CHAPTER 5
Wireless LAN

This chapter discusses how to configure the Wireless LAN screens for P-660HW or P-660W.

5.1 Wireless LAN Introduction

A wireless LAN can be as simple as two computers with wireless LAN adapters communicating in a peer-to-peer network or as complex as a number of computers with wireless LAN adapters communicating through access points which bridge network traffic to the wired LAN.

Refer to Section 5.3 on page 71 to configure wireless LAN settings.

Note: See the WLAN appendix for more detailed information on WLANs.

5.2 Wireless Security Overview

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

Wireless security methods available on the Prestige are data encryption, wireless client authentication, restricting access by device MAC address and hiding the Prestige identity.

5.2.1 Encryption

- Use WPA security if you have WPA-aware wireless clients and a RADIUS server. WPA has user authentication and improved data encryption over WEP.
- Use WPA-PSK if you have WPA-aware wireless clients but no RADIUS server.
- If you don't have WPA-aware wireless clients, then use WEP key encrypting. A higher bit key offers better security at a throughput trade-off. You can use Passphrase to automatically generate 64-bit or 128-bit WEP keys or manually enter 64-bit, 128-bit or 256-bit WEP keys.

5.2.2 Authentication

WPA has user authentication and you can also configure IEEE 802.1x to use the built-in database (Local User Database) or a RADIUS server to authenticate wireless clients before joining your network.

- Use RADIUS authentication if you have a RADIUS server. See the appendices for information on protocols used when a client authenticates with a RADIUS server via the Prestige.
- Use the Local User Database if you have less than 32 wireless clients in your network. The Prestige uses MD5 encryption when a client authenticates with the Local User Database

5.2.3 Restricted Access

The **MAC Filter** screen allows you to configure the AP to give exclusive access to devices (**Allow Association**) or exclude them from accessing the AP (**Deny Association**).

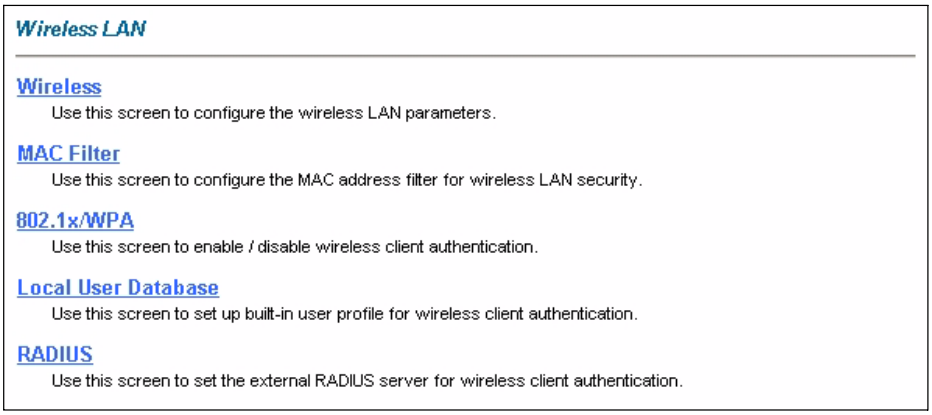
5.2.4 Hide Prestige Identity

If you hide the ESSID, then the Prestige cannot be seen when a wireless client scans for local APs. The trade-off for the extra security of "hiding" the Prestige may be inconvenience for some valid WLAN clients. If you don't hide the ESSID, at least you should change the default one.

5.3 The Main Wireless LAN Screen

Click **Wireless LAN** in the navigation panel to display the main **Wireless LAN** screen.

Figure 18 Wireless LAN



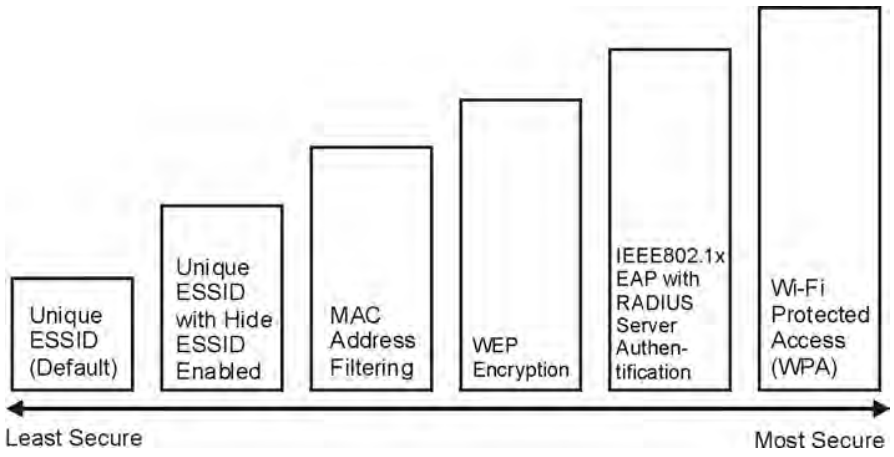
The following table describes the links in this screen.

Table 12 Wireless LAN

LINK	DESCRIPTION
Wireless	Click this link to go to a screen where you can configure the **ESSID** and **WEP**. **Note:** If you configure **WEP**, you can't configure **WPA** or **WPA-PSK**.
MAC Filter	Click this link to go to a screen where you can restrict access to your wireless network by MAC address.
802.1x/WPA	Click this link to go to a screen where you can configure WPA or WPA-PSK. You can also configure 802.1x wireless client authentication in this screen.
RADIUS	Click this link to go to a screen where you can configure the RADIUS authentication database settings.
Local User Database	Click this link to go to a screen where you can configure the built-in authentication database for user authentication.

The following figure shows the relative effectiveness of these wireless security methods available on your Prestige.

Figure 19 Wireless Security Methods



Note: You must enable the same wireless security settings on the Prestige and on all wireless clients that you want to associate with it.

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

5.4 Configuring the Wireless Screen

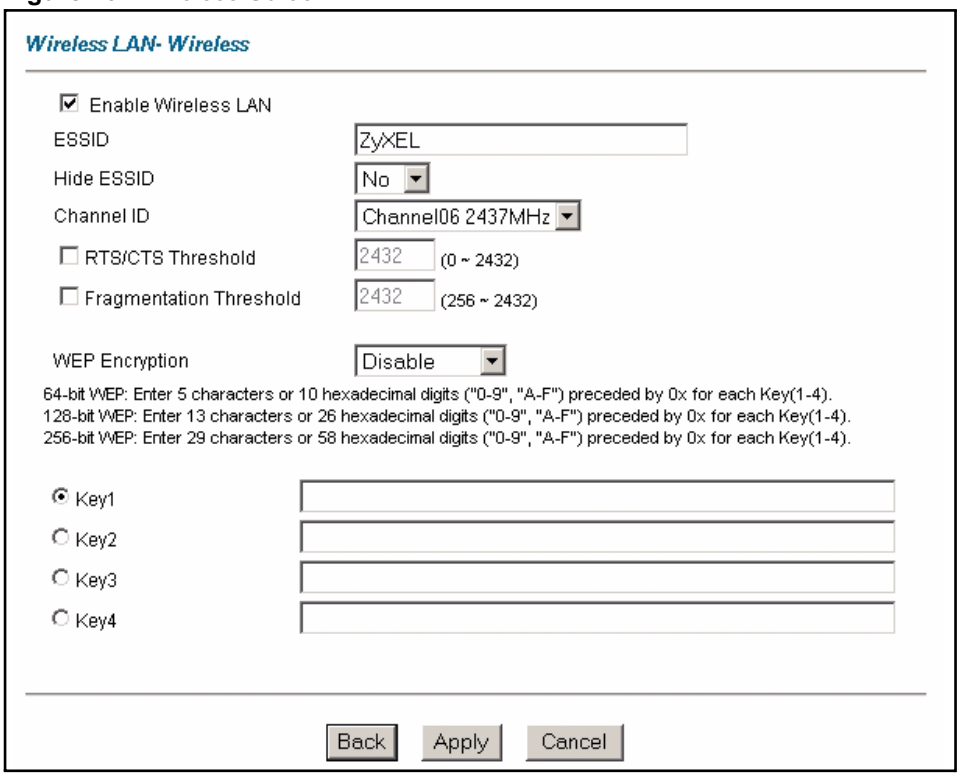
5.4.1 WEP Encryption

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.

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.

Figure 20 Wireless Screen



The following table describes the labels in this screen.

Table 13 Wireless LAN

LABEL	DESCRIPTION
Enable Wireless LAN	You should configure some wireless security (see Figure 19 on page 73) when you enable the wireless LAN. 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 of up to 32 printable characters (including spaces; alphabetic characters are case-sensitive).
Hide ESSID	Select **Yes** to hide the ESSID in so a station cannot obtain the ESSID through AP scanning. Select **No** to make the ESSID visible so a station can obtain the ESSID through AP scanning.
Channel ID	The radio frequency used by IEEE 802.11a, b or g 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) is for enabling RTS/CTS. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this value to be larger than the maximum MSDU (MAC service data unit) size turns off RTS/CTS. Setting this value to zero turns on RTS/CTS. Select the check box to change the default value and enter a new value between 0 and 2432.

Table 13 Wireless LAN (continued)

LABEL	DESCRIPTION
Fragmentation Threshold	This is the threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Select the check box to change the default value and enter a value between 256 and 2432.
You won't see the following WEP-related fields if you have **WPA** or **WPA-PSK** enabled.	
Passphrase	Enter a "passphrase" (password phrase) of up to 63 case-sensitive printable characters and click **Generate** to have the Prestige create four different WEP keys. At the time of writing, you cannot use passphrase to generate 256-bit WEP keys.
Generate	After you enter the passphrase, click **Generate** to have the Prestige generate four different WEP keys automatically. The keys display in the fields below.
WEP Encryption	WEP (Wired Equivalent Privacy) encrypts data frames before transmitting over the wireless network. Select **Disable** to allow all wireless stations 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 want to manually set the WEP keys, enter the key in the field provided. 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 used 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.

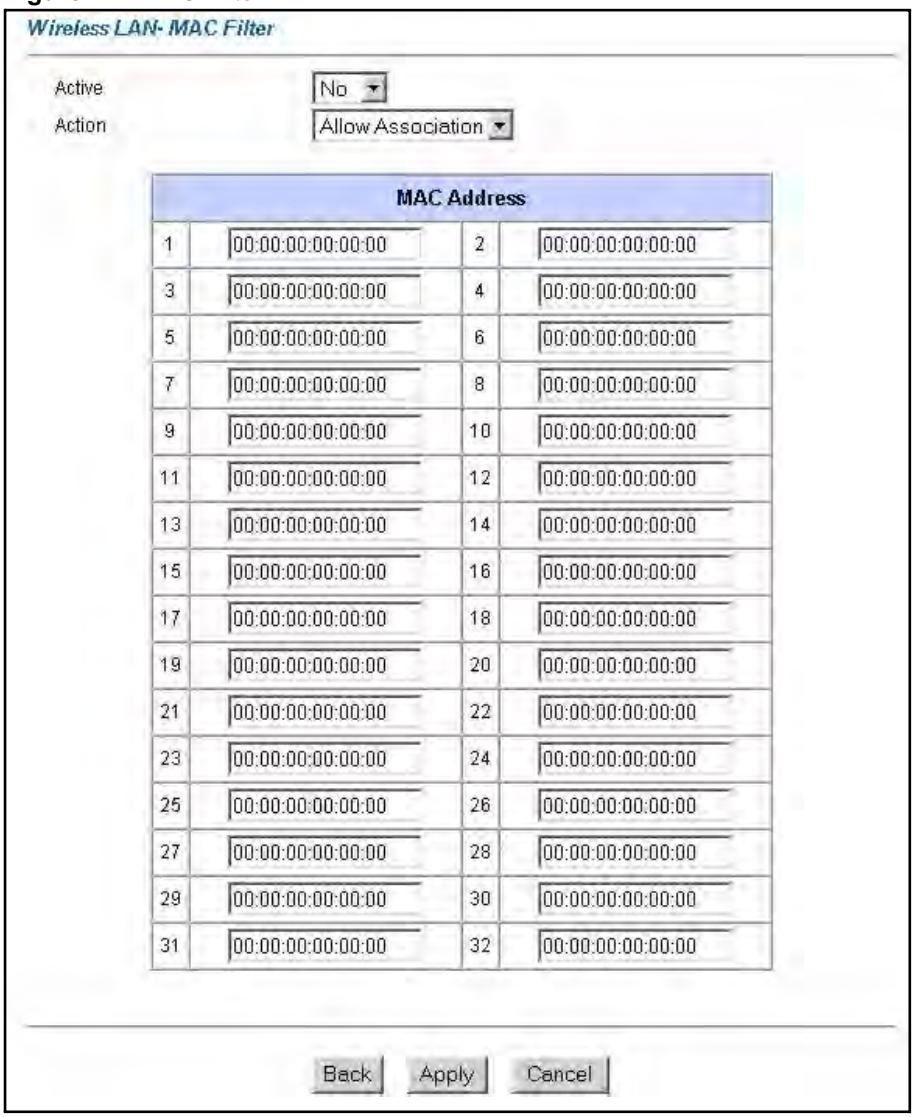
Note: If you are configuring the Prestige from a computer connected to the wireless LAN and you change the Prestige's ESSID or security settings (see Figure 19 on page 73), you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the Prestige's new settings.

5.5 Configuring MAC Filters

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 addresses 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 21 MAC Filter



The following table describes the fields in this menu.

Table 14 MAC 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.

Table 14 MAC Filter (continued)

LABEL	DESCRIPTION
MAC Address	Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc of the wireless stations 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.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to begin configuring this screen afresh.

5.6 Introduction to WPA

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA is preferred to WEP as WPA has user authentication and improved data encryption. See the appendix for more information on WPA user authentication and WPA encryption.

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

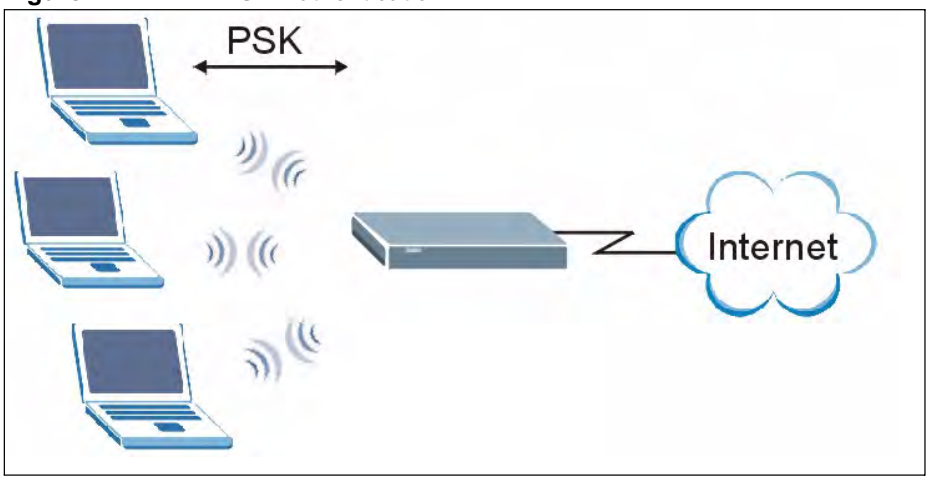
Note: You can't use the Local User Database for authentication when you select WPA.

5.6.1 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 be between 8 and 63 printable characters (including spaces; alphabetic characters are case-sensitive).
2. The AP checks each client's password and (only) allows it to join the network if the passwords match.
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 22 WPA - PSK Authentication

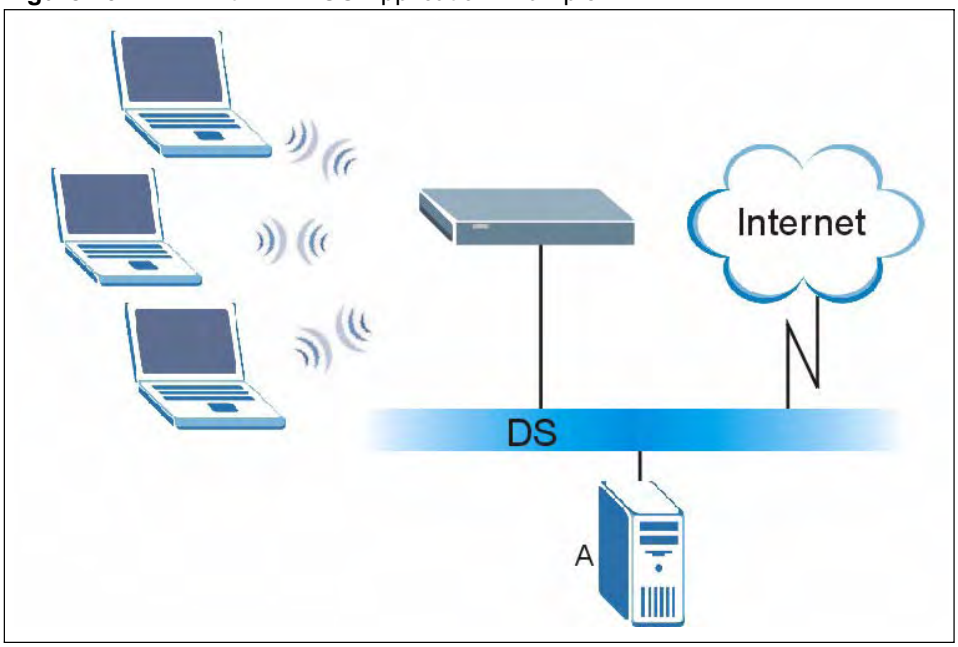


5.6.2 WPA with RADIUS Application Example

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

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 transmitted between the AP and the wireless clients

Figure 23 WPA with RADIUS Application Example2



5.6.3 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.

See Section 5.7.3 on page 82 and Section 5.7.4 on page 84 for configuration instruction.

5.7 Configuring IEEE 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.

- See Section 5.7.1 on page 80 if you want to allow unauthenticated wireless access or block wireless access on the Prestige.
- See Section 5.7.2 on page 80 to configure IEEE 802.1x authentication.
- See Section 5.7.3 on page 82 to configure WPA.
- See Section 5.7.4 on page 84 to configure WPA-PSK.

5.7.1 No Access Allowed or Authentication

Select **No Access Allowed** or **No Authentication Required** in the **Wireless Port Control** field.

Figure 24 Wireless LAN: 802.1x/WPA: No Access Allowed

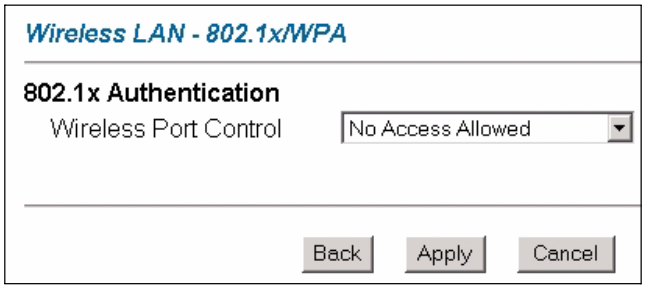
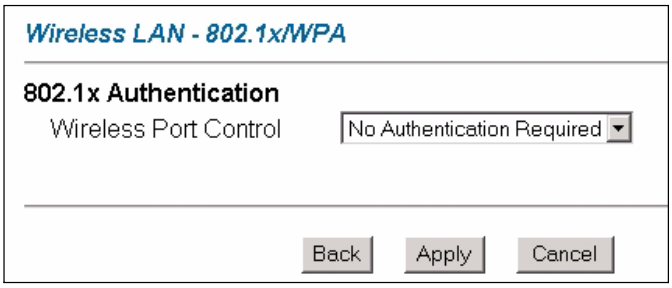


Figure 25 Wireless LAN: 802.1x/WPA: No Authentication



The following table describes the label in these screens.

Table 15 Wireless LAN: 802.1x/WPA: No Access/Authentication

LABEL	DESCRIPTION
Wireless Port Control	To control wireless station 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.

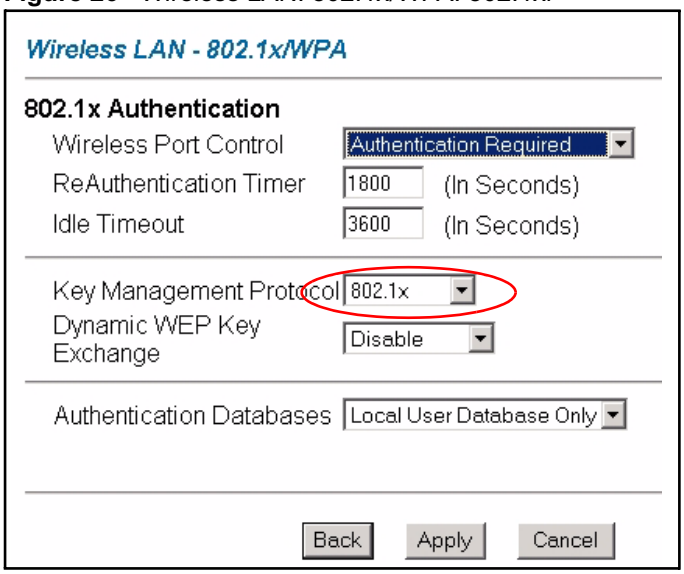
5.7.2 Authentication Required: 802.1x

You need the following for IEEE 802.1x authentication.

- A computer with an IEEE 802.11 a/b/g wireless LAN adapter 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 their 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.

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

Figure 26 Wireless LAN: 802.1x/WPA: 802.1xl



The following table describes the labels in this screen.

Table 16 Wireless LAN: 802.1x/WPA: 802.1x

LABEL	DESCRIPTION
Wireless Port Control	To control wireless station 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.

Table 16 Wireless LAN: 802.1x/WPA: 802.1x (continued)

LABEL	DESCRIPTION
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**, **128-bit WEP** or **256-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.
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.

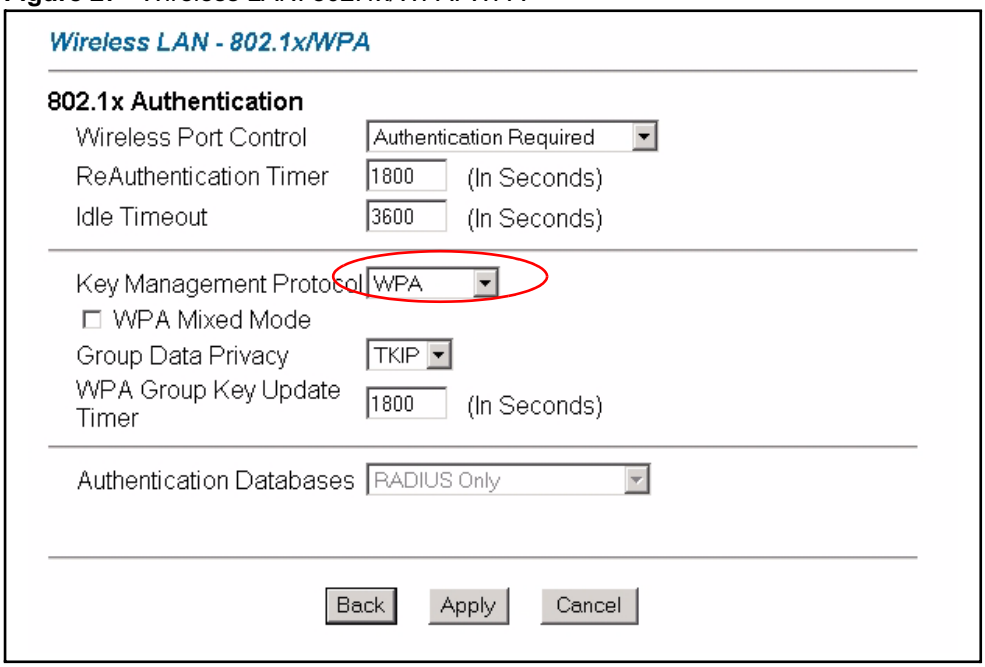
Note: Once you enable user authentication, you need to specify an external RADIUS server or create local user accounts on the Prestige for authentication.

5.7.3 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.

See Section 5.6 on page 77 for more information.

Figure 27 Wireless LAN: 802.1x/WPA: WPA



The following table describes the labels not previously discussed.

Table 17 Wireless LAN: 802.1x/WPA: WPA

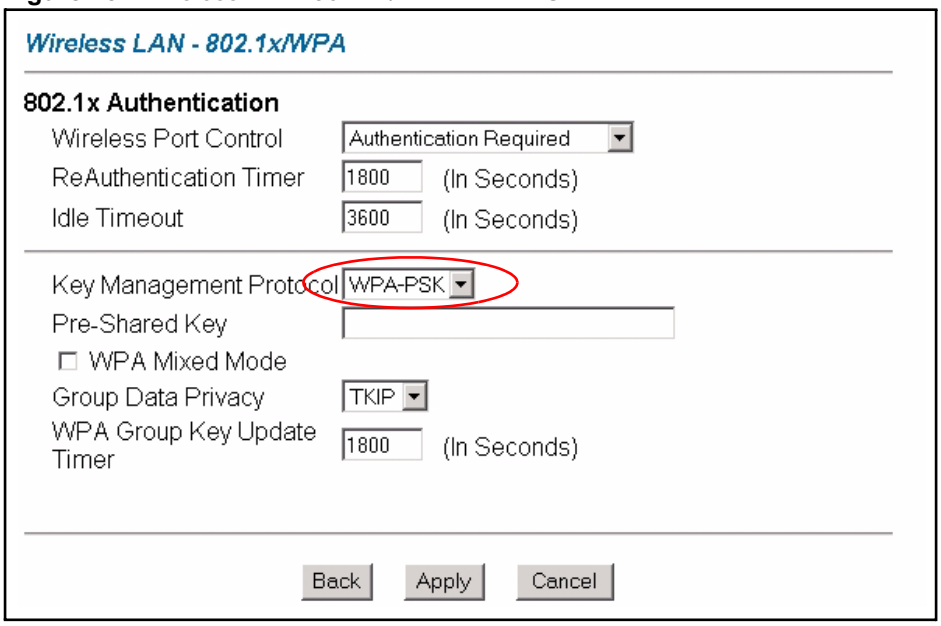
LABEL	DESCRIPTION
Key Management Protocol	Choose **WPA** in this field.
WPA Mixed Mode	The Prestige can operate in **WPA Mixed Mode**, which supports both clients running WPA and clients running dynamic WEP key exchange with 802.1x in the same Wi-Fi network. Select the check box to activate WPA mixed 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**.

5.7.4 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.

See Section 5.6 on page 77 for more information.

Figure 28 Wireless LAN: 802.1x/WPA:WPA-PSK



The following table describes the labels not previously discussed.

Table 18 Wireless LAN: 802.1x/WPA: WPA-PSK

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 printable characters (including spaces; alphabetic characters are case-sensitive).
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.

Table 18 Wireless LAN: 802.1x/WPA: WPA-PSK (continued)

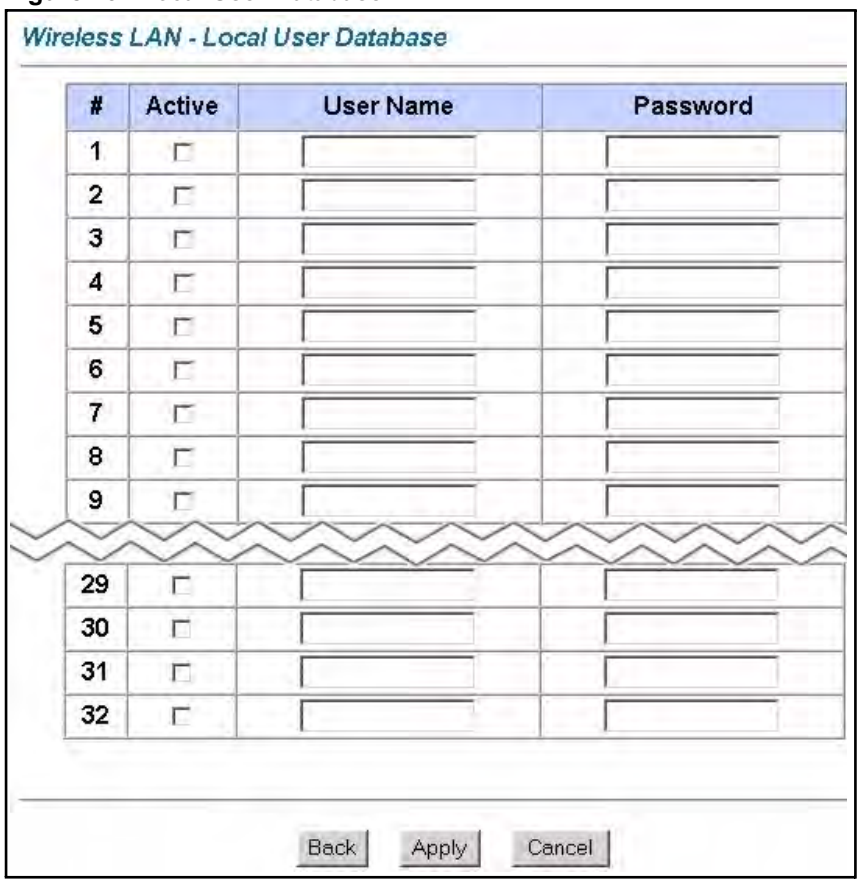
LABEL	DESCRIPTION
Group Data Privacy	**Group Data Privacy** allows you to choose **TKIP** (recommended) or **WEP** for broadcast and multicast ("group") traffic if the **Key Management Protocol** is **WPA** and **WPA Mixed Mode** is disabled. **WEP** is used automatically if you have enabled **WPA Mixed 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.

5.8 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 29 Local User Database



The following table describes the fields in this screen.

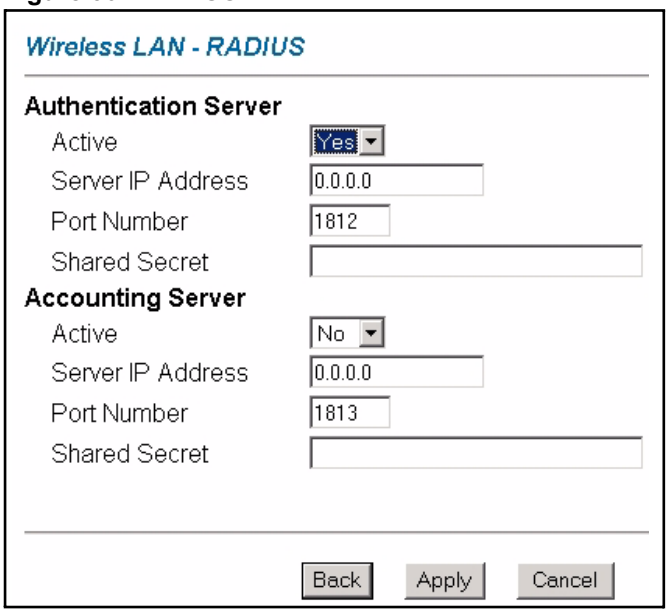
Table 19 Local User Database

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 a user name of up to 31 alphanumeric characters (case-sensitive), hyphens ('-') and underscores ('_') if you're using MD5 encryption and maximum 14 if you're using PEAP.
Password	Enter a password of up to 31 printable characters (including spaces; alphabetic characters are case-sensitive) if you're using MD5 encryption and maximum 14 if you're using PEAP.
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.

5.9 Configuring RADIUS

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

Figure 30 RADIUS



The following table describes the fields in this screen.

Table 20 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.

Table 20 RADIUS (continued)

LABEL	DESCRIPTION
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 6
WAN Setup

This chapter describes how to configure WAN settings.

6.1 WAN Overview

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

6.1.1 Encapsulation

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

6.1.1.1 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.

6.1.1.2 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.

6.1.1.3 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.

6.1.1.4 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.

6.1.2 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.

6.1.2.1 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.

6.1.2.2 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.

6.1.3 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.

6.1.4 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.

6.1.4.1 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.

6.1.4.2 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.

6.1.4.3 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.

6.1.5 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

6.1.6 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.

6.2 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 Section 6.7 on page 95)
- Traffic-redirect route (see Section 6.8 on page 98)
- WAN-backup route, also called dial-backup (see Section 6.9 on page 99)

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.

6.3 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.

6.4 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.

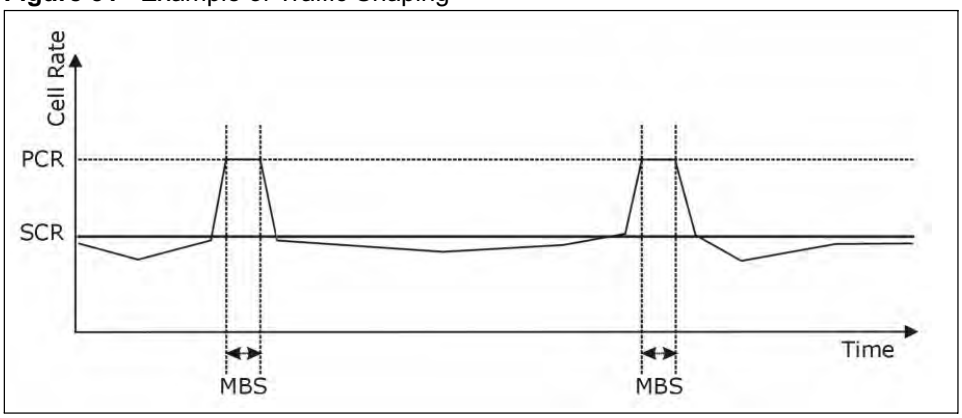
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

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 31 Example of Traffic Shaping



6.5 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

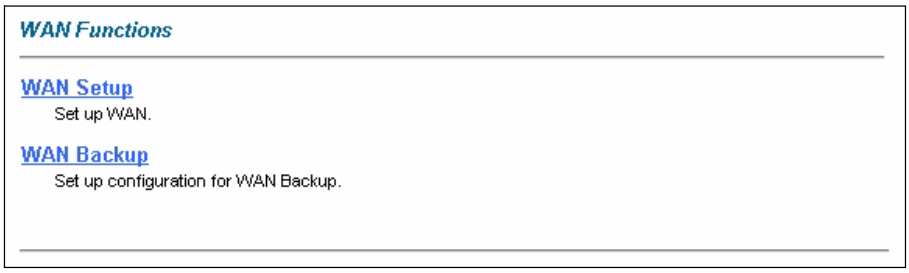
- the Prestige is in bridge mode
- you set the Prestige to use a static (fixed) WAN IP address.

6.6 The Main WAN Screen

Click **WAN** in the navigation panel to display the man **WAN** screen.

See Section 6.1 on page 90 for more information.

Figure 32 WAN



The following table describes the links in this screen.

Table 21 WAN

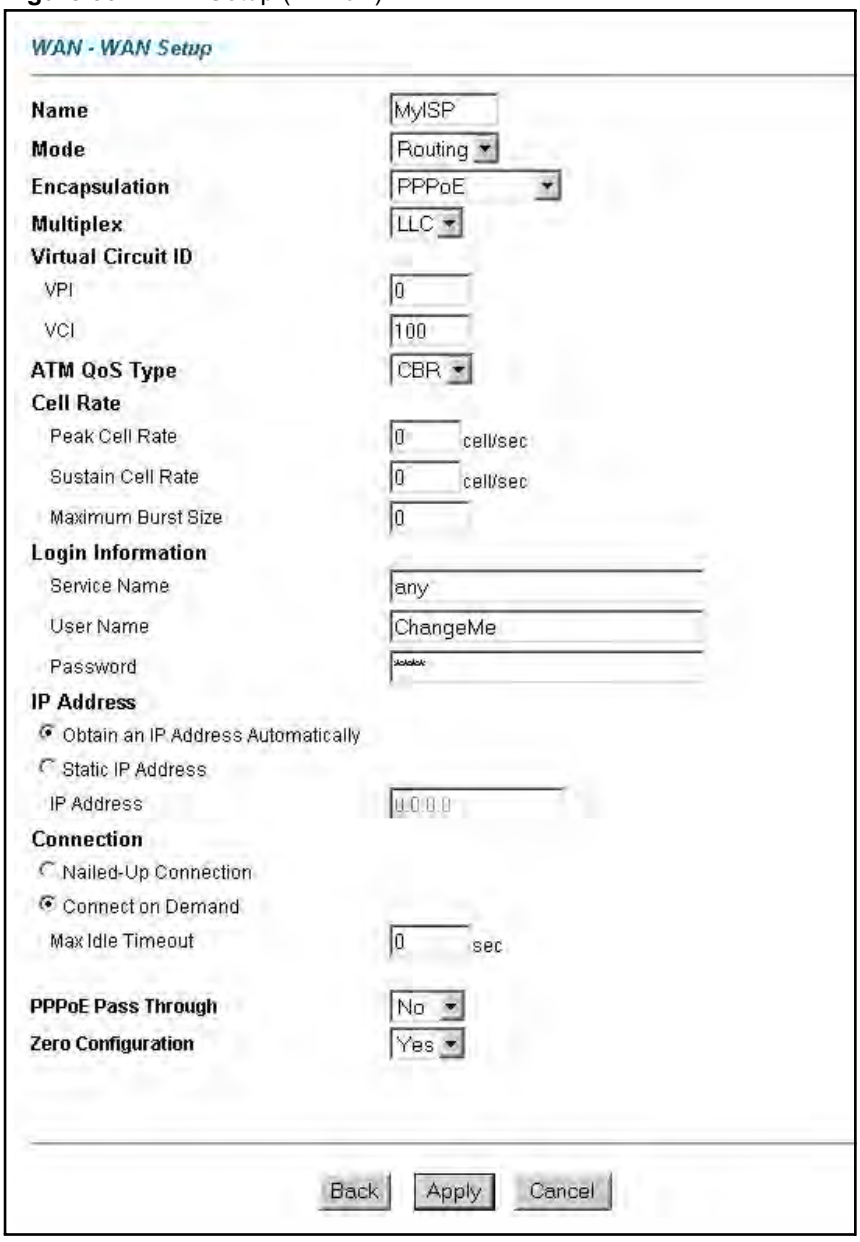
LINK	DESCRIPTION
WAN Setup	Click this link to go to the screen where you can configure your Prestige for an Internet connection.
WAN Backup	Click this link to go to the screen where you can configure WAN backup connections (traffic redirect and dial backup).

