

Prestige 861H Series

VDSL Router/Bridge

User's Guide

Version 3.40
8/2005

The logo for ZyXEL, featuring the word "ZyXEL" in a bold, blue, sans-serif font. The "y" is lowercase and has a distinctive shape, while "XEL" is uppercase. The letters are closely spaced and have a slight shadow effect.

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 commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

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

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

Notice 1

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

Information for Canadian Users

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.

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	SUPPORT E-MAIL	TELEPHONE ^A	WEB SITE	REGULAR MAIL
LOCATION	SALES E-MAIL	FAX	FTP SITE	
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		

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	22
List of Tables	28
Preface	32
Introduction to DSL	34
Chapter 1	
Getting To Know Your Prestige	36
1.1 Introducing the Prestige	36
1.1.1 Features of the Prestige	36
1.1.2 Applications for the Prestige	38
1.1.2.1 Home Gateway Applications	38
1.1.3 Front Panel LEDs	41
1.1.4 Rear Panel	42
1.1.4.1 VDSL Port	42
1.1.4.2 Ground (Available on some models)	42
1.1.4.3 LAN 1 ~ 4	42
1.1.4.4 Console Port	42
1.1.4.5 Reset Button	42
1.1.4.6 Power Port	43
1.1.4.7 Turning On Your Prestige	43
Chapter 2	
Introducing the Web Configurator	44
2.1 Web Configurator Overview	44
2.1.1 Accessing the Prestige Web Configurator	44
2.1.2 Navigating the Prestige Web Configurator	45
2.2 Password	47

Chapter 3	
Wizard Setup for Internet Access	48
3.1 Introduction	48
3.1.1 Internet Access Wizard Setup	48
3.1.1.1 Internet Access Wizard Setup : Routing	49
3.1.1.2 Internet Access Wizard Setup : Bridge	56
Chapter 4	
LAN Setup	62
4.1 LAN Overview	62
4.1.1 LANs, WANs and the Prestige	62
4.1.2 DHCP Setup	62
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	64
4.2.2 RIP Setup	65
4.2.3 Multicast	65
4.2.4 Configuring LAN	66
Chapter 5	
WAN Setup	70
5.1 WAN Overview	70
5.1.1 Encapsulation	70
5.1.1.1 ENET ENCAP	70
5.1.1.2 PPP over Ethernet	70
5.1.1.3 PPPoA	70
5.1.1.4 RFC 1483	71
5.1.2 LLC-based Multiplexing	71
5.1.3 VPI and VCI	71
5.1.4 IP Address Assignment	71
5.1.4.1 IP Assignment with PPPoA or PPPoE Encapsulation	71
5.1.4.2 IP Assignment with RFC 1483 Encapsulation	71
5.1.4.3 IP Assignment with ENET ENCAP Encapsulation	72
5.1.5 Nailed-Up Connection (PPP)	72
5.1.6 NAT	72
5.2 PPPoE Encapsulation	72
5.3 Traffic Shaping	73
5.3.1 ATM Traffic Classes	73
5.3.1.1 Constant Bit Rate (CBR)	73
5.3.1.2 Variable Bit Rate (VBR)	73

5.3.1.3 Unspecified Bit Rate (UBR)	73
5.3.2 Traffic Parameters	74
5.3.2.1 Peak Cell Rate (PCR)	74
5.3.2.2 Sustained Cell Rate (SCR)	74
5.3.2.3 Maximum Burst Size (MBS)	74
5.3.2.4 Minimum Cell Rate (MCR)	74
5.3.3 Cell Delay Variation Tolerance (CDVT)	75
5.3.4 Burst Tolerance (BT)	75
5.4 Permanent Virtual Circuit	75
5.4.1 PVC Example	75
5.5 Remote Node Screen	76
5.6 Zero Configuration Internet Access	78
5.7 Configuring WAN Setup	78
Chapter 6	
Network Address Translation (NAT) Screens	84
6.1 NAT Overview	84
6.1.1 NAT Definitions	84
6.1.2 What NAT Does	85
6.1.3 How NAT Works	85
6.1.4 NAT Application	86
6.1.5 NAT Mapping Types	87
6.2 SUA (Single User Account) Versus NAT	88
6.3 SUA Server	88
6.3.1 Default Server IP Address	88
6.3.2 Port Forwarding: Services and Port Numbers	88
6.3.3 Configuring Servers Behind SUA (Example)	89
6.4 Selecting the NAT Mode	89
6.5 Configuring SUA Server	90
6.6 Configuring Address Mapping	92
6.7 Editing an Address Mapping Rule	93
Chapter 7	
Dynamic DNS Setup.....	96
7.1 Dynamic DNS	96
7.1.1 DYNDNS Wildcard	96
7.2 Configuring Dynamic DNS	96
Chapter 8	
Time and Date.....	98
8.1 Configuring Time and Date	98

Chapter 9	
Remote Management Configuration	100
9.1 Remote Management Overview	100
9.1.1 Remote Management Limitations	100
9.1.2 Remote Management and NAT	101
9.1.3 System Timeout	101
9.2 Telnet	101
9.3 FTP	101
9.4 Web	101
9.5 SNMP	102
9.5.1 Supported MIBs	103
9.5.2 SNMP Traps	103
9.6 ICMP	103
9.7 Configuring Remote Management	104
Chapter 10	
Universal Plug-and-Play (UPnP)	106
10.1 Introducing Universal Plug and Play	106
10.1.1 How do I know if I'm using UPnP?	106
10.1.2 NAT Traversal	106
10.1.3 Cautions with UPnP	106
10.2 UPnP and ZyXEL	107
10.2.1 Configuring UPnP	107
10.3 Installing UPnP in Windows Example	108
10.4 Using UPnP in Windows XP Example	112
Chapter 11	
Logs Screens	120
11.1 Logs Overview	120
11.1.1 Alerts and Logs	120
11.2 Displaying the Logs	120
Chapter 12	
Maintenance	122
12.1 Maintenance Overview	122
12.2 System Status Screen	122
12.2.1 System Statistics	124
12.3 DHCP Table Screen	126
12.4 Diagnostic Screens	127
12.4.1 Diagnostic General Screen	127
12.4.2 Diagnostic DSL Line Screen	127
12.5 Firmware Screen	128
12.6 Configuration Screen	130

12.6.1 Backup Configuration	130
12.6.2 Restore Configuration	131
12.6.3 Default Screen	132
Chapter 13	
Introducing the SMT	134
13.1 SMT Introduction	134
13.1.1 Procedure for SMT Configuration via Telnet	134
13.1.2 Entering Password	134
13.1.3 Prestige SMT Menus Overview	135
13.2 Navigating the SMT Interface	136
13.2.1 System Management Terminal Interface Summary	137
13.3 Changing the System Password	138
Chapter 14	
Menu 1 General Setup	140
14.1 General Setup	140
14.2 Procedure To Configure Menu 1	140
14.2.1 Procedure to Configure Dynamic DNS	142
Chapter 15	
Menu 3 LAN Setup	144
15.1 LAN Setup	144
15.1.1 General Ethernet Setup	144
15.2 Protocol Dependent Ethernet Setup	145
15.3 TCP/IP Ethernet Setup and DHCP	145
Chapter 16	
Internet Access	148
16.1 Internet Access Overview	148
16.2 IP Policies	148
16.3 IP Alias	148
16.4 IP Alias Setup	149
16.5 Route IP Setup	150
16.6 Internet Access Configuration	151
Chapter 17	
Remote Node Configuration	154
17.1 Remote Node Setup Overview	154
17.2 Remote Node Setup	154
17.2.1 Remote Node Profile	154
17.2.2 Encapsulation and Multiplexing Scenarios	155
17.2.3 Outgoing Authentication Protocol	157

17.3 Remote Node Network Layer Options	158
17.3.1 My WAN Addr Sample IP Addresses	159
17.4 Remote Node Filter	160
17.5 Editing ATM Layer Options	161
17.5.1 LLC-based Multiplexing or PPP Encapsulation	161
17.5.2 Advance Setup Options	162
Chapter 18	
Static Route Setup	164
18.1 IP Static Route Overview	164
18.2 Configuration	164
Chapter 19	
Bridging Setup	168
19.1 Bridging in General	168
19.2 Bridge Ethernet Setup	168
19.2.1 Remote Node Bridging Setup	168
19.2.2 Bridge Static Route Setup	170
Chapter 20	
Network Address Translation (NAT)	172
20.1 Using NAT	172
20.1.1 SUA (Single User Account) Versus NAT	172
20.2 Applying NAT	172
20.3 NAT Setup	174
20.3.1 Address Mapping Sets	175
20.3.1.1 SUA Address Mapping Set	175
20.3.1.2 User-Defined Address Mapping Sets	176
20.3.1.3 Ordering Your Rules	177
20.4 Configuring a Server behind NAT	179
20.5 General NAT Examples	180
20.5.1 Example 1: Internet Access Only	180
20.5.2 Example 2: Internet Access with an Inside Server	181
20.5.3 Example 3: Multiple Public IP Addresses With Inside Servers	182
20.5.4 Example 4: NAT Unfriendly Application Programs	186
Chapter 21	
Filter Configuration	188
21.1 About Filtering	188
21.1.1 The Filter Structure of the Prestige	189
21.2 Configuring a Filter Set for the Prestige	190
21.3 Filter Rules Summary Menus	191
21.4 Configuring a Filter Rule	192

21.4.1 TCP/IP Filter Rule	193
21.4.2 Generic Filter Rule	195
21.5 Filter Types and NAT	197
21.6 Example Filter	197
21.7 Applying Filters and Factory Defaults	199
21.7.1 Ethernet Traffic	200
21.7.2 Remote Node Filters	200
Chapter 22	
SNMP Configuration	202
22.1 About SNMP	202
22.2 Supported MIBs	203
22.3 SNMP Configuration	203
22.4 SNMP Traps	204
Chapter 23	
System Information and Diagnosis	206
23.1 Overview	206
23.2 System Status	206
23.3 System Information	208
23.3.1 System Information	208
23.3.2 Console Port Speed	209
23.4 Log and Trace	210
23.4.1 Viewing Error Log	210
23.5 Diagnostic	211
Chapter 24	
Firmware and Configuration File Maintenance	214
24.1 Filename Conventions	214
24.2 Backup Configuration	215
24.2.1 Backup Configuration	215
24.2.2 Using the FTP Command from the Command Line	216
24.2.3 Example of FTP Commands from the Command Line	216
24.2.4 GUI-based FTP Clients	217
24.2.5 TFTP and FTP over WAN Management Limitations	217
24.2.6 Backup Configuration Using TFTP	218
24.2.7 TFTP Command Example	218
24.2.8 GUI-based TFTP Clients	218
24.3 Restore Configuration	219
24.3.1 Restore Using FTP	219
24.3.2 Restore Using FTP Session Example	220
24.4 Uploading Firmware and Configuration Files	221
24.4.1 Firmware File Upload	221

24.4.2 Configuration File Upload	221
24.4.3 FTP File Upload Command from the DOS Prompt Example	222
24.4.4 FTP Session Example of Firmware File Upload	223
24.4.5 TFTP File Upload	223
24.4.6 TFTP Upload Command Example	224
Chapter 25	
System Maintenance.....	226
25.1 Command Interpreter Mode	226
25.2 Call Control Support	227
25.2.1 Budget Management	227
25.3 Time and Date Setting	228
25.3.1 Resetting the Time	231
Chapter 26	
Remote Management.....	232
26.1 Remote Management Overview	232
26.2 Remote Management	232
26.2.1 Remote Management Setup	232
26.2.2 Remote Management Limitations	233
26.3 Remote Management and NAT	234
26.4 System Timeout	234
Chapter 27	
IP Policy Routing.....	236
27.1 IP Policy Routing Overview	236
27.2 Benefits of IP Policy Routing	236
27.3 Routing Policy	236
27.4 IP Routing Policy Setup	237
27.5 Applying an IP Policy	240
27.5.1 Ethernet IP Policies	240
27.6 IP Policy Routing Example	242
Chapter 28	
Call Scheduling.....	246
28.1 Introduction	246
Chapter 29	
Introduction to CLI.....	250
29.1 Command Line Interface Overview	250
29.1.1 Accessing the Command Line Interface	250
29.1.2 Command Conventions	250
29.1.3 Command Syntax Conventions	251