6.7 Configuring WAN Setup

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

See Section 6.1 on page 90 for more information.

Figure 33 WAN Setup (PPPoE)



The following table describes the fields in this screen.

Table 22 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 22 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.

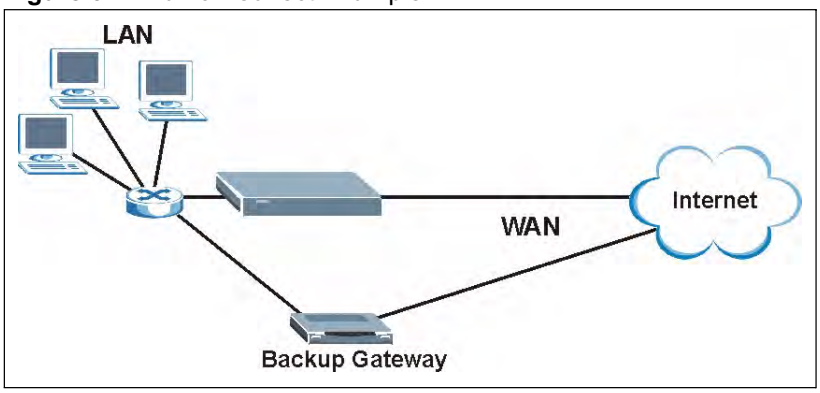
Table 22 WAN Setup (continued)

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 appendices 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.

6.8 Traffic Redirect

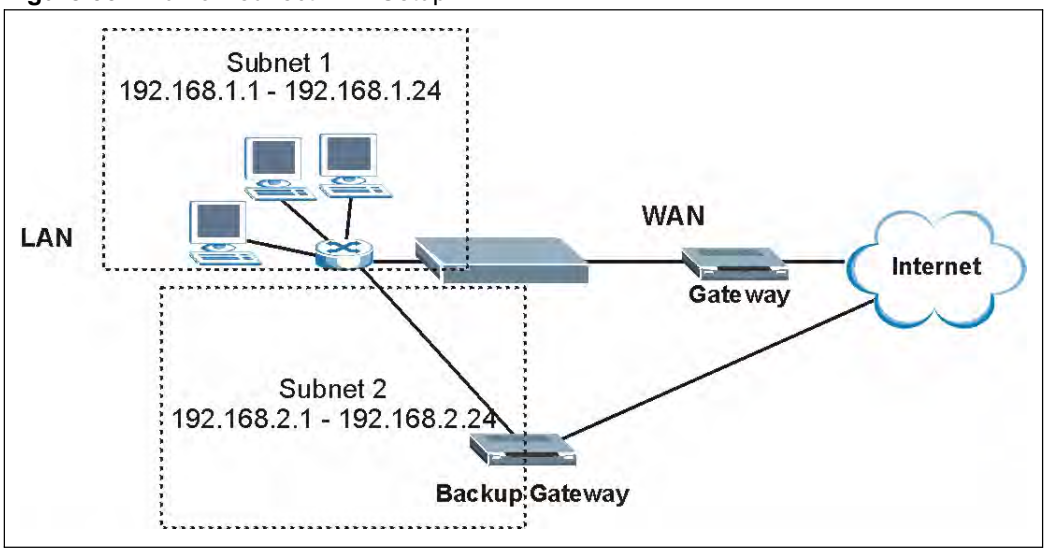
Traffic redirect forwards traffic to a backup gateway when the Prestige cannot connect to the Internet. An example is shown in the figure below.

Figure 34 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).

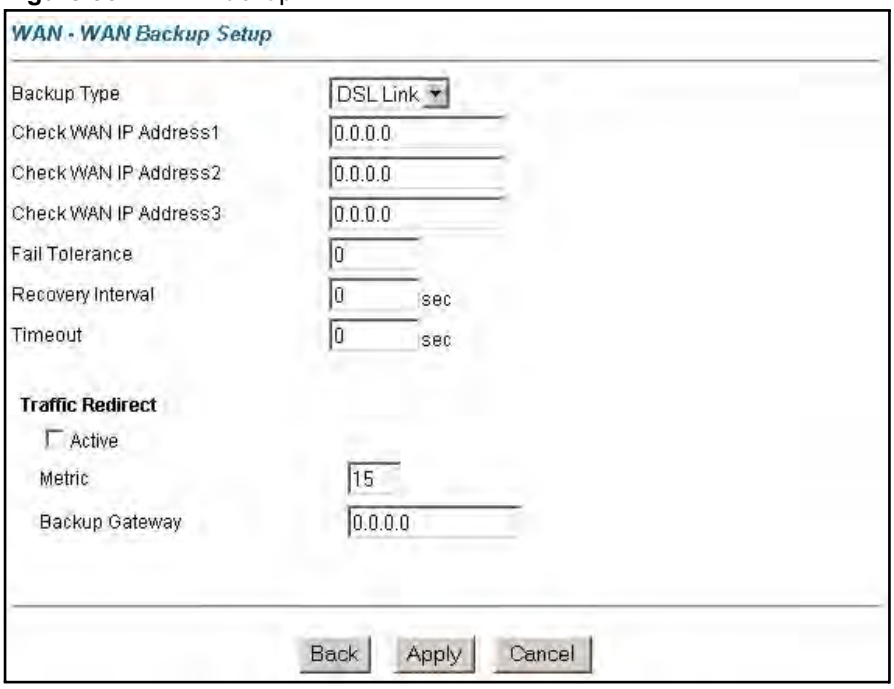
Figure 35 Traffic Redirect LAN Setup



6.9 Configuring WAN Backup

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

Figure 36 WAN Backup



The following table describes the fields in this screen.

Table 23 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).
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.

Table 23 WAN Backup (continued)

LABEL	DESCRIPTION
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	Traffic redirect forwards traffic to a backup gateway when the Prestige cannot connect to the Internet.
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.
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.

CHAPTER 7
Network Address Translation (NAT) Screens

This chapter discusses how to configure NAT on the Prestige.

7.1 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.

7.1.1 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 24 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.

7.1.2 What NAT Does

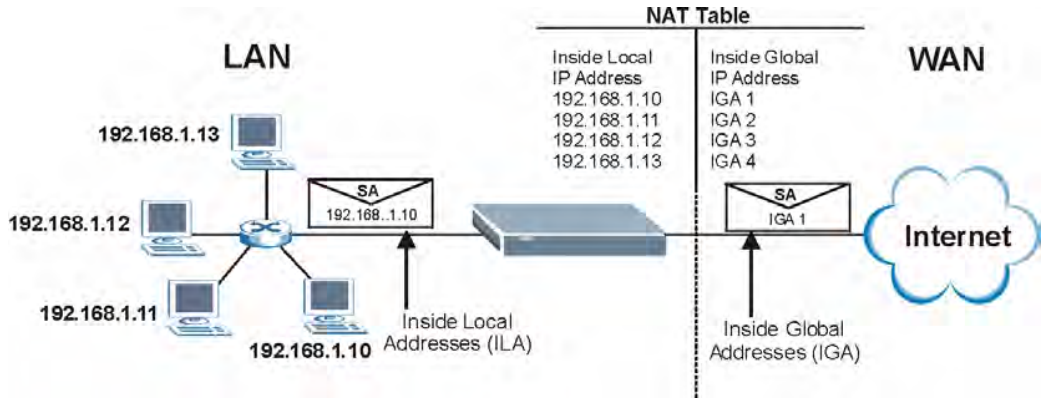
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) 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 25 on page 105), 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)*.

7.1.3 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.

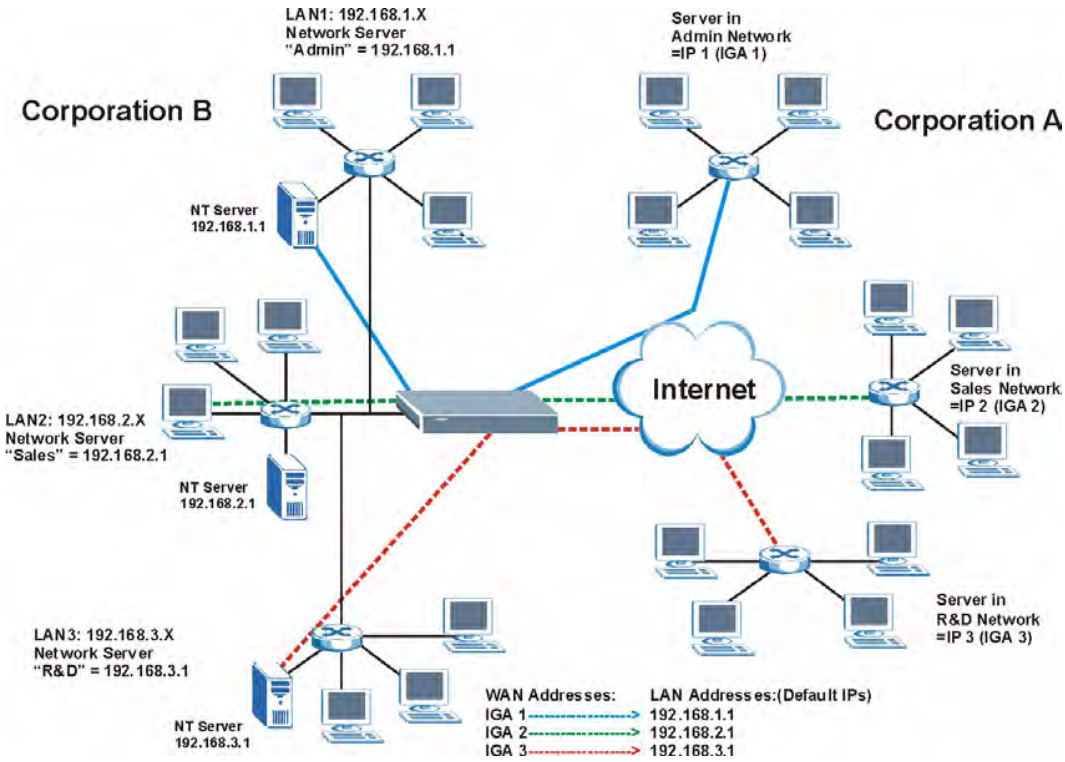
Figure 37 How NAT Works



7.1.4 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 38 NAT Application With IP Alias



7.1.5 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 25 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

7.2 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 25 on page 105.

- 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.

7.3 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.

7.3.1 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.

7.3.2 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 26 Services and Port Numbers

SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21

Table 26 Services and Port Numbers (continued)

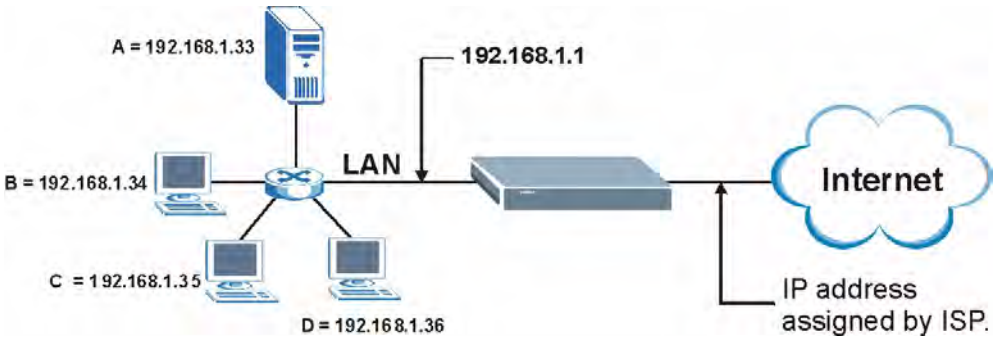
SERVICES	PORT NUMBER
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

7.3.3 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 39 Multiple Servers Behind NAT Example



7.4 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 40 NAT Mode

The following table describes the labels in this screen.

Table 27 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.

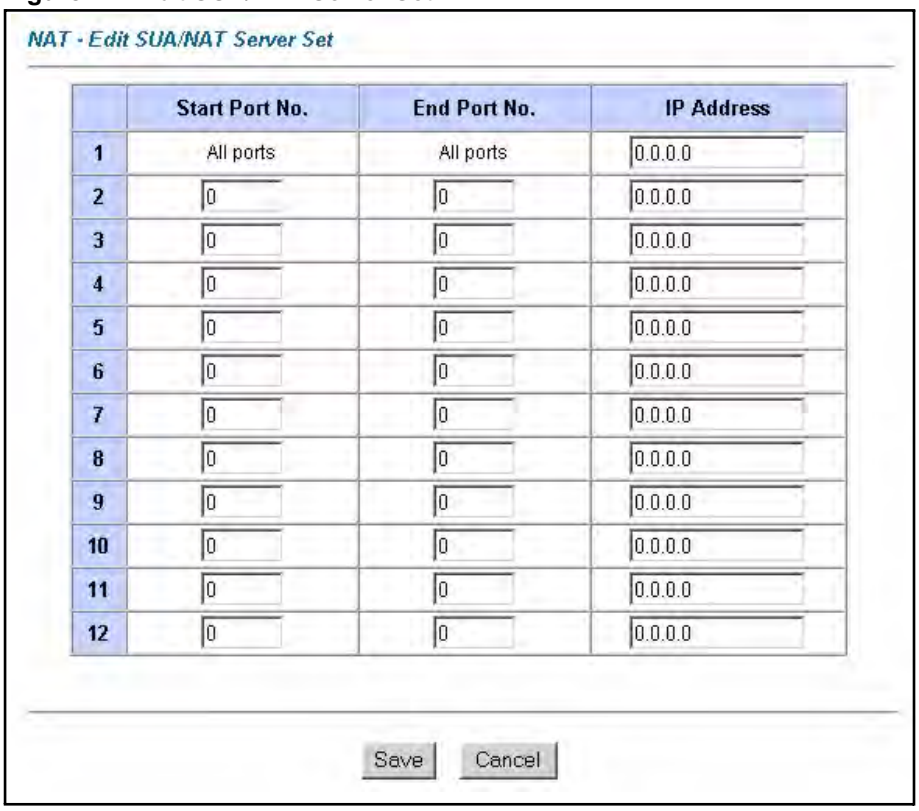
7.5 Configuring SUA Server Set

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.

See Section 7.3 on page 106 for more information. See Table 26 on page 106 for port numbers commonly used for particular services.

Figure 41 Edit SUA/NAT Server Set



The following table describes the fields in this screen.

Table 28 Edit SUA/NAT Server Set

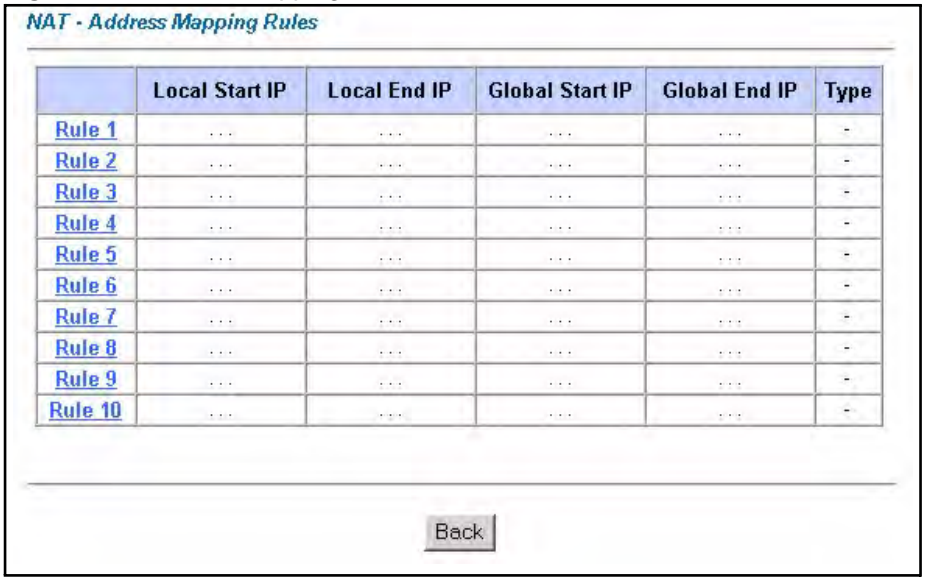
LABEL	DESCRIPTION
Start Port No.	Enter a port number in this field. To forward only one port, enter the port number again in the **End Port No.** field. To forward a series of ports, enter the start port number here and the end port number in the **End Port No.** field.
End Port No.	Enter a port number 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.

7.6 Configuring Address Mapping 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 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 42 Address Mapping Rules



The following table describes the fields in this screen.

Table 29 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.

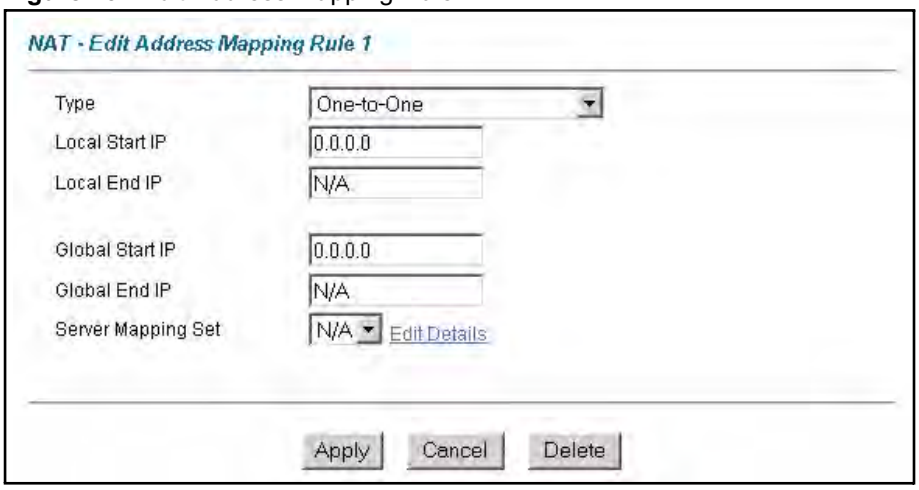
Table 29 Address Mapping Rules (continued)

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.

7.7 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 43 Edit Address Mapping Rule



The following table describes the fields in this screen.

Table 30 Edit Address Mapping Rule

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.

Table 30 Edit Address Mapping Rule (continued)

LABEL	DESCRIPTION
Cancel	Click **Cancel** to return to the previously saved settings.
Delete	Click **Delete** to exit this screen without saving.

CHAPTER 8
Dynamic DNS Setup

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

8.1 Dynamic DNS Overview

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.

8.1.1 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.

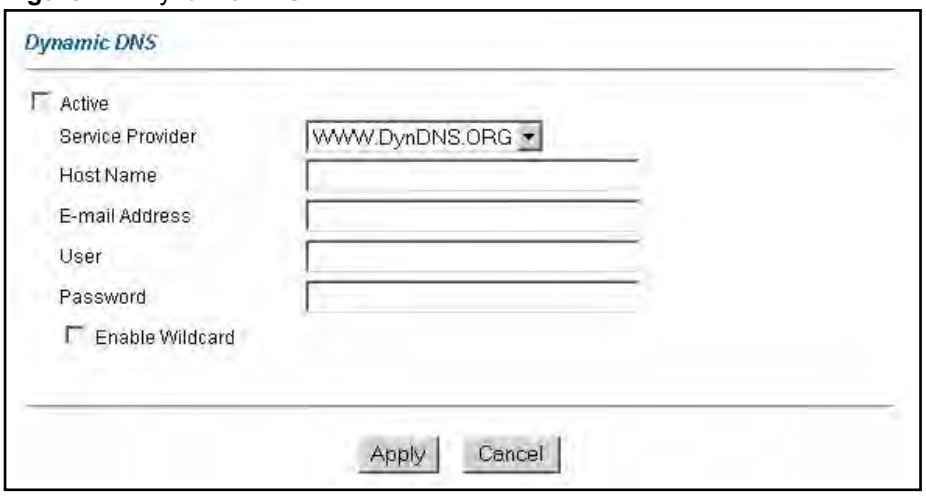
See Section 8.2 on page 114 for configuration instruction.

8.2 Configuring Dynamic DNS

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

See Section 8.1 on page 114 for more information.

Figure 44 Dynamic DNS



The following table describes the fields in this screen.

Table 31 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.

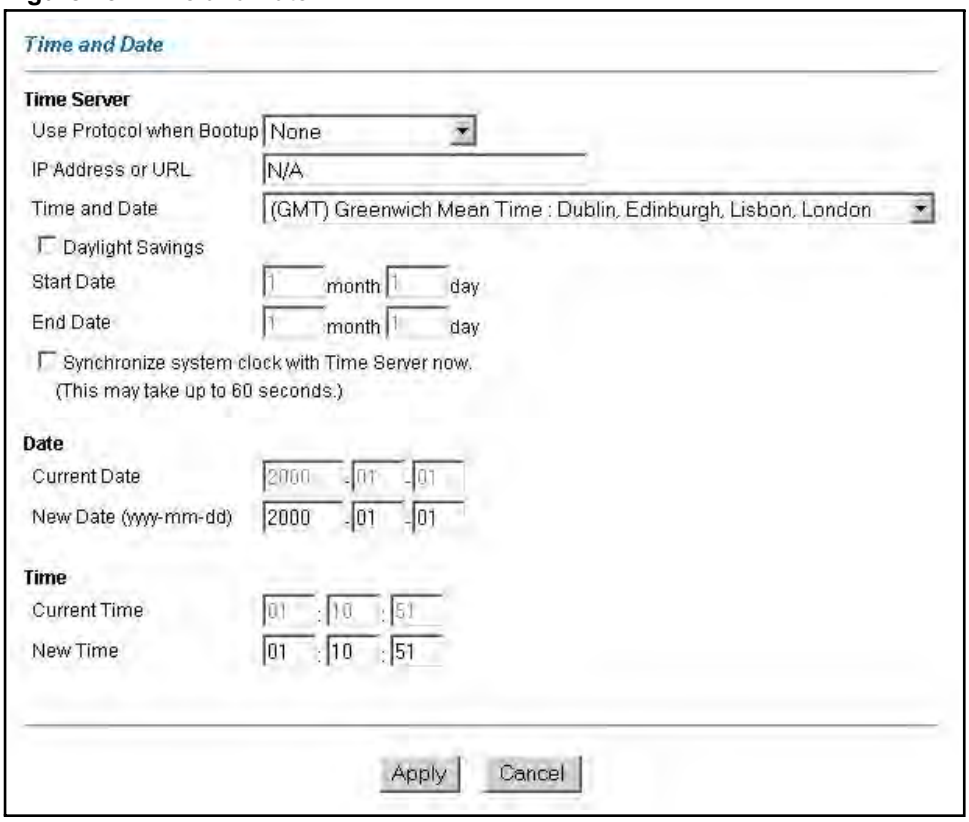
CHAPTER 9
Time and Date

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

9.1 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 45 Time and Date



The following table describes the fields in this screen.

Table 32 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 10
Firewalls

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

10.1 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.

Refer to Section 11.5 on page 135 to configure default firewall settings.

Refer to Section 11.6 on page 136 to view firewall rules.

Refer to Section 11.6.1 on page 138 to configure firewall rules.

Refer to Section 11.7 on page 141 to configure a custom service.

Refer to Section 11.12.3 on page 151 to configure firewall thresholds.

10.2 Types of Firewalls

There are three main types of firewalls:

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

10.2.1 Packet Filtering Firewalls

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

10.2.2 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.

10.2.3 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 Section 10.5 on page 124 for more information on stateful inspection.

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

10.3 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.

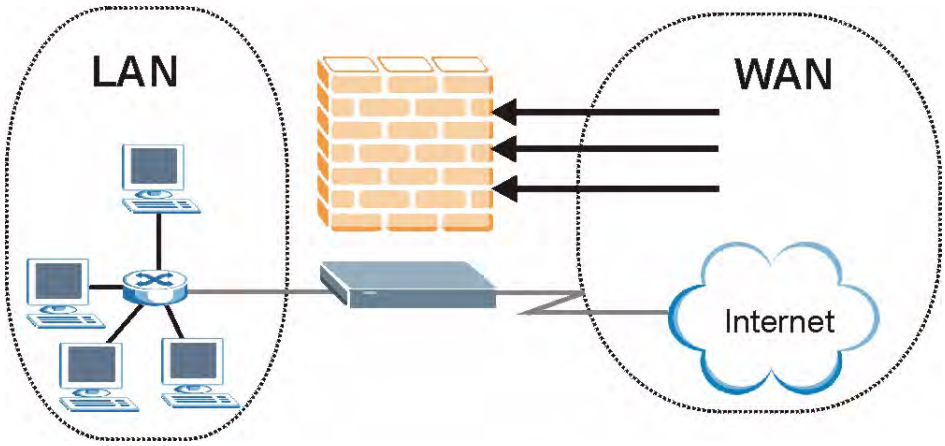
The Prestige has one DSL/ISDN port and one Ethernet LAN port, which physically separate the network into two areas.

- 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.

10.3.1 Denial of Service Attacks

Figure 46 Prestige Firewall Application



10.4 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.

10.4.1 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 33 Common IP Ports

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

10.4.2 Types of DoS Attacks

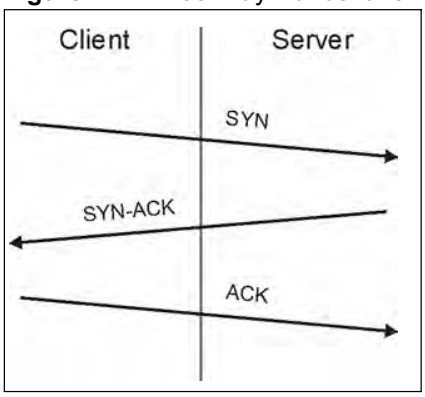
There are four types of DoS attacks:

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.

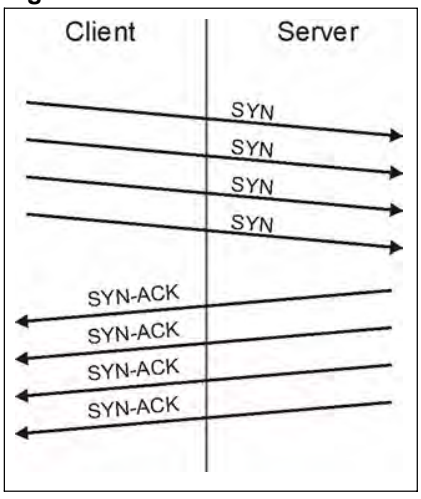
Figure 47 Three-Way Handshake



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 48 SYN Flood

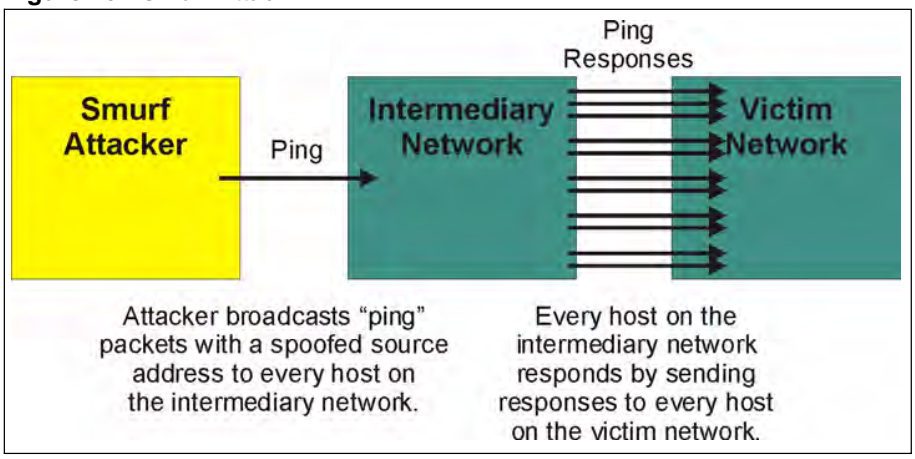


- In a **LAND Attack**, hackers flood SYN packets into the network with a spoofed source IP address of the targeted system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

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 49 Smurf Attack



10.4.2.1 ICMP Vulnerability

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

Table 34 ICMP Commands That Trigger Alerts

5	REDIRECT
13	TIMESTAMP_REQUEST
14	TIMESTAMP_REPLY
17	ADDRESS_MASK_REQUEST
18	ADDRESS_MASK_REPLY

10.4.2.2 Illegal Commands (NetBIOS and SMTP)

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

Table 35 Legal NetBIOS Commands

MESSAGE:
REQUEST:
POSITIVE:
VE:

Table 35 Legal NetBIOS Commands

RETARGET:
KEEPALIVE:

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

Table 36 Legal SMTP Commands

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

10.4.2.3 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.

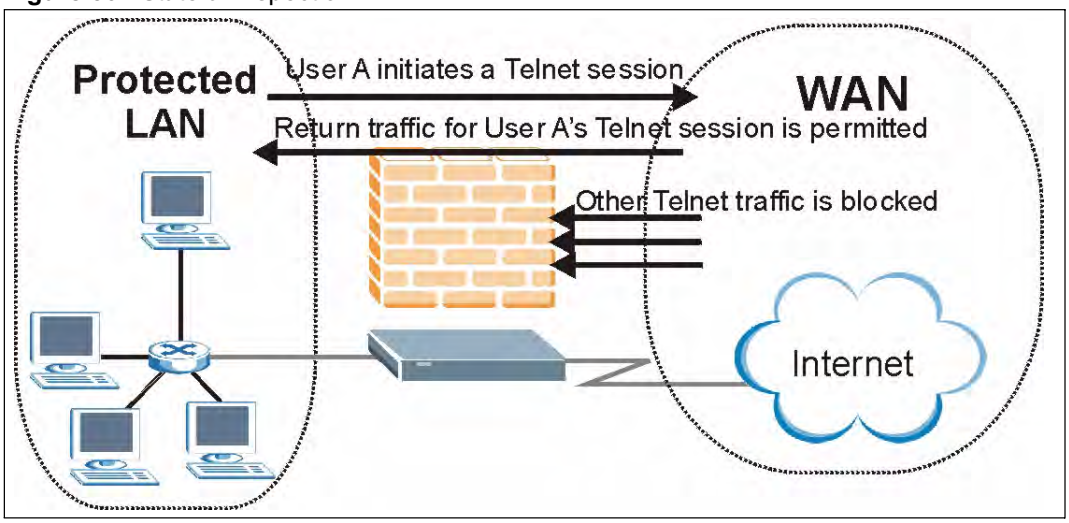
Often, many DoS attacks also employ a technique known as "**IP Spoofing**" as part of their attack. IP Spoofing may be used to break into systems, to hide the hacker's identity, or to magnify the effect of the DoS attack. IP Spoofing is a technique used to gain unauthorized access to computers by tricking 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.

10.5 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 50 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.

10.5.1 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.

10.5.2 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).

10.5.3 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).

10.5.4 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.

10.5.5 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.

10.6 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.

10.6.1 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.

10.7 Packet Filtering Vs Firewall

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

10.7.1 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.

10.7.1.1 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.

10.7.2 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.

10.7.2.1 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 11
Firewall Configuration

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

11.1 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.

11.2 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
- WAN to LAN
- WAN to WAN/ 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

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.

  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.

11.3 Rule Logic Overview

Note: Study these points carefully before configuring rules.

11.3.1 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?
3. What IP services will be affected?
4. What computers on the LAN 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.

11.3.2 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.

11.3.3 Key Fields For Configuring Rules

11.3.3.1 Action

Should the action be to **Block** or **Forward**? "Block" means the firewall silently discards the packet.

11.3.3.2 Service

Select the service from the **Service** scrolling list box. If the service is not listed, it is necessary to first define it. See Section 11.10 on page 146 for more information on predefined services.

11.3.3.3 Source Address

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

11.3.3.4 Destination Address

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

11.4 Connection Direction

This section describes examples for firewall rules for connections going from LAN to WAN and from WAN to LAN.

LAN to LAN/ Router, WAN to WAN/ Router rules apply to packets coming in on the associated interface (LAN, WAN 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 polices apply in the same way to the WAN ports.

11.4.1 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. 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.

11.4.2 Alerts

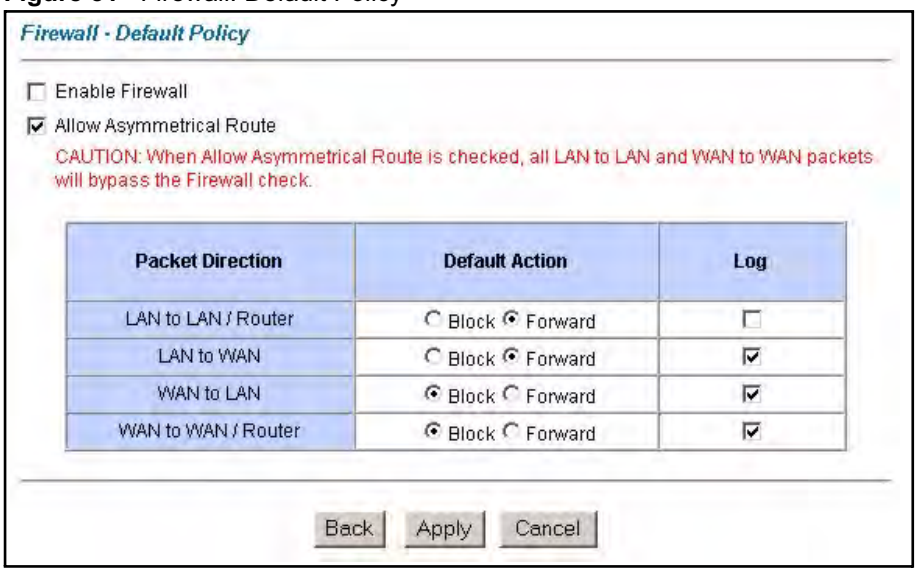
Alerts are reports on events, such as attacks, that you may want to know about right away. You can choose to generate an alert when an attack is detected in the **Edit Rule** screen *(*select the **Send Alert Message to Administrator When Matched** check box) or when a rule is matched in the **Edit Rule** screen. 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).

11.5 Configuring Default Firewall Policy

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.

Refer to Section 10.1 on page 118 for more information.

Figure 51 Firewall: Default Policy



The following table describes the labels in this screen.

Table 37 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.

Table 37 Firewall: Default Policy (continued)

LABEL	DESCRIPTION
Packet Direction	This is the direction of travel of packets (**LAN to LAN/Router, LAN to WAN**, **WAN to WAN/Router**, **WAN to LAN).** 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.

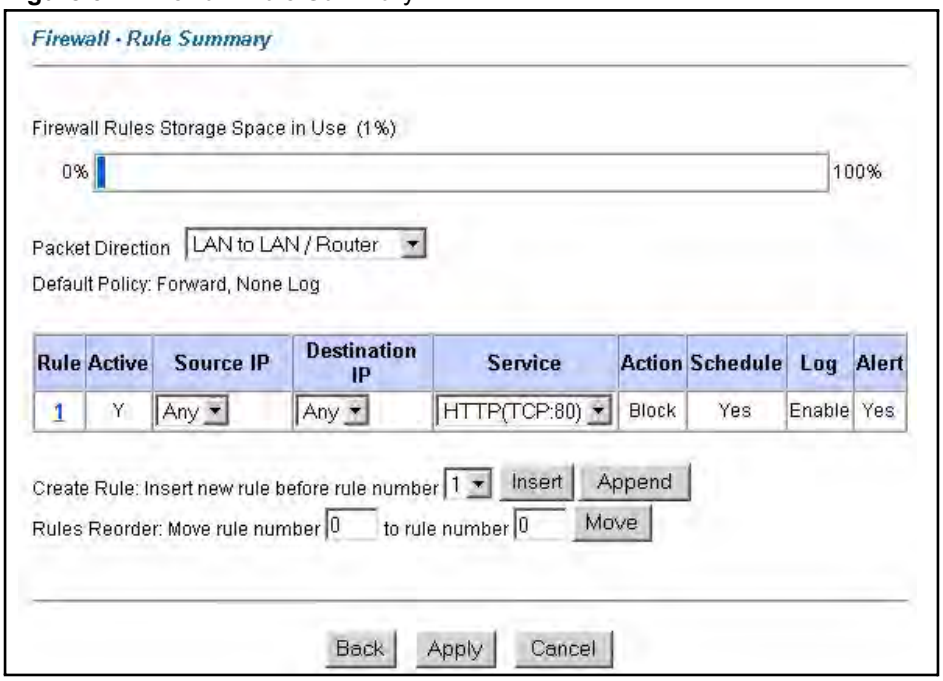
11.6 Rule Summary

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

Refer to Section 10.1 on page 118 for more information.

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 52 Firewall: Rule Summary



The following table describes the labels in this screen.

Table 38 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.
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 Section 11.10 on page 146 for more information.

Table 38 Rule Summary (continued)

LABEL	DESCRIPTION
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.

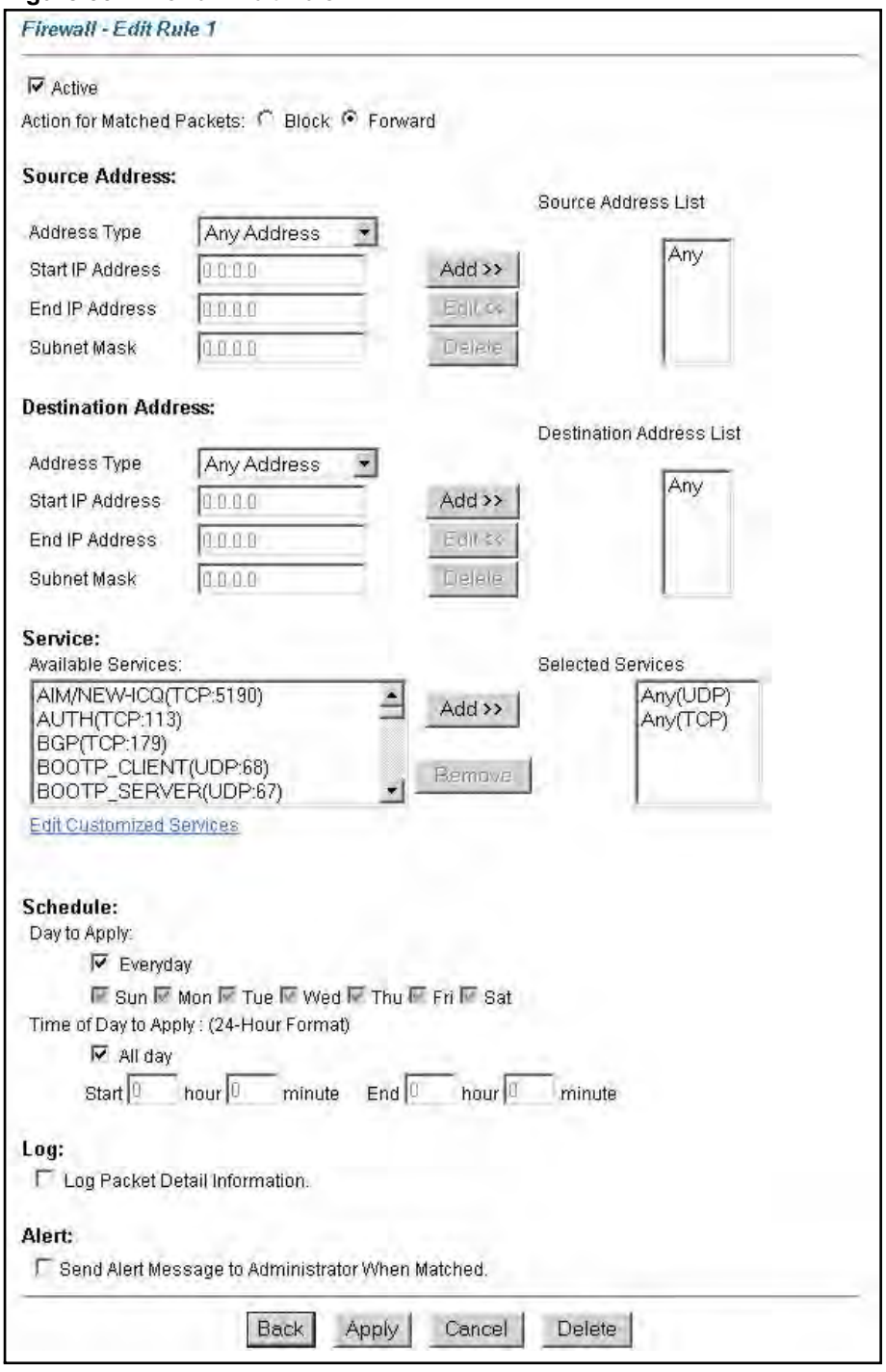
11.6.1 Configuring Firewall Rules

Refer to Section 10.1 on page 118 for more information.

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 53 Firewall: Edit Rule



The following table describes the labels in this screen.

Table 39 Firewall: Edit Rule

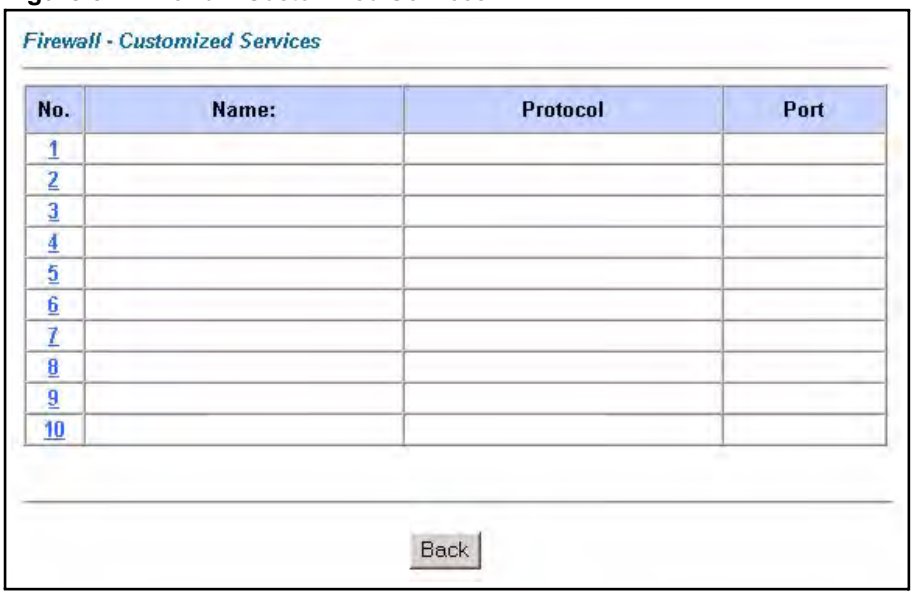
LABEL	DESCRIPTION
Active	Select this option to enable this firewall rule.
Action for Matched Packet	Use the radio button to select whether to discard (**Block**) or allow the passage of (**Forward**) packets that match this rule.
Source/Destination Address	
Address Type	Do you want your rule to apply 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 Section 11.10 on page 146 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.

11.7 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 Section 11.10 on page 146. Click the **Customized Services** link while editing a firewall rule to configure a custom service port. This displays the following screen.

Refer to Section 10.1 on page 118 for more information.

Figure 54 Firewall: Customized Services



The following table describes the labels in this screen.

Table 40 Customized Services

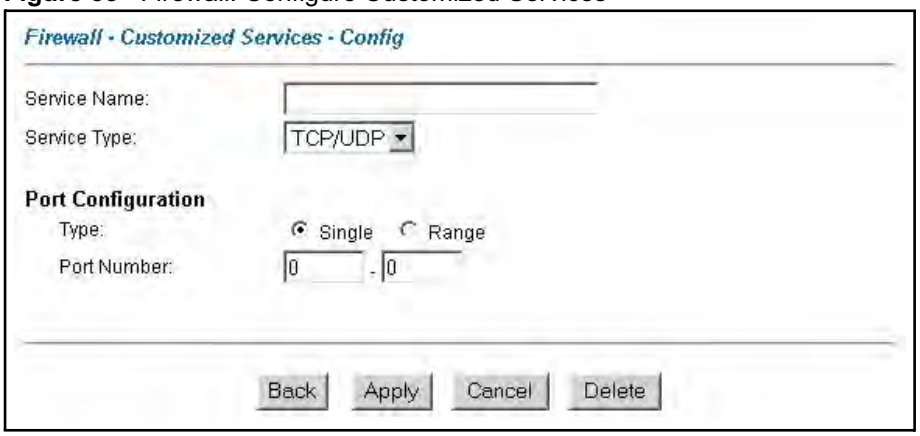
LABEL	DESCRIPTION
No.	This is the number of your customized port. Click a rule's number of a service to go to the **Firewall Customized Services Config** screen to configure or edit a customized service.
Name	This is the name of your customized service.
Protocol	This shows the IP protocol (**TCP**, **UDP** 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.

11.8 Configuring 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.

Refer to Section 10.1 on page 118 for more information.

Figure 55 Firewall: Configure Customized Services



The following table describes the labels in this screen.

Table 41 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.

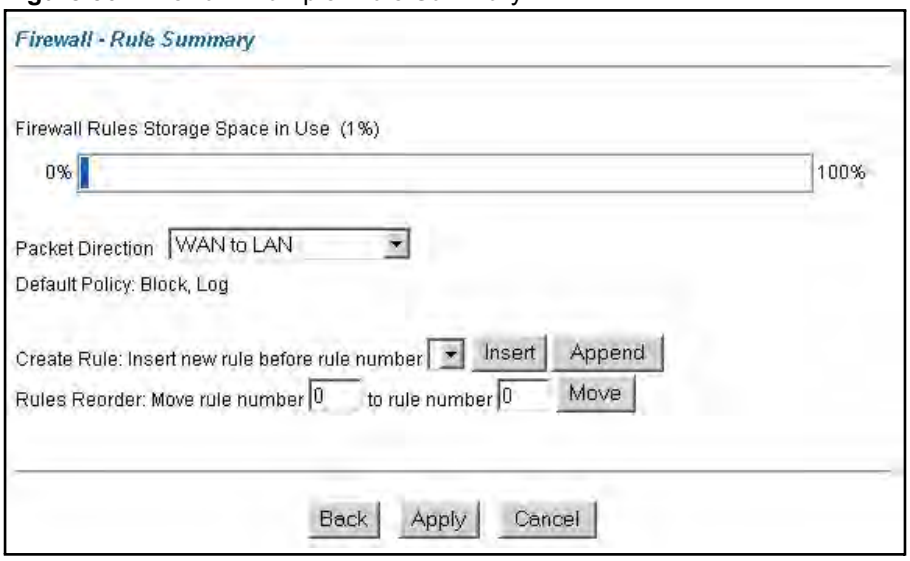
11.9 Example Firewall Rule

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 56 Firewall Example: Rule Summary



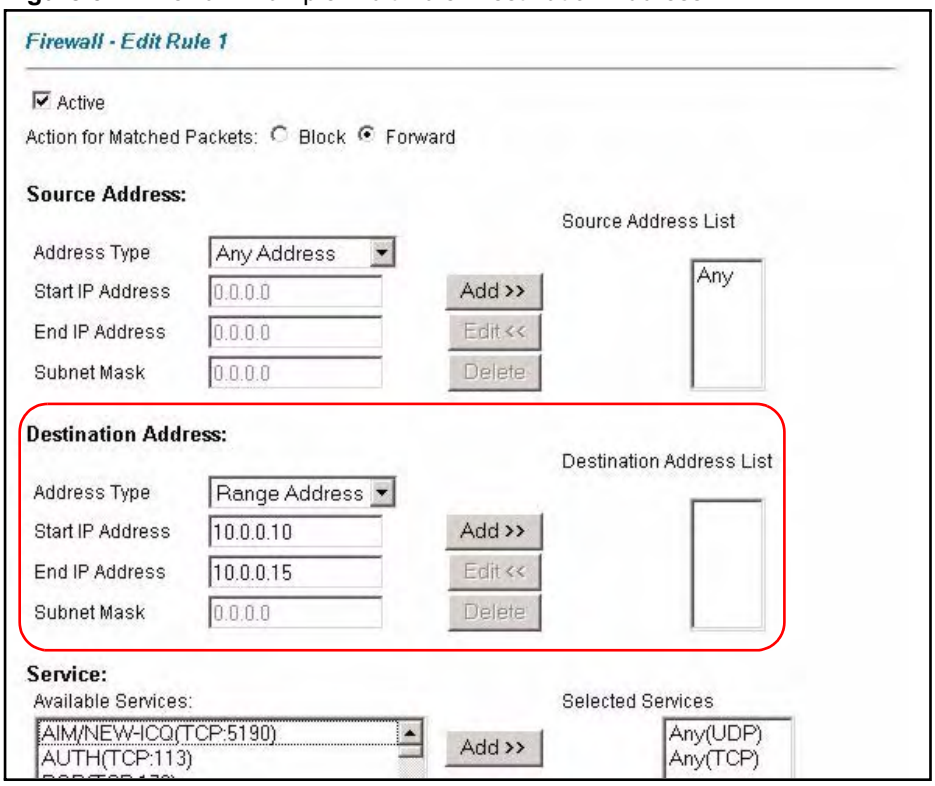
3 In the **Rule Summary** screen, type the index number for where you want to put the rule. For example, if you type "6", your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7.

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**.

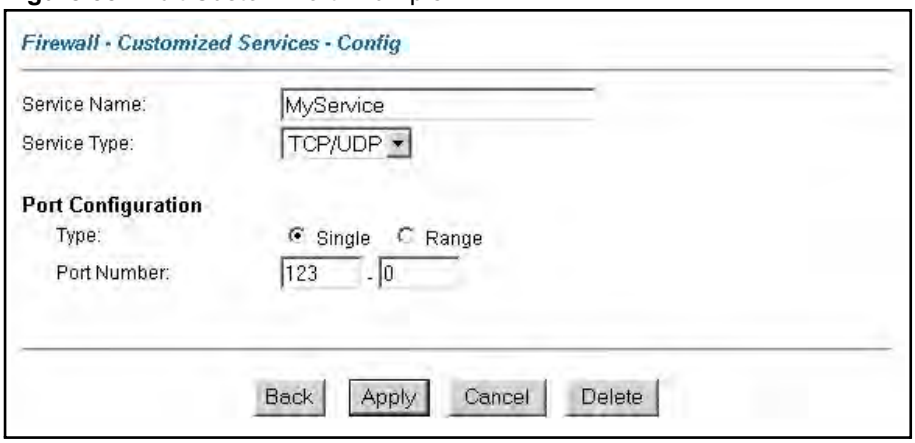
Figure 57 Firewall Example: Edit Rule: Destination Address



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

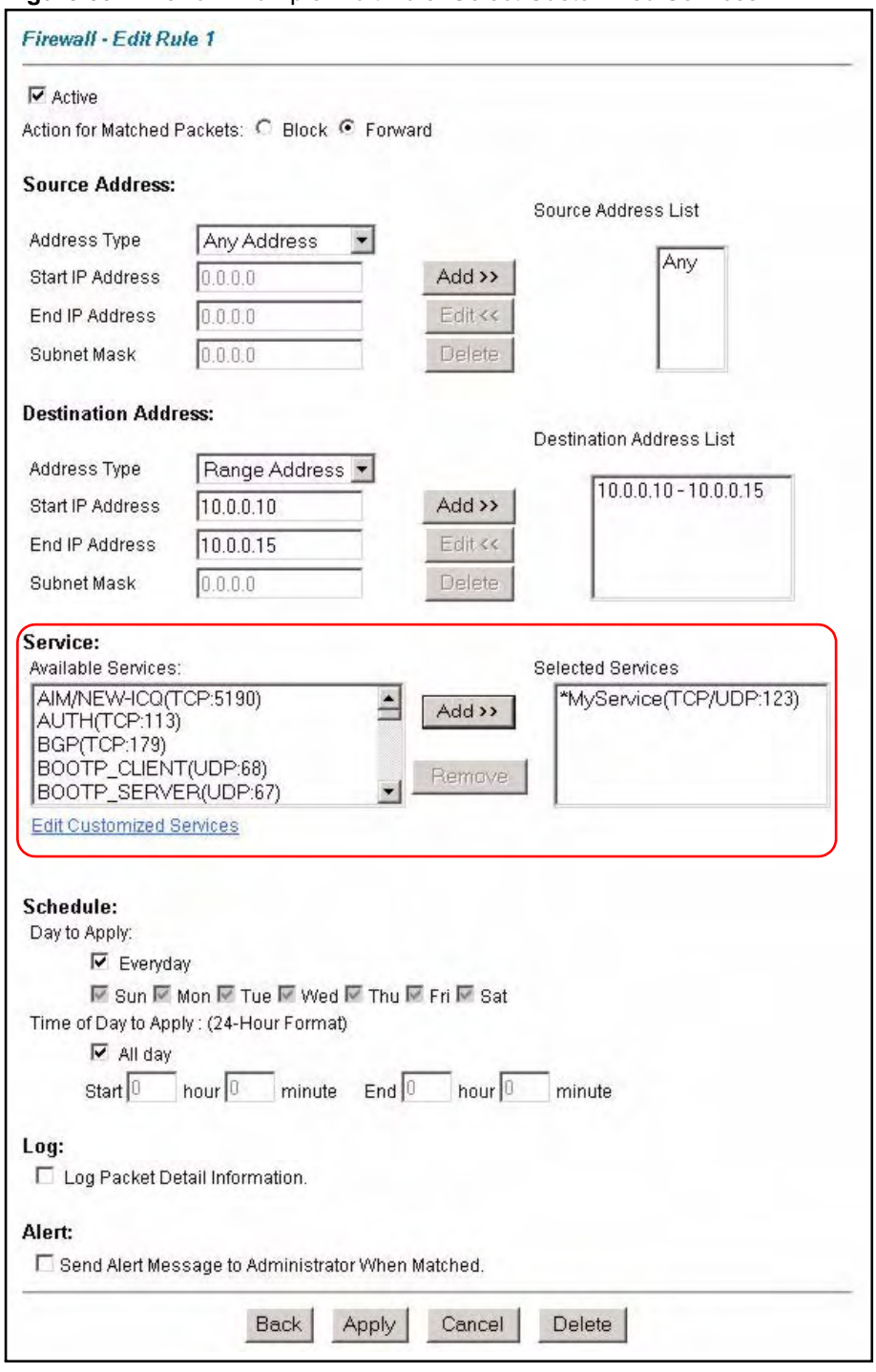
8 Click an index number to display the **Customized Services -Config** screen and configure the screen as follows and click **Apply**.

Figure 58 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 59 Firewall Example: Edit Rule: Select Customized Services

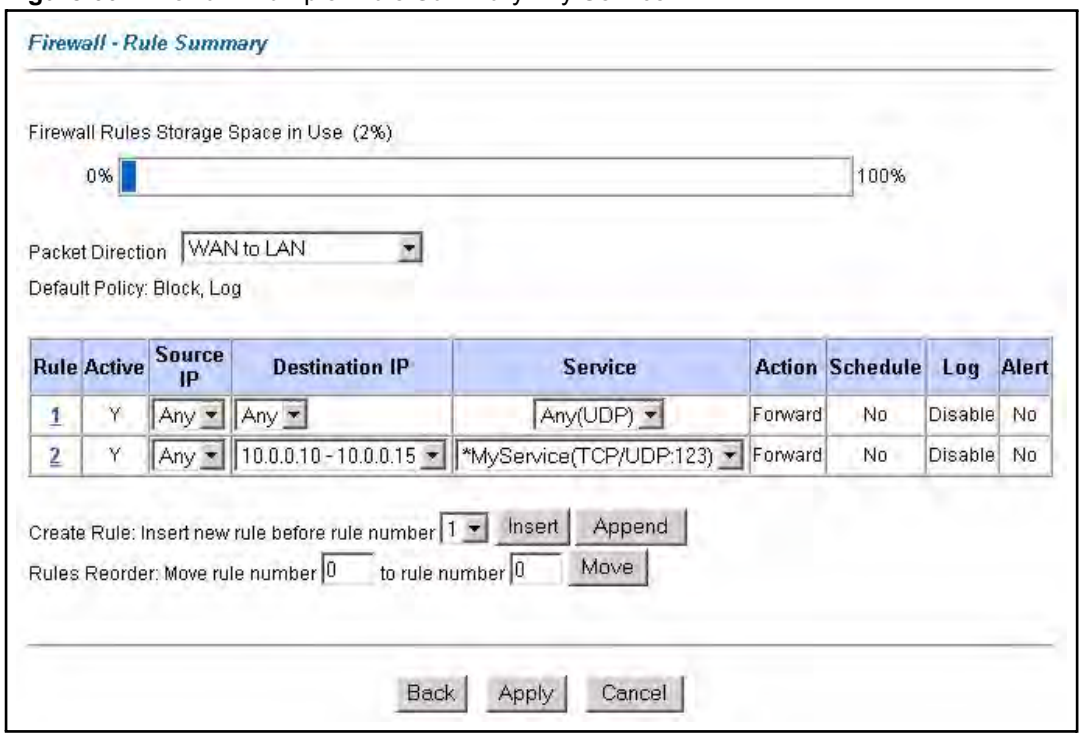


Note: Custom ports show up with an "*" before their names in the Services list box and the **Rule Summary** list box. Click **Apply** after you've created your custom port.

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 60 Firewall Example: Rule Summary: My Service



11.10 Predefined Services

The **Available Services** list box in the **Edit Rule** screen (see Section 11.6.1 on page 138) 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 42 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.
BOOTP_SERVER(UDP:67)	DHCP Server.

Table 42 Predefined Services (continued)

SERVICE	DESCRIPTION
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 42 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.

11.11 Anti-Probing

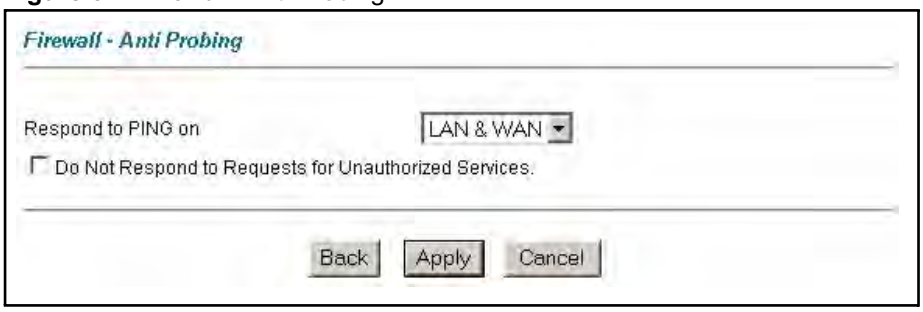
If an outside user attempts to probe an unsupported port on your Prestige, an ICMP response packet is automatically returned. This allows the outside user to know the Prestige exists. The Prestige supports anti-probing, which prevents the ICMP response packet from being sent. This keeps outsiders from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

Refer to Section 10.1 on page 118 for more information.

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

Figure 61 Firewall: Anti Probing



The following table describes the labels in this screen.

Table 43 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. Otherwise select **LAN & WAN** to reply to both incoming LAN and WAN 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.

11.12 DoS Thresholds

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.

Refer to Section 11.12.3 on page 151 to configure thresholds.

11.12.1 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.

11.12.2 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 47 on page 122). 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.

11.12.2.1 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:

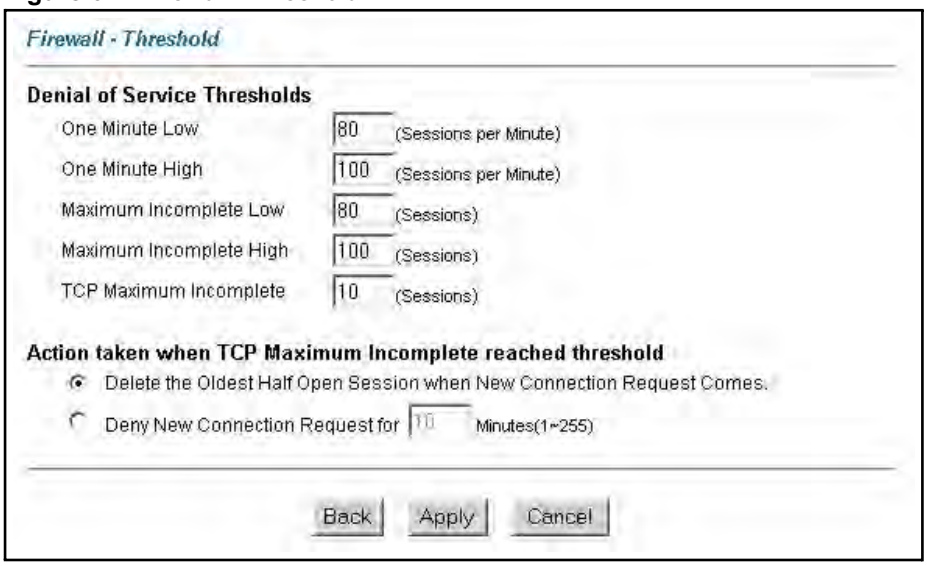
- If the **Blocking Time** timeout is 0 (the default), then the Prestige deletes the oldest existing half-open session for the host for every new connection request to the host. This ensures that the number of half-open sessions to a given host will never exceed the threshold.
- If the **Blocking Time** 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.

11.12.3 Configuring Firewall Thresholds

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 62 Firewall: Threshold



The following table describes the labels in this screen.

Table 44 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.
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 Incomplete 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.	

Table 44 Firewall: Threshold (continued)

LABEL	DESCRIPTION	DEFAULT VALUES
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 12
Content Filtering

This chapter covers how to configure content filtering.

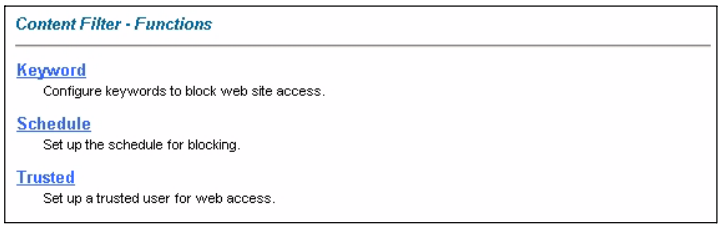
12.1 Content Filtering Overview

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.

12.2 The Main Content Filter Screen

Click **Content Filter** to display the main Content Filtering screen.

Figure 63 Content Filtering



The following table describes the links in this screen.

Table 45

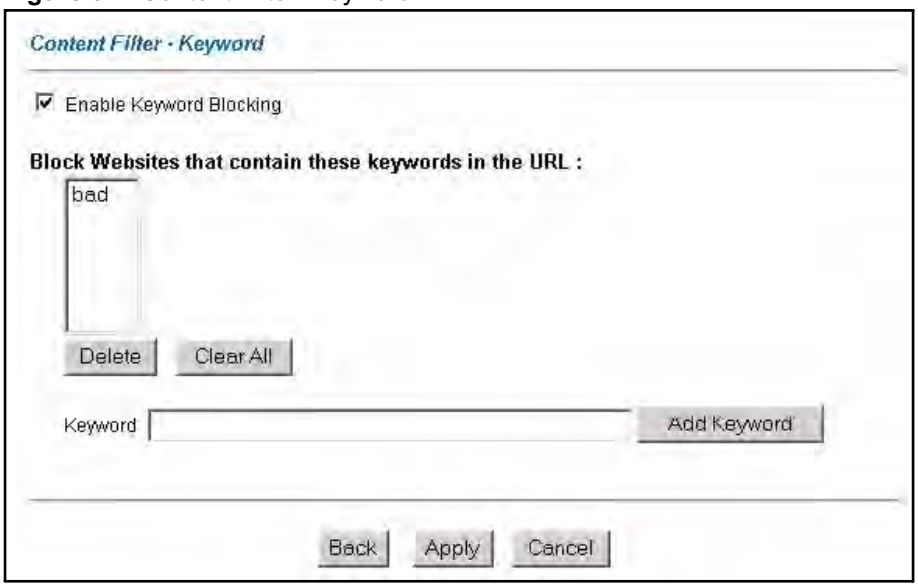
LINK	DESCRIPTION
Keyword	Click this link to display a screen where you can configure your Prestige to block Web sites containing keywords in their URLs,
Schedule	Click this link to display a screen where you can set the days and times for the Prestige to perform content filtering,
Trusted	Click this link to display a screen where you can exclude a range of users on the LAN from content filtering on your Prestige

12.3 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 64 Content Filter: Keyword



The following table describes the labels in this screen.

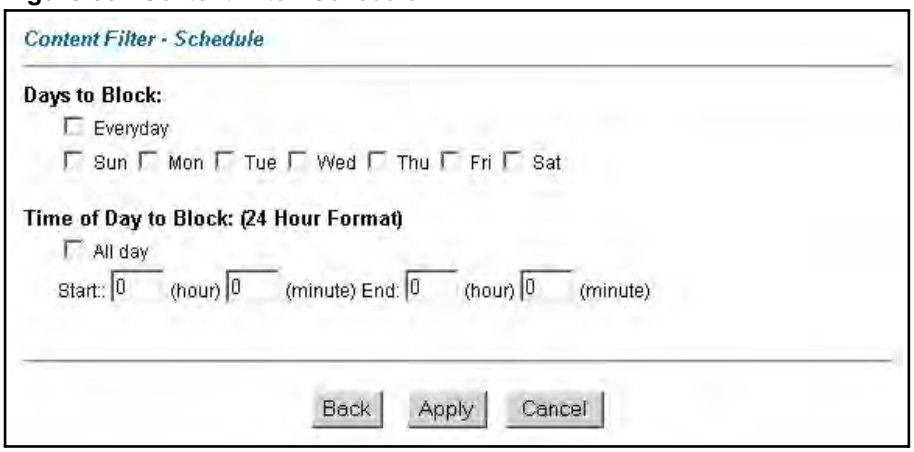
Table 46 Content Filter: Keyword

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.

12.4 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 65 Content Filter: Schedule



The following table describes the labels in this screen.

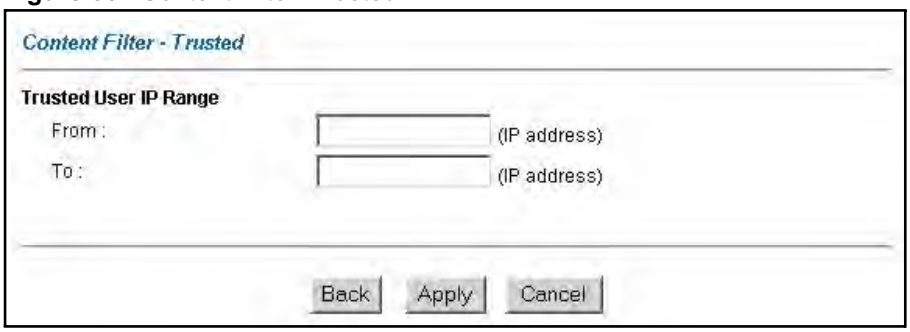
Table 47 Content Filter: Schedule

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.

12.5 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 66 Content Filter: Trusted



The following table describes the labels in this screen.

Table 48 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 13
Remote Management Configuration

This chapter provides information on configuring remote management.

13.1 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.

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

13.1.1 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.

13.1.2 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.

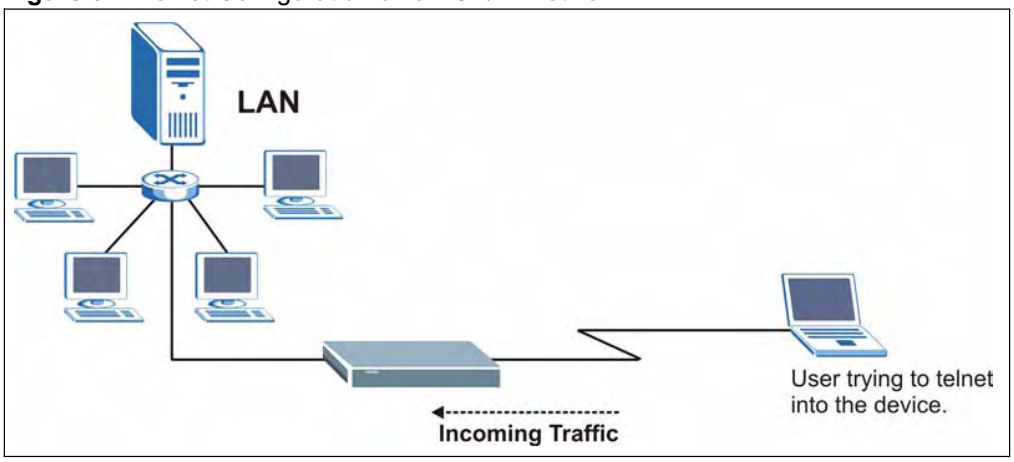
13.1.3 System Timeout

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.

13.2 Telnet

You can configure your Prestige for remote Telnet access as shown next.

Figure 67 Telnet Configuration on a TCP/IP Network



13.3 FTP

You can upload and download Prestige firmware and configuration files using FTP. To use this feature, your computer must have an FTP client.

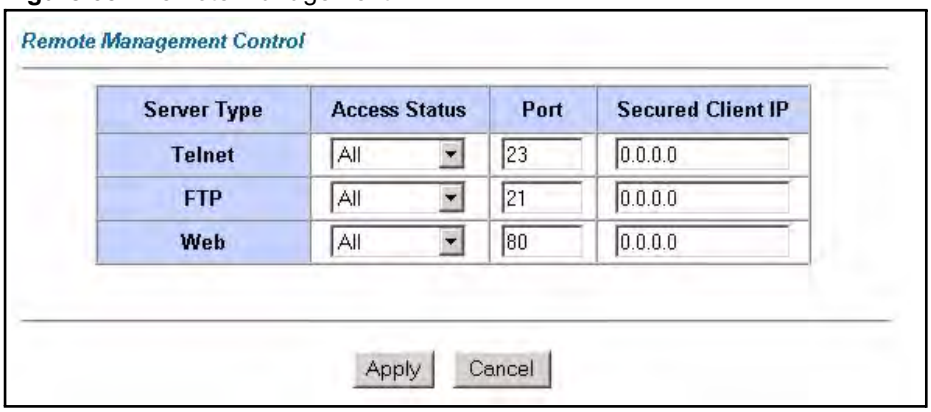
13.4 Web

You can use the Prestige's embedded web configurator for configuration and file management. See the online help for details.

13.5 Configuring Remote Management

Click **Remote Management** to open the following screen. See Section 13.1 on page 158 for more information.

Figure 68 Remote Management



The following table describes the fields in this screen.

Table 49 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 14
Universal Plug-and-Play (UPnP)

This chapter introduces the UPnP feature in the web configurator.

14.1 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.

See Section 14.2.1 on page 163 for configuration instructions.

14.1.1 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.

14.1.2 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 NAT chapter for more information on NAT.

14.1.3 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.

14.2 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.

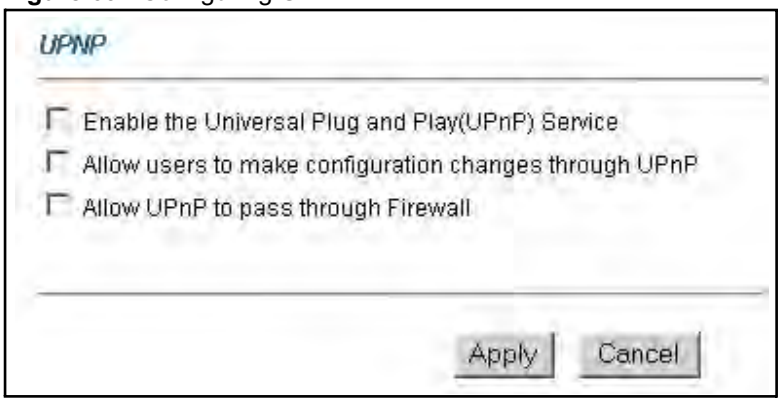
See later sections for examples of installing UPnP in Windows XP and Windows Me as well as an example of using UPnP in Windows.

14.2.1 Configuring UPnP

From the **Site Map** in the main menu, click **UPnP** under **Advanced Setup** to display the screen shown next.

See Section 14.1 on page 162 for more information.

Figure 69 Configuring UPnP



The following table describes the fields in this screen.

Table 50 Configuring UPnP

LABEL	DESCRIPTION
Enable the Universal Plug and Play (UPnP) Service	Select this check box 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.

14.3 Installing UPnP in Windows Example

This section shows how to install UPnP in Windows Me and Windows XP.

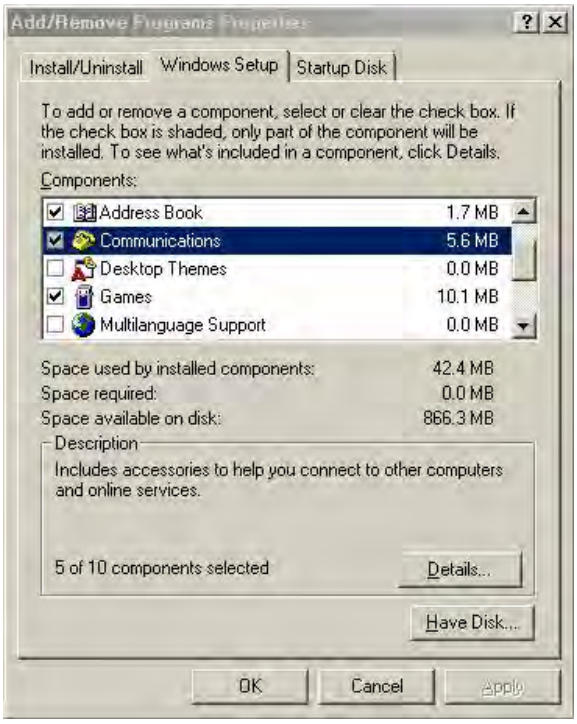
Installing UPnP in Windows Me

Follow the steps below to install the UPnP in Windows Me.

1 Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.

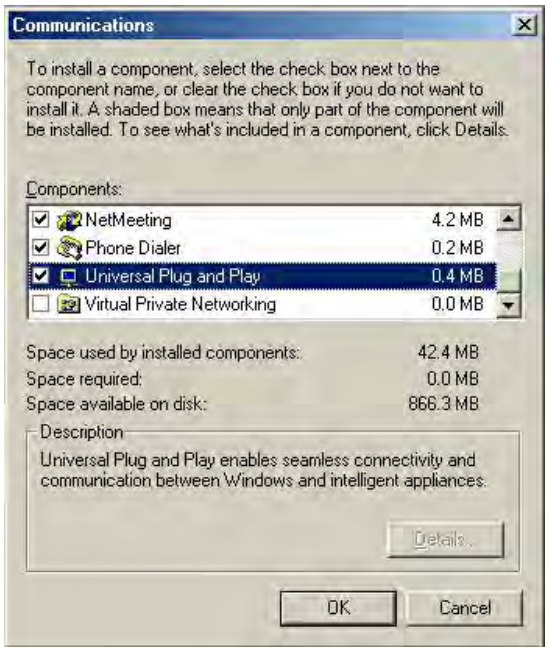
2 Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.

Figure 70 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 71 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**.