29.2 help Command	251
29.3 exit Command	251
Chapter 30	
System Commands	252
30.1 System Commands Overview	252
30.2 System Configuring	252
30.3 sys Commands	252
30.4 sys Command Examples	255
30.4.1 sys version	255
30.4.2 sys logs errlog disp	256
30.4.3 sys logs errlog clear Command Example	256
Chapter 31	
Ethernet, IP and WAN Commands	258
31.1 Ethernet Commands	258
31.2 IP Commands	258
31.3 ip Command Examples	261
31.3.1 ip ping	261
31.3.2 ip route status	262
31.3.3 ip arp status	262
31.4 WAN Commands	263
Chapter 32	
VDSL Commands	264
32.1 VDSL Commands Overview	264
32.2 Command Summary	264
32.2.1 vdsl Commands	264
32.3 VDSL Default Values	265
32.3.1 Service Categories	265
32.4 Interleave Delay	266
32.5 SNR (Signal-to-Noise-Ratio)	266
32.6 VDSL Command Examples	267
32.6.1 VDSL Port Command	267
32.6.2 VDSL Clear Port Clear Counter	268
32.6.3 PVC List Command	268
32.6.4 Activate the VDSL Current Port Profile	269
32.6.5 Reset VDSL Profile	270
32.6.6 Band Plans	270
32.6.7 Show Profile Command	270
32.6.8 VDSL Version Command	271

Chapter 33	
Troubleshooting	272
33.1 Problems Starting Up the Prestige	272
33.2 Problems with the LAN	272
33.3 Problems with the WAN	273
33.4 Problems Accessing the Prestige	274
33.4.1 Pop-up Windows, JavaScripts	274
33.4.1.1 Internet Explorer Pop-up Blockers	274
33.4.1.2 JavaScripts	277
Appendix A	
Product Specifications	280
Appendix B	
Setting up Your Computer's IP Address.....	284
Windows 95/98/Me.....	284
Installing Components	285
Configuring	286
Verifying Settings.....	287
Windows 2000/NT/XP	287
Verifying Settings.....	292
Macintosh OS 8/9.....	292
Verifying Settings.....	294
Macintosh OS X	294
Verifying Settings.....	295
Appendix C	
IP Subnetting	296
IP Addressing.....	296
IP Classes	296
Subnet Masks	297
Subnetting	297
Example: Two Subnets	298
Example: Four Subnets.....	300
Example Eight Subnets.....	301
Subnetting With Class A and Class B Networks.....	302
Appendix D	
Boot Commands	304
Appendix E	
NetBIOS Filter Commands	306
Introduction	306

Display NetBIOS Filter Settings	306
NetBIOS Filter Configuration.....	307

Appendix F

Splitters and Microfilters 310

Connecting a POTS Splitter	310
Telephone Microfilters	310
Prestige With ISDN	311

Appendix G

PPPoE 312

PPPoE in Action	312
Benefits of PPPoE.....	312
Traditional Dial-up Scenario	312
How PPPoE Works	313
Prestige as a PPPoE Client	313

Appendix H

Log Descriptions..... 314

Log Commands.....	328
Configuring What You Want the Prestige to Log	328
Displaying Logs	329
Log Command Example.....	329

Appendix I

Loop Reach..... 330

Testing Conditions.....	330
Band Plan : 998_138_12000(4B).....	331
Band Plan : 998_138_8500(3B).....	331
Band Plan : 997_138_8500(4B).....	331

Appendix J

ASCII Characters..... 332

ASCII Code	332
------------------	-----

Index..... 334

List of Figures

Figure 1 Prestige Home Gateway Applications	39
Figure 2 Prestige Internet Access Application	40
Figure 3 Prestige LAN-to-LAN Application	40
Figure 4 P-861H Front Panel	41
Figure 5 P-861H Rear Panel	42
Figure 6 Password Screen	45
Figure 7 Web Configurator: P-861H Site Map Screen	46
Figure 8 Password	47
Figure 9 Internet Access Wizard Setup: ISP Parameters	49
Figure 10 Internet Connection with PPPoE: Routing	50
Figure 11 Internet Connection with RFC 1483	51
Figure 12 Internet Connection with ENET ENCAP	52
Figure 13 Internet Connection with PPPoA	53
Figure 14 Internet Access Wizard Setup: Third Screen	54
Figure 15 Internet Access Wizard Setup: LAN Configuration	55
Figure 16 Internet Access Wizard Setup: Connection Tests	56
Figure 17 Internet Access Wizard Setup: ISP Parameters	57
Figure 18 Internet Connection with RFC 1483	58
Figure 19 Internet Connection with PPPoA	58
Figure 20 Internet Access Wizard Setup: Third Screen	59
Figure 21 Internet Access Wizard Setup: Connection Tests	59
Figure 22 LAN and WAN IP Addresses	62
Figure 23 LAN Setup	67
Figure 24 PCR, SCR, MCR and MBS in Traffic Shaping	75
Figure 25 Remote Node Configuration Example	76
Figure 26 WAN Remote Nodes	77
Figure 27 WAN Setup (PPPoE)	79
Figure 28 How NAT Works	86
Figure 29 NAT Application With IP Alias	86
Figure 30 Multiple Servers Behind NAT Example	89
Figure 31 NAT Mode	90
Figure 32 Edit SUA/NAT Server Set	91
Figure 33 Address Mapping Rules	92
Figure 34 Address Mapping Rule Edit	93
Figure 35 Dynamic DNS	97
Figure 36 Time and Date	98
Figure 37 Telnet Configuration on a TCP/IP Network	101
Figure 38 SNMP Management Mode	102

Figure 39 Remote Management	104
Figure 40 Configuring UPnP	107
Figure 41 Add/Remove Programs: Windows Setup: Communication	109
Figure 42 Add/Remove Programs: Windows Setup: Communication: Components	109
Figure 43 Network Connections	110
Figure 44 Windows Optional Networking Components Wizard	111
Figure 45 Networking Services	112
Figure 46 Network Connections	113
Figure 47 Internet Connection Properties	114
Figure 48 Internet Connection Properties: Advanced Settings	115
Figure 49 Internet Connection Properties: Advanced Settings: Add	115
Figure 50 System Tray Icon	116
Figure 51 Internet Connection Status	116
Figure 52 Network Connections	117
Figure 53 Network Connections: My Network Places	118
Figure 54 Network Connections: My Network Places: Properties: Example	118
Figure 55 View Logs	121
Figure 56 System Status	123
Figure 57 System Status: Show Statistics	125
Figure 58 DHCP Table	126
Figure 59 Diagnostic: General	127
Figure 60 Diagnostic: DSL Line	128
Figure 61 Firmware Upgrade	129
Figure 62 Network Temporarily Disconnected	129
Figure 63 Error Message	130
Figure 64 Maintenance Configuration	130
Figure 65 Maintenance Backup Configuration	131
Figure 66 Maintenance Restore Configuration	131
Figure 67 Temporarily Disconnected	132
Figure 68 Error Message	132
Figure 69 Maintenance Reset to Factory Defaults	132
Figure 70 Login Screen	135
Figure 71 Menu 23.1 Change Password	138
Figure 72 Menu 1 General Setup	141
Figure 73 Menu 1.1 Configure Dynamic DNS	142
Figure 74 Menu 3 LAN Setup	144
Figure 75 Menu 3.1 LAN Port Filter Setup	144
Figure 76 Menu 3.2 TCP/IP and DHCP Ethernet Setup	145
Figure 77 IP Alias Network Example	149
Figure 78 Menu 3.2 TCP/IP and DHCP Setup	149
Figure 79 Menu 3.2.1 IP Alias Setup	150
Figure 80 Menu 1 General Setup	151
Figure 81 Menu 4 Internet Access Setup	152

Figure 82 Menu 11 Remote Node Setup	155
Figure 83 Menu 11.1 Remote Node Profile	156
Figure 84 Menu 11.3 Remote Node Network Layer Options	158
Figure 85 Sample IP Addresses for a TCP/IP LAN-to-LAN Connection	160
Figure 86 Menu 11.5 Remote Node Filter (RFC 1483 or ENET Encapsulation)	160
Figure 87 Menu 11.5 Remote Node Filter (PPPoA or PPPoE Encapsulation)	161
Figure 88 Menu 11.6 for LLC-based Multiplexing or PPP Encapsulation	161
Figure 89 Menu 11.1 Remote Node Profile	162
Figure 90 Menu 11.8 Advance Setup Options	163
Figure 91 Sample Static Routing Topology	164
Figure 92 Menu 12 Static Route Setup	165
Figure 93 Menu 12.1 IP Static Route Setup	165
Figure 94 Menu 12.1.1 Edit IP Static Route	165
Figure 95 Menu 11.1 Remote Node Profile	169
Figure 96 Menu 11.3 Remote Node Network Layer Options	170
Figure 97 Menu 12.3.1 Edit Bridge Static Route	171
Figure 98 Menu 4 Applying NAT for Internet Access	173
Figure 99 Applying NAT in Menus 4 & 11.3	174
Figure 100 Menu 15 NAT Setup	175
Figure 101 Menu 15.1 Address Mapping Sets	175
Figure 102 Menu 15.1.255 SUA Address Mapping Rules	176
Figure 103 Menu 15.1.1 First Set	177
Figure 104 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set	178
Figure 105 Menu 15.2 NAT Server Setup	179
Figure 106 Menu 15.2.1 NAT Server Setup	179
Figure 107 Multiple Servers Behind NAT Example	180
Figure 108 NAT Example 1	181
Figure 109 Menu 4 Internet Access & NAT Example	181
Figure 110 NAT Example 2	182
Figure 111 Menu 15.2.1 Specifying an Inside Server	182
Figure 112 NAT Example 3	183
Figure 113 Example 3: Menu 11.3	184
Figure 114 Example 3: Menu 15.1.1.1	184
Figure 115 Example 3: Final Menu 15.1.1	185
Figure 116 Example 3: Menu 15.2.1	185
Figure 117 NAT Example 4	186
Figure 118 Example 4: Menu 15.1.1.1 Address Mapping Rule	186
Figure 119 Example 4: Menu 15.1.1 Address Mapping Rules	187
Figure 120 Outgoing Packet Filtering Process	188
Figure 121 Filter Rule Process	189
Figure 122 Menu 21 Filter Set Configuration	190
Figure 123 NetBIOS_WAN Filter Rules Summary	190
Figure 124 NetBIOS_LAN Filter Rules Summary	191

Figure 125 IGMP Filter Rules Summary	191
Figure 126 Menu 21.1.x.1 TCP/IP Filter Rule	193
Figure 127 Executing an IP Filter	195
Figure 128 Menu 21.1.5.1 Generic Filter Rule	196
Figure 129 Protocol and Device Filter Sets	197
Figure 130 Sample Telnet Filter	198
Figure 131 Menu 21.1.6.1 Sample Filter	198
Figure 132 Menu 21.1.6.1 Sample Filter Rules Summary	199
Figure 133 Filtering Ethernet Traffic	200
Figure 134 Filtering Remote Node Traffic	200
Figure 135 SNMP Management Model	202
Figure 136 Menu 22 SNMP Configuration	204
Figure 137 Menu 24 System Maintenance	206
Figure 138 Menu 24.1 System Maintenance : Status	207
Figure 139 Menu 24.2 System Information and Console Port Speed	208
Figure 140 Menu 24.2.1 System Maintenance: Information	209
Figure 141 Menu 24.2.2 System Maintenance : Change Console Port Speed	210
Figure 142 Menu 24.3 System Maintenance: Log and Trace	210
Figure 143 Sample Error and Information Messages	211
Figure 144 Menu 24.4 System Maintenance : Diagnostic	211
Figure 145 Telnet in Menu 24.5	216
Figure 146 FTP Session Example	217
Figure 147 Telnet into Menu 24.6	220
Figure 148 Restore Using FTP Session Example	220
Figure 149 Telnet Into Menu 24.7.1 Upload System Firmware	221
Figure 150 Telnet Into Menu 24.7.2 System Maintenance	222
Figure 151 FTP Session Example of Firmware File Upload	223
Figure 152 Command Mode in Menu 24	226
Figure 153 Valid Commands	226
Figure 154 Menu 24.9 System Maintenance: Call Control	227
Figure 155 Menu 24.9.1 System Maintenance: Budget Management	228
Figure 156 Menu 24 System Maintenance	229
Figure 157 Menu 24.10 System Maintenance: Time and Date Setting	230
Figure 158 Menu 24.11 Remote Management Control	233
Figure 159 Menu 25 IP Routing Policy Setup	237
Figure 160 Menu 25.1 IP Routing Policy Setup	238
Figure 161 Menu 25.1.1 IP Routing Policy	239
Figure 162 Menu 3.2 TCP/IP and DHCP Ethernet Setup	241
Figure 163 Menu 11.3 Remote Node Network Layer Options	242
Figure 164 Example of IP Policy Routing	243
Figure 165 IP Routing Policy Example	243
Figure 166 IP Routing Policy Example	244
Figure 167 Applying IP Policies Example	245