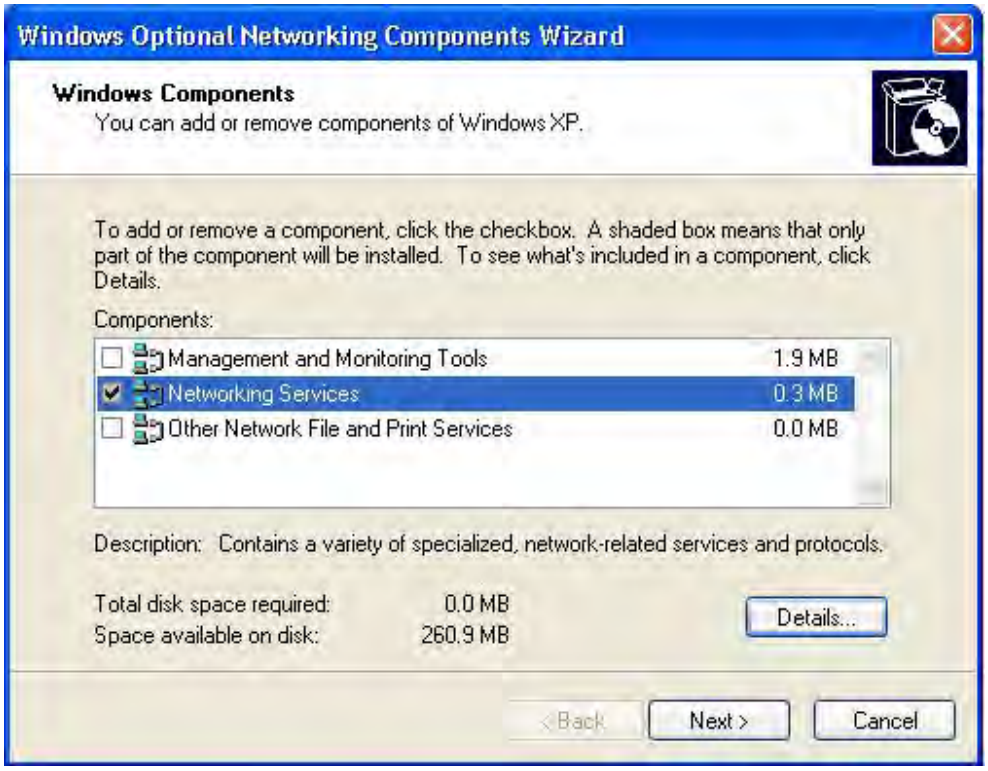
2 Double-click **Network Connections**.

3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ….**

Figure 72 Network Connections

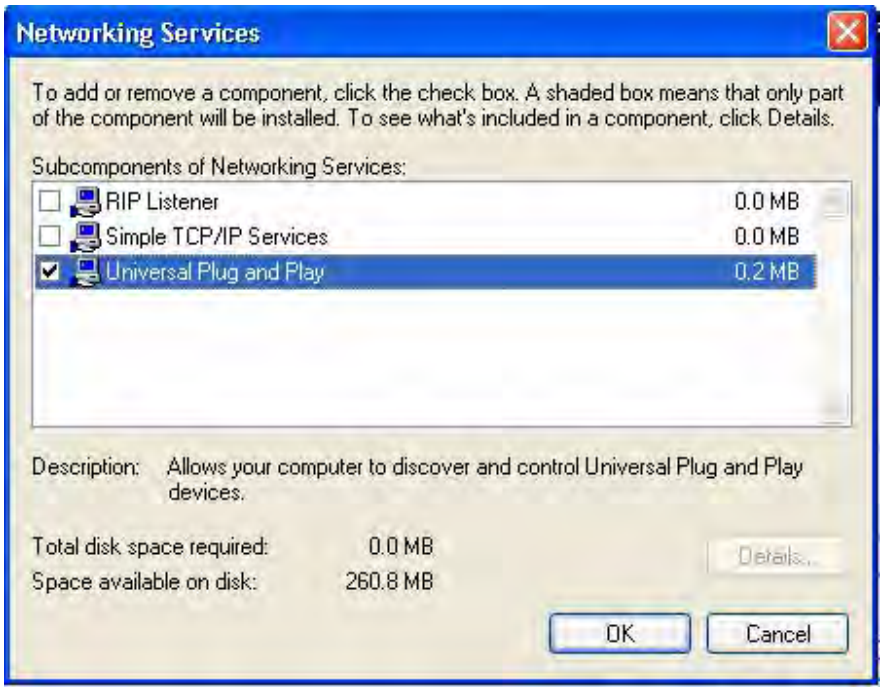
4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.

Figure 73 Windows Optional Networking Components Wizard



5 In the **Networking Services** window, select the **Universal Plug and Play** check box.

Figure 74 Networking Services



6 Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.

14.4 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 75 Network Connections

3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

Figure 76 Internet Connection Properties

4 You may edit or delete the port mappings or click **Add** to manually add port mappings.

Figure 77 Internet Connection Properties: Advanced Settings

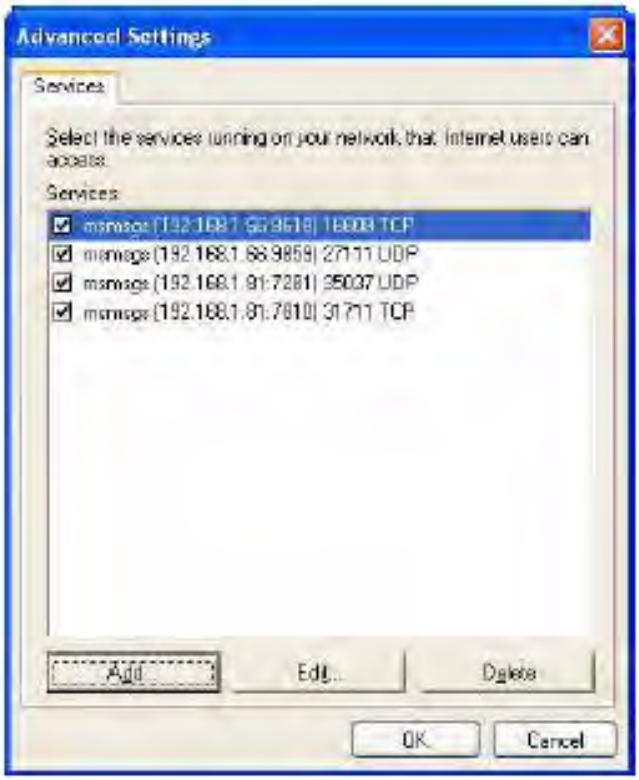


Figure 78 Internet Connection Properties: Advanced Settings: Add

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 79 System Tray Icon

7 Double-click on the icon to display your current Internet connection status.

Figure 80 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.

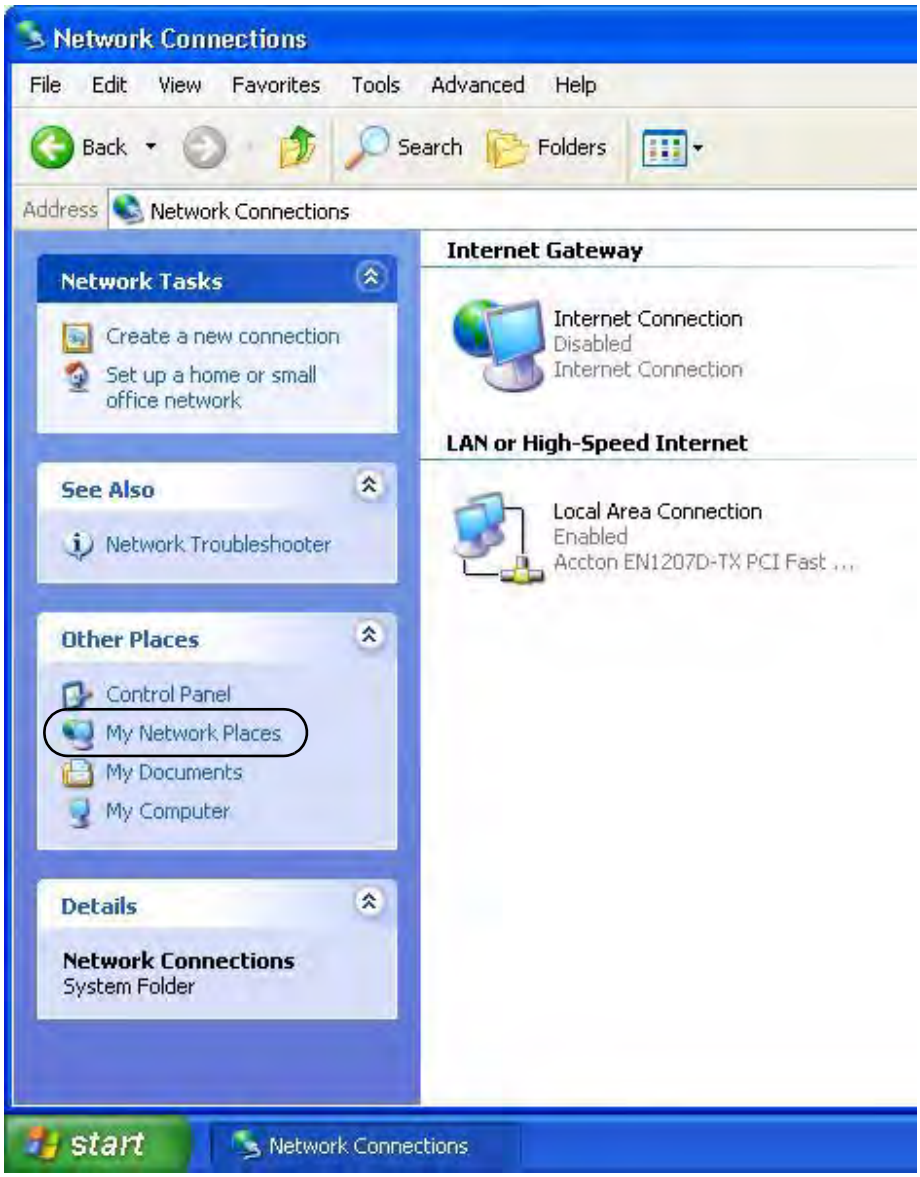
Follow the steps below to access the web configurator.

1 Click **Start** and then **Control Panel**.

2 Double-click **Network Connections**.

3 Select **My Network Places** under **Other Places**.

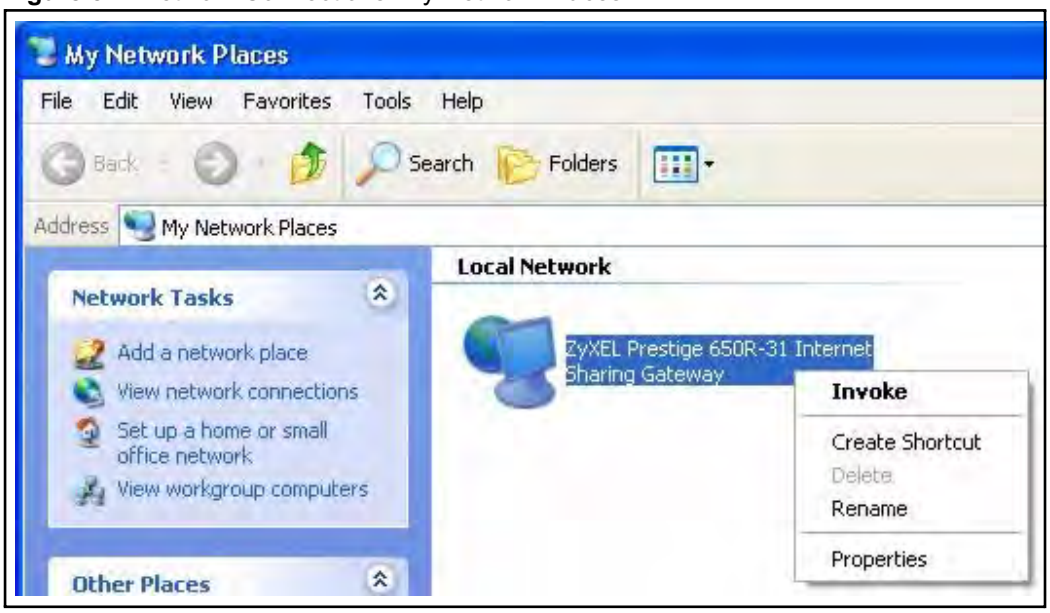
Figure 81 Network Connections



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 82 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 83 Network Connections: My Network Places: Properties: Example

CHAPTER 15
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.

15.1 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.

15.1.1 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.

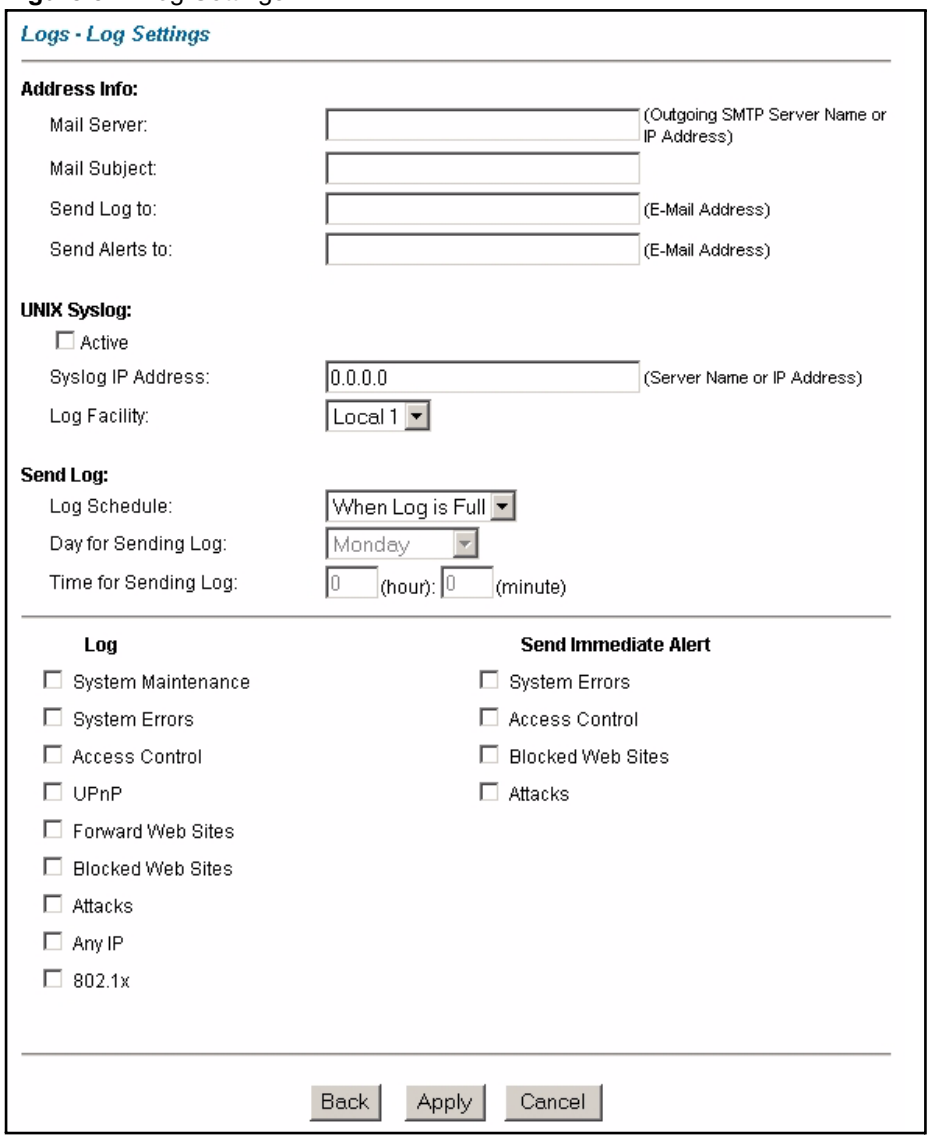
15.2 Configuring Log Settings

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. See Section 15.1 on page 176 for more information.

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. Selecting many alert and/or log categories (especially **Access Control**) may result in many e-mails being sent.

Figure 84 Log Settings



The following table describes the fields in this screen.

Table 51 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.
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.

Table 51 Log Settings

LABEL	DESCRIPTION
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.

15.3 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 Section 15.2 on page 176).

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 85 View Logs

The following table describes the fields in this screen.

Table 52 View Logs

LABEL	DESCRIPTION
Display	The categories that you select in the **Log Settings** screen 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.
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**).
Refresh	Click **Refresh** to renew the log screen.
Clear Log	Click **Clear Log** to delete all the logs.

15.4 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 53 SMTP Error Messages

-1 means Prestige out of socket
-2 means tcp SYN fail
-3 means smtp server OK fail
-4 means HELO fail
-5 means MAIL FROM fail

Table 53 SMTP Error Messages

-6 means RCPT TO fail
-7 means DATA fail
-8 means mail data send fail

15.4.1 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 86 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 16
Media Bandwidth Management Advanced Setup

This chapter describes bandwidth management with one level of child class.

16.1 Media Bandwidth Management 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 1Mbps. 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.

Refer to Section 16.9 on page 188 to enable and configure bandwidth on the interfaces.

Refer to Section 16.10 on page 190 to configure bandwidth classes.

Refer to Section 16.11 on page 194 to view bandwidth usage information.

16.2 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 Section 16.10 on page 190) 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 Section 16.10 on page 190 for details).

The total of the configured bandwidth budgets for child-classes cannot exceed the configured bandwidth budget speed of the parent class.

16.3 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.

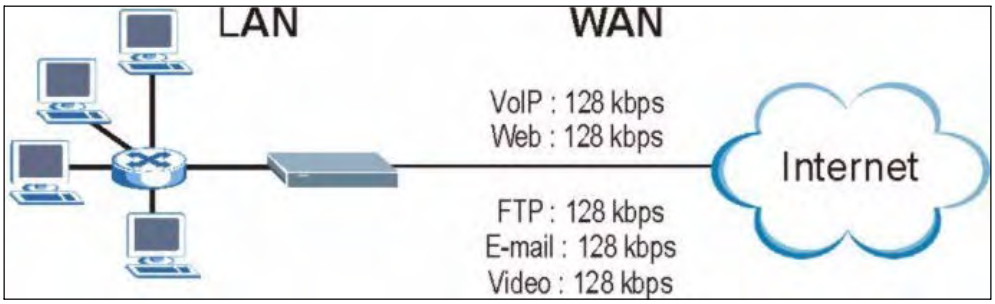
16.4 Bandwidth Management Usage Examples

These examples show bandwidth management allotments on a WAN interface that is configured for 640Kbps.

16.4.1 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.

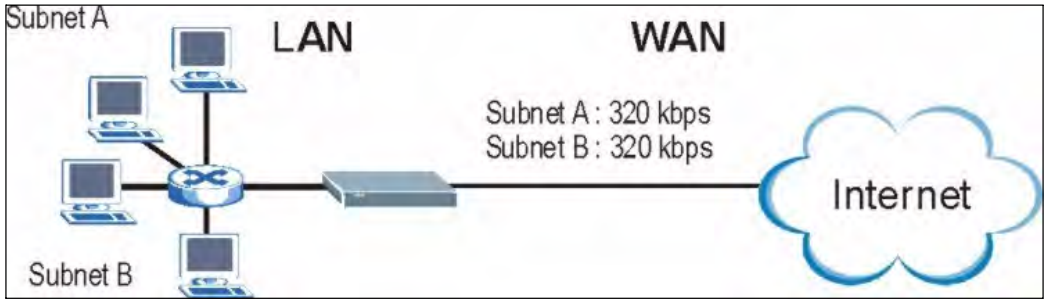
Figure 87 Application-based Bandwidth Management Example



16.4.2 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 88 Subnet-based Bandwidth Management Example



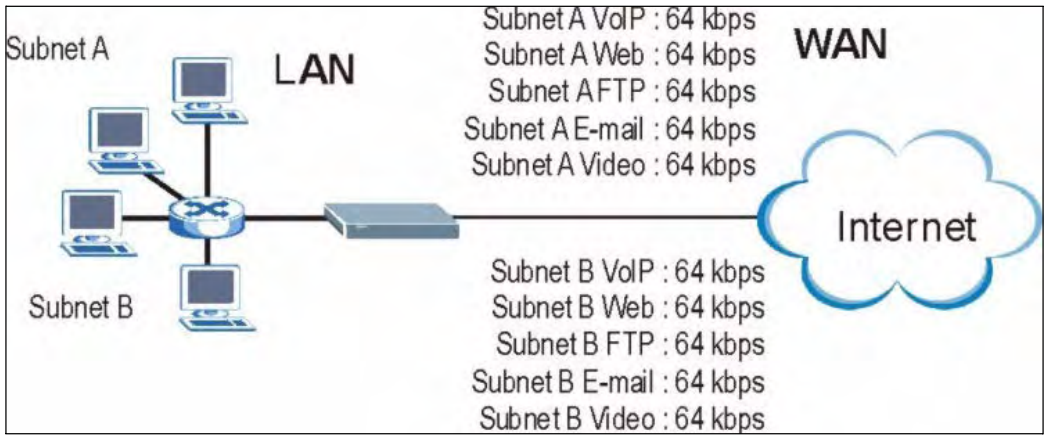
16.4.3 Application and Subnet-based Bandwidth Management Example

The following example uses bandwidth classes based on LAN subnets and applications (specific applications in each subnet are allotted bandwidth).

Table 54 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 89 Application and Subnet-based Bandwidth Management Example



16.5 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.

16.5.1 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.

16.5.2 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.

16.6 Maximize Bandwidth Usage

The maximize bandwidth usage option (see Section 16.7.1 on page 187) 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.

16.6.1 Reserving Bandwidth for Non-Bandwidth Class Traffic

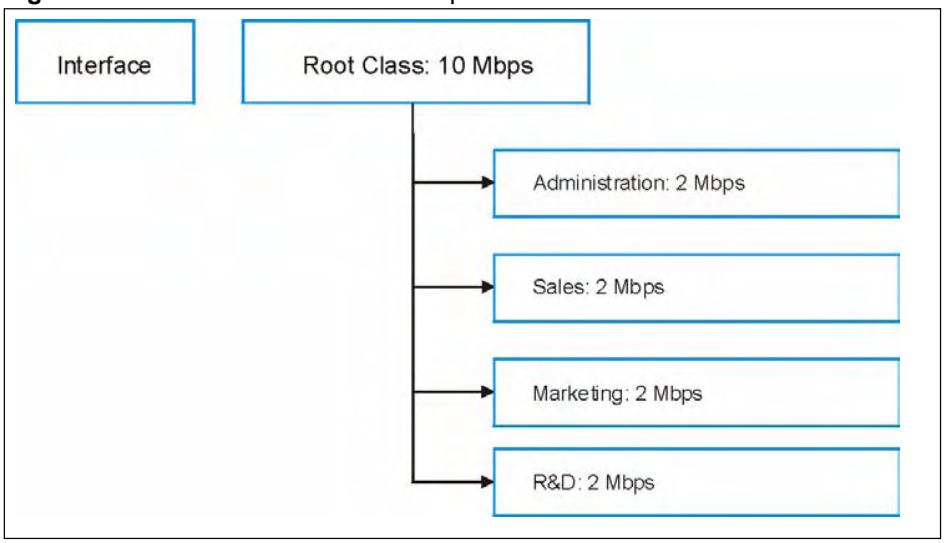
Do the following three steps to configure the Prestige to allow bandwidth for traffic that is not defined in a bandwidth filter.

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 Section 16.7 on page 187).

16.6.2 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 90 Bandwidth Allotment Example

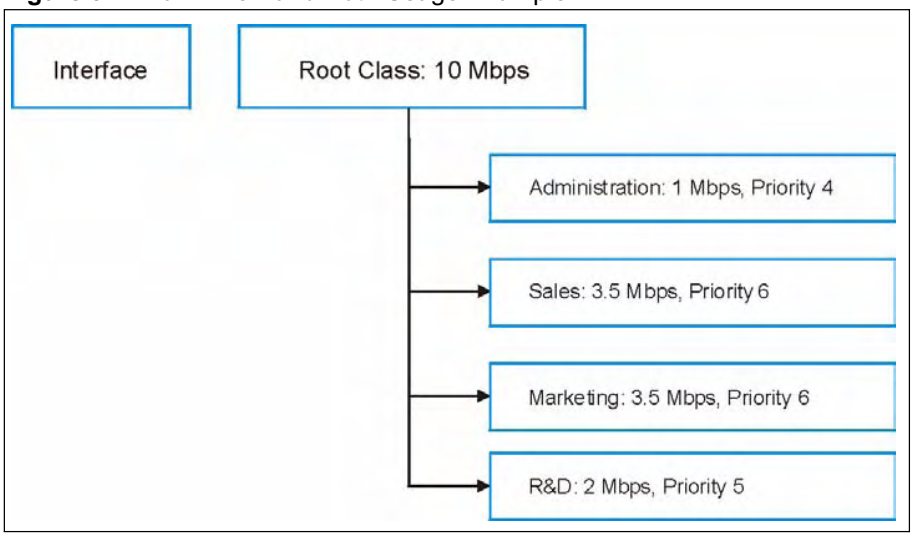


The following figure shows the bandwidth usage with the maximize bandwidth usage option enabled. The Prestige divides up the unbudgeted 2 Mbps among the classes that require more bandwidth. If the administration department only uses 1 Mbps of the budgeted 2 Mbps, the Prestige also divides the remaining 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 91 Maximize Bandwidth Usage Example



16.7 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 that has bandwidth borrowing configured, first.

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.

16.7.1 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.

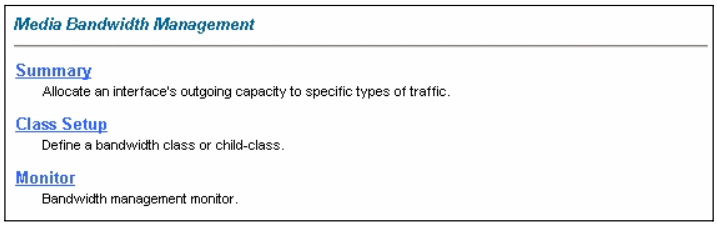
1. The Prestige sends traffic according to each bandwidth class's bandwidth budget.
2. The Prestige assigns a parent class's unused bandwidth to its child-classes that have more traffic than their budgets and have bandwidth borrowing enabled. The Prestige gives priority to bandwidth child-classes of 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.

16.8 The Main Media Bandwidth Management Screen

Click **Media Bandwidth Mgnt.** to display the main **Media Bandwidth Management** screen as shown.

Figure 92 Media Bandwidth Mgnt.



The following table describes the links in this screen.

Table 55 Media Bandwidth Mgnt.

LINK	DESCRIPTION
Summary	Click this link to display a screen where you can enable bandwidth management on an interface and set the maximum allowed bandwidth for that interface.
Class Setup	Click this link to display a screen thwere you can configure bandwidth classes.
Monitor	Click this link to display a screen wehre you can view bandwidth usage.

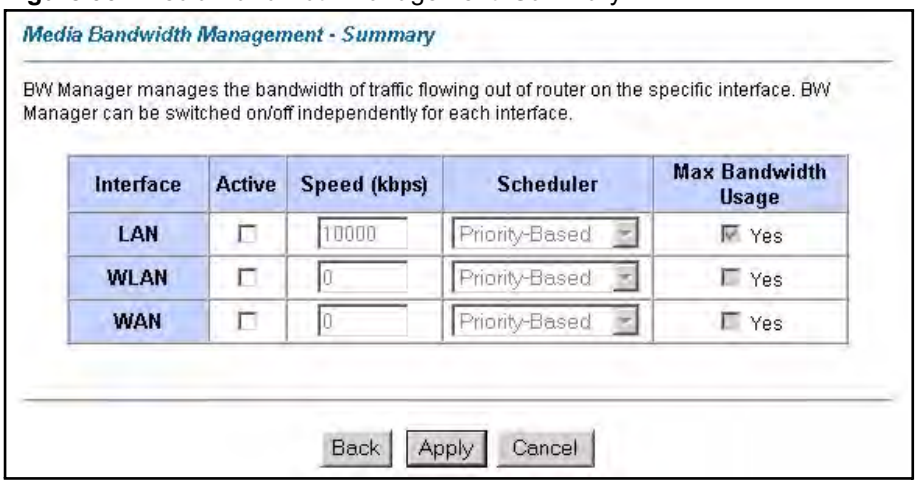
16.9 Configuring Summary

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.

Refer to Section 16.1 on page 182 for more information.

Figure 93 Media Bandwidth Management: Summary



The following table describes the labels in this screen.

Table 56 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 10000 kbps if the ADSL connection has an upstream speed of 10Mbps.
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.

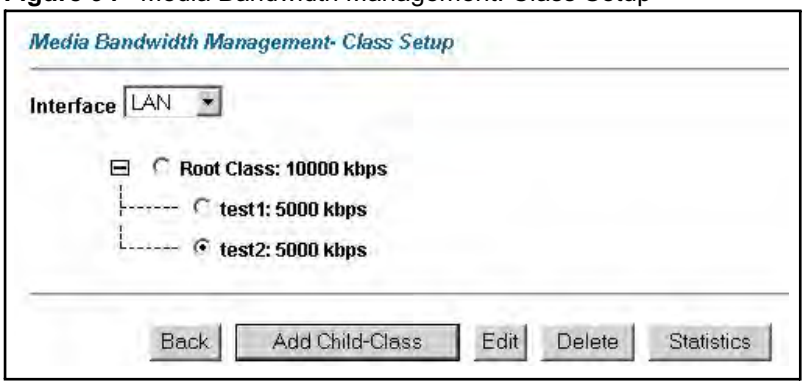
16.10 Configuring Class Setup

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 Section 16.9 on page 188 to configure the speed of the interface). Configure child-class layers for the root class.

Refer to Section 16.1 on page 182 for more information.

To add or delete child classes on an interface, click **Media Bandwidth Management**, then **Class Setup**. The screen appears as shown (with example classes).

Figure 94 Media Bandwidth Management: Class Setup



The following table describes the labels in this screen.

Table 57 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.

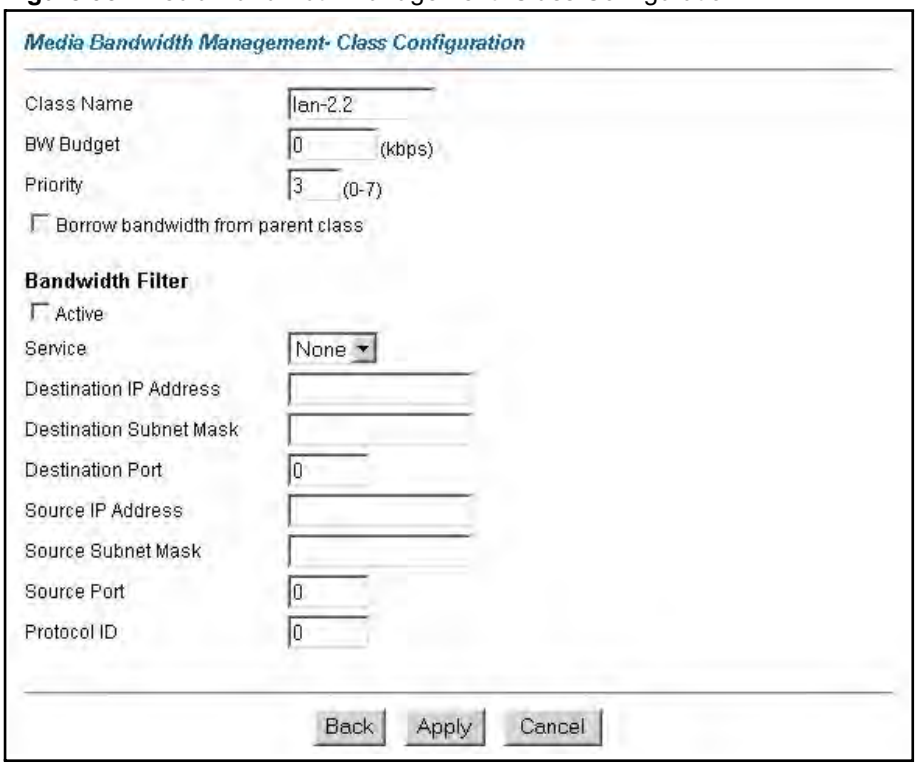
16.10.1 Media Bandwidth Management Class Configuration

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.

Refer to Section 16.1 on page 182 for more information.

To add a child class, click **Media Bandwidth Management**, then **Class Setup**. Click the **Add Child-Class** button to open the following screen.

Figure 95 Media Bandwidth Management: Class Configuration



The following table describes the labels in this screen.

Table 58 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.	

Table 58 Media Bandwidth Management: Class Configuration (continued)

LABEL	DESCRIPTION
Active	Select the check box to have the Prestige use this bandwidth filter when it performs bandwidth management.
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 59 Services and Port Numbers

SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21

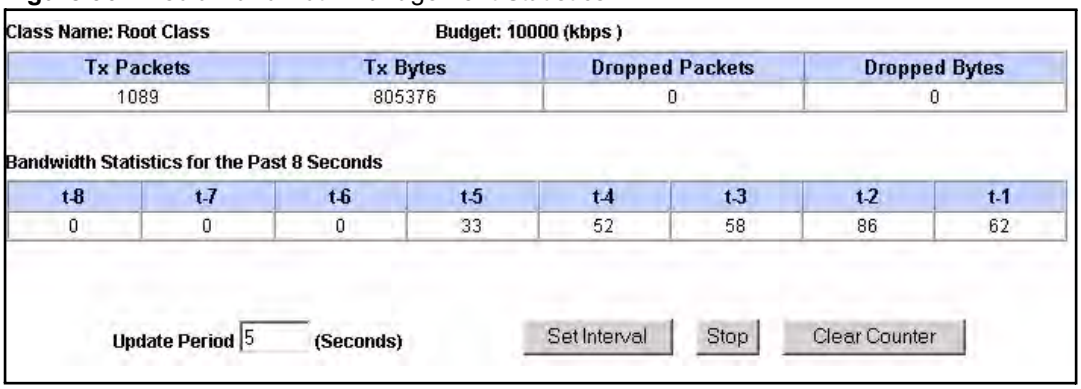
Table 59 Services and Port Numbers

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

16.10.2 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 96 Media Bandwidth Management Statistics



The following table describes the labels in this screen.

Table 60 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)	

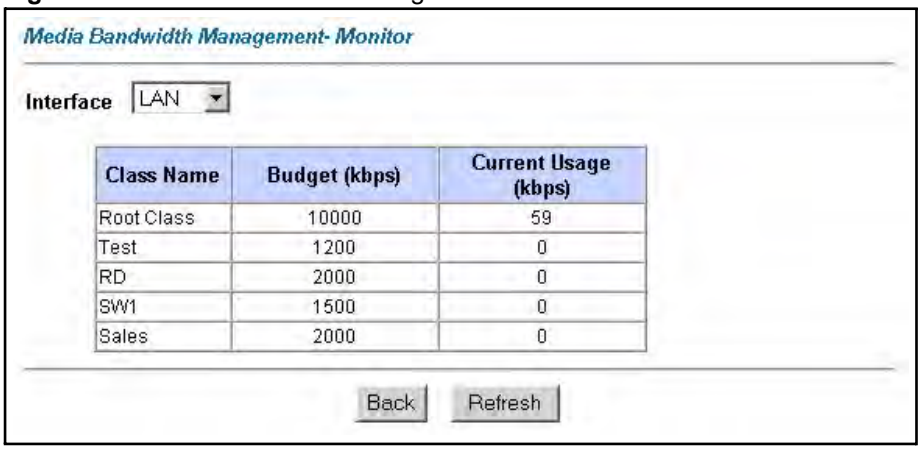
Table 60 Media Bandwidth Management Statistics

LABEL	DESCRIPTION
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.
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.

16.11 Bandwidth Monitor

To view the Prestige's bandwidth usage and allotments, click **Media Bandwidth Management**, then **Monitor**. The screen appears as shown.

Figure 97 Media Bandwidth Management: Monitor



The following table describes the labels in this screen.

Table 61 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 17
Maintenance

This chapter displays system information such as ZyNOS firmware, port IP addresses and port traffic statistics.

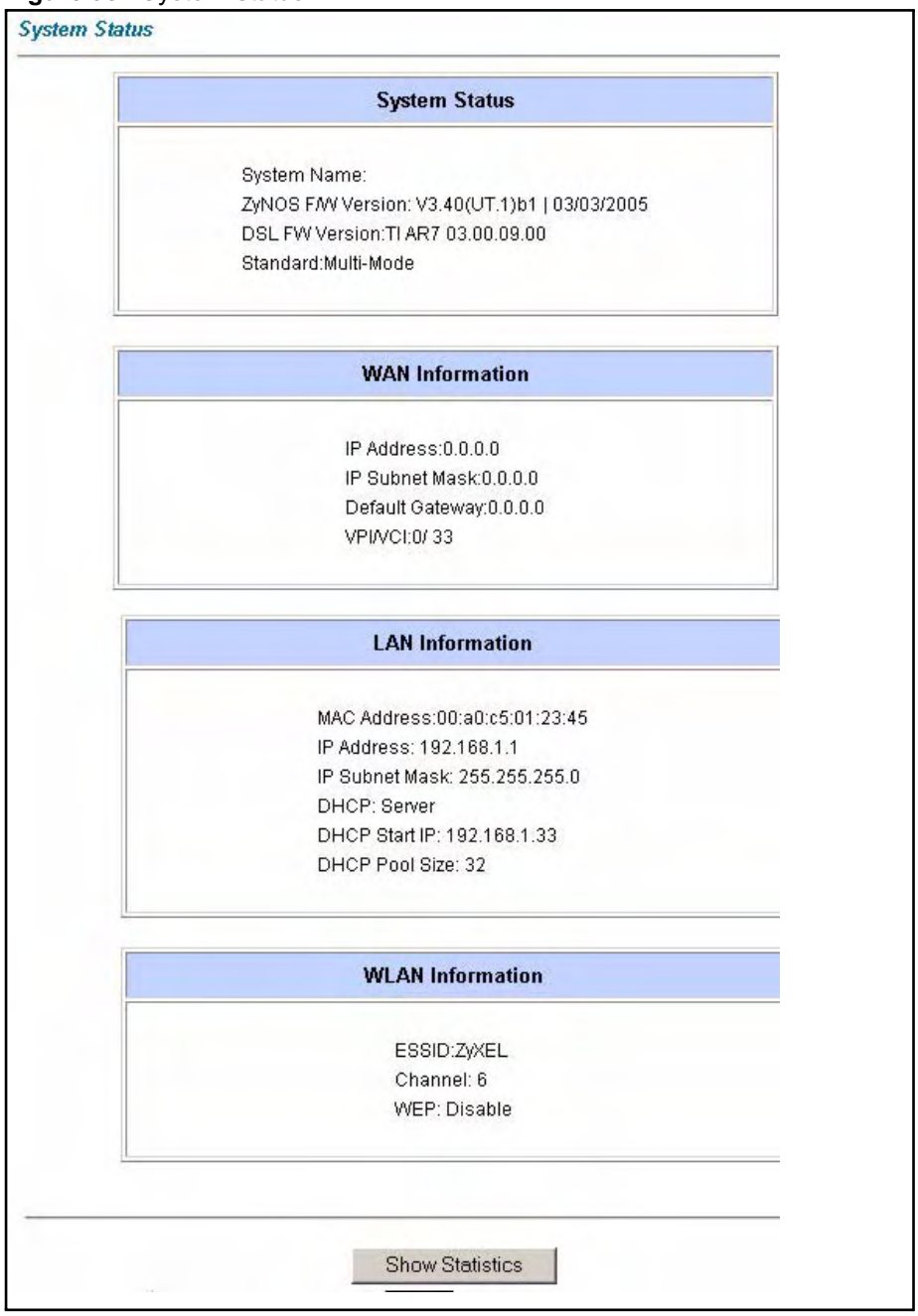
17.1 Maintenance Overview

The maintenance screens can help you view system information, upload new firmware, manage configuration and restart your Prestige.

17.2 System Status Screen

Click **System Status** under **Maintenance** 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 98 System Status



The following table describes the fields in this screen.

Table 62 System Status

LABEL	DESCRIPTION
System Status	
System Name	This is the name of your Prestige. It is for identification purposes.

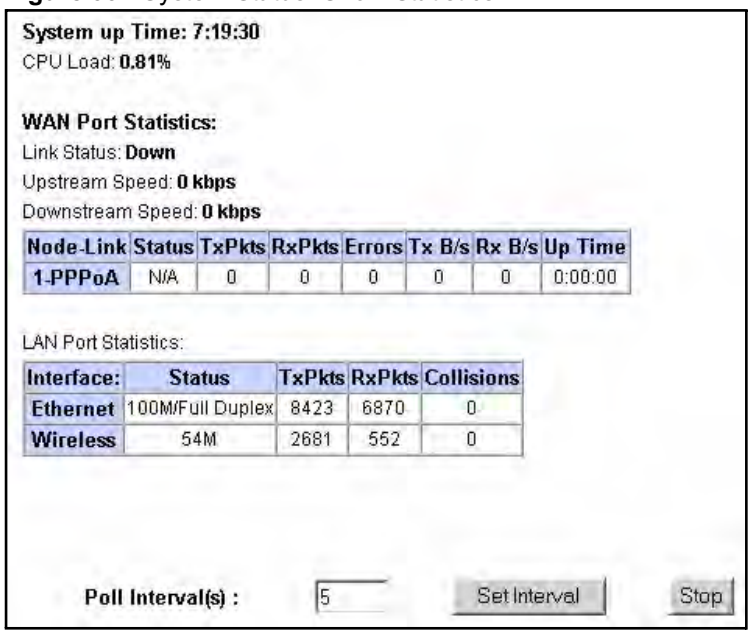
Table 62 System Status (continued)

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.

17.2.1 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 99 System Status: Show Statistics



The following table describes the fields in this screen.

Table 63 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 63 System Status: Show Statistics (continued)

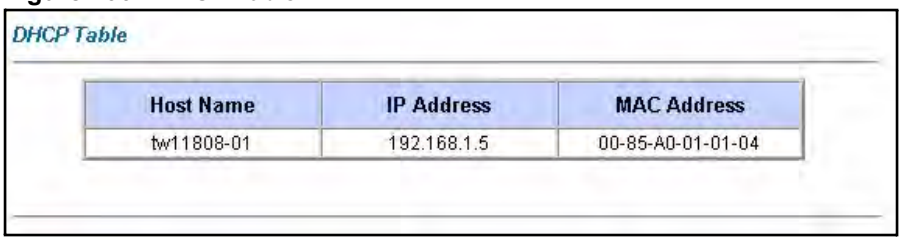
LABEL	DESCRIPTION
Poll Interval(s)	Type the time interval for the browser to refresh system statistics.
Set Interval	Click this button to apply the new poll interval you entered in the **Poll Interval** field above.
Stop	Click this button to halt the refreshing of the system statistics.

17.3 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 100 DHCP Table



The following table describes the fields in this screen.

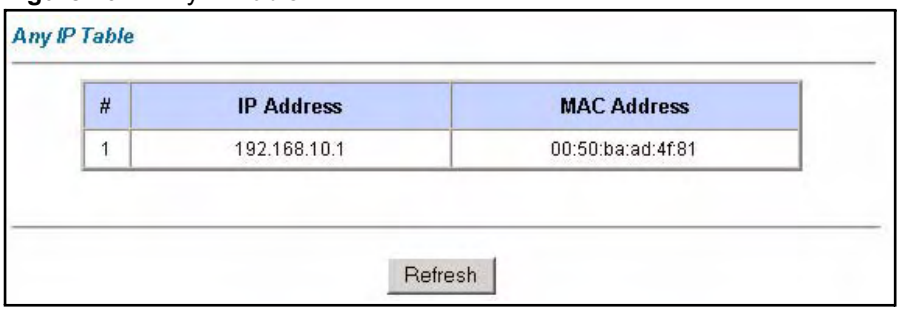
Table 64 DHCP Table

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.

17.4 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.

Figure 101 Any IP Table



The following table describes the labels in this screen.

Table 65 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.

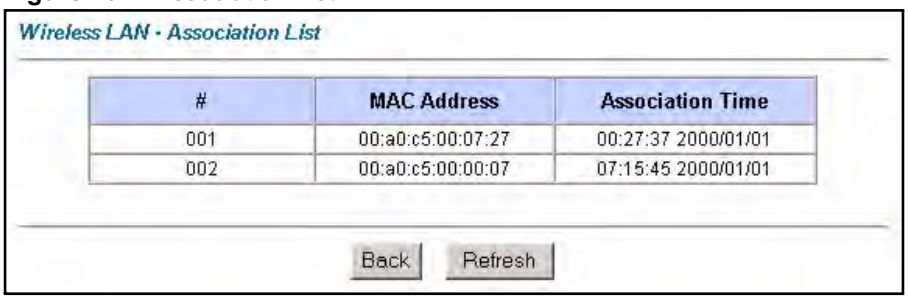
17.5 Wireless Screen

The read-only screen displays information about the Prestige's wireless LAN.

17.5.1 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 102 Association List



The following table describes the fields in this screen.

Table 66 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.

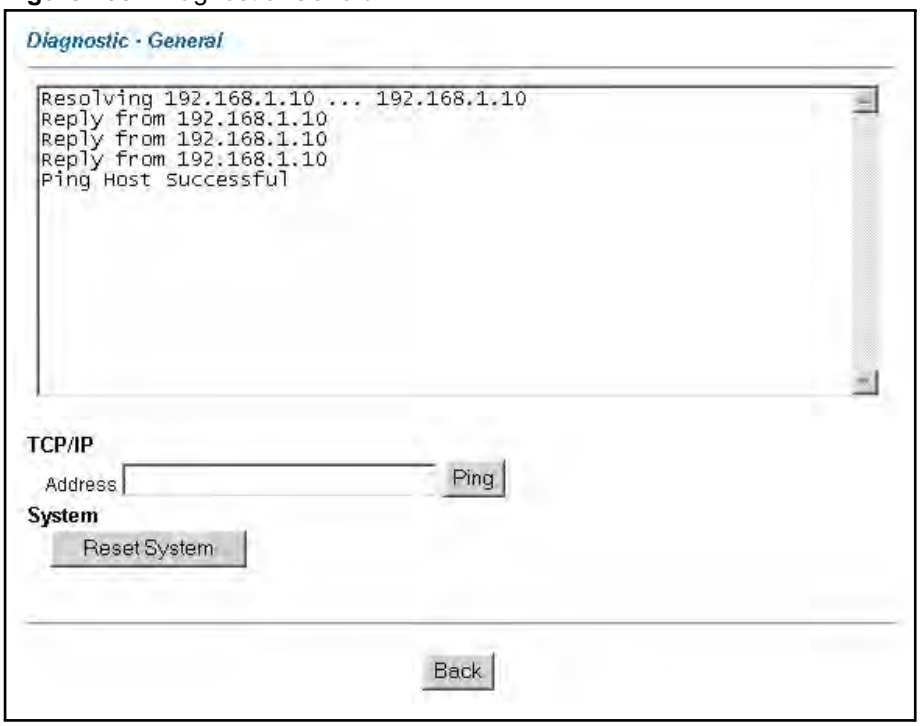
17.6 Diagnostic Screens

These read-only screens display information to help you identify problems with the Prestige.

17.6.1 General Diagnostic

Click **Diagnostic** and then **General** to open the screen shown next.

Figure 103 Diagnostic: General



The following table describes the fields in this screen.

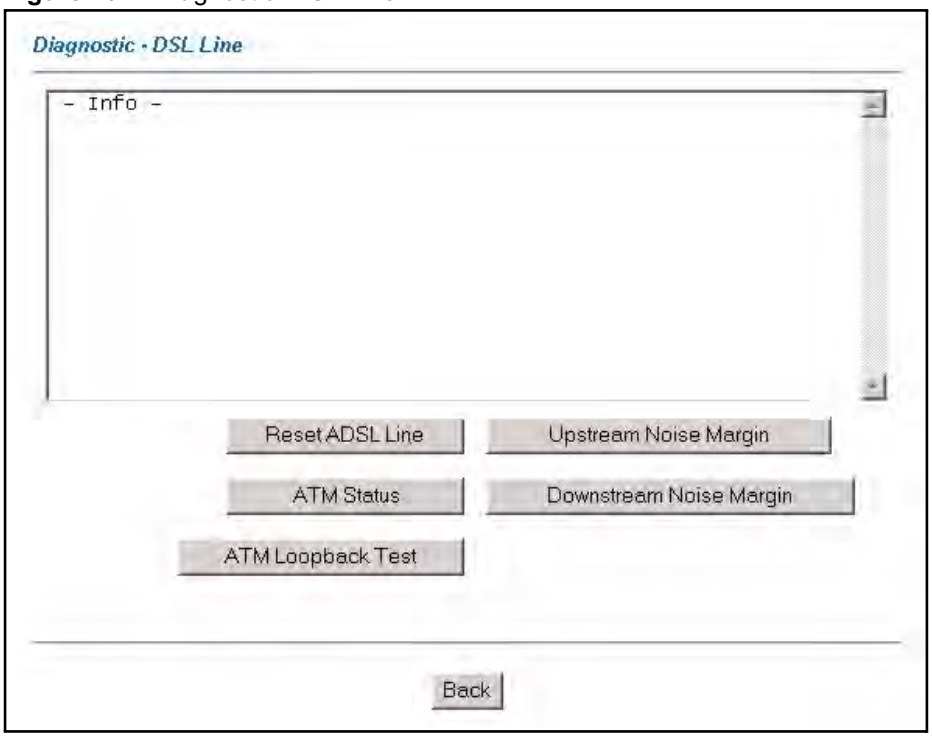
Table 67 Diagnostic: General

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.

17.6.2 DSL Line Diagnostic

Click **Diagnostic** and then **DSL Line** to open the screen shown next.

Figure 104 Diagnostic: DSL Line



The following table describes the fields in this screen.

Table 68 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.

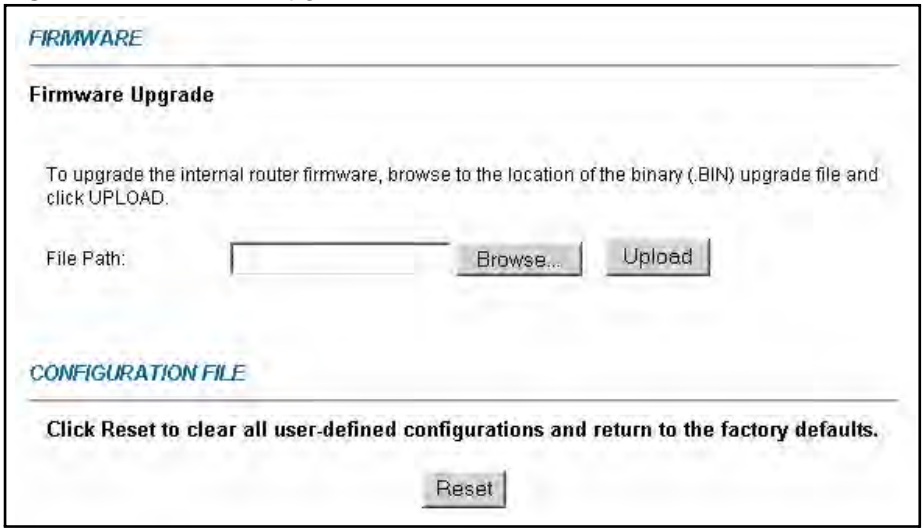
17.7 Firmware Upgrade

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a.bin extension, for example, "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 33 on page 306 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 105 Firmware Upgrade



The following table describes the labels in this screen.

Table 69 Firmware Upgrade

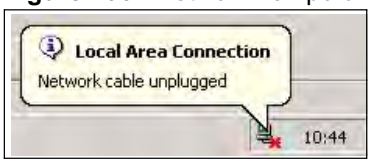
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **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.

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.

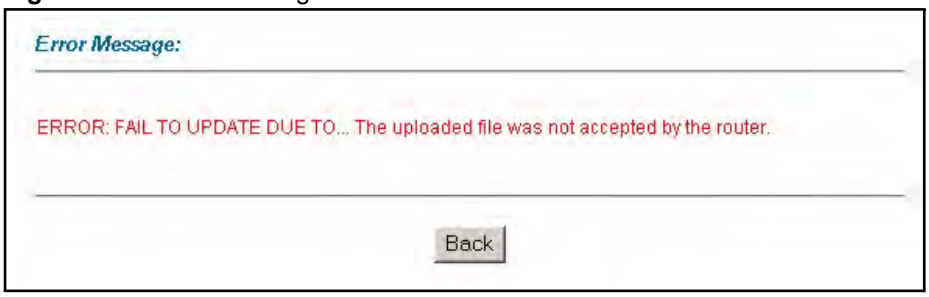
Figure 106 Network Temporarily Disconnected



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 107 Error Message



CHAPTER 18
Introducing the SMT

This chapter explains how to access and navigate the System Management Terminal and gives an overview of its menus.

18.1 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.

18.1.1 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.

18.1.2 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 108 Login Screen

18.1.3 Prestige SMT Menus Overview

The following table gives you an overview of your Prestige's various SMT menus.

Table 70 SMT Menus Overview

MENUS	SUB MENUS		
1 General Setup	1.1 Configure Dynamic DNS		
2 WAN Backup Setup			
3 LAN Setup	3.1 LAN Port Filter Setup		
	3.2 TCP/IP and DHCP Setup	3.2.1 IP Alias Setup	
	3.5 Wireless LAN Setup	3.5.1 WLAN MAC Address Filter	
4 Internet Access Setup			
11 Remote Node Setup	11.1 Remote Node Profile		
	11.3 Remote Node Network Layer Options		
	11.5 Remote Node Filter		
	11.6 Remote Node ATM Layer Options		
	11.8 Advance Setup Options (PPPoE passthrough)		
12 Static Routing Setup	12.1 Edit Static Route Setup	12.1.1 Edit IP Static Route	
	12.3 Bridge Static Route Setup	12.3.1 Edit Bridge Static Route	
14 Dial-in User Setup	14.1 Edit Dial-in User		
15 NAT Setup	15.1 Address Mapping Sets	15.1.x Address Mapping Rules	15.1.x.x Address Mapping Rule
	15.2 NAT Server Sets	15.2.x NAT Server Setup	
21 Filter and Firewall Rule Setup	21.1 Filter Setup	21.1 Filter Rules Summary	21.1.x.1 Generic Filter Rule
			21.1.x.1 TCP/IP Filter Rule
	21.2 Firewall Setup		
22 SNMP Configuration			
23 System Security	23.1 Change Password		
	23.2 RADIUS Server		
	23.4 IEEE 802.1X		

Table 70 SMT Menus Overview (continued)

MENUS	SUB MENUS		
24 System Maintenance	24.1 Status		
	24.2 System Information and Console Port Speed	24.2.1 Information	
		24.2.2 Change Console Port Speed	
	24.3 Log and Trace	24.3.1 View Error Log	
		24.3.2 UNIX Syslog	
	24.4 Diagnostic		
	24.5 Backup Configuration		
	24.6 Restore Configuration		
	24.7 Upload Firmware	24.7.1 Upload System Firmware	
		24.7.2 Upload System Configuration File	
	24.8 Command Interpreter Mode		
	24.9 Call Control	24.9.1 Budget Management	
	24.10 Time and Date Setting		
	24.11 Remote Management Control		
25 IP Routing Policy Setup	25.1 IP Routing Policy Setup	25.1.1 IP Routing Policy	
26 Schedule Setup	26.1 Schedule Set Setup		

18.2 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 71 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.

Table 71 Navigating the SMT Interface

OPERATION	KEY STROKE	DESCRIPTION
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 72 SMT Main Menu

```
                Copyright (c) 1994 - 2004 ZyXEL Communications Corp.

                          Prestige 660W-T1  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
    12. Static Routing Setup
    14. Dial-in User Setup                99. Exit
    15. NAT Setup




                        Enter Menu Selection Number:
```

18.2.1 System Management Terminal Interface Summary

Table 73 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.

Table 73 Main Menu Summary

#	MENU TITLE	DESCRIPTION
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.
99	Exit	Use this to exit from SMT and return to a blank screen.

18.3 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 109 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 19
Menu 1 General Setup

Menu 1 - General Setup contains administrative and system-related information.

19.1 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.

19.2 Procedure To Configure Menu 1

Enter 1 in the Main Menu to open **Menu 1 — General Setup** (shown next).

Figure 110 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 74 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.	

19.2.1 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 111 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 75 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 20
Menu 2 WAN Backup Setup

This chapter describes how to configure traffic redirect and dial-backup using menu 2 and 2.1.

20.1 Introduction to WAN Backup Setup

This chapter explains how to configure the Prestige for traffic redirect and dial backup connections.

20.2 Configuring Dial Backup in Menu 2

From the main menu, enter 2 to open menu 2.

Figure 112 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

          Press ENTER to Confirm or ESC to Cancel:
```

The following table describes the fields in this menu.

Table 76 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 76 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.
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.	

20.2.1 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 113 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 77 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 77 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.	

CHAPTER 21
Menu 3 LAN Setup

This chapter covers how to configure your wired Local Area Network (LAN) settings.

21.1 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 114 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:
```

21.1.1 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 115 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 29 on page 272 first, then return to this menu to define the filter sets.

21.2 Protocol Dependent Ethernet Setup

Depending on the protocols for your applications, you need to configure the respective Ethernet Setup, as outlined below.

- TCP/IP Ethernet setup
- Bridging Ethernet setup

21.3 TCP/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 116 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 78 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 79 TCP/IP Ethernet Setup

FIELD	DESCRIPTION
TCP/IP Setup	
IP Address	Enter the (LAN) 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 (refer to the appendices 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 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 22
Wireless LAN Setup

This chapter covers how to configure wireless LAN settings in SMT menu 3.5 for P-660HW and P-660W.

22.1 Wireless LAN Overview

Refer to the chapter on the wireless LAN screens for wireless LAN background information.

22.2 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 117 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 80 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 80 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.	

22.2.1 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 118 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 81 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 23
Internet Access

This chapter shows you how to configure the LAN and WAN of your Prestige for Internet access.

23.1 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.

23.2 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 and apply them on the Prestige LAN and/or WAN interfaces using menus 3.2 (LAN) and 11.3 (WAN).

23.3 IP Alias

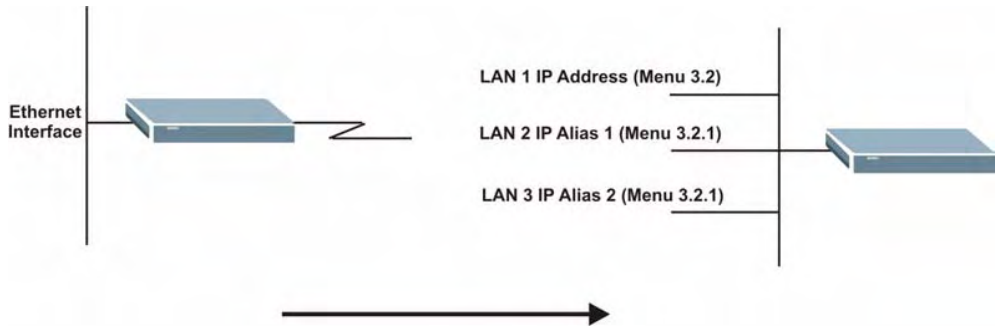
IP alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The Prestige supports three logical LAN interfaces via its single physical Ethernet interface with the Prestige itself as the gateway for each LAN network.

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 119 IP Alias Network Example



Use menu 3.2.1 to configure IP Alias on your Prestige.

23.4 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 120 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 121 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 82 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.	

23.5 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 122 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:
```

23.6 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 123 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 83 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 the NAT chapter 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.
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 24
Remote Node Configuration

This chapter covers remote node configuration.

24.1 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.

24.2 Remote Node Setup

This section describes the protocol-independent parameters for a remote node.

24.2.1 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 124 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:
```

24.2.2 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.

24.2.2.1 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.

24.2.2.2 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.

24.2.2.3 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 125 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 84 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 84 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 37 on page 338.
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 Chapter 29 on page 272 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.	

24.2.3 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.

24.3 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 126 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 85 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 (seeFigure 144 on page 257). Select **None** to disable NAT.

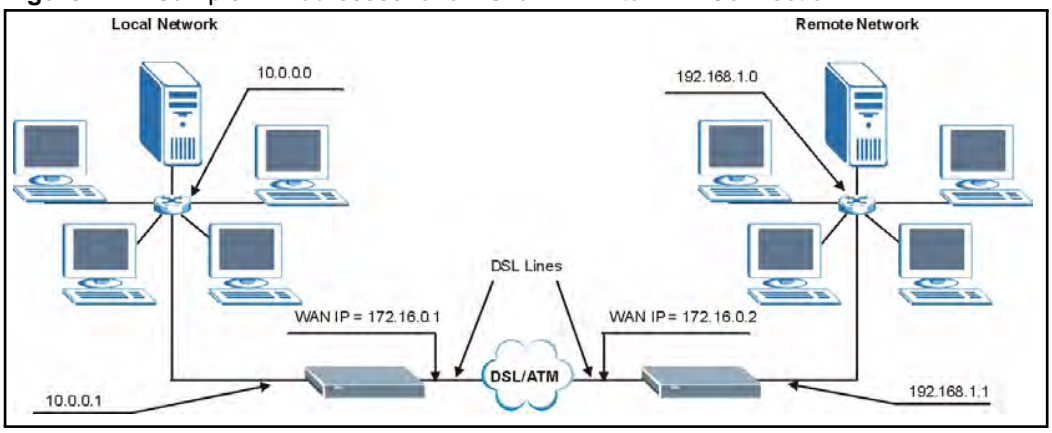
Table 85 Menu 11.3 Remote Node Network Layer Options (continued)

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 27 on page 254 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 27 on page 254 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 36 on page 328) 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.	

24.3.1 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. **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 127 Sample IP Addresses for a TCP/IP LAN-to-LAN Connection



24.4 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 128 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 129 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:
```

24.5 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.

24.5.1 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 130 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:
```

24.5.2 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 131 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 #= 0
                                  VCI #= 38
                                  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).

24.5.3 Advance Setup Options

In menu 11.1, select **PPPoE** in the **Encapsulation** field.

Figure 132 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 133 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 86 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 25
Static Route Setup

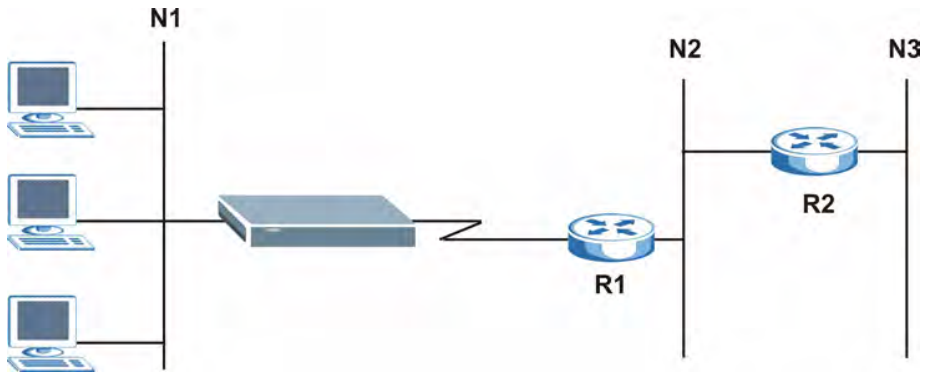
This chapter shows how to setup IP static routes.

25.1 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 134 Sample Static Routing Topology



25.2 Configuration

To configure an IP static route, use **Menu 12 – Static Route Setup** (shown next).

Figure 135 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 136 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 137 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 87 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.
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 26
Bridging Setup

This chapter shows you how to configure the bridging parameters of your Prestige.

26.1 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.

26.2 Bridge Ethernet Setup

Basically, all non-local packets are bridged to the WAN. Your Prestige does not support IPX.

26.2.1 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 138 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 139 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:
```

The following table describes the fields in this menu.

Table 88 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.

26.2.2 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 140 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 89 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 27
Network Address Translation (NAT)

This chapter discusses how to configure NAT on the Prestige.

27.1 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.

27.1.1 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 Section 27.3 on page 256 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.

27.2 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 141 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 142 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 90 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 (seeFigure 144 on page 257).
	Select **None** to disable NAT.
	When you select **SUA Only**, the SMT uses Address Mapping Set 255 (seeFigure 145 on page 257). Choose **SUA Only** if you have just one public WAN IP address for your Prestige.

27.3 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 web configurator NAT chapter for further information on these menus. To configure NAT, enter 15 from the main menu to bring up the following screen.

Figure 143 Menu 15 NAT Setup

```
              Menu 15 - NAT Setup

                    1. Address Mapping Sets

                    2. NAT Server Sets

              Enter Menu Selection Number:
```

27.3.1 Address Mapping Sets

Enter 1 to bring up **Menu 15.1 — Address Mapping Sets**.

Figure 144 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:
```

27.3.1.1 SUA Address Mapping Set

Enter 255 to display the next screen (see also Section 27.1.1 on page 254). The fields in this menu cannot be changed.

Figure 145 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 91 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).

Table 91 SUA Address Mapping Rules (continued)

FIELD	DESCRIPTION
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.
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.	

27.3.1.2 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 146 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.

27.3.1.3 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 92 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 147 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 93 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 web configurator NAT chapter. Server allows you to specify multiple servers of different types behind NAT to this computer.
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.	

27.4 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 148 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 149 Menu 15.2.1 NAT Server Setup

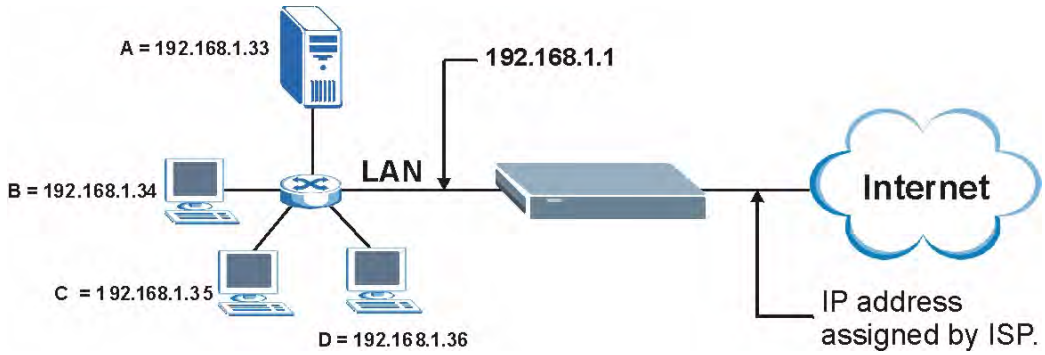
```
            Menu 15.2 - NAT Server Setup
 Rule    Start Port No.    End Port No.    IP Address
-------------------------------------------------------
   1.     Default           Default         0.0.0.0
   2.       21                21            192.168.1.33
   3.       0                 0             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 150 Multiple Servers Behind NAT Example



27.5 General NAT Examples

The following are some examples of NAT configuration.

27.5.1 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 151 NAT Example 1

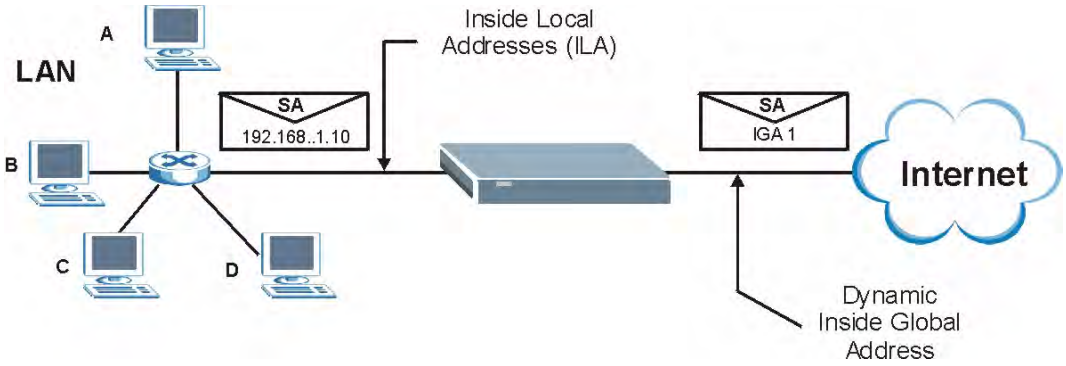


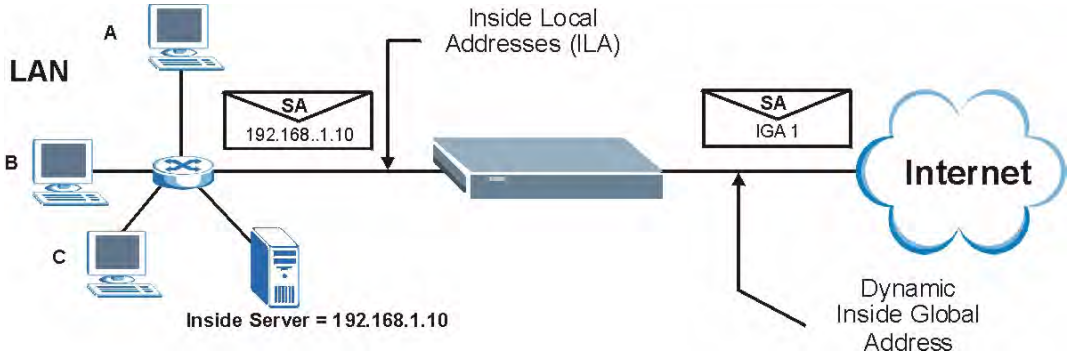
Figure 152 Menu 4 Internet Access & NAT Example

```
                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 Section 27.5 on page 261. 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.

27.5.2 Example 2: Internet Access with an Inside Server

Figure 153 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 154 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:
```

27.5.3 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).

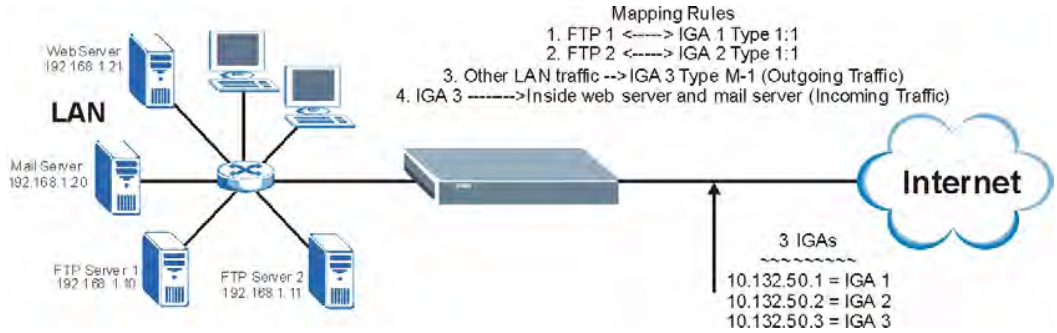
Map the second IGA to our second inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).

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 155 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) inFigure 156 on page 265.

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). (SeeFigure 157 on page 265).
5. Repeat the previous step for rules 2 to 4 as outlined above.

When finished, menu 15.1.1 should look like as shown inFigure 158 on page 266.

Figure 156 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 157 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 158 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.

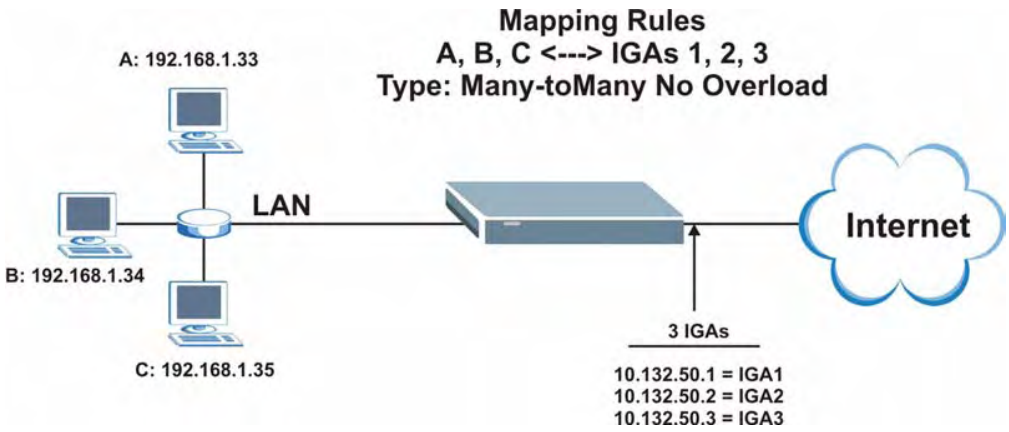
Figure 159 Example 3: Menu 15.2.1

```
              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:
```

27.5.4 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 160 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 161 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 162 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 28
Enabling the Firewall

This chapter shows you how to get started with the Prestige firewall.

28.1 Remote Management and the Firewall

When SMT menu 24.11 is configured to allow management 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.

28.2 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.

28.3 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 163 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 29
Filter Configuration

This chapter shows you how to create and apply filters.

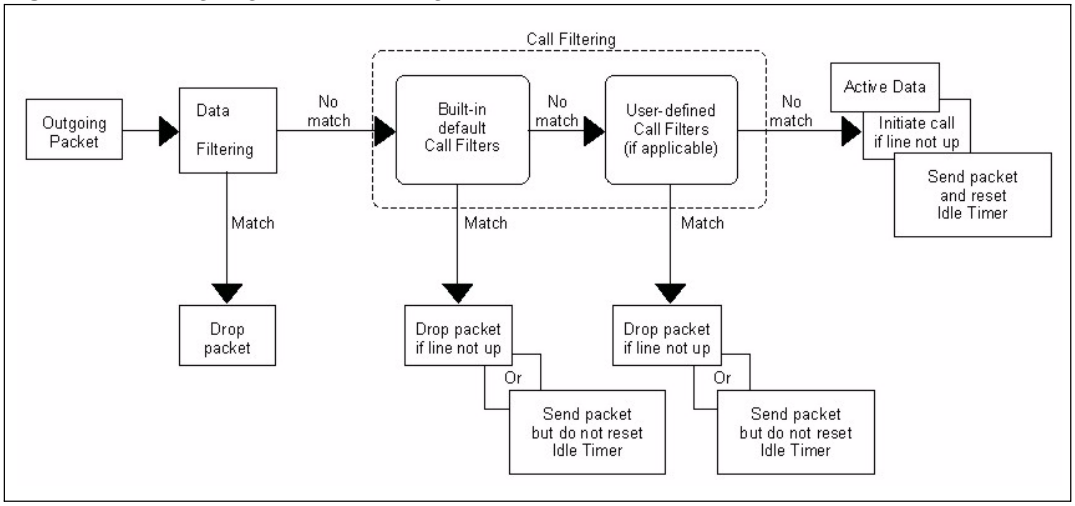
29.1 About Filtering

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.

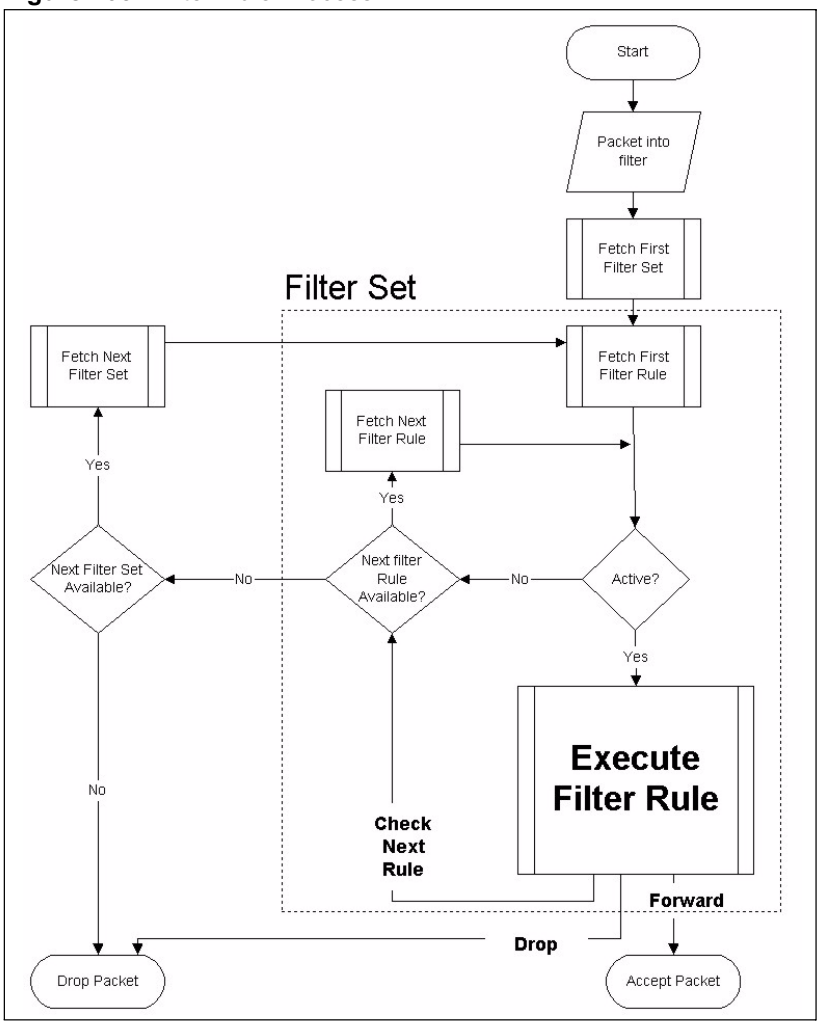
Figure 164 Outgoing Packet Filtering Process



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 165 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.

29.1.1 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.

29.2 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 166 Menu 21 Filter Set Configuration