Figure 168 Menu 26 Schedule Setup	246
Figure 169 Menu 26.1 Schedule Set Setup	247
Figure 170 Applying Schedule Set(s) to a Remote Node (PPPoE)	248
Figure 171 CLI Help : Sample Output	251
Figure 172 ip ping	262
Figure 173 ip route status	262
Figure 174 ip arp status	263
Figure 175 VDSL Port Speed Commands Example (Link Down)	267
Figure 176 VDSL Port Speed Commands Example (Link Up)	267
Figure 177 VDSL Clear Port Counter Command Example	268
Figure 178 vdsl pvc list Command Example	269
Figure 179 Reset VDSL Profile	270
Figure 180 VDSL Profile Show Command Example	271
Figure 181 DSL Version Command Example	271
Figure 182 Pop-up Blocker	275
Figure 183 Internet Options	275
Figure 184 Internet Options	276
Figure 185 Pop-up Blocker Settings	277
Figure 186 Internet Options	278
Figure 187 Security Settings - Java Scripting	279
Figure 188 Windows 95/98/Me: Network: Configuration	285
Figure 189 Windows 95/98/Me: TCP/IP Properties: IP Address	286
Figure 190 Windows 95/98/Me: TCP/IP Properties: DNS Configuration	287
Figure 191 Windows XP: Start Menu	288
Figure 192 Windows XP: Control Panel	288
Figure 193 Windows XP: Control Panel: Network Connections: Properties	289
Figure 194 Windows XP: Local Area Connection Properties	289
Figure 195 Windows XP: Internet Protocol (TCP/IP) Properties	290
Figure 196 Windows XP: Advanced TCP/IP Properties	291
Figure 197 Windows XP: Internet Protocol (TCP/IP) Properties	292
Figure 198 Macintosh OS 8/9: Apple Menu	293
Figure 199 Macintosh OS 8/9: TCP/IP	293
Figure 200 Macintosh OS X: Apple Menu	294
Figure 201 Macintosh OS X: Network	295
Figure 202 Option to Enter Debug Mode	304
Figure 203 Boot Module Commands	305
Figure 204 Single-Computer per Router Hardware Configuration	313
Figure 205 Prestige as a PPPoE Client	313
Figure 206 Displaying Log Categories Example	328
Figure 207 Displaying Log Parameters Example	328

List of Tables

Table 1 Front Panel LEDs	41
Table 2 Web Configurator Screens Summary	46
Table 3 Password	47
Table 4 Internet Access Wizard Setup: ISP Parameters	49
Table 5 Internet Connection with PPPoE: Routing	50
Table 6 Internet Connection with RFC 1483	51
Table 7 Internet Connection with ENET ENCAP	52
Table 8 Internet Connection with PPPoA	53
Table 9 Internet Access Wizard Setup: LAN Configuration	55
Table 10 Internet Access Wizard Setup: ISP Parameters	57
Table 11 Internet Connection with PPPoA	58
Table 12 LAN Setup	67
Table 13 WAN Remote Nodes	77
Table 14 WAN Setup	79
Table 15 NAT Definitions	84
Table 16 NAT Mapping Types	87
Table 17 Services and Port Numbers	88
Table 18 NAT Mode	90
Table 19 Edit SUA/NAT Server Set	91
Table 20 Address Mapping Rules	92
Table 21 Address Mapping Rule Edit	94
Table 22 Dynamic DNS	97
Table 23 Time and Date	99
Table 24 SNMP Traps	103
Table 25 Remote Management	104
Table 26 Configuring UPnP	108
Table 27 View Logs	121
Table 28 System Status	123
Table 29 System Status: Show Statistics	125
Table 30 DHCP Table	126
Table 31 Diagnostic: General	127
Table 32 Diagnostic: DSL Line	128
Table 33 Firmware Upgrade	129
Table 34 Maintenance Restore Configuration	131
Table 35 SMT Menus Overview	135
Table 36 Navigating the SMT Interface	136
Table 37 SMT Main Menu	137
Table 38 Main Menu Summary	137

Table 39 Menu 1 General Setup	141
Table 40 Menu 1.1 Configure Dynamic DNS	142
Table 41 DHCP Ethernet Setup	146
Table 42 TCP/IP Ethernet Setup	146
Table 43 Menu 3.2.1 IP Alias Setup	150
Table 44 Menu 4 Internet Access Setup	152
Table 45 Menu 11.1 Remote Node Profile	156
Table 46 Menu 11.3 Remote Node Network Layer Options	158
Table 47 Menu 11.8 Advance Setup Options	163
Table 48 Menu 12.1.1 Edit IP Static Route	166
Table 49 Remote Node Network Layer Options: Bridge Fields	170
Table 50 Menu 12.3.1 Edit Bridge Static Route	171
Table 51 Applying NAT in Menus 4 & 11.3	174
Table 52 SUA Address Mapping Rules	176
Table 53 Menu 15.1.1 First Set	177
Table 54 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set	178
Table 55 Abbreviations Used in the Filter Rules Summary Menu	191
Table 56 Rule Abbreviations Used	192
Table 57 Menu 21.1.x.1 TCP/IP Filter Rule	193
Table 58 Menu 21.1.5.1 Generic Filter Rule	196
Table 59 Filter Sets Table	199
Table 60 Menu 22 SNMP Configuration	204
Table 61 SNMP Traps	204
Table 62 Ports and Permanent Virtual Circuits	205
Table 63 Menu 24.1 System Maintenance: Status	207
Table 64 Menu 24.2.1 System Maintenance: Information	209
Table 65 Menu 24.4 System Maintenance Menu: Diagnostic	212
Table 66 Filename Conventions	215
Table 67 General Commands for GUI-based FTP Clients	217
Table 68 General Commands for GUI-based TFTP Clients	219
Table 69 Menu 24.9.1 System Maintenance: Budget Management	228
Table 70 Menu 24.10 System Maintenance: Time and Date Setting	230
Table 71 Menu 24.11 Remote Management Control	233
Table 72 Menu 25.1 IP Routing Policy Setup	238
Table 73 Menu 25.1.1 IP Routing Policy	239
Table 74 Menu 26.1 Schedule Set Setup	247
Table 75 sys Command Summary	252
Table 76 sys version	256
Table 77 sys logs errlog disp	256
Table 78 ether Command Summary	258
Table 79 IP Command Summary	258
Table 80 WAN Command Summary	263
Table 81 vdsl Command Summary	264

Table 82 VDSL Default Values	265
Table 83 Service Characteristic	266
Table 84 VDSL Port Speed Commands	268
Table 85 PVC List	269
Table 86 VDSL Mode and Frequency Ranges	270
Table 87 Troubleshooting Starting Up Your Prestige	272
Table 88 Troubleshooting the LAN	272
Table 89 Troubleshooting the WAN	273
Table 90 Troubleshooting Accessing the Prestige	274
Table 91 Device	280
Table 92 Firmware	281
Table 93 Classes of IP Addresses	296
Table 94 Allowed IP Address Range By Class	297
Table 95 "Natural" Masks	297
Table 96 Alternative Subnet Mask Notation	298
Table 97 Two Subnets Example	298
Table 98 Subnet 1	299
Table 99 Subnet 2	299
Table 100 Subnet 1	300
Table 101 Subnet 2	300
Table 102 Subnet 3	300
Table 103 Subnet 4	301
Table 104 Eight Subnets	301
Table 105 Class C Subnet Planning	301
Table 106 Class B Subnet Planning	302
Table 107 NetBIOS Filter Default Settings	307
Table 108 System Maintenance Logs	314
Table 109 System Error Logs	315
Table 110 Access Control Logs	315
Table 111 TCP Reset Logs	316
Table 112 Packet Filter Logs	316
Table 113 ICMP Logs	317
Table 114 CDR Logs	317
Table 115 PPP Logs	317
Table 116 UPnP Logs	318
Table 117 Content Filtering Logs	318
Table 118 Attack Logs	319
Table 119 IPsec Logs	320
Table 120 IKE Logs	320
Table 121 PKI Logs	323
Table 122 Certificate Path Verification Failure Reason Codes	324
Table 123 802.1X Logs	325
Table 124 ACL Setting Notes	326

Table 125 ICMP Notes	326
Table 126 Syslog Logs	327
Table 127 RFC-2408 ISAKMP Payload Types	327
Table 128	
Band Plan : 998_138_12000(4B)	331
Table 129	
Band Plan : 998_138_8500(3B)	331
Table 130 Band Plan : 997_138_8500(4B)	331

Preface

Congratulations on your purchase of the Prestige 861H Series VDSL Router/Bridge.

The Prestige is a high-performance, cost-effective VDSL (Very High Speed Digital Subscriber Line) modem with a built-in four-port switch. Your Prestige can access the Internet via a telephone line. See the following section for more background information on DSL.

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 **Start, (All) Programs, Accessories** and then **Command Prompt**” means first click **Start**, then point your mouse pointer to **Programs**, point your mouse pointer to **Accessories** and then click **Command Prompt**.
- For brevity’s sake, we will use “e.g.,” as a shorthand for “for instance”, and “i.e.,” for “that is” or “in other words” throughout this manual.
- The Prestige 861H Series may be referred to as simply the “Prestige” in this User’s guide.

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.

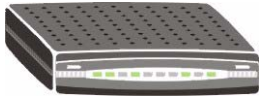








- ZyXEL Glossary and Web Site

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 

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 VDSL?

VDSL is the next generation of DSL technology that offers a much higher bandwidth than most DSL technologies. VDSL is the only feasible solution for bandwidth-demanding and video-rich applications such as video-on-demand, high definition television, tele-medicine, surveillance systems and other switched video services. VDSL supports both symmetric and asymmetric applications using existing copper wire (telephone wire) and therefore saving the cost of using traditional T1/E1 service for small/medium-sized business and residential users.

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 can be used for high-speed Internet access through a VDSL connection over the telephone line. The Prestige supports data transmission speeds of 60 Mbps downstream and 34 Mbps upstream. Its 10/100M auto-negotiating LAN interface enables fast data transfer of either 10Mbps or 100Mbps in either half-duplex or full-duplex mode depending on your Ethernet network.

Note: The standard your ISP supports determines the maximum upstream and downstream speeds attainable. Actual speeds attained depend on the copper category of your telephone wires, distance from the central office, the type of DSL service you subscribe to, noise, etc.

By integrating DSL and NAT, the Prestige provides ease of installation and Internet access. In the Prestige product name, “H” denotes an integrated 4-port switch (hub). The “Series” denotes different band plans G1 and G2. G1 represents a VDSL band plan specific to North America, whereas G2 represents a VDSL band plan specific to Europe.

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

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

1.1.1 Features of the Prestige

The following sections describe the features of the Prestige.

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

Built-in Switch

The 10/100 Mbps auto-negotiating Ethernet ports allow the Prestige to detect the speed of incoming transmissions and adjust appropriately without manual intervention. It allows data transfer of either 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode depending on your Ethernet network. The ports are also auto-crossover (MDI/MDI-X) meaning they automatically adjust to either a crossover or straight-through Ethernet cable.

High Speed Internet Access

The Prestige supports transmission speeds of up to 60 Mbps downstream and 34 Mbps upstream. Actual speeds attained depend on ISP DSLAM environment, and how your prestige is configured.

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 VDSL. 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.

Multiple PVC (Permanent Virtual Circuits) Support

Your Prestige supports up to 10 PVCs including UBR, CBR and VBR.

Multiplexing

The Prestige supports LLC-based multiplexing only.

Networking Compatibility

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

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.