```
             Menu 21.1 - Filter Set Configuration
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 167 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 168 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 169 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:
```

29.3 Filter Rules Summary Menus

The following tables briefly describe the abbreviations used in menus 21.1.1 and 21.1.2.

Table 94 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 94 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 95 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

29.4 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.

29.4.1 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 170 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 96 Menu 21.1.x.1 TCP/IP Filter Rule

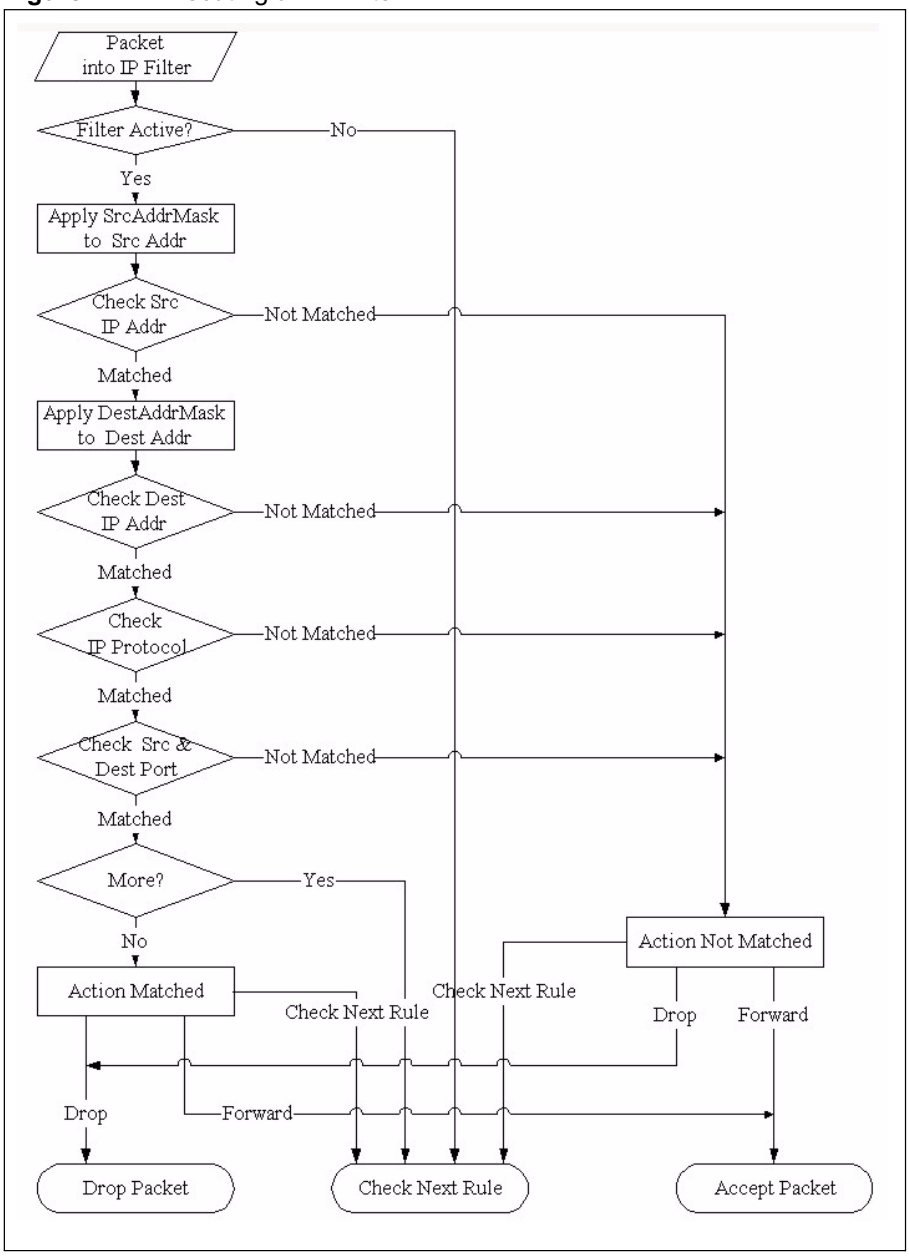
FIELD	DESCRIPTION
Filter #	This is the filter set, filter rule coordinates, for instance, 2, 3 refers to the second filter set and the third filter rule of that set.
Filter Type	Use [SPACE BAR] and then [ENTER] to choose a rule. Parameters displayed for each type will be different. Choices are **TCP/IP 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 96 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 171 Executing an IP Filter



29.4.2 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 172 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 97 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**.

Table 97 Menu 21.1.5.1 Generic Filter Rule (continued)

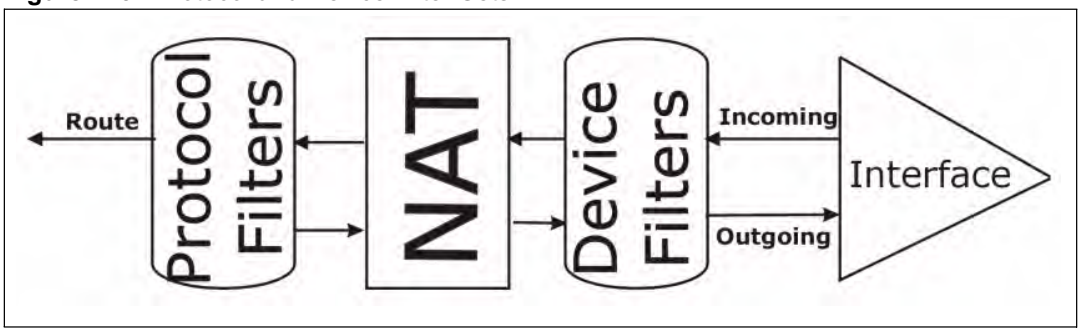
FIELD	DESCRIPTION
Log	Select the logging option from the following: **None** – No packets will be logged. **Action Matched** – Only matching packets and rules will be logged. **Action Not Matched** – Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.
Action Matched	Select the action for a matching packet. Choices are **Check Next Rule**, **Forward** or **Drop**.
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.	

29.5 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.

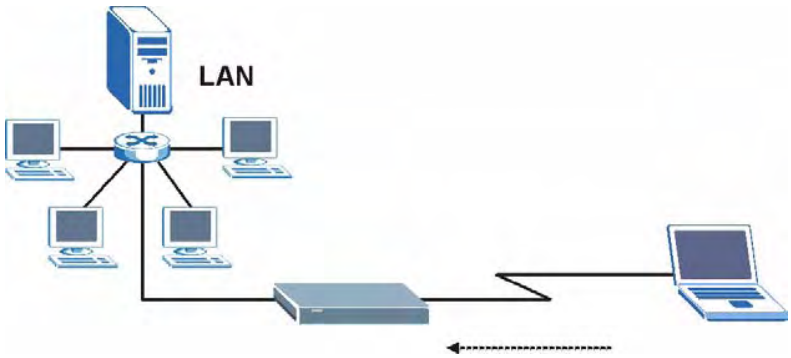
Figure 173 Protocol and Device Filter Sets



29.6 Example Filter

Let's look at an example to block outside users from telnetting into the Prestige.

Figure 174 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 175 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 176 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
```

29.7 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 98 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.

29.7.1 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 177 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:
```

29.7.2 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 178 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.

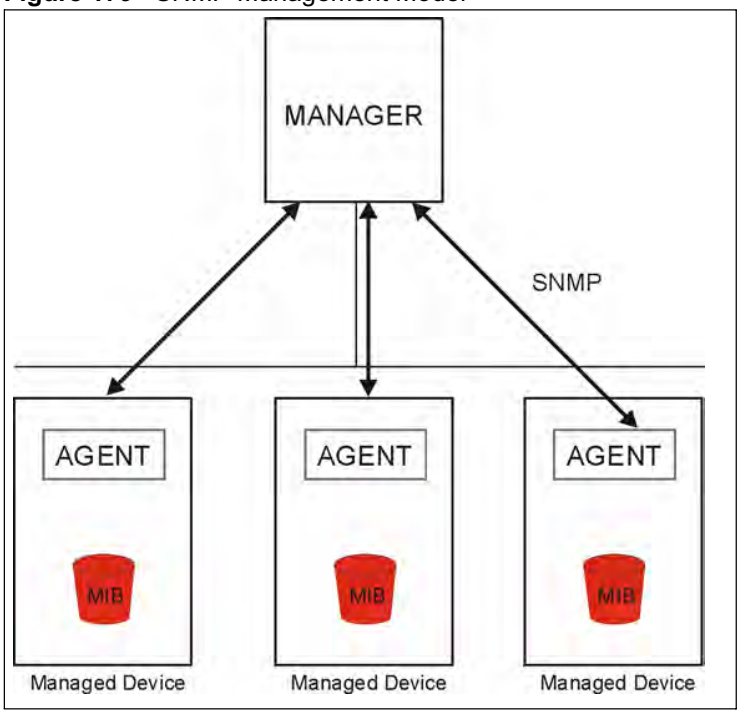
CHAPTER 30
SNMP Configuration

This chapter explains SNMP Configuration menu 22.

30.1 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 179 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.

30.2 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.

30.3 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 180 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 99 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.	

30.4 SNMP Traps

The Prestige will send traps to the SNMP manager when any one of the following events occurs:

Table 100 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 100 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 101 Ports and Permanent Virtual Circuits

PORT	PVC (PERMANENT VIRTUAL CIRCUIT)
1	Ethernet LAN
2	1
3	2
…	…
13	12
14	xDSL

CHAPTER 31
System Security

This chapter describes how to configure the system security on the Prestige.

31.1 System Security

You can configure the system password.

31.1.1 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.

Figure 181 Menu 23 – System Security

```
            Menu 23 - System Security

                  1. Change Password
                  2. RADIUS Server
                  4. IEEE802.1x

            Enter Menu Selection Number:
```

31.1.2 Configuring External RADIUS Server

From **Menu 23- System Security**, enter 2 to display **Menu 23.2 - System Security-RADIAS Server**.

Figure 182 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 102 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.	

31.1.3 IEEE 802.1x

The IEEE 802.1x 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 183 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 – IEEE 802.1x**.

Figure 184 Menu 23.4 System Security: IEEE 802.1x

```
Menu 23.4 - System Security - IEEE 802.1x

      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 103 Menu 23.4 System Security: IEEE 802.1x

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 103 Menu 23.4 System Security: IEEE 802.1x (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.

31.2 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 185 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 186 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 104 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 32
System Information and Diagnosis

This chapter covers the information and diagnostic tools in SMT menus 24.1 to 24.4.

32.1 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 187 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:
```

32.2 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 188 Menu 24.1 System Maintenance : Status

```
                  Menu 24.1 - System Maintenance - Status          23:08:47
                                                          Sat. Jan. 01, 2000

Node-Lnk Status      TxPkts      RxPkts      Errors  Tx B/s  Rx B/s     Up
Time
 1-ENET  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
 8       N/A             0           0           0       0       0     0:00:00

My WAN IP (from ISP): 0.0.0.0

    Ethernet:                                        WAN:
      Status: 100M/Full Duplex Tx Pkts: 5731          Line Status: Down
      Collisions: 0           Rx Pkts: 8314         Upstream Speed:     0 kbps
    CPU Load =   25.52%                           Downstream Speed:     0 kbps
                                  Press Command:
              COMMANDS: 1-Reset Counters  TAB-Next Page  ESC-Exit
```

The following table describes the fields present in **Menu 24.1 — System Maintenance — Status**.

Table 105 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.
Rx Pkts	This is the number of received packets from the LAN.

Table 105 Menu 24.1 System Maintenance: Status (continued)

FIELD	DESCRIPTION
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.

32.3 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 189 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:
```

32.3.1 System Information

Enter 1 in menu 24.2 to display the screen shown next.

Figure 190 Menu 24.2.1 System Maintenance: Information

```
              Menu 24.2.1 - System Maintenance - Information

            Name:
            Routing: IP
            ZyNOS F/W Version: V3.40(ACC.0)| 04/26/2005
            ADSL Chipset Vendor: DMT FwVer: 3.0.11.11_A_TC, HwVer: T14F+
            Standard: Multi-Mode

            LAN
              Ethernet Address: 00:13:49:11:11:35
              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 106 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.

32.3.2 Console Port Speed

Note: The console port is internal and reserved for technician use only.

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 191 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.

32.4 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.

32.4.1 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 192 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 193 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):
```

32.4.2 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 194 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 107 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 195 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 195 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
```

32.5 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 196 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 108 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 33
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.

33.1 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.

Note: 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 109 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

33.2 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.

33.2.1 Backup Configuration

Follow the instructions as shown in the next screen.

Figure 197 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:
```

33.2.2 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.

33.2.3 Example of FTP Commands from the Command Line

Figure 198 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
```

33.2.4 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 110 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).

33.2.5 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.

33.2.6 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.

33.2.7 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.

33.2.8 GUI-based TFTP Clients

The following table describes some of the fields that you may see in GUI-based TFTP clients.

Table 111 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 Section 33.2.5 on page 309 to read about configurations that disallow TFTP and FTP over WAN.

33.3 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.

33.3.1 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 199 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.

33.3.2 Restore Using FTP Session Example

Figure 200 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 Section 33.2.5 on page 309 to read about configurations that disallow TFTP and FTP over WAN.

33.4 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 Section 33.2 on page 307 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.

33.4.1 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 201 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:
```

33.4.2 Configuration File Upload

You see the following screen when you telnet into menu 24.7.2.

Figure 202 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

33.4.3 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.

33.4.4 FTP Session Example of Firmware File Upload

Figure 203 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 Section 33.2.5 on page 309 to read about configurations that disallow TFTP and FTP over WAN.

33.4.5 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.

33.4.6 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.

CHAPTER 34
System Maintenance

This chapter leads you through SMT menus 24.8 to 24.10.

34.1 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 204 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 205 Valid Commands

```
Copyright (c) 1994 - 2004 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys             exit            device          ether
wan             poe             config          pci
wlan            ip              ppp             bridge
hdap            bm              lan             radius
8021x
ras>
```

34.2 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 206 Menu 24.9 System Maintenance: Call Control

```
            Menu 24.9 - System Maintenance - Call Control

            1. Budget Management

            Enter Menu Selection Number:
```

34.2.1 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 207 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 112 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.	

34.3 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 208 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 209 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 113 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 113 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.	

34.3.1 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 35
Remote Management

This chapter covers remote management (SMT menu 24.11).

35.1 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.

35.2 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**.

35.2.1 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 210 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 114 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.	

35.2.2 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.

35.3 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.

35.4 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 36
IP Policy Routing

This chapter covers setting and applying policies used for IP routing.

36.1 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.

36.2 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.

36.3 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.

36.4 IP Routing Policy Setup

Menu 25 shows all the policies defined.

Figure 211 Menu 25 IP Routing Policy Setup

```
                Menu 25 - IP Routing Policy Setup

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 212 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 115 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 213 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 116 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 116 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.	

36.5 Applying an IP Policy

This section shows you where to apply the IP policies after you design them.

36.5.1 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 214 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 215 Menu 11.3 Remote Node Network Layer Options

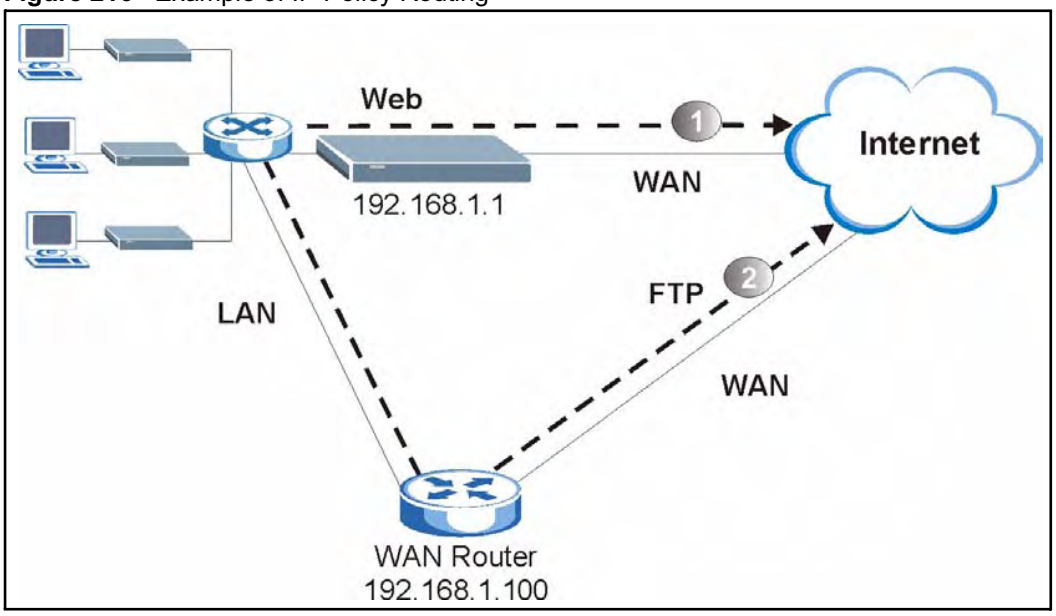
```
            Menu 11.3 - Remote Node Network Layer Options

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:
```

36.6 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 216 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 217 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 218 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 219 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 37
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.

37.1 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 220 Menu 26 Schedule Setup

```
            Menu 26 - Schedule Setup

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 221 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 117 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 117 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 222 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 38
Troubleshooting

This chapter covers potential problems and the corresponding remedies.

38.1 Problems Starting Up the Prestige

Table 118 Troubleshooting Starting Up 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. Make sure 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.

38.2 Problems with the LAN

Table 119 Troubleshooting the LAN

PROBLEM	CORRECTIVE ACTION
The LAN LEDs do not turn on.	Check your Ethernet cable connections (refer to the *Quick Start Guide* for details). Check for faulty Ethernet cables.
	Make sure your computer's Ethernet Card is working properly.
I cannot access the Prestige from the LAN.	If **Any IP** is disabled, make sure that the IP address and the subnet mask of the Prestige and your computer(s) are on the same subnet.

38.3 Problems with the WAN

Table 120 Troubleshooting the WAN

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 Table 68 on page 204 (web configurator) or Table 108 on page 304 (SMT).
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 SMT).
I cannot access the Internet.	Make sure the Prestige is turned on and connected to the network. 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 mode is turned on.
The Internet connection disconnects.	Check the schedule rules. Refer to Chapter 37 on page 338 (SMT). If you use PPPoA or PPPoE encapsulation, check the idle time-out setting. Refer to the Chapter 6 on page 90 (web configurator) or Chapter 24 on page 236 (SMT). Contact your ISP.

38.4 Problems Accessing the Prestige

Table 121 Troubleshooting Accessing the Prestige

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. This restores all of the factory defaults including the password.
I cannot access the web configurator.	Make sure that there is not an SMT console session running. Use the Prestige's WAN IP address when configuring from the WAN. Refer to the instructions on checking your WAN connection. Use the Prestige's LAN IP address when configuring from the LAN. Refer to for instructions on checking your LAN connection. 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. 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 the following section to check that pop-up windows, JavaScripts and Java permissions are allowed.

38.4.1 Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

38.4.1.1 Internet Explorer Pop-up Blockers

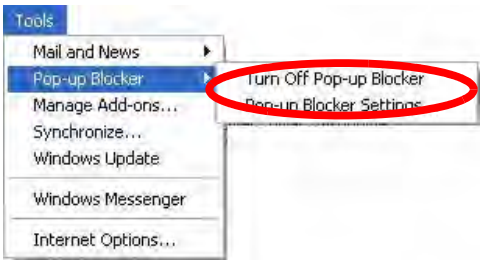
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

38.4.1.1.1 Disable pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 223 Pop-up Blocker

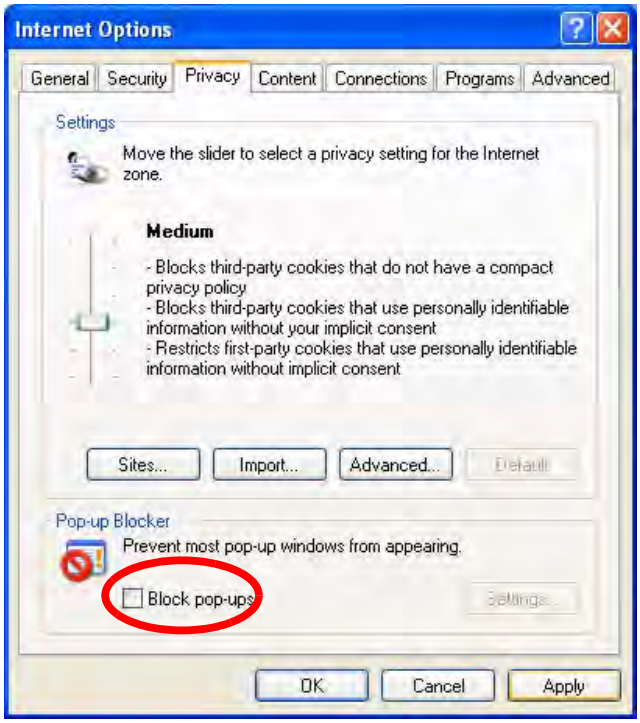


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 224 Internet Options



3 Click **Apply** to save this setting.

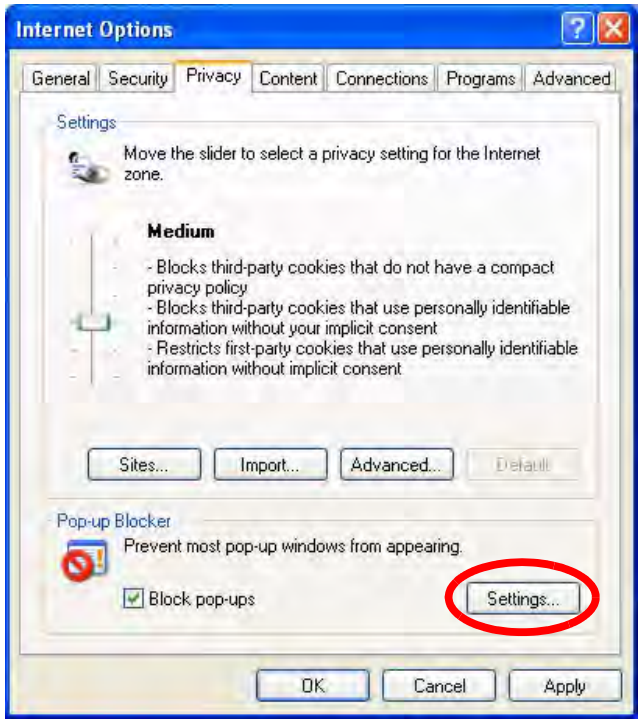
38.4.1.1.2 Enable pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings…**to open the **Pop-up Blocker Settings** screen.

Figure 225 Internet Options



3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.1.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 226 Pop-up Blocker Settings

5 Click **Close** to return to the **Privacy** screen.

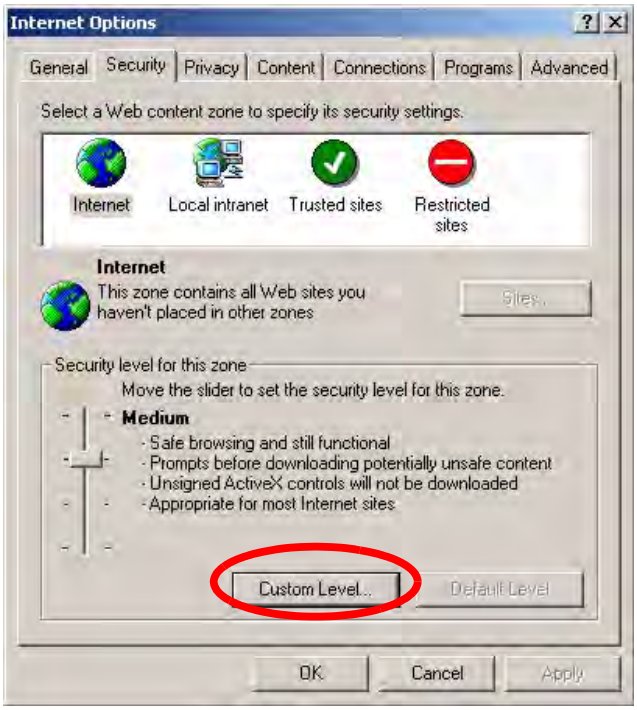
6 Click **Apply** to save this setting.

38.4.1.2 JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 227 Internet Options



2 Click the **Custom Level...** button.

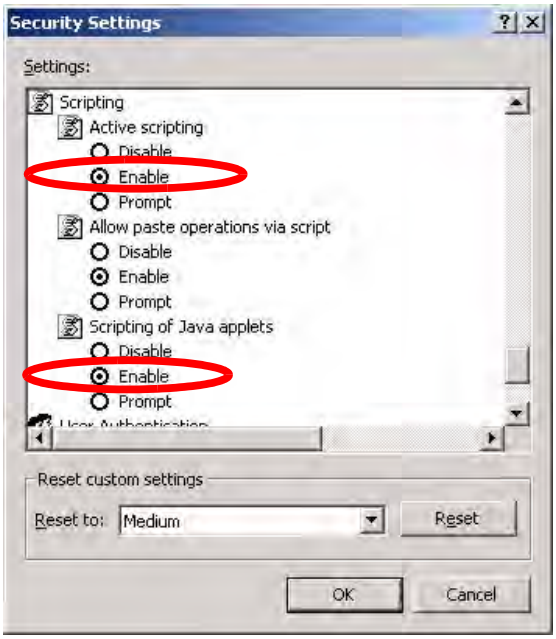
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

Figure 228 Security Settings - Java Scripting



38.4.1.3 Java Permissions

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

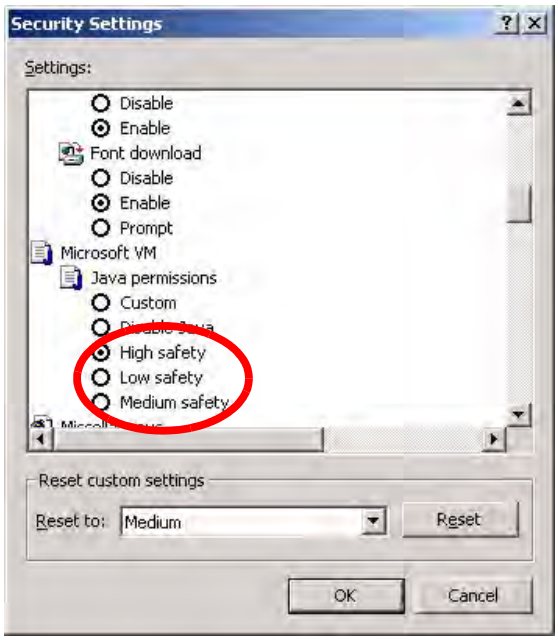
2 Click the **Custom Level...** button.

3 Scroll down to **Microsoft VM**.

4 Under **Java permissions** make sure that a safety level is selected.

5 Click **OK** to close the window.

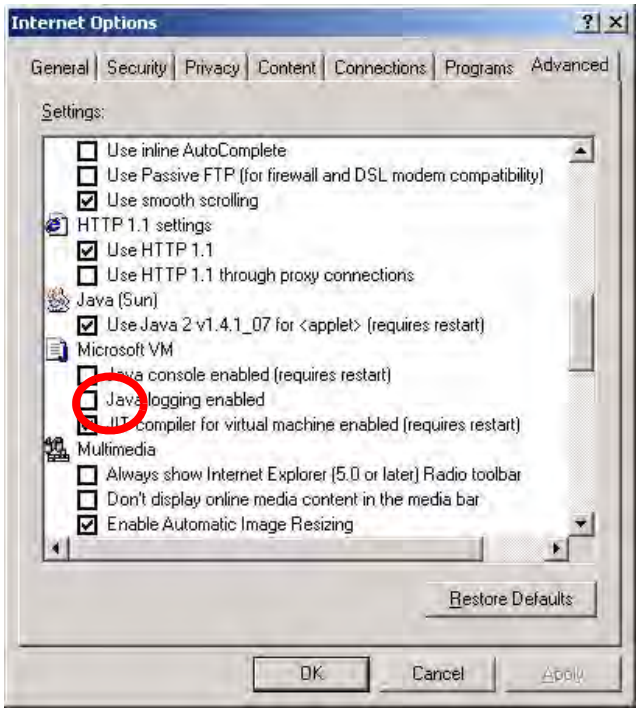
Figure 229 Security Settings - Java



38.4.1.3.1 JAVA (Sun)

1. From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.
2. make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.
3. Click **OK** to close the window.

Figure 230 Java (Sun)



38.4.2 ActiveX Controls in Internet Explorer

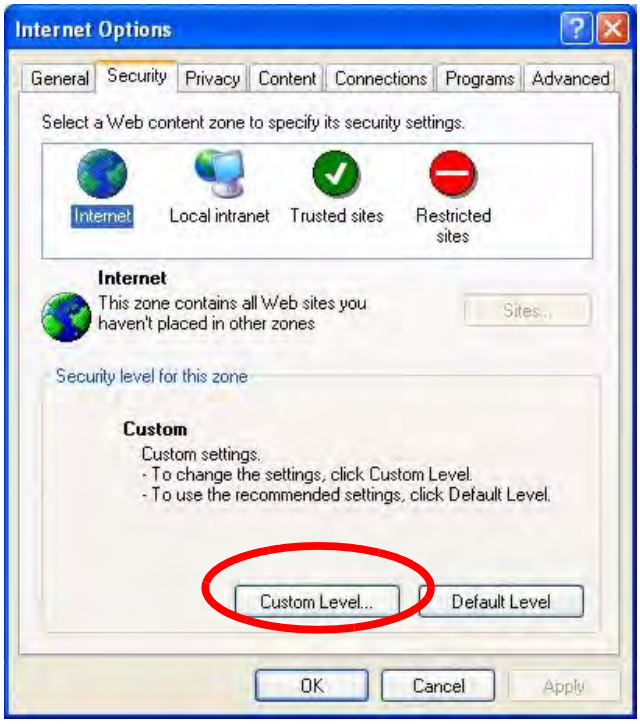
If ActiveX is disabled, you will not be able to download ActiveX controls or to use Trend Micro Security Services. Make sure that ActiveX controls are allowed in Internet Explorer.

Screen shots for Internet Explorer 6 are shown. Steps may vary depending on your version of Internet Explorer.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

2 In the **Internet Options** window, click **Custom Level**.

Figure 231 Internet Options Security



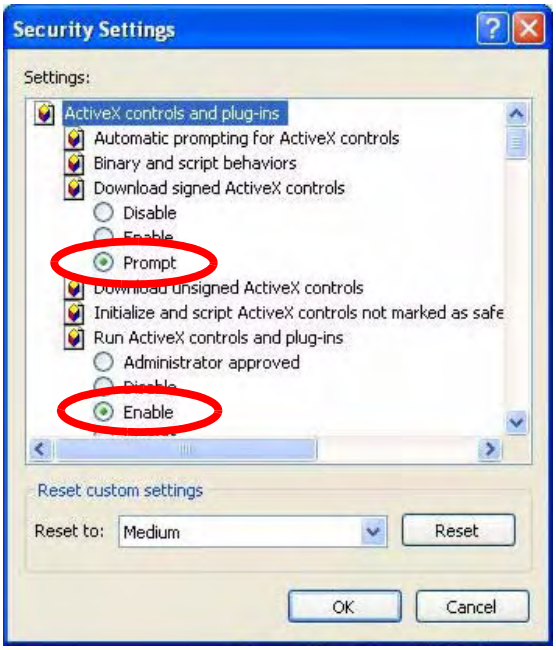
3 Scroll down to **ActiveX controls and plug-ins**.

4 Under **Download signed ActiveX controls** select the **Prompt** radio button.

5 Under **Run ActiveX controls and plug-ins** make sure the **Enable** radio button is selected.

6 Then click the **OK** button.

Figure 232 Security Setting ActiveX Controls



Appendix A Product Specifications

See also the Introduction chapter for a general overview of the key features.

Specification Tables

Table 122 Device

Default IP Address	192.168.1.1
Default Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234
DHCP Pool	192.168.1.32 to 192.168.1.64
Dimensions (W x D x H)	180 x 128 x 36 mm
Power Specification	12VDC 1A
Built-in Switch (P-660H/ P-660HW)	Four auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet ports
Operation Temperature	0º C ~ 40º C
Storage Temperature	-20º ~ 60º C
Operation Humidity	20% ~ 85% RH
Storage Humidity	10% ~ 90% RH

Table 123 Firmware

ADSL Standards	Multi-Mode standard (ANSI T1.413,Issue 2; G.dmt(G.992.1); G.lite(G992.2)). ADSL2 G.dmt.bis (G.992.3) ADSL2 G.lite.bis (G.992.4) ADSL2+ (G.992.5) Reach-Extended ADSL (RE ADSL) SRA (Seamless Rate Adaptation) Auto-negotiating rate adaptation ADSL physical connection ATM AAL5 (ATM Adaptation Layer type 5) Multi-protocol over AAL5 (RFC2684/1483) PPP over ATM AAL5 (RFC 2364) PPP over Ethernet (RFC 2516) RFC 1483 encapsulation over ATM MAC encapsulated routing (ENET encapsulation) VC-based and LLC-based multiplexing Up to 8 PVCs (Permanent Virtual Circuits) I.610 F4/F5 OAM
Other Protocol Support	PPP (Point-to-Point Protocol) link layer protocol. Transparent bridging for unsupported network layer protocols. DHCP Server/Client/Relay RIP I/RIP II ICMP ATM QoS SNMP v1 and v2c with MIB II support (RFC 1213) IP Multicasting IGMP v1 and v2 IGMP Proxy UPnP
Management	Embedded Web Configurator Menu-driven SMT (System Management Terminal) management CLI (Command Line Interpreter) Remote Management via Telnet or Web SNMP manageable FTP/TFTP for firmware downloading, configuration backup and restoration. Syslog Built-in Diagnostic Tools for FLASH memory, ADSL circuitry, RAM and LAN port MAP - "Multimedia Auto Provisioner" (multimedia installation tutorial and automatic configurator) (P-660HW)
Wireless (P-660HW/ P-660W)	IEEE 802.11g compliance Frequency Range: 2.4 GHz Advanced Orthogonal Frequency Division Multiplexing (OFDM) Data Rates: 54Mbps and Auto Fallback Wired Equivalent Privacy (WEP) Data Encryption 64/128/256 bit WLAN bridge to LAN Up to 32 MAC address filters WPA(2), WPA(2)-PSK IEEE 802.1x Store up to 32 built-in user profiles using EAP-MD5 (Local User Database) External RADIUS server using EAP-MD5, TLS, TTLS

Table 123 Firmware (continued)

Firewall	Stateful Packet Inspection. Prevent Denial of Service attacks such as Ping of Death, SYN Flood, LAND, Smurf etc. Real time E-mail alerts. Reports and logs.
NAT/SUA	Port Forwarding 1024 NAT sessions Multimedia application PPTP under NAT/SUA IPSec passthrough SIP ALG passthrough VPN passthrough
Content Filtering	Web page blocking by URL keyword.
Static Routes	16 IP and 4 Bridge
Other Features	Any IP Zero Configuration (VC auto-hunting) Traffic Redirect Dynamic DNS IP Alias IP Policy Routing MBM (Multimedia Bandwidth Management) QoS (Quality of Service)

APPENDIX B
Wall-mounting Instructions

Do the following to hang your Prestige on a wall.

Note: See the product specifications appendix for the size of screws to use and how far apart to place them.

1. Locate a high position on wall that is free of obstructions. Use a sturdy wall.
2. Drill two holes for the screws. Make sure the distance between the centers of the holes matches what is listed in the product specifications appendix.

Note: Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.

3. Do not screw the screws all the way into the wall. Leave a small gap of about 0.5 cm between the heads of the screws and the wall.
4. Make sure the screws are snugly fastened to the wall. They need to hold the weight of the Prestige with the connection cables.
5. Align the holes on the back of the Prestige with the screws on the wall. Hang the Prestige on the screws.

Appendix C
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.

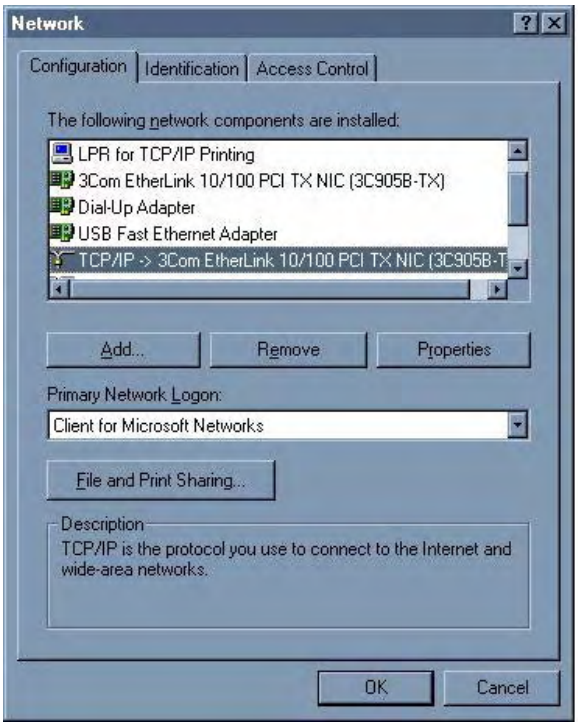
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

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 233 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.