1.1.2 Applications for the Prestige

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

1.1.2.1 Home Gateway Applications

Some applications for your Prestige are explained below. Other applications include Video, Voice over IP (VoIP), Internet Group Multicast Protocol (IGMP) and Data, see sections on Internet Access, Internet Single User Account and LAN to LAN Application.

Middleware

This is software that provides a way for two systems to exchange information or connect with one another even though they have different interfaces. For example, you can use middleware to have a VDSL based bridge communicate with a Set Top Box.

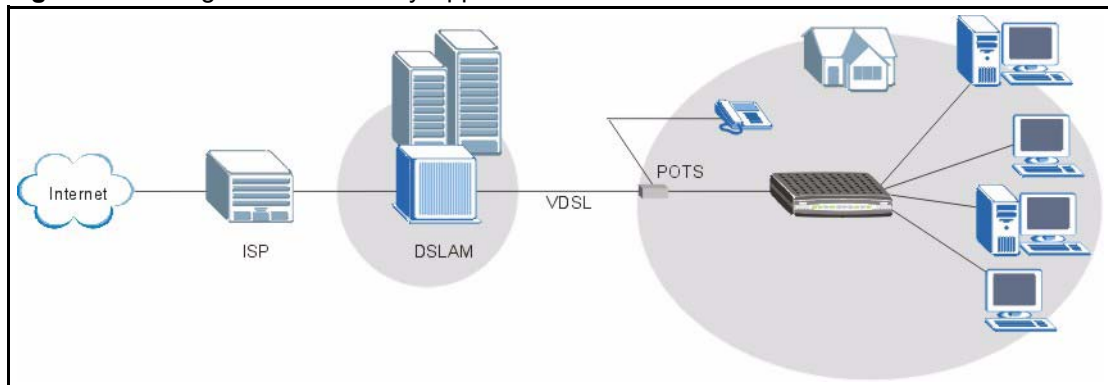
Set Top Box

A Set Top Box (STB) is a device that provides services such as High Definition Television (HDTV), content decryption, personal video recorder, electronic programming guide, VoIP, Web browsing and interactive television features.

Home Gateway

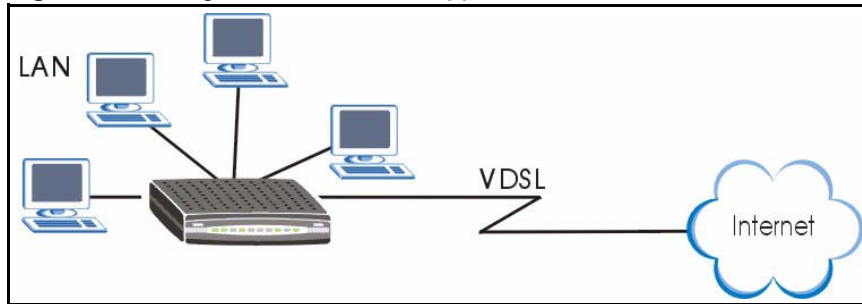
A Home Gateway is an intelligent network device located in the home. Users can access the home gateway device from a remote location. Examples of home gateways include computers, routers or modems, LAN access points, WLAN access points, and digital Set Top Boxes.

Figure 1 Prestige Home Gateway Applications



Internet Access

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

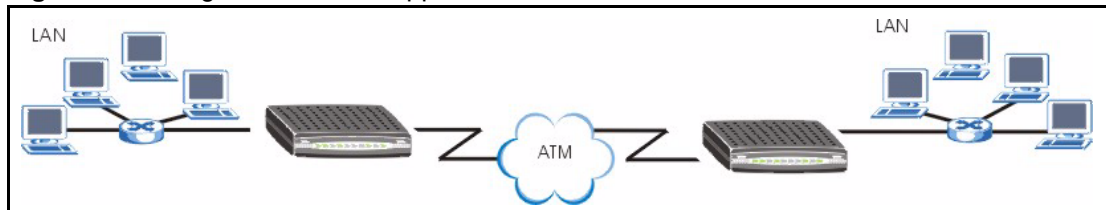
Figure 2 Prestige Internet Access Application

Internet Single User Account

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

LAN to LAN Application

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

Figure 3 Prestige LAN-to-LAN Application

1.1.3 Front Panel LEDs

Figure 4 P-861H Front Panel



The following table describes the LEDs.

Table 1 Front Panel LEDs

	COLOR	STATUS	DESCRIPTION
SYS	Green	On	The Prestige is receiving power and functioning properly.
		Blinking	The Prestige is rebooting.
	None	Off	The system is not ready or has malfunctioned.
LAN 1-4	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.
None	Off	The LAN is not connected.	
VDSL	Green	On	The Prestige is connected to a DSL line.
		Slow Blinking	The Prestige is initializing the DSL line.
		Fast Blinking	Data is being transmitted or received.
	None	Off	The DSL link is down.

1.1.4 Rear Panel

Figure 5 P-861H Rear Panel



1.1.4.1 VDSL Port

Connect the Prestige directly to the wall jack using a telephone wire (RJ-11 connector).

1.1.4.2 Ground (Available on some models)

Connect a grounding cable to the ground connector to protect your device from electrical surges.

1.1.4.3 LAN 1 ~ 4

The Prestige has four 10/100Mbps auto-negotiating, auto-crossover Ethernet ports. The LAN interface is auto-crossover, so you may use a crossover cable or a straight-through Ethernet cable to connect your Prestige to a computer/external hub.

1.1.4.4 Console Port

You can configure the Prestige via a terminal emulator software on a computer that is connected to the Prestige through the console port. Connect the male end of the console cable to the console port of the Prestige and the female end to a serial port (COM1, COM2 or other COM port) of your computer.

1.1.4.5 Reset Button

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".

1.1.4.5.1 Using the Reset Button

- 1 Make sure the **SYS** LED is on (not blinking).
- 2 Press the **RESET** button for five seconds or until the **SYS** LED begins to blink and then release it. When the **SYS** LED begins to blink, the defaults have been restored and the Prestige restarts.

1.1.4.6 Power Port

Connect the power adaptor to the port labeled **POWER** on the rear panel of your Prestige. Push in the power button to turn on the Prestige.

Note: To avoid damage to the Prestige, make sure you use the supplied power adaptor.

1.1.4.7 Turning On Your Prestige

You can turn on your Prestige by pushing in the power button.

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

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 an 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).

See the Troubleshooting chapter to see how to make sure these functions are allowed in Internet Explorer.

2.1.1 Accessing the Prestige Web Configurator

- 1** Make sure your Prestige hardware is properly connected (refer to the Quick Start Guide).
- 2** Prepare your computer/computer network to connect to the Prestige (refer to the Quick Start Guide).
- 3** Launch your web browser.
- 4** Type "192.168.1.1" as the URL.
- 5** An **Enter Network Password** window displays. Enter the user name ("admin" is the default), password ("1234" is the default) and click **OK**.

Figure 6 Password Screen



6 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 Navigating the Prestige Web Configurator

The following summarizes how to navigate the web configurator from the **SITE MAP** screen.

- 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 7 Web Configurator: P-861H Site Map Screen



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

Table 2 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.
Advanced Setup		
Password		Use this screen to change your password.
LAN		Use this screen to configure LAN DHCP and TCP/IP settings.
WAN	WAN Setup	Use this screen to change the Prestige's WAN remote node settings.
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.
Remote Management		Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet/FTP/Web/SNMP/ICMP to manage the Prestige.
UPnP		Use this screen to enable UPnP on the Prestige.
Logs	View Log	Use this screen to view the logs for the categories that you selected.
Maintenance		
System Status		This screen contains administrative and system-related information.
DHCP Table		This screen displays DHCP (Dynamic Host Configuration Protocol) related information and is READ-ONLY.
Diagnostic	General	These screens display information to help you identify problems with the Prestige general connection.

Table 2 Web Configurator Screens Summary (continued)

LINK	SUB-LINK	FUNCTION
	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
Configuration		Use this screen to backup and restore the configuration or reset the factory defaults to your Prestige.
LOGOUT		Click Logout to exit the web configurator.

2.2 Password

It is highly recommended that you periodically change the password for accessing the Prestige. Click **Password** in the **Site Map** screen to display the screen as shown next.

Figure 8 Password

The following table describes the fields in this screen.

Table 3 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 9 Internet Access Wizard Setup: ISP Parameters

The following table describes the fields in this screen.

Table 4 Internet Access Wizard Setup: ISP Parameters

LABEL	DESCRIPTION
Mode	From the Mode drop-down list box, select Routing if your ISP allows multiple computers to share an Internet account. Otherwise select Bridge and proceed to section 3.1.1.2 .
Encapsulation	Select the encapsulation type your ISP uses from the Encapsulation drop-down list box. Select PPPoA , RFC 1483 , ENET ENCAP or PPPoE .
Multiplex	The multiplexing method used by your ISP is LLC-based.
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit. Refer to the appendix for more information.
VPI	Enter the VPI assigned to you. This field may already be configured.
VCI	Enter the VCI assigned to you. This field may already be configured.
Next	Click this button to go to the next wizard screen. The next wizard screen you see depends on what protocol you chose above. Click on the protocol link to see the next wizard screen for that protocol.

3.1.1.1 Internet Access Wizard Setup : Routing

The ISP Parameters for Internet Access screen varies depending on what mode and encapsulation type you use. Configure the fields and click **Next** to continue.

Figure 10 Internet Connection with PPPoE: Routing

Wizard Setup - ISP Parameters for Internet Access

Service Name

User Name

Password

IP Address

Obtain an IP Address Automatically

Static IP Address

Connection

Connect on Demand: Max Idle Timeout sec

Nailed-Up Connection

Network Address Translation

▼

PPPoE Pass Through

▼

The following table describes the fields in this screen.

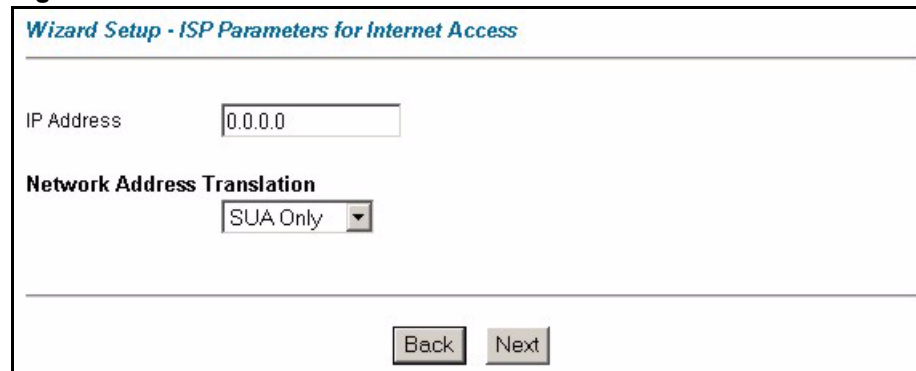
Table 5 Internet Connection with PPPoE: Routing

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

Table 5 Internet Connection with PPPoE: Routing (continued)

LABEL	DESCRIPTION
PPPoE Pass Through	Select Yes from the PPPoE Pass Through drop-down list box 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.
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 RFC 1483



The following table describes the fields in this screen.

Table 6 Internet Connection with RFC 1483

	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.
Back	Click Back to go back to the first wizard screen.
Next	Click Next to continue to the next wizard screen.

Figure 12 Internet Connection with ENET ENCAP

The following table describes the fields in this screen.

Table 7 Internet Connection with ENET ENCAP

	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-down 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 13 Internet Connection with PPPoA

Wizard Setup - ISP Parameters for Internet Access

User Name:

Password:

IP Address

Obtain an IP Address Automatically

Static IP Address

Connection

Connect on Demand: Max Idle Timeout sec

Nailed-Up Connection

Network Address Translation

▾

The following table describes the fields in this screen.

Table 8 Internet Connection with PPPoA

	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-down 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.

- 2 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 final wizard screen.

Figure 14 Internet Access Wizard Setup: Third Screen

Wizard Setup - ISP Parameters for Internet Access

WAN Information:
Mode: **Routing**
Encapsulation: **PPPoE**
Multiplexing: **LLC**
VPI/VCI: **8/35**
Service Name :
User Name : **test**
Password : *********
IP Address : **0.0.0.0**
Network Address Translation: **SUA Only**
Connect on Demand: **Max Idle Timeout 0 sec.**

LAN Information:
IP Address: **192.168.1.1**
IP Mask: **255.255.255.0**
DHCP: **ON**
Client IP Pool Starting Address: **192.168.1.33**
Size of Client IP Pool: **32**

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

Figure 15 Internet Access Wizard Setup: LAN Configuration

Wizard Setup - ISP Parameters for Internet Access

LAN IP Address: 192.168.1.1

LAN Subnet Mask: 255.255.255.0

DHCP

DHCP Server: ON

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

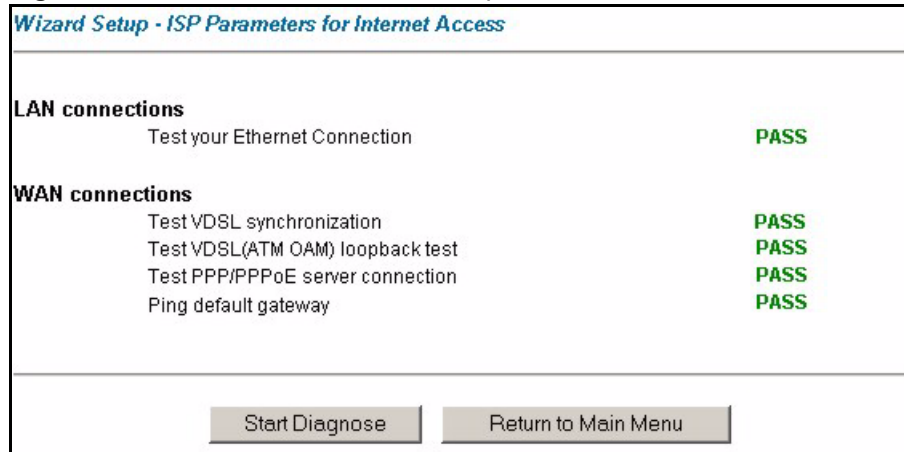
Back Finish

The following table describes the fields in this screen.

Table 9 Internet Access Wizard Setup: LAN Configuration

	DESCRIPTION
LAN IP Address	Enter the IP address of your Prestige in dotted decimal notation, for example, 192.168.1.1 (factory default). Note: 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.

- 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 16 Internet Access Wizard Setup: Connection Tests

- 4 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.

3.1.1.2 Internet Access Wizard Setup : Bridge

If you want to set up your Prestige in bridge mode, proceed from this section.

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

Figure 17 Internet Access Wizard Setup: ISP Parameters

Wizard Setup - ISP Parameters for Internet Access

Mode

Encapsulation

Multiplex

Virtual Circuit ID

VPI

VCI

The following table describes the fields in this screen.

Table 10 Internet Access Wizard Setup: ISP Parameters

LABEL	DESCRIPTION
Mode	From the Mode drop-down list box, 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. Select either PPPoA or RFC 1483 .
Multiplex	The multiplexing method used by your ISP is 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.

If you select **PPPoA** encapsulation in the previous screen, proceed to table 4.16. If you select **RFC 1483** encapsulation in the previous screen, verify the settings in the screen shown next. Click **Save Settings** to save the configuration and test the connection to the computer(s) connected to the LAN ports.

Figure 18 Internet Connection with RFC 1483

Wizard Setup - ISP Parameters for Internet Access

WAN Information:
 Mode: **Bridge**
 Encapsulation: **RFC 1483**
 Multiplexing: **LLC**
 VPI/VCI: **8/35**

LAN Information:
 IP Address: **192.168.1.1**
 IP Mask: **255.255.255.0**
 DHCP: **OFF**

Save Settings

Select **PPPoA** encapsulation in the screen as displayed in [Figure 17 on page 57](#). Configure the fields and click **Next** to continue. Type a user name and password assigned by your ISP in the following screen.

Figure 19 Internet Connection with PPPoA

Wizard Setup - ISP Parameters for Internet Access

User Name

Password

Connection

Connect on Demand: Max Idle Timeout sec

Nailed-Up Connection

Back Next

The following table describes the fields in this screen.

Table 11 Internet Connection with PPPoA

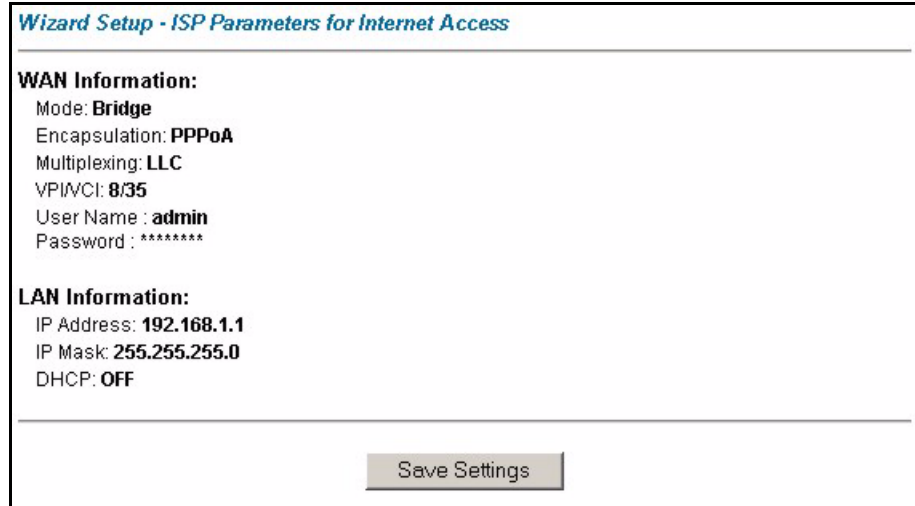
LABEL	DESCRIPTION
User Name	Enter the login name that your ISP gives you.
Password	Enter the password associated with the user name above.
Connection	<p>Select Connect on Demand when you don't want the connection up all the time and specify an idle time-out (in seconds) in the Max. Idle Timeout field. The default setting selects Connection on Demand with 0 as the idle time-out, which means the Internet session will not timeout.</p> <p>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.</p> <p>The schedule rule(s) in SMT menu 26 has priority over your Connection settings.</p>

Table 11 Internet Connection with PPPoA (continued)

LABEL	DESCRIPTION
Back	Click Back to go back to the first wizard screen.
Next	Click Next to continue to the next wizard screen.

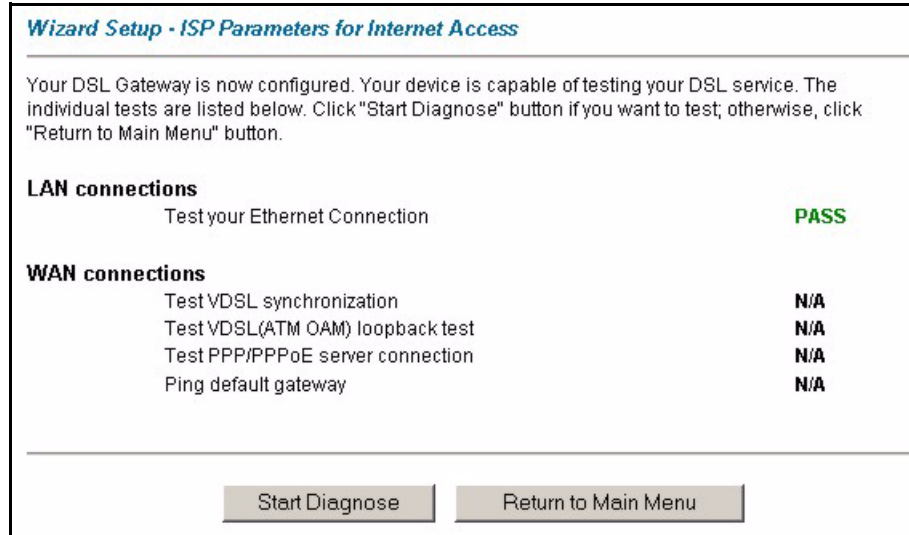
Verify the settings in the screen shown next. Click **Save Settings** to save the configuration and skip to the final wizard screen.

Figure 20 Internet Access Wizard Setup: Third Screen



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 21 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 and set up static DHCP.

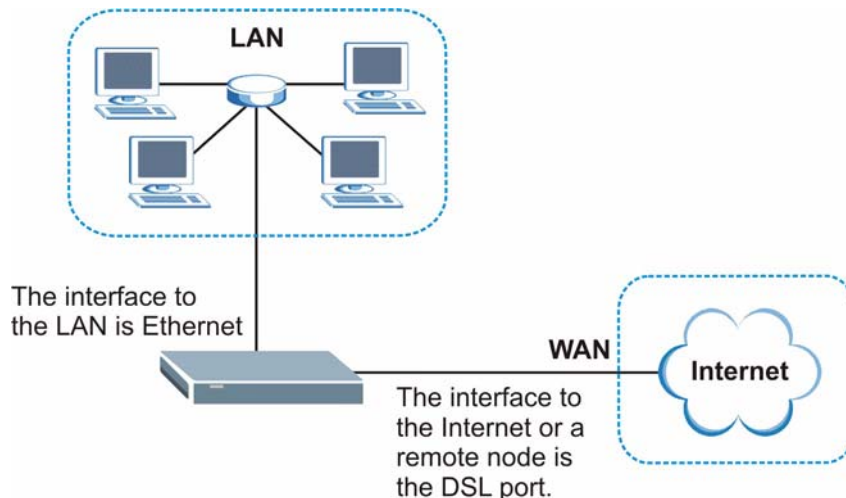
4.1 LAN Overview

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.

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 22 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 Configuring LAN

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

Figure 23 LAN Setup

The following table describes the fields in this screen.

Table 12 LAN Setup

LABEL	DESCRIPTION
DHCP	
DHCP	<p>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.</p> <p>If set to None, the DHCP server will be disabled.</p> <p>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.</p> <p>Note: The DHCP requests are forwarded to the middleware remote node of the Prestige.</p> <p>When DHCP is used, the following items need to be set:</p>
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.

Table 12 LAN Setup (continued)

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

CHAPTER 5

WAN Setup

This chapter describes how to configure WAN settings.

5.1 WAN Overview

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

5.1.1 Encapsulation

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

5.1.1.1 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.

5.1.1.2 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 VDSL 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.

5.1.1.3 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.

5.1.1.4 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.

5.1.2 LLC-based Multiplexing

Multiplexing is used to identify what protocols the virtual circuit (VC) is carrying. LLC-based multiplexing uses a single VC to carry 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.

5.1.3 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.

5.1.4 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.

5.1.4.1 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.

5.1.4.2 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.

5.1.4.3 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.

5.1.5 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

5.1.6 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.

5.2 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.

5.3 Traffic Shaping

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

5.3.1 ATM Traffic Classes

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

5.3.1.1 Constant Bit Rate (CBR)

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

5.3.1.2 Variable Bit Rate (VBR)

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

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

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

5.3.1.3 Unspecified Bit Rate (UBR)

The Unspecified Bit Rate (UBR) ATM traffic class is used for bursty data transfers. UBR doesn't guarantee any bandwidth and only delivers traffic when the network has spare bandwidth. End devices using UBR get feedback from the network and can use flow-control to dynamically adjust transmission rates.

UBR uses RM (Resource Management) cells to send feedback information from the connection's destination and/or intervening network switches to the connection's source. A source generates forward RM cells, which the destination returns to the source as backward RM cells. Along the way, network switches can adjust the fields in the RM cells depending on network conditions. Number of Resource Management (NRM) is the maximum number of cells a source may send for each forward Resource Management cell.

5.3.2 Traffic Parameters

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

5.3.2.1 Peak Cell Rate (PCR)

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

5.3.2.2 Sustained Cell Rate (SCR)

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

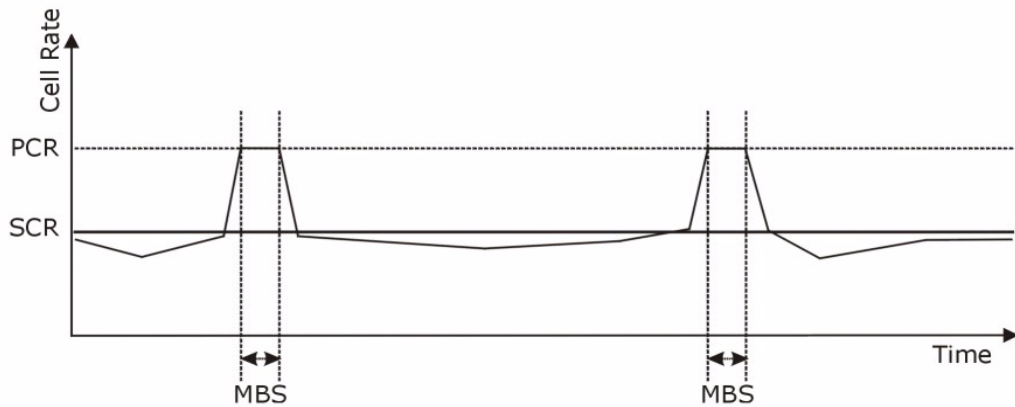
5.3.2.3 Maximum Burst Size (MBS)

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

5.3.2.4 Minimum Cell Rate (MCR)

Minimum Cell Rate (MCR) is the minimum rate at which the sender can send cells.