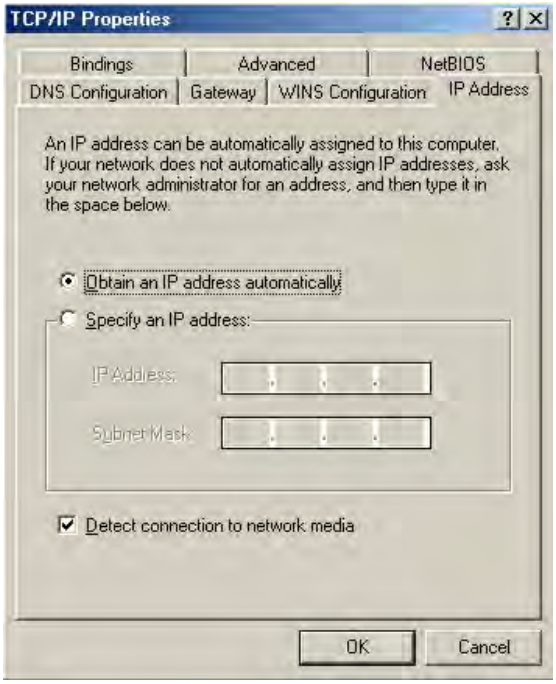
Configuring

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.

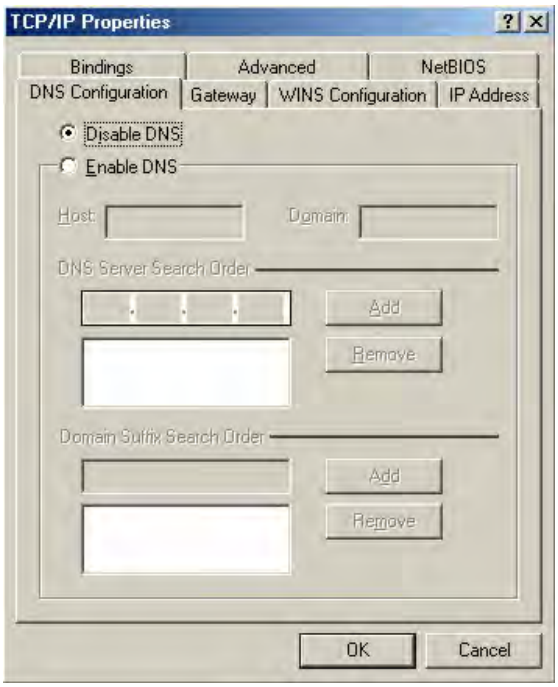
Figure 234 Windows 95/98/Me: TCP/IP Properties: IP Address



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 235 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.

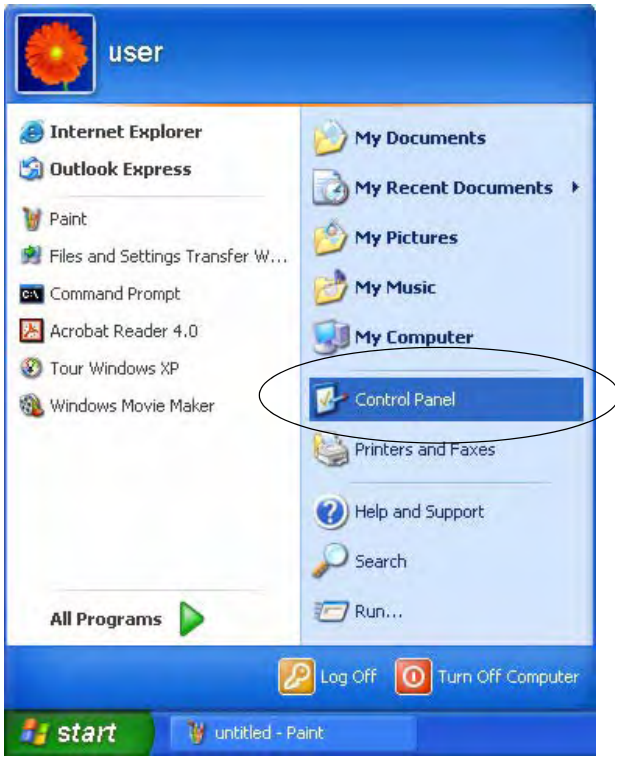
3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

1 Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

Figure 236 Windows XP: Start Menu

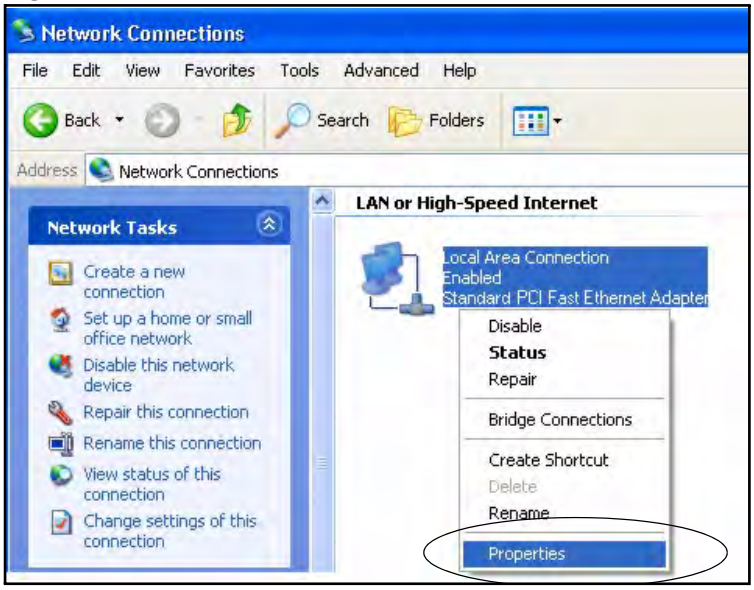


2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

Figure 237 Windows XP: Control Panel

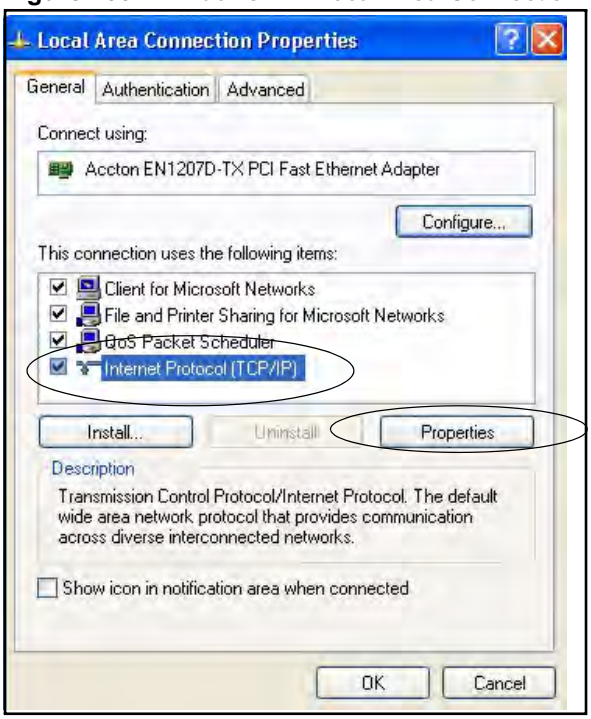
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 238 Windows XP: Control Panel: Network Connections: Properties



4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

Figure 239 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**.

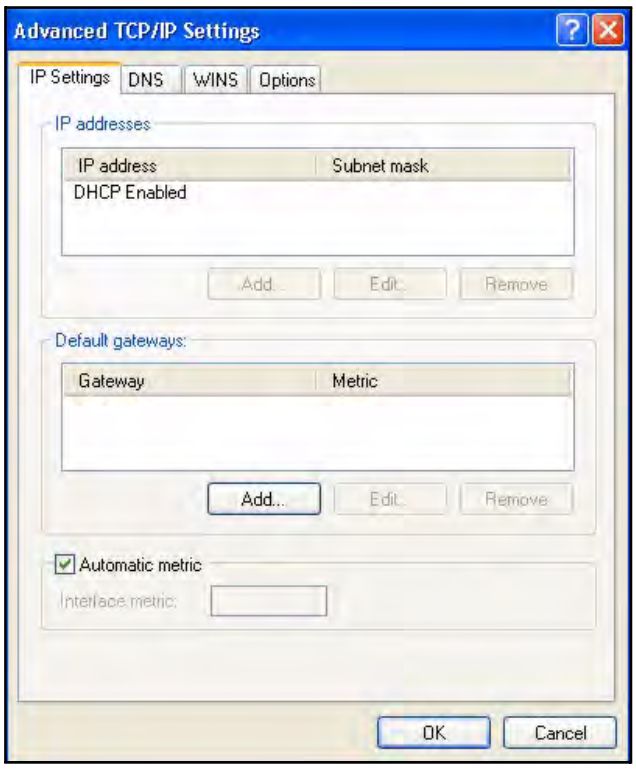
Figure 240 Windows XP: Internet Protocol (TCP/IP) Properties

6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** 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.

Figure 241 Windows XP: Advanced TCP/IP Properties



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 242 Windows XP: Internet Protocol (TCP/IP) Properties

8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **Close** (**OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.

10 Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).

11 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.

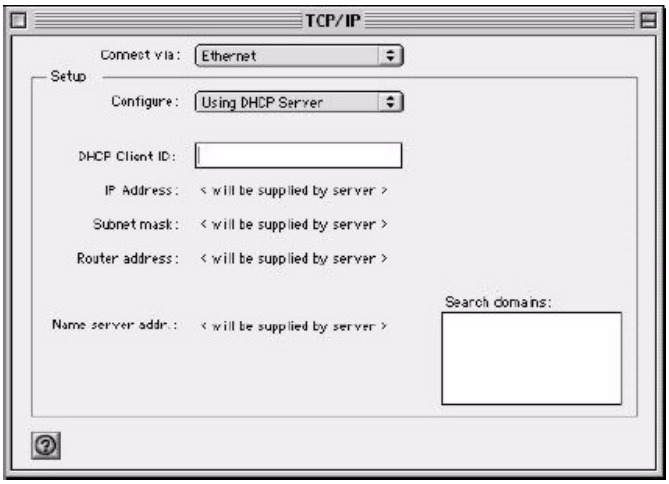
Macintosh OS 8/9

1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 243 Macintosh OS 8/9: Apple Menu

2 Select **Ethernet built-in** from the **Connect via** list.

Figure 244 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).

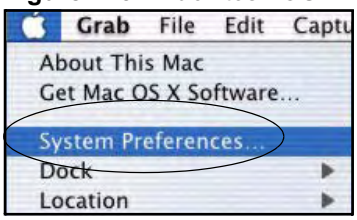
Verifying Settings

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 245 Macintosh OS X: Apple Menu

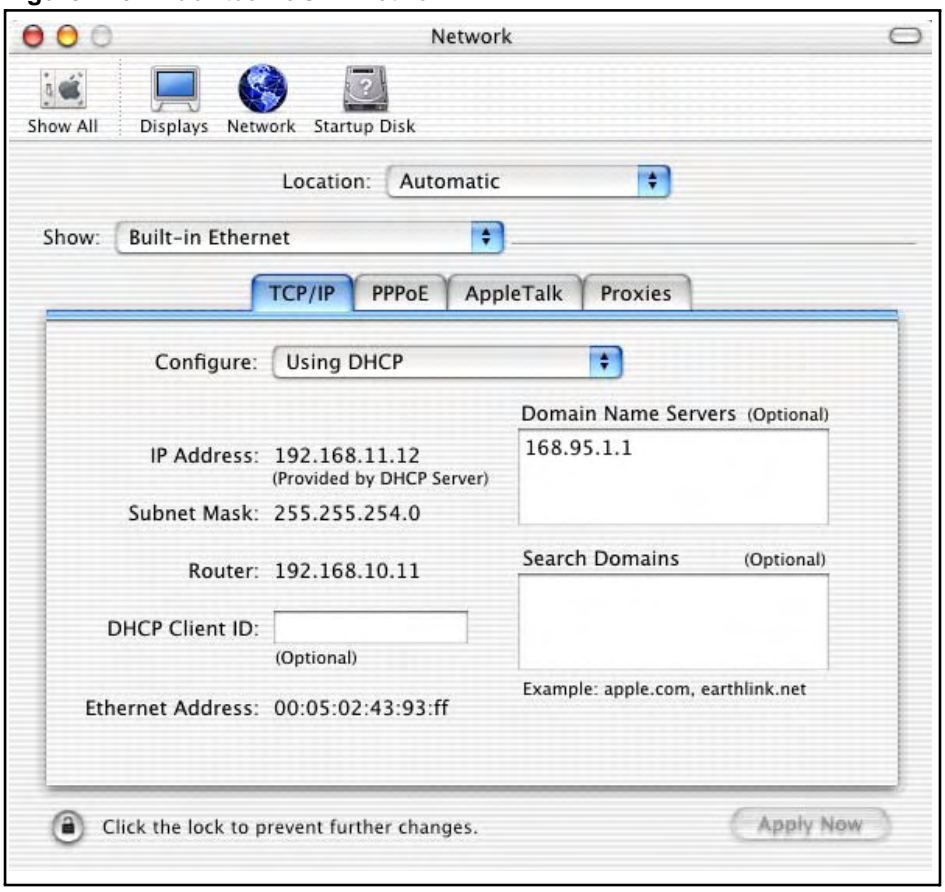


2 Click **Network** in the icon bar.

- 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 246 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.

Linux

This section shows you how to configure your computer's TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.

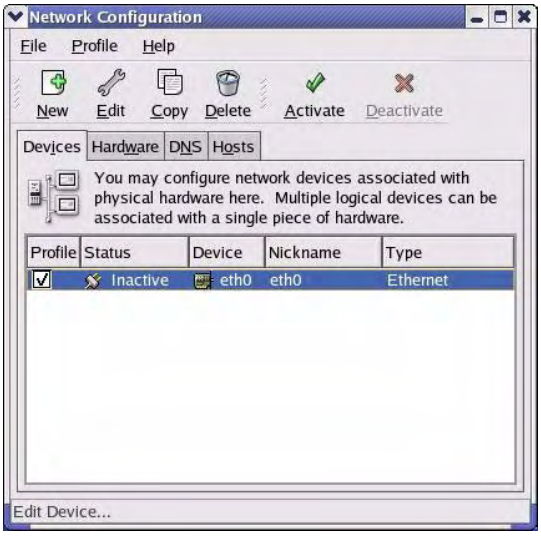
Note: Make sure you are logged in as the root administrator.

Using the K Desktop Environment (KDE)

Follow the steps below to configure your computer IP address using the KDE.

1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

Figure 247 Red Hat 9.0: KDE: Network Configuration: Devices



2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

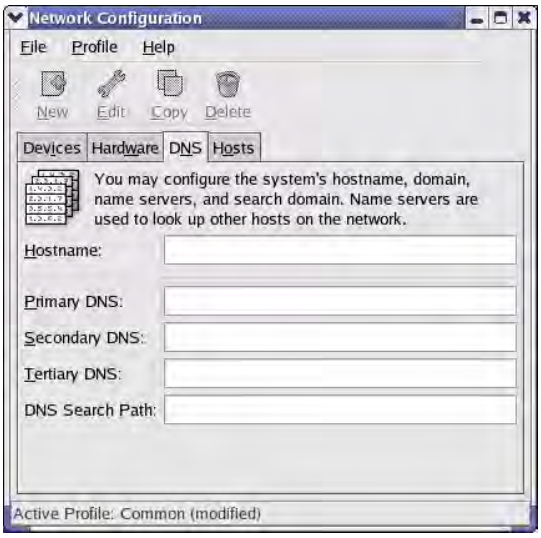
Figure 248 Red Hat 9.0: KDE: Ethernet Device: General

- If you have a dynamic IP address click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
- If you have a static IP address click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.

3 Click **OK** to save the changes and close the **Ethernet Device General** screen.

4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

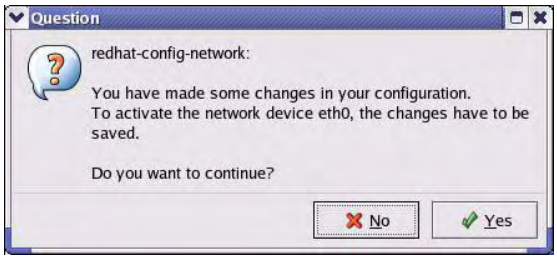
Figure 249 Red Hat 9.0: KDE: Network Configuration: DNS



5 Click the **Devices** tab.

6 Click the **Activate** button to apply the changes. The following screen displays. Click **Yes** to save the changes in all screens.

Figure 250 Red Hat 9.0: KDE: Network Configuration: Activate



7 After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

Using Configuration Files

Follow the steps below to edit the network configuration files and set your computer IP address.

1 Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.

- If you have a dynamic IP address, enter **`dhcp`** in the `BOOTPROTO=` field. The following figure shows an example.

Figure 251 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- If you have a static IP address, enter **`static`** in the `BOOTPROTO=` field. Type `IPADDR=` followed by the IP address (in dotted decimal notation) and type `NETMASK=` followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

Figure 252 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

2 If you know your DNS server IP address(es), enter the DNS server information in the `resolv.conf` file in the `/etc` directory. The following figure shows an example where two DNS server IP addresses are specified.

Figure 253 Red Hat 9.0: DNS Settings in resolv.conf

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

3 After you edit and save the configuration files, you must restart the network card. Enter `./network restart` in the `/etc/rc.d/init.d` directory. The following figure shows an example.

Figure 254 Red Hat 9.0: Restart Ethernet Card

```
[root@localhost init.d]# network restart

Shutting down interface eth0:                [OK]
Shutting down loopback interface:            [OK]
Setting network parameters:                  [OK]
Bringing up loopback interface:              [OK]
Bringing up interface eth0:                  [OK]
```

Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

Figure 255 Red Hat 9.0: Checking TCP/IP Properties

```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129  Bcast:172.23.19.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb)  TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```

Appendix D
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 124 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 125 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 126 "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 127 Alternative Subnet Mask Notation

SUBNET MASK	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 128 Two Subnets Example

IP/SUBNET MASK	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/bolded 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 129 Subnet 1

IP/SUBNET MASK	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 130 Subnet 2

IP/SUBNET MASK	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 131 Subnet 1

IP/SUBNET MASK	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 132 Subnet 2

IP/SUBNET MASK	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 133 Subnet 3

IP/SUBNET MASK	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 134 Subnet 4

IP/SUBNET MASK	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 135 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	225	254	255

The following table is a summary for class "C" subnet planning.

Table 136 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 124 on page 376) available for subnetting.

The following table is a summary for class "B" subnet planning.

Table 137 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 E
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 256 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 257 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 F
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 G Firewall Commands

The following describes the firewall commands.

Table 138 Firewall Commands

FUNCTION	COMMAND	DESCRIPTION
Firewall SetUp		
	`config edit firewall active <yes | no>`	This command turns the firewall on or off.
	`config retrieve firewall`	This command returns the previously saved firewall settings.
	`config save firewall`	This command saves the current firewall settings.
Display		
	`config display firewall`	This command shows the of all the firewall settings including e-mail, attack, and the sets/ rules.
	`config display firewall set <set #>`	This command shows the current configuration of a set; including timeout values, name, default-permit, and etc.If you don't put use a number (#) after "set", information about all of the sets/rules appears.
	`config display firewall set <set #> rule <rule #>`	This command shows the current entries of a rule in a firewall rule set.
	`config display firewall attack`	This command shows all of the attack response settings.
	`config display firewall e-mail`	This command shows all of the e-mail settings.
	`config display firewall?`	This command shows all of the available firewall sub commands.
Edit		
E-mail	`config edit firewall e-mail mail-server <ip address of mail server>`	This command sets the IP address to which the e-mail messages are sent.

Table 138 Firewall Commands (continued)

FUNCTION	COMMAND	DESCRIPTION
	`config edit firewall e-mail return-addr <e-mail address>`	This command sets the source e-mail address of the firewall e-mails.
	`config edit firewall e-mail email-to <e-mail address>`	This command sets the e-mail address to which the firewall e-mails are sent.
	`config edit firewall e-mail policy <full | hourly | daily | weekly>`	This command sets how frequently the firewall log is sent via e-mail.
	`config edit firewall e-mail day <sunday | monday | tuesday | wednesday | thursday | friday | saturday>`	This command sets the day on which the current firewall log is sent through e-mail if the Prestige is set to send it on a weekly basis.
	`config edit firewall e-mail hour <0-23>`	This command sets the hour when the firewall log is sent through e- mail if the Prestige is set to send it on an hourly, daily or weekly basis.
	`config edit firewall e-mail minute <0-59>`	This command sets the minute of the hour for the firewall log to be sent via e- mail if the Prestige is set to send it on a hourly, daily or weekly basis.
Attack	`config edit firewall attack send-alert <yes | no>`	This command enables or disables the immediate sending of DOS attack notification e-mail messages.
	`config edit firewall attack block <yes | no>`	Set this command to yes to block new traffic after the tcp-max-incomplete threshold is exceeded. Set it to no to delete the oldest half-open session when traffic exceeds the tcp-max-incomplete threshold.
	`config edit firewall attack block-minute <0-255>`	This command sets the number of minutes for new sessions to be blocked when the tcp-max-incomplete threshold is reached. This command is only valid when block is set to yes.
	`config edit firewall attack minute-high <0-255>`	This command sets the threshold rate of new half-open sessions per minute where the Prestige starts deleting old half-opened sessions until it gets them down to the minute-low threshold.

Table 138 Firewall Commands (continued)

FUNCTION	COMMAND	DESCRIPTION
	`config edit firewall attack minute-low <0-255>`	This command sets the threshold of half-open sessions where the Prestige stops deleting half-opened sessions.
	`config edit firewall attack max-incomplete-high <0-255>`	This command sets the threshold of half-open sessions where the Prestige starts deleting old half-opened sessions until it gets them down to the max incomplete low.
	`config edit firewall attack max-incomplete-low <0-255>`	This command sets the threshold where the Prestige stops deleting half-opened sessions.
	`config edit firewall attack tcp-max-incomplete <0-255>`	This command sets the threshold of half-open TCP sessions with the same destination where the Prestige starts dropping half-open sessions to that destination.
Sets	`config edit firewall set <set #> name <desired name>`	This command sets a name to identify a specified set.
	`Config edit firewall set <set #> default-permit <forward | block>`	This command sets whether a packet is dropped or allowed through, when it does not meet a rule within the set.
	`Config edit firewall set <set #> icmp-timeout <seconds>`	This command sets the time period to allow an ICMP session to wait for the ICMP response.
	`Config edit firewall set <set #> udp-idle-timeout <seconds>`	This command sets how long a UDP connection is allowed to remain inactive before the Prestige considers the connection closed.
	`Config edit firewall set <set #> connection-timeout <seconds>`	This command sets how long Prestige waits for a TCP session to be established before dropping the session.
	`Config edit firewall set <set #> fin-wait-timeout <seconds>`	This command sets how long the Prestige leaves a TCP session open after the firewall detects a FIN-exchange (indicating the end of the TCP session).
	`Config edit firewall set <set #> tcp-idle-timeout <seconds>`	This command sets how long Prestige lets an inactive TCP connection remain open before considering it closed.

Table 138 Firewall Commands (continued)

FUNCTION	COMMAND	DESCRIPTION
	`Config edit firewall set <set #> log <yes | no>`	This command sets whether or not the Prestige creates logs for packets that match the firewall's default rule set.
Rules	`Config edit firewall set <set #> rule <rule #> permit <forward | block>`	This command sets whether packets that match this rule are dropped or allowed through.
	`Config edit firewall set <set #> rule <rule #> active <yes | no>`	This command sets whether a rule is enabled or not.
	`Config edit firewall set <set #> rule <rule #> protocol <integer protocol value >`	This command sets the protocol specification number made in this rule for ICMP.
	`Config edit firewall set <set #> rule <rule #> log <none | match | not-match | both>`	This command sets the Prestige to log traffic that matches the rule, doesn't match, both or neither.
	`Config edit firewall set <set #> rule <rule #> alert <yes | no>`	This command sets whether or not the Prestige sends an alert e-mail when a DOS attack or a violation of a particular rule occurs.
	`config edit firewall set <set #> rule <rule #> srcaddr-single <ip address>`	This command sets the rule to have the Prestige check for traffic with this individual source address.
	`config edit firewall set <set #> rule <rule #> srcaddr-subnet <ip address> <subnet mask>`	This command sets a rule to have the Prestige check for traffic from a particular subnet (defined by IP address and subnet mask).
	`config edit firewall set <set #> rule <rule #> srcaddr-range <start ip address> <end ip address>`	This command sets a rule to have the Prestige check for traffic from this range of addresses.
	`config edit firewall set <set #> rule <rule #> destaddr-single <ip address>`	This command sets the rule to have the Prestige check for traffic with this individual destination address.
	`config edit firewall set <set #> rule <rule #> destaddr-subnet <ip address> <subnet mask>`	This command sets a rule to have the Prestige check for traffic with a particular subnet destination (defined by IP address and subnet mask).

Table 138 Firewall Commands (continued)

FUNCTION	COMMAND	DESCRIPTION
	config edit firewall set <set #> rule <rule #> destaddr-range <start ip address> <end ip address>	This command sets a rule to have the Prestige check for traffic going to this range of addresses.
	config edit firewall set <set #> rule <rule #> TCP destport-single <port #>	This command sets a rule to have the Prestige check for TCP traffic with this destination address. You may repeat this command to enter various, non-consecutive port numbers.
	config edit firewall set <set #> rule <rule #> TCP destport-range <start port #> <end port #>	This command sets a rule to have the Prestige check for TCP traffic with a destination port in this range.
	config edit firewall set <set #> rule <rule #> UDP destport-single <port #>	This command sets a rule to have the Prestige check for UDP traffic with this destination address. You may repeat this command to enter various, non-consecutive port numbers.
	config edit firewall set <set #> rule <rule #> UDP destport-range <start port #> <end port #>	This command sets a rule to have the Prestige check for UDP traffic with a destination port in this range.
Delete		
	config delete firewall e-mail	This command removes all of the settings for e-mail alert.
	config delete firewall attack	This command resets all of the attack response settings to their defaults.
	config delete firewall set <set #>	This command removes the specified set from the firewall configuration.
	config delete firewall set <set #> rule<rule #>	This command removes the specified rule in a firewall configuration set.

Appendix H
NetBIOS Filter Commands

The following describes the NetBIOS packet filter commands.

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 139 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 I
Splitters and Microfilters

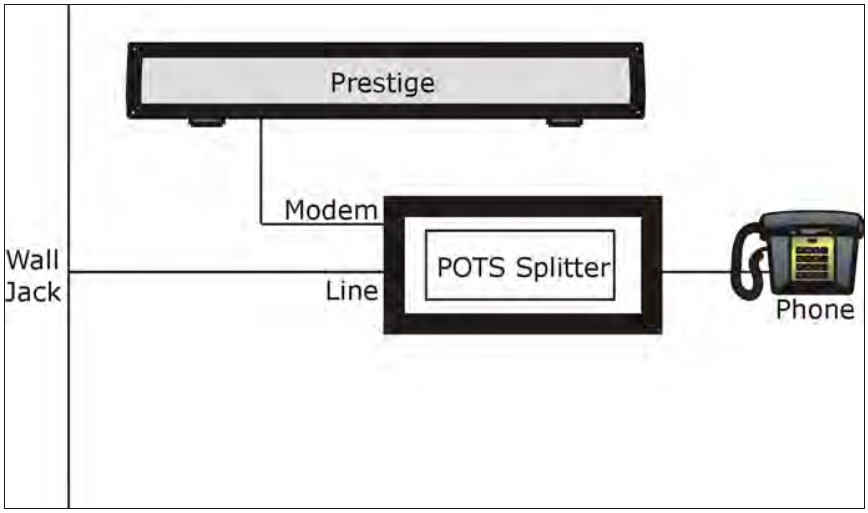
This appendix tells you how to install a POTS splitter or a telephone microfilter.

Connecting a POTS Splitter

When you use the Full Rate (G.dmt) ADSL standard, you can use a POTS (Plain Old Telephone Service) splitter to separate the telephone and ADSL signals. This allows simultaneous Internet access and telephone service on the same line. A splitter also eliminates the destructive interference conditions caused by telephone sets.

Install the POTS splitter at the point where the telephone line enters your residence, as shown in the following figure.

Figure 258 Connecting a POTS Splitter



1. Connect the side labeled "Phone" to your telephone.
2. Connect the side labeled "Modem" to your Prestige.
3. Connect the side labeled "Line" to the telephone wall jack.

Telephone Microfilters

Telephone voice transmissions take place in the lower frequency range, 0 - 4KHz, while ADSL transmissions take place in the higher bandwidth range, above 4KHz. A microfilter acts as a low-pass filter, for your telephone, to ensure that ADSL transmissions do not interfere with your telephone voice transmissions. The use of a telephone microfilter is optional.

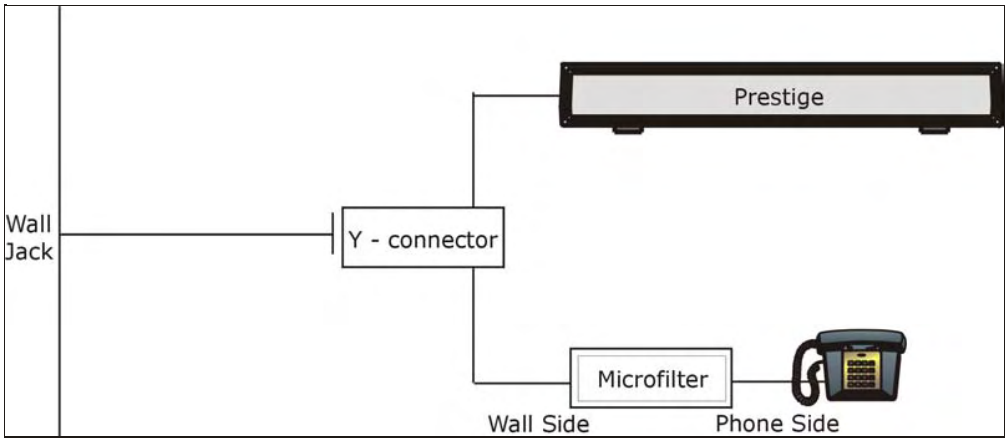
1 Connect a phone cable from the wall jack to the single jack end of the Y- Connector.

2 Connect a cable from the double jack end of the Y-Connector to the "wall side" of the microfilter.

3 Connect another cable from the double jack end of the Y-Connector to the Prestige.

4 Connect the "phone side" of the microfilter to your telephone as shown in the following figure.

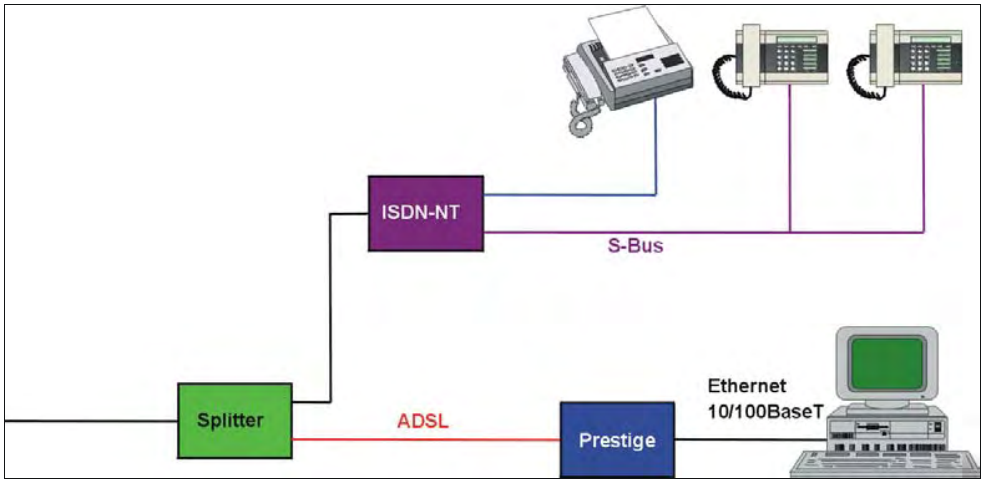
Figure 259 Connecting a Microfilter



Prestige With ISDN

This section relates to people who use their Prestige with ADSL over ISDN (digital telephone service) only. The following is an example installation for the Prestige with ISDN.

Figure 260 Prestige with ISDN



Appendix J
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 261 on page 403). 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.

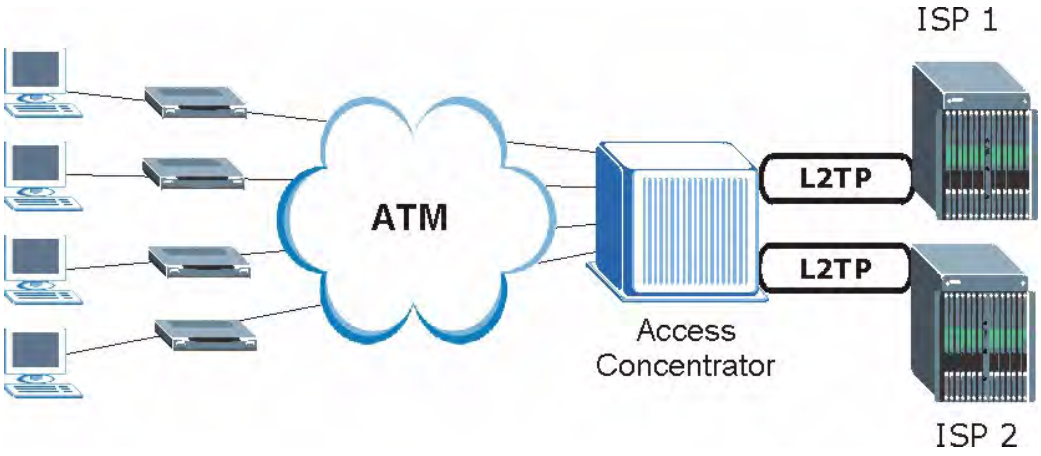
It lessens the burden on the carriers of provisioning virtual circuits all the way to the ISP on multiple switches for thousands of users. For GSTN (PSTN and ISDN), the switching fabric is already in place.

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 261 Single-Computer per Router Hardware Configuration



How PPPoE Works

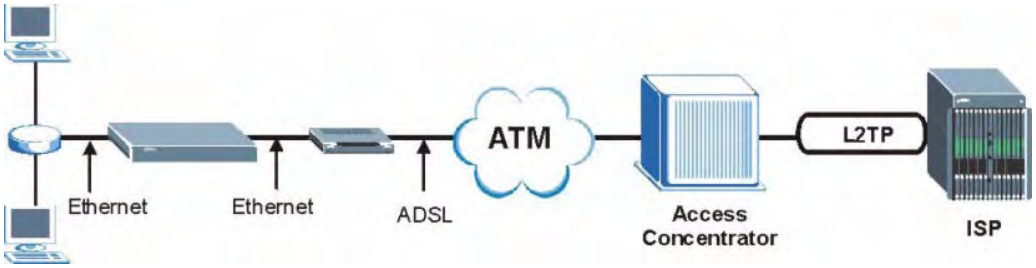
The PPPoE driver makes the Ethernet appear as a serial link to the computer and the computer runs PPP over it, while the modem bridges the Ethernet frames to the Access Concentrator (AC). Between the AC and an ISP, the AC is acting as a L2TP (Layer 2 Tunneling Protocol) LAC (L2TP Access Concentrator) 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 262 Prestige as a PPPoE Client



Appendix K
Log Descriptions

This appendix provides descriptions of example log messages.

Table 140 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 140 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 141 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 142 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 143 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. The default timeout values are as follows: ICMP idle timeout: 3 minutes UDP idle timeout: 3 minutes TCP connection (three way handshaking) timeout: 270 seconds TCP FIN-wait timeout: 2 MSL (Maximum Segment Lifetime set in the TCP header). TCP idle (established) timeout (s): 150 minutes TCP reset timeout: 10 seconds
`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 144 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 145 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 157 on page 416.
`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 157 on page 416.
`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 146 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 147 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.

Table 147 PPP Logs (continued)

LOG MESSAGE	DESCRIPTION
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 148 UPnP Logs

LOG MESSAGE	DESCRIPTION
UPnP pass through Firewall	UPnP packets can pass through the firewall.

Table 149 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" check box, 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.

Table 149 Content Filtering Logs (continued)

LOG MESSAGE	DESCRIPTION
`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 150 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 157 on page 416.
`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 157 on page 416.
`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 157 on page 416.
`icmp echo: ICMP (type:%d, code:%d)`	The firewall detected an ICMP echo attack. For type and code details, see Table 157 on page 416.
`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 157 on page 416.
`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 157 on page 416.
`traceroute ICMP (type:%d, code:%d)`	The firewall detected an ICMP traceroute attack. For type and code details, see Table 157 on page 416.

Table 151 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 152 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 152 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 152 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 152 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 153 PKI Logs

LOG MESSAGE	DESCRIPTION
`Enrollment successful`	The SCEP online certificate enrollment was successful. The Destination field records the certification authority server IP address and port.
`Enrollment failed`	The SCEP online certificate enrollment failed. The Destination field records the certification authority server's IP address and port.
`Failed to resolve <SCEP CA server url>`	The SCEP online certificate enrollment failed because the certification authority server's address cannot be resolved.
`Enrollment successful`	The CMP online certificate enrollment was successful. The Destination field records the certification authority server's IP address and port.
`Enrollment failed`	The CMP online certificate enrollment failed. The Destination field records the certification authority server's IP address and port.
`Failed to resolve <CMP CA server url>`	The CMP online certificate enrollment failed because the certification authority server's IP address cannot be resolved.
`Rcvd ca cert: <subject name>`	The router received a certification authority certificate, with subject name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
`Rcvd user cert: <subject name>`	The router received a user certificate, with subject name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
`Rcvd CRL <size>: <issuer name>`	The router received a CRL (Certificate Revocation List), with size and issuer name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
`Rcvd ARL <size>: <issuer name>`	The router received an ARL (Authority Revocation List), with size and issuer name as recorded, from the LDAP server whose address and port are recorded in the Source field.
`Failed to decode the received ca cert`	The router received a corrupted certification authority certificate from the LDAP server whose address and port are recorded in the Source field.
`Failed to decode the received user cert`	The router received a corrupted user certificate from the LDAP server whose address and port are recorded in the Source field.
`Failed to decode the received CRL`	The router received a corrupted CRL (Certificate Revocation List) from the LDAP server whose address and port are recorded in the Source field.
`Failed to decode the received ARL`	The router received a corrupted ARL (Authority Revocation List) from the LDAP server whose address and port are recorded in the Source field.

Table 153 PKI Logs (continued)

LOG MESSAGE	DESCRIPTION
`Rcvd data <size> too large! Max size allowed: <max size>`	The router received directory data that was too large (the size is listed) from the LDAP server whose address and port are recorded in the Source field. The maximum size of directory data that the router allows is also recorded.
`Cert trusted: <subject name>`	The router has verified the path of the certificate with the listed subject name.
`Due to <reason codes>, cert not trusted: <subject name>`	Due to the reasons listed, the certificate with the listed subject name has not passed the path verification. The recorded reason codes are only approximate reasons for not trusting the certificate. Please see Table 154 on page 414 for the corresponding descriptions of the codes.

Table 154 Certificate Path Verification Failure Reason Codes

CODE	DESCRIPTION
1	Algorithm mismatch between the certificate and the search constraints.
2	Key usage mismatch between the certificate and the search constraints.
3	Certificate was not valid in the time interval.
4	(Not used)
5	Certificate is not valid.
6	Certificate signature was not verified correctly.
7	Certificate was revoked by a CRL.
8	Certificate was not added to the cache.
9	Certificate decoding failed.
10	Certificate was not found (anywhere).
11	Certificate chain looped (did not find trusted root).
12	Certificate contains critical extension that was not handled.
13	Certificate issuer was not valid (CA specific information missing).
14	(Not used)
15	CRL is too old.
16	CRL is not valid.
17	CRL signature was not verified correctly.
18	CRL was not found (anywhere).
19	CRL was not added to the cache.
20	CRL decoding failed.
21	CRL is not currently valid, but in the future.
22	CRL contains duplicate serial numbers.
23	Time interval is not continuous.
24	Time information not available.
25	Database method failed due to timeout.

Table 154 Certificate Path Verification Failure Reason Codes (continued)

CODE	DESCRIPTION
26	Database method failed.
27	Path was not verified.
28	Maximum path length reached.

Table 155 802.1X 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 156 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/ZW)	LAN to LAN/ Prestige	ACL set for packets traveling from the LAN to the LAN or the Prestige.
(W to W/ZW)	WAN to WAN/ Prestige	ACL set for packets traveling from the WAN to the WAN or the Prestige.
(D to D/ZW)	DMZ to DMZ/ Prestige	ACL set for packets traveling from the DMZ to the DM or the Prestige.

Table 157 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 157 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 158 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 159 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 159 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.

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 263 Displaying Log Categories Example

```
Copyright (c) 1994 - 2004 ZyXEL Communications Corp.
ras>?
Valid commands are:
sys             exit            ether           aux
ip              ipsec           bridge          bm
certificates    cnm             8021x           radius
ras>
```

3 Use sys logs category followed by a log category to display the parameters that are available for the category.

Figure 264 Displaying Log Parameters Example

```
ras> sys logs category access
Usage: [0:none/1:log/2:alert/3:both] [0:don't show debug type/
1:show debug type]
```

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 Step 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.