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

Figure 24 PCR, SCR, MCR and MBS in Traffic Shaping

5.3.3 Cell Delay Variation Tolerance (CDVT)

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

5.3.4 Burst Tolerance (BT)

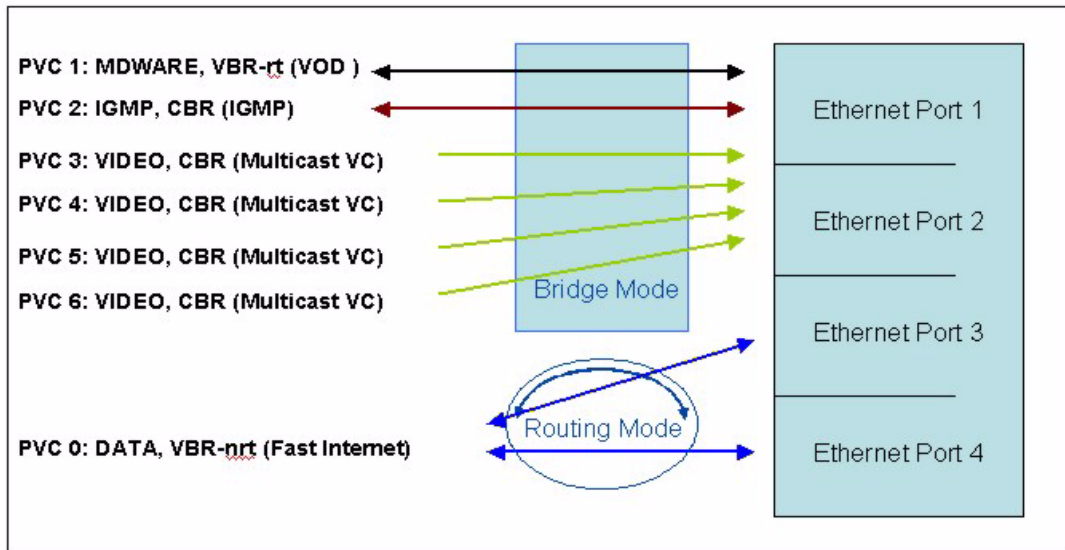
Burst Tolerance (BT) is the maximum number of cells that the port is guaranteed to handle without any discards. BT controls the time scale over which the SCR is enforced. BT is used to determine if a cell arrived too early in relation to SCR. Use this formula to calculate BT: $(MBS - 1) \times (1 / SCR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

5.4 Permanent Virtual Circuit

Permanent Virtual Circuit (PVC) is a logical point-to-point circuit between customer sites. PVC's are low-delay circuits because routing decisions do not need to be made along the way. Permanent means that the circuit is preprogrammed by the carrier as a path through the network. It does not need to be set up or torn down for each session.

5.4.1 PVC Example

In the following example, a fast Internet connection uses Ethernet ports three and four to communicate through PVC 0. The other PVCs use Ethernet ports one and two to communicate with a set top box or home gateway. This is the default remote node setup.

Figure 25 Remote Node Configuration Example

See section [5.7](#) for more information on how to set up the WAN remote nodes.

5.5 Remote Node Screen

To view your Prestige's WAN remote node settings, click **WAN**. The **Remote Node** screen allows you to select a node number, so that you can configure the **WAN Setup** screen.

Figure 26 WAN Remote Nodes

Remote Node													
Num	Name	Active	Encap	VPI	VCI	QoS	PCR	CDVT	SCR	MBS	Application	Ether	IP
1	MyISP	Yes	PPPoA	8	35	VBR-nRT	4830	1	604	32	Data	3,4	IP
2	MDWARE	Yes	1483	0	32	VBR-RT	360	1	360	32	Middleware	1,2	BDG
3	IGMP	Yes	1483	1	32	CBR	360	1	N/A	N/A	IGMP	1,2	BDG
4	VIDEO-1	Yes	1483	1	33	CBR	N/A	N/A	N/A	N/A	Video	1,2	BDG
5	VIDEO-2	Yes	1483	1	34	CBR	N/A	N/A	N/A	N/A	Video	1,2	BDG
6	VIDEO-3	Yes	1483	1	35	CBR	N/A	N/A	N/A	N/A	Video	1,2	BDG
7	VIDEO-4	Yes	1483	1	36	CBR	N/A	N/A	N/A	N/A	Video	1,2	BDG
8	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
9	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
10	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

The following table describes the fields in this screen.

Table 13 WAN Remote Nodes

LABEL	DESCRIPTION
Num	Select a remote node number to display the WAN Setup configuration screen.
Name	This field displays the name of the remote node, e.g., MDWARE. This information is for identification purposes only.
Active	This field displays the status of a remote node
Encap	This field displays the method of encapsulation used by your ISP. Choices vary depending on the operating mode of each remote node. If the operating mode is set as Bridge , this field displays either PPPoA or RFC 1483 . If the operating mode is set as Routing , this field displays PPPoA , RFC 1483 , ENET ENCAP or PPPoE .
VPI	This field displays the VPI assigned to you. The valid range for the VPI is 0 to 255.
VCI	This field displays the VCI assigned to you. The valid range for the VCI is 32 to 65535 (0 to 31 is reserved for local management of ATM traffic).
QoS	This field displays the ATM QoS Type. CBR (Constant Bit Rate) specifies a fixed (always-on) bandwidth for voice or data traffic. UBR (Unspecified Bit Rate) is used for applications that are non-time sensitive, such as e-mail. VBR-RT (Real Time Variable Bit Rate) or VBR-nRT (non Real Time Variable Bit Rate) is used with bursty traffic and bandwidth sharing with other applications.
PCR	This field displays the Peak Cell Rate (PCR). This is the maximum rate at which the sender can send cells.
CDVT	This field displays the accepted tolerance of the difference between a cell's transfer delay and the expected transfer delay.
SCR	This field displays the Sustain Cell Rate (SCR). The SCR sets the average cell rate (long-term) that can be transmitted.

Table 13 WAN Remote Nodes

LABEL	DESCRIPTION
MBS	This field displays the Maximum Burst Size (MBS). MBS refers to the maximum number of cells that can be sent at the peak rate.
Application	This field displays the application type that the remote node uses.
Ether	This field displays the Ethernet port(s) that the remote node uses. If there is no application assigned to an Ethernet port, this field displays Null .
IP	This field displays whether the remote node is configured as a router (IP) or as a bridge (BDG).

5.6 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 disabled when:

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

5.7 Configuring WAN Setup

To change your Prestige's WAN remote node settings, click **WAN** and select a node number in the **Remote Node** screen. The **WAN Setup** screen differs by the encapsulation you select.

Figure 27 WAN Setup (PPPoE)

WAN - WAN Setup

Name

Active Yes No

Mode

Encapsulation

Multiplex

Virtual Circuit ID

VPI

VCI

ATM QoS Type

Cell Rate

Peak Cell Rate cell/sec

Cell Delay Variation Tolerance cell

Sustain Cell Rate cell/sec

Maximum Burst Size cell

Application

Ethernet Port 1 2 3 4

Login Information

Service Name

User Name

Password

IP Address

Obtain an IP Address Automatically

Static IP Address

IP Address

Connection

Nailed-Up Connection

Connect on Demand

Max Idle Timeout sec

PPPoE Pass Through

PPPoE + PPPoE_Client_PC

The following table describes the fields in this screen.

Table 14 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 14 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	This field displays the method of multiplexing used by your ISP.
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 (Constant Bit Rate) to specify fixed (always-on) bandwidth for voice or data traffic. Select UBR (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select VBR-RT (Real Time Variable Bit Rate) or VBR-nRT (non Real Time 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.
Cell Delay Variation Tolerance	This field displays the accepted tolerance of the difference between a cell's transfer delay and the expected transfer delay.
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 100.
Application	Select an application that you want to apply to this remote node from the drop-down list box. The application types are: Middleware , Video , IGMP , Data , VoIP and Home Gateway . The defaults available will depend on which services you subscribe to. For example, you can subscribe to request video services in which case you can use Middleware , Video and IGMP for remote node applications. Select Middleware to have the remote node connect to a device through another intermediary device, for example, to connect to a set-top box. Select Video to have the remote node connect to downstream video applications, for example, IP Video on Demand. Select IGMP (Internet Group Multicast Protocol) to have the Prestige establish membership in a multicast group; it is not used to carry user data. Select Data if you only have an Internet access subscription from your ISP and no other services. Select VoIP to have the remote node use real-time applications such as Voice-over-IP. Select Home Gateway to have the remote node use network devices located in your home, for example, security surveillance, remote meter reading and home appliances (such as fridges or air-conditioners).

Table 14 WAN Setup (continued)

LABEL	DESCRIPTION
Ethernet Port	<p>Note: To assign all Ethernet ports to a service, you must first disable the remote nodes of the services you do not want to use. Select No in the Active field to do this.</p> <p>If you select Middleware, VoIP or Home Gateway from the Application field, you can choose which Ethernet port(s) you want assign to an application. Video and IGMP use the same ports assigned to use the Middleware application.</p> <p>Data applications automatically use the port(s) that you have NOT selected to use with Middleware, VoIP or Home Gateway applications.</p>
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	<p>This option is available if you select Routing in the Mode field.</p> <p>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.</p> <p>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.</p>
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.
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)	<p>This field is available when you select PPPoE encapsulation.</p> <p>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.</p> <p>PPPoE pass through is an alternative to NAT for application where NAT is not appropriate.</p> <p>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.</p>
Subnet Mask (ENET ENCAP encapsulation only)	<p>Enter a subnet mask in dotted decimal notation.</p> <p>Refer to the appendices to calculate a subnet mask If you are implementing subnetting.</p>

Table 14 WAN Setup (continued)

LABEL	DESCRIPTION
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
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 6

Network Address Translation (NAT) Screens

This chapter discusses how to configure NAT on the Prestige.

6.1 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.

6.1.1 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 15 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.

6.1.2 What NAT Does

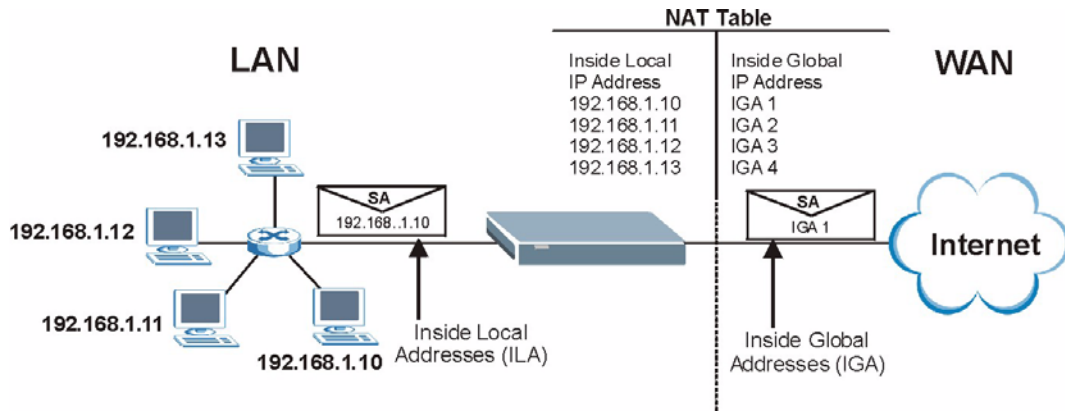
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) 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 16 on page 87](#)), 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)*.

6.1.3 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.

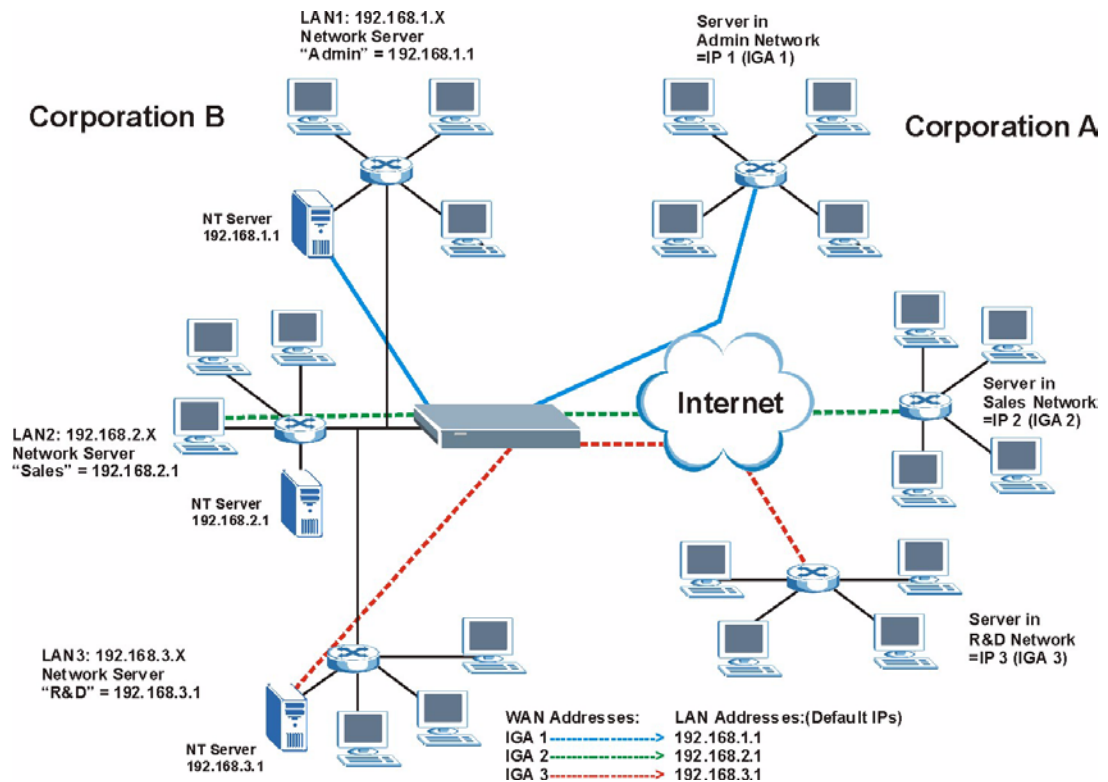
Figure 28 How NAT Works



6.1.4 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 29 NAT Application With IP Alias



6.1.5 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 16 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

6.2 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 16 on page 87](#).

- 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.

6.3 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.

6.3.1 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.

6.3.2 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 17 Services and Port Numbers

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

Table 17 Services and Port Numbers (continued)

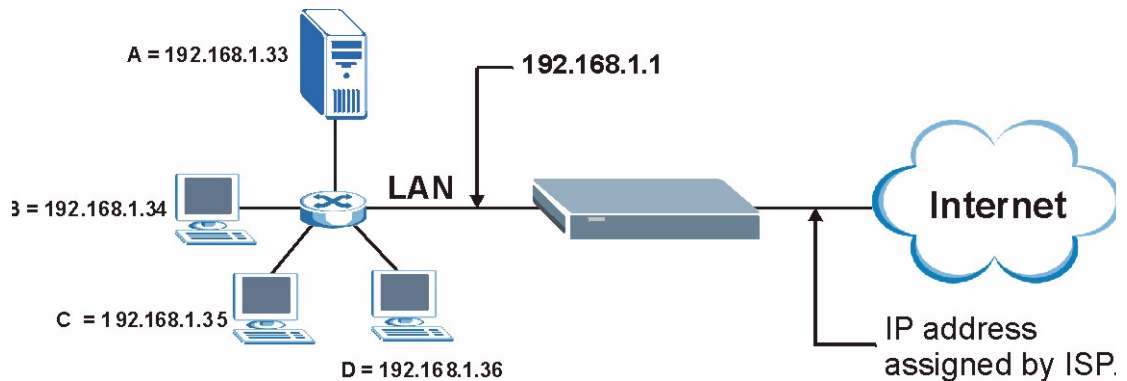
SERVICES	PORT NUMBER
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point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

6.3.3 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 30 Multiple Servers Behind NAT Example



6.4 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 31 NAT Mode

NAT - Mode

Network Address Translation

None

SUA Only [Edit Details](#)

Full Feature [Edit Details](#)

The following table describes the labels in this screen.

Table 18 NAT Mode

	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.

6.5 Configuring SUA Server

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

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

Refer to [Table 17 on page 88](#) for port numbers commonly used for particular services.

Figure 32 Edit SUA/NAT Server Set

NAT - Edit SUA/NAT Server Set

	Start Port No.	End Port No.	IP Address
1	All ports	All ports	0.0.0.0
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

Save Cancel

The following table describes the fields in this screen.

Table 19 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.

6.6 Configuring Address Mapping

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

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

Figure 33 Address Mapping Rules

	Local Start IP	Local End IP	Global Start IP	Global End IP	Type
Rule 1	-
Rule 2	-
Rule 3	-
Rule 4	-
Rule 5	-
Rule 6	-
Rule 7	-
Rule 8	-
Rule 9	-
Rule 10	-

Back

The following table describes the fields in this screen.

Table 20 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 20 Address Mapping Rules (continued)

LABEL	DESCRIPTION
Type	<p>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.</p> <p>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.</p> <p>M-M Ov (Overload): Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses.</p> <p>MM No (No Overload): Many-to-Many No Overload mode maps each local IP address to unique global IP addresses.</p> <p>Server: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.</p>
Back	Click Back to return to the NAT Mode screen.

6.7 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 34 Address Mapping Rule Edit

The screenshot shows a web-based configuration interface titled "NAT - Edit Address Mapping Rule 1". It contains several input fields and a dropdown menu:

- Type:** A dropdown menu currently set to "One-to-One".
- Local Start IP:** A text input field containing "0.0.0.0".
- Local End IP:** A text input field containing "N/A".
- Global Start IP:** A text input field containing "0.0.0.0".
- Global End IP:** A text input field containing "N/A".
- Server Mapping Set:** A dropdown menu currently set to "N/A", with a blue link "Edit Details" next to it.

At the bottom of the form, there are three buttons: "Apply", "Cancel", and "Delete".

The following table describes the fields in this screen.

Table 21 Address Mapping Rule Edit

LABEL	DESCRIPTION
Type	Choose the port mapping type from one of the following. <ul style="list-style-type: none"> • One-to-One: One-to-One mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-one NAT mapping type. • Many-to-One: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only. • Many-to-Many Overload: Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. • Many-to-Many No Overload: Many-to-Many No Overload mode maps each local IP address to unique global IP addresses. • Server: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Local Start IP	This is the starting local IP address (ILA). Local IP addresses are N/A for Server port mapping.
Local End IP	This is the end local IP address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address. This field is N/A for One-to-One and Server mapping types.
Global Start IP	This is the starting global IP address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP.
Global End IP	This is the ending global IP address (IGA). This field is N/A for One-to-One , Many-to-One and Server mapping types.
Server Mapping Set	Only available when Type is set to Server . Select a number from the drop-down menu to choose a server set from the NAT - Address Mapping Rules screen.
Edit Details	Click this link to go to the NAT - Edit SUA/NAT Server Set screen to edit a server set that you have selected in the Server Mapping Set field.
Apply	Click Apply to save your changes back to the Prestige.
Cancel	Click Cancel to return to the previously saved settings.
Delete	Click Delete to exit this screen without saving.

CHAPTER 7

Dynamic DNS Setup

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

7.1 Dynamic DNS

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

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

7.1.1 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.

7.2 Configuring Dynamic DNS

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

Figure 35 Dynamic DNS

Dynamic DNS

Active

Service Provider

Host Name

E-mail Address

User

Password

Enable Wildcard

The following table describes the fields in this screen.

Table 22 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 8

Time and Date

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

8.1 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 36 Time and Date

Time and Date

Time Server

Use Protocol when Bootup: None

IP Address or URL: N/A

Time and Date: (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

Daylight Savings

Start Date: 1 month 1 day

End Date: 1 month 1 day

Synchronize system clock with Time Server now.
(This may take up to 60 seconds.)

Date

Current Date: 2000 - 01 - 01

New Date (yyy-mm-dd): 2000 - 01 - 01

Time

Current Time: 01 : 10 : 51

New Time: 01 : 10 : 51

Apply Cancel

The following table describes the fields in this screen.

Table 23 Time and Date

	DESCRIPTION
Time Server	
	<p>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.</p> <p>Daytime (RFC 867) format is day/month/year/time zone of the server.</p> <p>Time (RFC 868) format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.</p> <p>NTP (RFC 1305) is similar to Time (RFC 868).</p> <p>Select None to enter the time and date manually.</p>
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.	<p>Select this option to have your Prestige use the time server (that you configured above) to set its internal system clock.</p> <p>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.</p>
Date	
	<p>This field displays the date of your Prestige.</p> <p>Each time you reload this page, the Prestige synchronizes the time with the time server.</p>
New Date (yyyy-mm-dd)	<p>This field displays the last updated date from the time server.</p> <p>When you select None in the Use Protocol when Bootup field, enter the new date in this field and then click Apply.</p>
Time	
	<p>This field displays the time of your Prestige.</p> <p>Each time you reload this page, the Prestige synchronizes the time with the time server.</p>
New Time	<p>This field displays the last updated time from the time server.</p> <p>When you select None in the Use Protocol when Bootup field, enter the new time in this field and then click Apply.</p>
Apply	Click Apply to save your changes back to the Prestige.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 9

Remote Management Configuration

This chapter provides information on configuring remote management.

9.1 Remote Management Overview

Remote management allows you to determine which services/protocols can access which Prestige interface (if any) from which computers.

You may manage your Prestige from a remote location via:

- Internet (WAN only)
- ALL (LAN and WAN)
- LAN only,
- Neither (Disable).

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

9.1.1 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.

9.1.2 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.

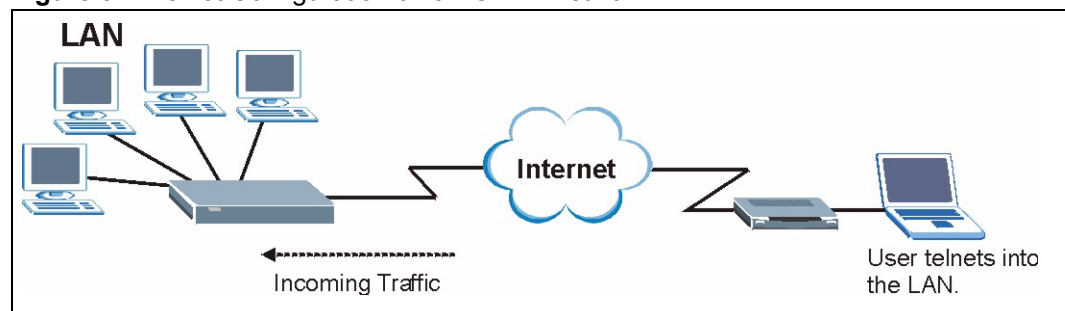
9.1.3 System Timeout

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.

9.2 Telnet

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

Figure 37 Telnet Configuration on a TCP/IP Network



9.3 FTP

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

9.4 Web

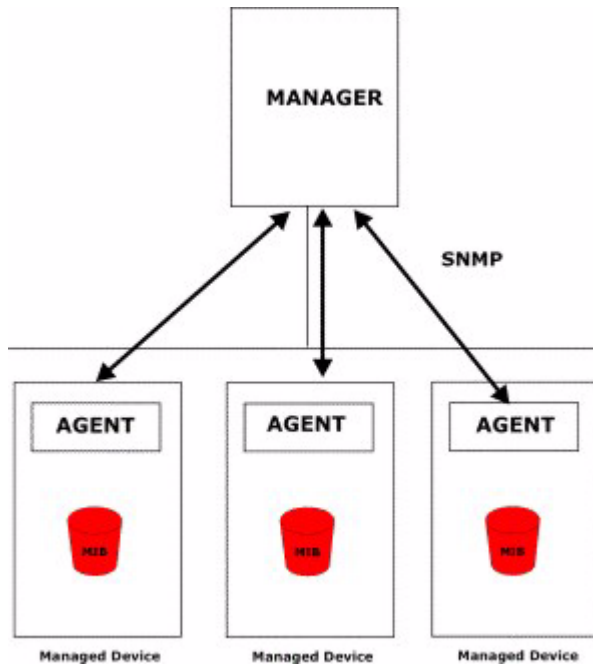
You can use the Prestige's embedded web configurator for configuration and file management. See the online help for details.