```
ras> sys logs load
ras> sys logs category access 3
ras> sys logs save
ras> sys logs display access

#.time                  source                  destination            notes

    message
 0|06/08/2004 05:58:21 |172.21.4.154          |224.0.1.24            |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
 1|06/08/2004 05:58:20 |172.21.3.56           |239.255.255.250       |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
 2|06/08/2004 05:58:20 |172.21.0.2            |239.255.255.254       |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
 3|06/08/2004 05:58:20 |172.21.3.191          |224.0.1.22            |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
 4|06/08/2004 05:58:20 |172.21.0.254          |224.0.0.1             |ACCESS
BLOCK
    Firewall default policy: IGMP (W to W/ZW)
 5|06/08/2004 05:58:20 |172.21.4.187:137      |172.21.255.255:137    |ACCESS
BLOCK
    Firewall default policy: UDP (W to W/ZW)
```

Appendix L
Wireless LANs

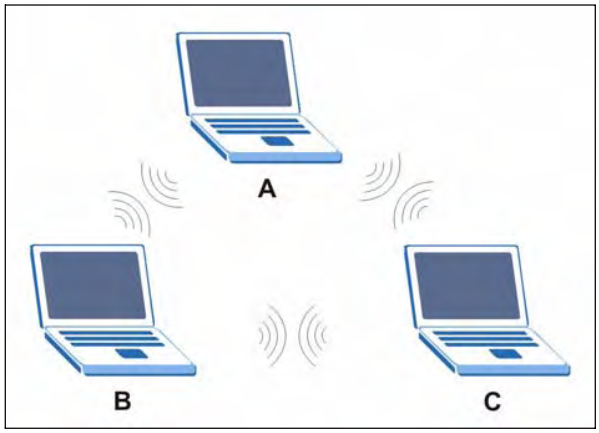
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless stations (A, B, C). 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 265 Peer-to-Peer Communication in an Ad-hoc Network

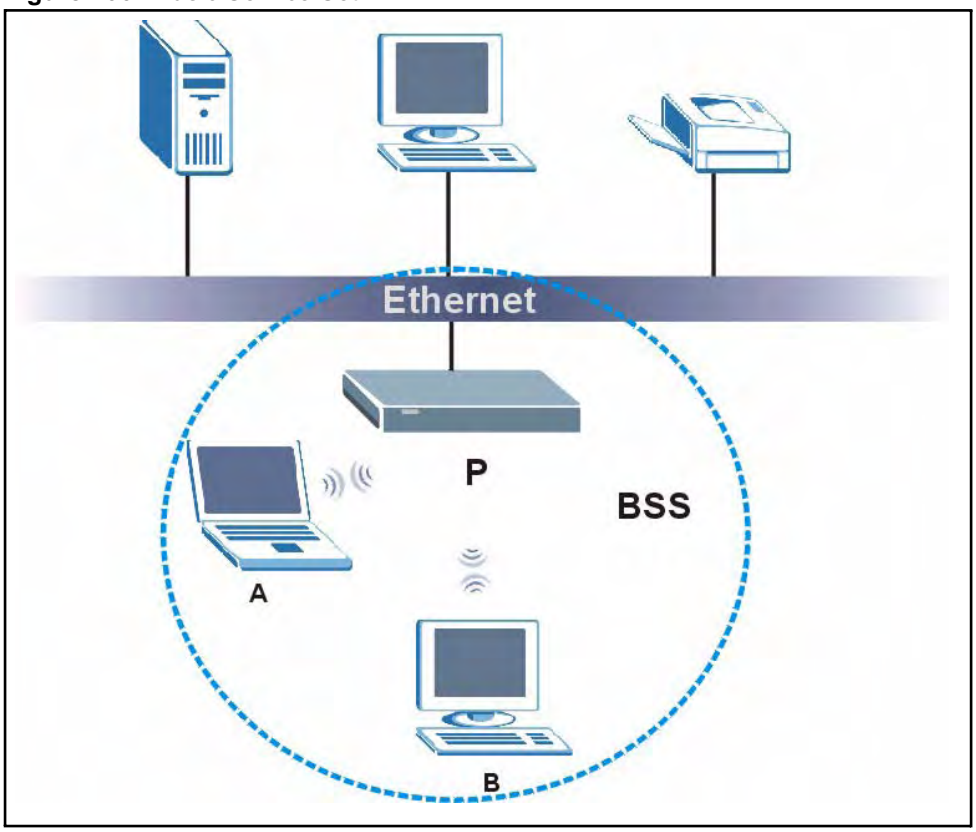


BSS

A Basic Service Set (BSS) exists when all communications between wireless stations or between a wireless station and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless stations in the BSS. When Intra-BSS is enabled, wireless station A and B can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless station A and B can still access the wired network but cannot communicate with each other.

Figure 266 Basic Service Set



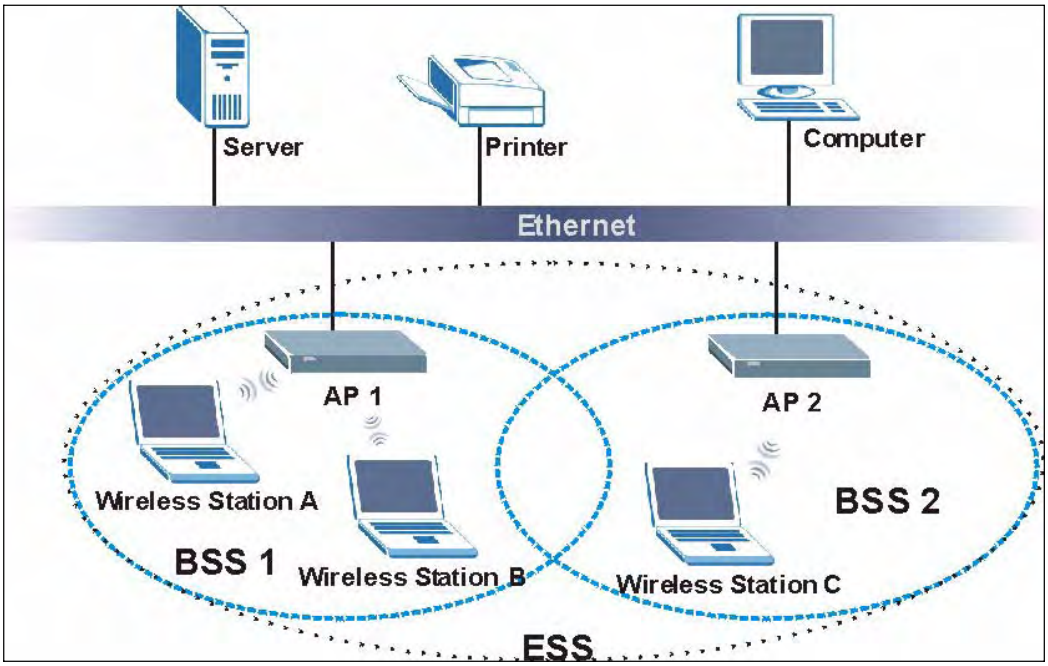
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless stations within the same ESS must have the same ESSID in order to communicate.

Figure 267 Infrastructure WLAN



Channel

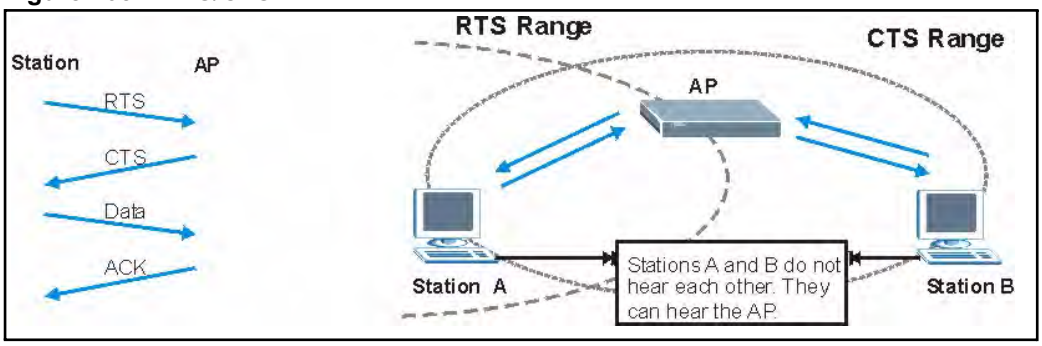
A channel is the radio frequency(ies) used by IEEE 802.11a/b/g wireless devices. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel than an adjacent AP (access point) to reduce interference. Interference occurs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

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 268 RTS/CTS



When station A sends data to the AP, 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.

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 AP 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.

Preamble Type

A preamble is used to synchronize the transmission timing in your wireless network. There are two preamble modes: **Long** and **Short**.

Short preamble takes less time to process and minimizes overhead, so it should be used in a good wireless network environment when all wireless stations support it.

Select **Long** if you have a 'noisy' network or are unsure of what preamble mode your wireless stations support as all IEEE 802.11b compliant wireless adapters must support long preamble. However, not all wireless adapters support short preamble. Use long preamble if you are unsure what preamble mode the wireless adapters support, to ensure interpretability between the AP and the wireless stations and to provide more reliable communication in 'noisy' networks.

Select **Dynamic** to have the AP automatically use short preamble when all wireless stations support it, otherwise the AP uses long preamble.

Note: The AP and the wireless stations MUST use the same preamble mode in order to communicate.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter 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 160 IEEE 802.11g

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)

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. Some advantages of IEEE 802.1x are:

- 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 stations.

RADIUS

RADIUS is based on a client-server 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 AP acts as a message relay between the wireless station and the network RADIUS server.

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.

Types of Authentication

This appendix discusses some popular authentication types: **EAP-MD5**, **EAP-TLS**, **EAP-TTLS**, **PEAP** and **LEAP**.

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.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the Wireless screen. You may still configure and store keys here, but they will not be used while Dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 161 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

WPA

User Authentication

WPA applies IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless stations using an external RADIUS database.

Encryption

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

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 PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless stations. This all happens in the background automatically.

AES (Advanced Encryption Standard) also uses a secret key. This implementation of AES applies a 128-bit key to 128-bit blocks of data.

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 decrypt 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.

Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each Authentication Method/ key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 162 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
WPA	WEP	No	Yes
WPA	TKIP	No	Yes
WPA-PSK	WEP	Yes	Yes
WPA-PSK	TKIP	Yes	Yes

APPENDIX M
Internal SPTGEN

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.

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 269 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*.

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 269 on page 430), 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 270 on page 431, 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 269 on page 430).

Figure 270 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 271 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
```

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 272 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.

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 273 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
```

Example Internal SPTGEN Screens

This section covers Prestige Internal SPTGEN screens.

Table 163 Abbreviations Used in the Example Internal SPTGEN Screens Table

ABBREVIATION	MEANING
FIN	Field Identification Number (not seen in SMT screens)
FN	Field Name

Table 163 Abbreviations Used in the Example Internal SPTGEN Screens Table (continued)

ABBREVIATION	MEANING
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.

Table 164 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 165 Menu 3 (SMT Menu 3)

/ 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
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)			

Table 165 Menu 3 (SMT Menu 3 (continued))

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
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

Table 165 Menu 3 (SMT Menu 3 (continued))

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
30201026 =	IP Alias #2 Outgoing protocol filters Set 4		= 256
*/ Menu 3.5 Wireless LAN Setup (SMT Menu 3.5)			
FIN	FN	PVA	INPUT
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

Table 165 Menu 3 (SMT Menu 3 (continued))

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		=
30500012 =	Wlan Active	<0(Disable) | 1(Enable)>	= 0
*/ MENU 3.5.1 WLAN MAC ADDRESS FILTER (SMT MENU 3.5.1)			
FIN	FN	PVA	INPUT
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 166 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

Table 166 Menu 4 Internet Access Setup (SMT Menu 4) (continued)

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
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

Table 166 Menu 4 Internet Access Setup (SMT Menu 4) (continued)

40000032=	RIP Version	<0(Rip-1) | 1(Rip-2B) |2(Rip-2M)>	= 0
40000033=	Nailed-up Connection	<0(No) |1(Yes)>	= 0

Table 167 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>	=
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

Table 167 Menu 12 (SMT Menu 12) (continued)

/ 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)			
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

Table 167 Menu 12 (SMT Menu 12) (continued)

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
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

Table 167 Menu 12 (SMT Menu 12) (continued)

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
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>	=

Table 167 Menu 12 (SMT Menu 12) (continued)

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 168 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
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

Table 168 Menu 15 SUA Server Setup (SMT Menu 15) (continued)

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
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

Table 168 Menu 15 SUA Server Setup (SMT Menu 15) (continued)

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

Table 169 Menu 21.1 Filter Set #1 (SMT Menu 21.1)

/ Menu 21 Filter set #1 (SMT Menu 21)			
FIN	FN	PVA	INPUT
210100001 =	Filter Set 1, Name	<Str>	=
/ Menu 21.1.1.1 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
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

Table 169 Menu 21.1 Filter Set #1 (SMT Menu 21.1) (continued)

/ 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
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

Table 169 Menu 21.1 Filter Set #1 (SMT Menu 21.1) (continued)

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
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

Table 169 Menu 21.1 Filter Set #1 (SMT Menu 21.1) (continued)

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
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 170 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

Table 170 Menu 21.1 Filer Set #2, (SMT Menu 21.1) (continued)

/ 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
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

Table 170 Menu 21.1 Filer Set #2, (SMT Menu 21.1) (continued)

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
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

Table 170 Menu 21.1 Filer Set #2, (SMT Menu 21.1) (continued)

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
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

Table 170 Menu 21.1 Filer Set #2, (SMT Menu 21.1) (continued)

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
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
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

Table 171 Menu 23 System Menus (SMT Menu 23)

*/ 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: IEEE 802.1x (SMT Menu 23.4)			
FIN	FN	PVA	INPUT
230400001 =	Wireless Port Control	<0(Authentication Required) |1(No Access Allowed) |2(No Authentication Required)>	= 2
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
230400005 =	Key Management Protocol	<0(8021x) |1(WPA) |2(WPAPSK)>	= 0
230400006 =	Dynamic WEP Key Exchange	<0(Disable) |1(64-bit WEP) |2(128-bit WEP)>	= 0
230400007 =	PSK =		=

Table 171 Menu 23 System Menus (SMT Menu 23) (continued)

230400008 =	WPA Mixed Mode	<0(Disable) |1(Enable)>	= 0
230400009 =	Data Privacy for Broadcast/ Multicast packets	<0(TKIP) |1(WEP)>	= 0
230400010 =	WPA Broadcast/Multicast Key Update Timer		= 0

Table 172 Menu 24.11 Remote Management Control (SMT Menu 24.11)

/ 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
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 173 Command Examples

	FIN	**FN**	**PVA**	**INPUT**
/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				

Table 173 Command Examples (continued)

	FIN	FN	PVA	INPUT
	FIN	FN	PVA	INPUT
	990000001 =	ADSL OPMD	<0(etsi)|1(normal)|2(gdmt)|3(multimode)>	= 3

Index

Numerics

110V AC 5
230V AC 5

A

Abnormal Working Conditions 6
AC 5
Access methods 270
Accessories 5
Acts of God 6
Address Assignment 63
Address mapping 110
Address Resolution Protocol (ARP) 67
ADSL, what is it? 40
ADSLstandards 42
Airflow 5
Alternative Subnet Mask Notation 378
American Wire Gauge 5
Any IP 43, 66
  How it works 67
  note 67
Any IP Setup 69
Any IP table 201
AP (access point) 422
applicaions
  Internet access 46
Application-level Firewalls 119
AT command 307
ATM Adaptation Layer 5 (AAL5) 90
ATM layer options 243
Attack Alert 151
Attack Types 123
Authentication 238, 239
Authentication databases 82
authentication databases 294
Authentication protocol 239
AWG 5

B

Backup 307
Backup Typ 100
Bandwidth Borrowing 187
bandwidth budget 182
bandwidth capacity 182
Bandwidth Class 182
bandwidth class 182
Bandwidth Filter 183
bandwidth filter 183
Bandwidth Management 182
Bandwidth Management Statistics 193
Bandwidth Manager Class Configuration 190
Bandwidth Manager Class Setup 190
Bandwidth Manager Monitor 194
Bandwidth Manager Summary 188
Basement 5
Blocking Time 150, 151
Borrow bandwidth from parent class 191
Bridging 239, 250
  Ether Address 252
  Ethernet 250
  Ethernet Addr Timeout 251
  Remote Node 250
  Static Route Setup 252
bridging 215
Brute-force Attack, 122
BSS 420
Budget Management 319, 320
BW Budget 191

C

CA 427
Cables, Connecting 5
Call filtering 272
Call filters
  Built-in 272
  User-defined 272
Call Scheduling 338
  Maximum Number of Schedule Sets 338
  PPPoE 340

Precedence 338
Precedence Example 338
CBR (Continuous Bit Rate) 97
CDR 302
CDR (Call Detail Record) 301
Certificate Authority 427
Certifications 4
change password at login 49
Channel 422
Interference 422
Channel ID 227
CHAP 238
Charge 6
Circuit 3
Class B 3
Class Name 191
Collision 298
Command Interpreter Mode 318
Communications 3
Community 287
compact 45
compact guide 48
Compliance, FCC 3
Components 6
Computer Name 214
Condition 6
Conditions that prevent TFTP and FTP from working over WAN 309
Configuration 63, 200
configuration file 306
Connecting Cables 5
Consequential Damages 6
Contact Information 7
Contacting Customer Support 7
Content Filtering 154
Categories 154
Schedule 156
Tursted computers 156
URL keyword blocking 155
Content filtering 154
content filtering 43
Copyright 2
Correcting Interference 3
Corrosive Liquids 5
Cost Of Transmission 241, 248
Country Code 299
Covers 5
CPU Load 298
CTS (Clear to Send) 423
Custom Ports
Creating/Editing 141
Customer Support 7
Customized Services 141
Customized services 141

D

Damage 5
Dampness 5
Danger 5
Data Filtering 272
data privacy 293
Dealer 3
default LAN IP address 48
Defective 6
Denial of Service 119, 120, 150, 270
Denmark, Contact Information 7
Destination Address 134
Device Filter rules 281
device model number 205
Device rule 281
DHCP 44, 63, 64, 114, 200, 224, 299
DHCP client 44
DHCP relay 44
DHCP server 44, 200, 224
DHCP table 200
diagnostic 202
Diagnostic Tools 296
Disclaimer 2
Discretion 6
Distribution System (DS) 78
DNS 224
Domain Name 63, 107
domain name 214
Domain Name System 63
DoS 120
Basics 120
Types 121
DoS (Denial of Service) 43
DoS attacks, types of 121
DSL (Digital Subscriber Line) 40
DSL line, reinitialize 204
DSL, What Is It? 40
DSLAM (Digital Subscriber Line Access Multiplexer) 46
Dust 5
Dynamic DNS 44, 114, 215
dynamic DNS 44, 215
Dynamic Host Configuration Protocol 44
Dynamic WEP Key Exchange 427

Dynamic WEP key exchange 82
dynamic WEP key exchange 293
DYNDNS Wildcard 114

E

EAP 70
EAP Authentication 426
EAP authentication 292
ECHO 106
Electric Shock 5
Electrical Pipes 5
Electrocution 5
E-mail
  Log Example 180
embedded help 50
Encapsulated Routing Link Protocol (ENET ENCAP) 90
Encapsulation 90, 234, 237
  ENET ENCAP 90
  PPP over Ethernet 90
  PPPoA 90
  RFC 1483 91
Encryption 428
Equal Value 6
Error Log 300
ESS 421
ESSID (Extended Service Set Identification) 74
Ethernet 355
Europe 5
Exposure 5
Extended Service Set 421

F

Failure 6
Fairness-based Scheduler 185
FCC 3
  Rules, Part 15 3
FCC Rules 3
Federal Communications Commission 3
Filename Conventions 306
filename conventions 307
Filter 222, 272
  Applying Filters 283
  Ethernet Traffic 284
  Ethernet traffic 284
  Filter Rules 275
  Filter structure 273
  Generic Filter Rule 279
  Remote Node 242
  Remote Node Filter 242
  Remote Node Filters 284
  Sample 282
  SUA 281
  TCP/IP Filter Rule 277
Filter Log 302
Filter Rule Process 273
Filter Rule Setup 276
Filter Set
  Class 276
Filtering 272, 276
Filtering Process
  Outgoing Packets 272
Finger 107
Finland, Contact Information 7
Firewall
  Access Methods 132, 270
  Address Type 140
  Alerts 135
  Anti-Probing 148
  Creating/Editing Rules 138
  Custom Ports 141
  Enabling 135
  Firewall Vs Filters 129
  Guidelines For Enhancing Security 127
  Introduction 119
  LAN to WAN Rules 134
  Policies 132
  Remote Management 270
  Rule Checklist 133
  Rule Logic 133
  Rule Security Ramifications 133
  Services 146
  SMT menus 270
  Types 118
  When To Use 129
firmware 205, 306
  upgrade 205
  upload 205
  upload error 206
Fitness 6
Fragment Threshold 227
Fragmentation Threshold 423
Fragmentation threshold 423
France, Contact Information 7
FTP 106, 158, 325
  Restrictions 325
FTP File Transfer 313
FTP Restrictions 158, 309
FTP Server 264
Full Rate 398
Functionally Equivalent 6

G

Gas Pipes 5
Gateway 248
Gateway Node 252
General Setup 214
Generic filter 281
Germany, Contact Information 7
God, act of 6

H

Half-Open Sessions 150
Harmful Interference 3
Hidden Menus 210
Hidden node 422
High Voltage Points 5
Hop Count 241, 248
Host 53
Host IDs 376
HTTP 107, 119, 120, 121
HTTP (Hypertext Transfer Protocol) 205

I

IANA 65
IANA (Internet Assigned Number Authority) 141
IBSS 420
ICMP echo 123
Idle timeout 239
IEEE 802.11g 45, 424
IEEE 802.11i 45
IEEE802.1x 292
IGMP 66
IGMP support 241
Independent Basic Service Set 420
Indirect Damages 6
initialization vector (IV) 428
Install UPnP 164
  Windows Me 164
  Windows XP 166
Insurance 6
Integrated Services Digital Network 42
Interactive Applications 328
Interference 3
Interference Correction Measures 3
Interference Statement 3
Internal SPTGEN 430
  FTP Upload Example 432
  Points to Remember 430
  Text File 430
Internet Access 43, 46, 230, 233, 234
Internet access 54, 230
Internet Access Setup 254, 343
Internet access wizard setup 54
Internet Assigned Numbers AuthoritySee IANA 65
Internet Control Message Protocol (ICMP) 123, 148
IP Address 64, 106, 200, 224, 248, 252, 278, 299, 304, 330
IP Address Assignment 91
  ENET ENCAP 92
  PPPoA or PPPoE 91
  RFC 1483 92
IP Addressing 376
IP alias 44, 230
IP Alias Setup 231
IP Classes 376
IP Filter 279
  Logic Flow 278
IP mask 277
IP Packet 279
IP Policies 332
IP policy 230
IP policy routing 328
IP Policy Routing (IPPR) 44, 230
  Applying an IP Policy 332
  Ethernet IP Policies 332
  Gateway 332
IP Pool Setup 63
IP Protocol 331
IP protocol 328
IP protocol type 146
IP Routing Policy (IPPR) 328
  Benefits 328
  Cost Savings 328
  Criteria 328
  Load Sharing 328
  Setup 329
IP Spoofing 121, 124
IP Static Route 246
IP Static Route Setup 247
ISDN (Integrated Services Digital Network) 42

K

Key Fields For Configuring Rules 134

Key management protocol 293

L

Labor 6
LAN 297
LAN Setup 62, 90
LAN TCP/IP 64
LAN to WAN Rules 134
LAND 121, 122
Legal Rights 6
Liability 2
License 2
Lightning 5
Link type 297
Liquids, Corrosive 5
LLC-based Multiplexing 243
Local Network
  Rule Summary 136
Local User Database 294
Local user database 85
Log and Trace 300
Log Facility 301
Logging Option 278, 281
Logical networks 230
Login 238
Logs 176

M

MAC (Media Access Control) 200
MAC (Media Access Control) address. 75
MAC address 252
MAC Address Filter 227
MAC address filter 227
  Filter action 228
MAC Address Filter Action 76, 228
MAC Address Filtering 75
MAC filter 71
Main Menu 211
maintenance 196
management idle timeout period 49
Management Information Base (MIB) 287
Materials 6
Maximize Bandwidth Usage 185
Maximum Burst Size (MBS) 94, 97
Max-incomplete High 150
Max-incomplete Low 150
MBSSee Maximum Burst Size 234
Media Access Control 250
Media Bandwidth Management 43
Merchantability 6
Message Integrity Check (MIC) 428
Message Logging 300
Metric 92, 241, 248
MSDU (MAC Service Data Unit) 227
Multicast 66, 241
Multiplexing 91, 234, 237
multiplexing 91
  LLC-based 91
  VC-based 91
Multiprotocol Encapsulation 91
My WAN Address 240

N

Nailed-Up Connection 92
NAT 64, 106, 107, 281
  Address mapping rule 111
  Application 104
  Applying NAT in the SMT Menus 254
  Configuring 256
  Definitions 102
  Examples 261
  How it works 103
  Mapping Types 105
  Non NAT Friendly Application Programs 267
  Ordering Rules 259
  What it does 103
  What NAT does 103
NAT (Network Address Translation) 102
NAT mode 108
NAT Traversal 162
navigating the web configurator 50
NetBIOS commands 123
Network Address Translation 234
Network Address Translation (NAT) 44, 254
Network Management 107
New 6
NNTP 107
North America 5
North America Contact Information 7
Norway, Contact Information 7

O

One-Minute High 150
Opening 5
Operating Condition 6
Operating frequency 227
Out-dated Warranty 6
Outlet 3

P

Packet
  Error 297
  Received 297
  Transmitted 297
Packet Filtering 129
Packet filtering
  When to use 129
Packet Filtering Firewalls 118
Packet Triggered 302
Packets 297
Pairwise Master Key (PMK) 428
PAP 239
Parts 6
Password 208, 212, 238, 287
password 208
Patent 2
Peak Cell Rate (PCR) 94, 97
Permission 2
Photocopying 2
Ping 304
Ping of Death 121
Pipes 5
Point to Point Protocol over ATM Adaptation Layer 5 (AAL5) 90
Point-to-Point 40
Point-to-Point Tunneling Protocol 107
policy-based routing 328
Pool 5
POP3 107, 120, 121
Port Numbers 106
Postage Prepaid. 6
Power Adaptor 5
Power Cord 5
Power Outlet 5
Power Supply 5
Power Supply, repair 5
PPP Encapsulation 243
PPP Log 303
PPP session over Ethernet (PPP over Ethernet, RFC 2516) 90
PPPoA 237
PPPoE 93, 402
  Benefits 93
PPPoE (Point-to-Point Protocol over Ethernet) 44, 93
PPPoE pass-through 245
PPTP 107
Preamble Mode 424
Precedence 328, 331
Pre-Shared Key 293
  Format 77
Prestige model 306
Priority 191
Priority-based Scheduler 185
Private 241, 248
Product Model 7
Product Page 4
Product Serial Number 7
Products 6
Proof of Purchase 6
Proper Operating Condition 6
Proportional Bandwidth Allocation 183
Protocol 277
Protocol filter 281
Protocol Filter Rules 281
PSK 293
Purchase, Proof of 6
Purchaser 6
PVC (Permanent Virtual Circuit) 90

Q

Qualified Service Personnel 5
Quality of Service 328
Quick Start Guide 38

R

Radio Communications 3
Radio frequency 74
Radio Frequency Energy 3
Radio Interference 3
Radio Reception 3
Radio Technician 3

RADIUS 425
Configuring 87
Shared Secret Key 426
RADIUS Message Types 425
RADIUS Messages 425
RADIUS server 290
RAS 299, 329
Rate
Receiving 297
Transmission 297
real-time application 182
Receiving Antenna 3
Registered 2
Registered Trademark 2
Regular Mail 7
reinitialize the ADSL line 204
Related Documentation 38
Relocate 3
Re-manufactured 6
Remote DHCP Server 224
Remote Management
Firewall 270
Remote Management and NAT 159
Remote Management Limitations 158, 325
Remote Management Setup 324
Remote Node 236, 297
Remote Node Profile 238
Remote Node Setup 236
Remote node 236
Remote Node Index Number 297
Removing 5
Reorient 3
Repair 5, 6
Replace 6
Replacement 6
Reproduction 2
Required fields 211
Reset button, the 49
resetting the Prestige 49
Restore 6
Restore Configuration 311
Return Material Authorization (RMA) Number 6
Returned Products 6
Returns 6
RF (Radio Frequency) 45
RFC 1483 91
RFC 1631 102
RFC-1483 237
RFC-2364 237, 238
RFC2516 44
Rights 2
Rights, Legal 6
RIP 224, 241
RIPSee Routing Information Protocol 65
Risk 5
Risks 5
RMA 6
romfile 306
Root Class 190
Routing 230
Routing Information Protocol 65
Direction 65
Version 65
Routing Policy 328
RTS (Request To Send) 423
RTS (Request To Send) threshold 74
RTS Threshold 227, 422, 423
RTS(Request To Send) 227
Rule Summary 136
Rules 134
Checklist 133
Key Fields 134
LAN to WAN 134
Logic 133
Predefined Services 146
Summary 136

S

Safety Warnings 5
Sample IP Addresses 241
Saving the State 124
Schedule Sets
Duration 339
Scheduler 185
SCRSee Sustain Cell Rate 234
Security In General 128
Security Parameters 429
Security Ramifications 133
Separation Between Equipment and Receiver 3
Serial Number 7
Server 105, 256, 258, 260, 261, 262, 263, 264, 321
Server behind NAT 260
Service 5, 6, 134
Service Personnel 5
Service Type 142, 343
Services 106
setup a schedule 339
Shared secret 88, 291
Shipping 6

Shock, Electric 5
SMT Menu Overview 209
SMTP 107
SMTP Error Messages 179
Smurf 122, 123
SNMP 107
  Community 288
  Configuration 287
  Get 287
  GetNext 287
  Manager 286
  MIBs 287
  Set 287
  Trap 287
  Trusted Host 288
Source Address 134, 140
Source-Based Routing 328
Spain, Contact Information 7
Splitters 398
Stateful Inspection 43, 118, 119, 124, 125
  Prestige 126
  Process 125
Static route 246
Static Routing Topology 246
SUA 106, 107
SUA (Single User Account) 106, 254
SUA server 106, 108
  Default server set 106
SUA vs NAT 106
SUA/NAT Server Set 109
Sub-class Layers 190
Subnet Mask 64, 140, 224, 240, 248, 299
Subnet Masks 377
Subnetting 377
Supply Voltage 5
Support E-mail 7
Supporting Disk 38
Sustain Cell Rate (SCR) 97
Sustained Cell Rate (SCR) 94
Sweden, Contact Information 7
Swimming Pool 5
SYN Flood 121, 122
SYN-ACK 122
Syntax Conventions 38
Syslog 146, 301
Syslog IP Address 301
Syslog Server 301
System
  Console Port Speed 299
  Diagnostic 303
  Log and Trace 300
  Syslog and Accounting 301
  System Information 298
  System Status 296
System Information 298
System Information & Diagnosis 296
System Maintenance 296, 298, 307, 310, 315, 318, 319, 321
System Management Terminal 210
System Parameter Table Generator 430
System password 290
System Security 290
System Status 297
System Timeout 159, 326

T

Tampering 6
TCP Maximum Incomplete 150, 151
TCP Security 126
TCP/IP 120, 121, 159, 281, 304
Teardrop 121
Telecommunication Line Cord. 5
Telephone 7
Television Interference 3
Television Reception 3
Telnet 159, 208
Telnet Configuration 159
Temporal Key Integrity Protocol (TKIP) 428
Text File Format 430
TFTP
  Restrictions 325
TFTP File Transfer 315
TFTP Restrictions 158, 309
Three-Way Handshake 122
Threshold Values 150
Thunderstorm 5
Time and Date Setting 320, 321
Time Zone 322
Timeout 219
TOS (Type of Service) 328
Trace Records 300
Traceroute 124
Trademark 2
Trademark Owners 2
Trademarks 2
Traffic Redirect 98, 99
  Setup 219
Traffic redirect 98, 101
traffic redirect 43

Traffic shaping 93
Translation 2
Transmission Rates 43
TV Technician 3
Type of Service 328, 330, 331, 332

U

UBR (Unspecified Bit Rate) 97
UDP/ICMP Security 127
Undesired Operations 3
Universal Plug and Play 162
  Application 162
  Security issues 163
Universal Plug and Play (UPnP) 44
Universal Plug and Play Forum 163
UNIX Syslog 300, 301
UNIX syslog parameters 301
Upload Firmware 313
UPnP 162
Upper Layer Protocols 126, 127
User Authentication 428
User Name 115
User Profiles 85
user profiles 294

V

Value 6
VBR (Variable Bit Rate) 97
VC-based Multiplexing 237
Vendor 5
Ventilation Slots 5
Viewing Certifications 4
Virtual Channel Identifier (VCI) 91
virtual circuit (VC) 91
Virtual Path Identifier (VPI) 91
Voice-over-IP (VoIP) 182
Voltage Supply 5
Voltage, High 5
VPI & VCI 91

W

Wall Mount 5
WAN (Wide Area Network) 90
WAN backup 99
WAN Setup 218
WAN to LAN Rules 134
Warnings 5
Warranty 6
Warranty Information 7
Warranty Period 6
Water 5
Water Pipes 5
Web Configurator 48, 50, 119, 127, 134, 271
web configurator screen summary 50
Web Site 7
WEP
  Default Key 227
WEP (Wired Equivalent Privacy) 45, 75, 227
WEP Encryption 227
WEP encryption 73
Wet Basement 5
Wi-Fi Protected Access 77
Wi-Fi Protected Access (WPA) 45
Wireless Client WPA Supplicants 79
Wireless LAN 226
  Configuring 73
Wireless LAN MAC Address Filtering 45
Wireless LAN Setup 226
Wireless port control 80, 293
Wireless security 70
WLAN
  Interference 422
  Security parameters 429
Workmanship 6
Worldwide Contact Information 7
WPA 77, 293
  Supplicants 79
  with RADIUS Application Example 78
WPA Mixed Mode 293
WPA -Pre-Shared Key 77
WPA with RADIUS Application 78
WPA-PSK 77
WPA-PSK Application 77
Written Permission 2

X

XMODEM protocol **307**

Z

Zero Configuration Internet Access **43**
Zero configuration Internet access **94**
ZyNOS **2**, **307**
ZyNOS (ZyXEL Network Operating System) **306**
ZyNOS F/W Version **307**
ZyXEL Communications Corporation **2**
ZyXEL Home Page **4**
ZyXEL Limited Warranty
  Note **6**
ZyXEL Network Operating System **2**
ZyXEL_s Firewall
  Introduction **119**