9.5 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 (SNMPv2). The next figure illustrates an SNMP management operation.

Note: SNMP is only available if TCP/IP is configured.

Figure 38 SNMP Management Mode



An SNMP managed network consists of two main types of component: 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 such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

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

- 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.

9.5.1 Supported MIBs

The Prestige supports MIB II that is defined in RFC-1213 and RFC-1215. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.

9.5.2 SNMP Traps

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

Table 24 SNMP Traps

	TRAP NAME	DESCRIPTION
0	coldStart (defined in RFC-1215)	A trap is sent after booting (power on).
1	warmStart (defined in RFC-1215)	A trap is sent after booting (software reboot).
4	authenticationFailure (defined in RFC-1215)	A trap is sent to the manager when receiving any SNMP get or set requirements with the 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, CLI command "sys reboot", etc.).
6b	For fatal error :	A trap is sent with the message of the fatal code if the system reboots because of fatal errors

9.6 ICMP

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. Your 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.

9.7 Configuring Remote Management

Click **Remote Management** to open the following screen.

Figure 39 Remote Management

Remote Management Control

Server Type	Access Status	Port	Secured Client IP
Telnet	All	23	0.0.0.0
FTP	All	21	0.0.0.0
Web	All	80	0.0.0.0
SNMP	All	161	0.0.0.0
ICMP	All		0.0.0.0

Apply Cancel

The following table describes the fields in this screen.

Table 25 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 10

Universal Plug-and-Play (UPnP)

This chapter introduces the UPnP feature in the web configurator.

10.1 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.

10.1.1 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.

10.1.2 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.

10.1.3 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.

10.2 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.

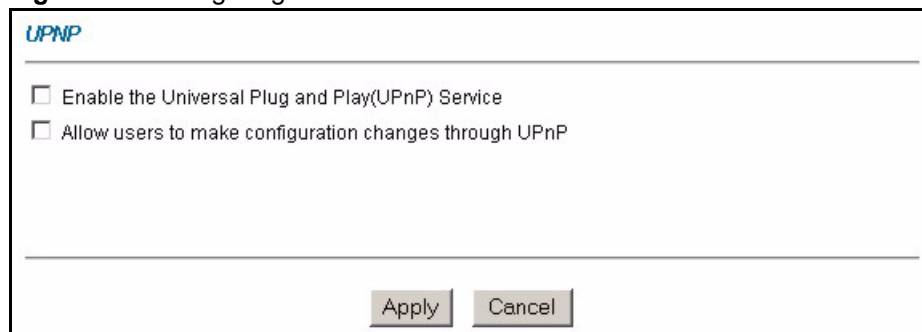
UPnP broadcasts are only allowed on the LAN.

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

10.2.1 Configuring UPnP

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

Figure 40 Configuring UPnP



The screenshot shows a configuration window titled "UPNP". It contains two unchecked checkboxes: "Enable the Universal Plug and Play(UPnP) Service" and "Allow users to make configuration changes through UPnP". At the bottom of the window are two buttons: "Apply" and "Cancel".

The following table describes the fields in this screen.

Table 26 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.
Apply	Click Apply to save the setting to the Prestige.
Cancel	Click Cancel to return to the previously saved settings.

10.3 Installing UPnP in Windows Example

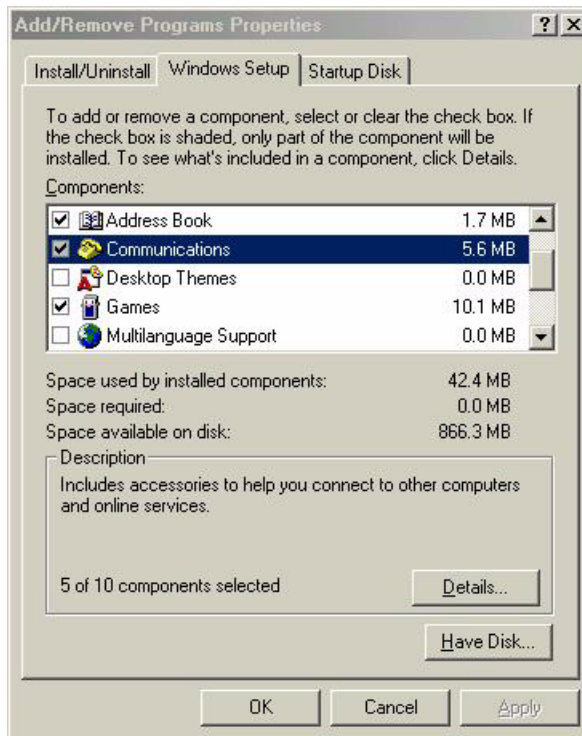
This section shows how to install UPnP in Windows Me and Windows XP.

Installing UPnP in Windows Me

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

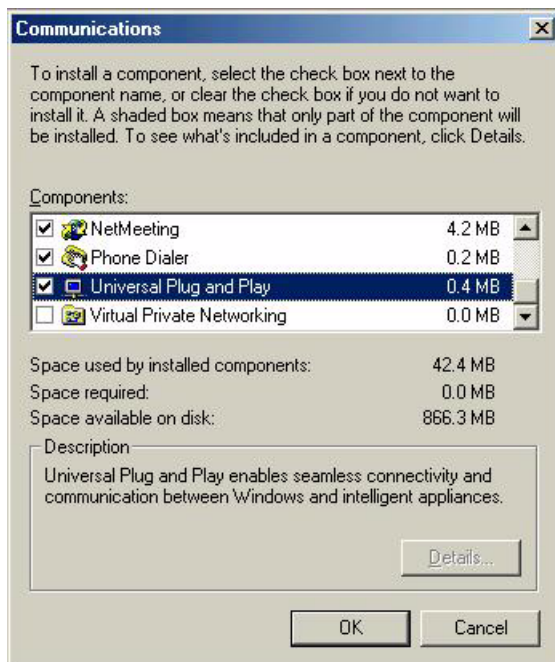
- 1** Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.
- 2** Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.

Figure 41 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 42 Add/Remove Programs: Windows Setup: Communication: Components



4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.

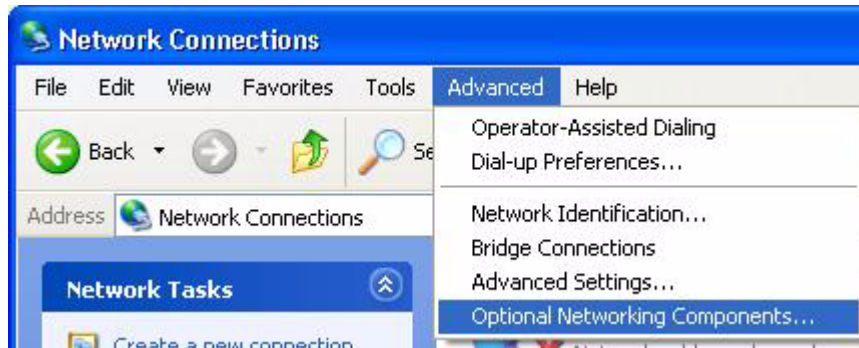
5 Restart the computer when prompted.

Installing UPnP in Windows XP

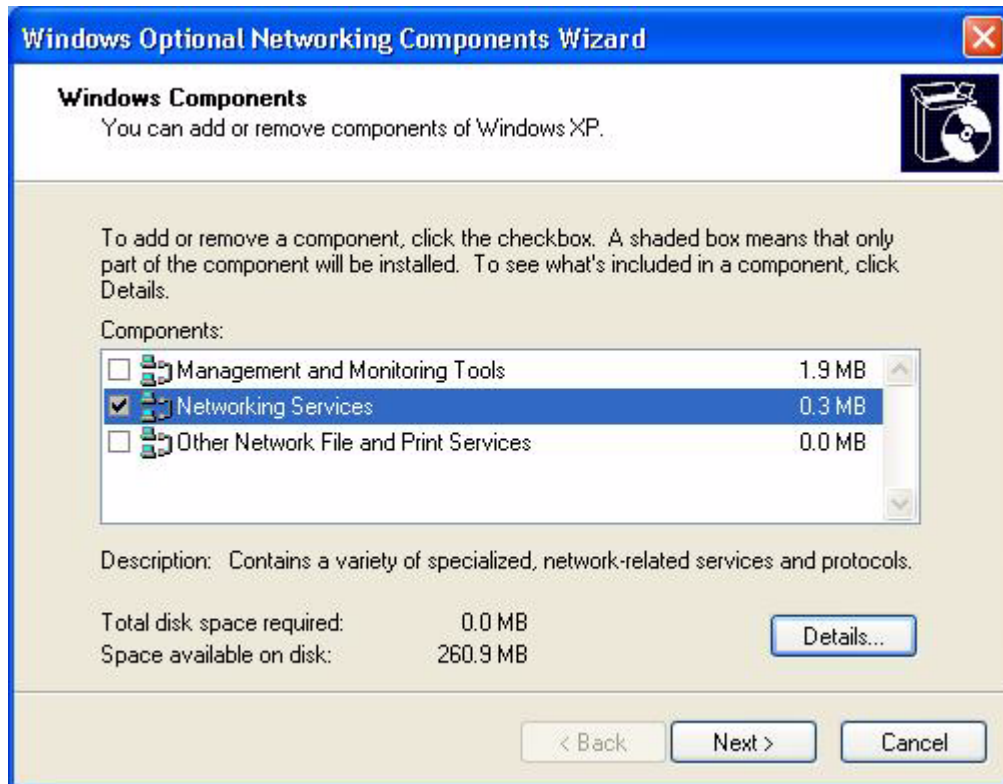
Follow the steps below to install the UPnP in Windows XP.

- 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**

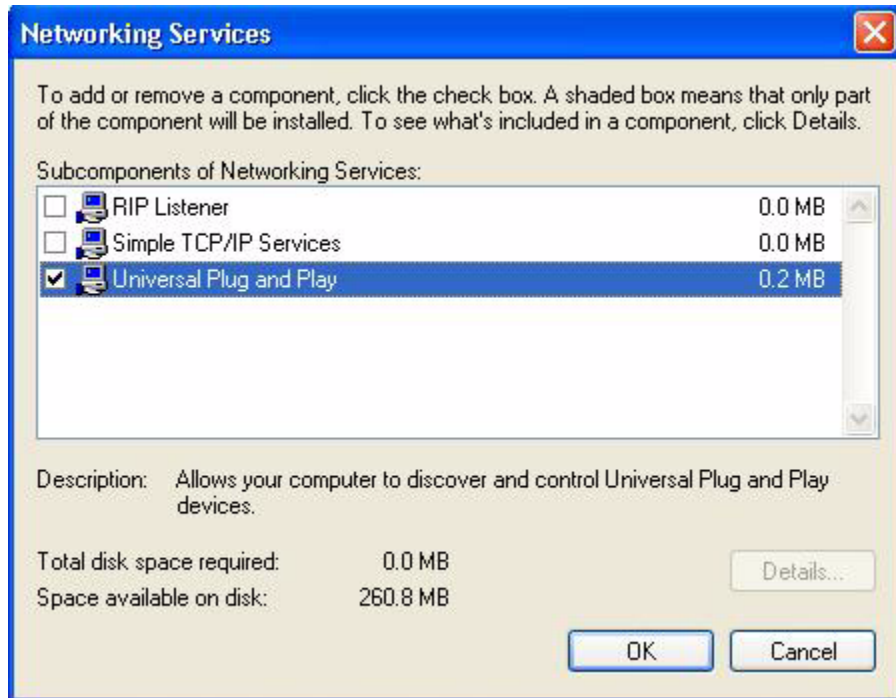
Figure 43 Network Connections



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

Figure 44 Windows Optional Networking Components Wizard

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

Figure 45 Networking Services

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

10.4 Using UPnP in Windows XP Example

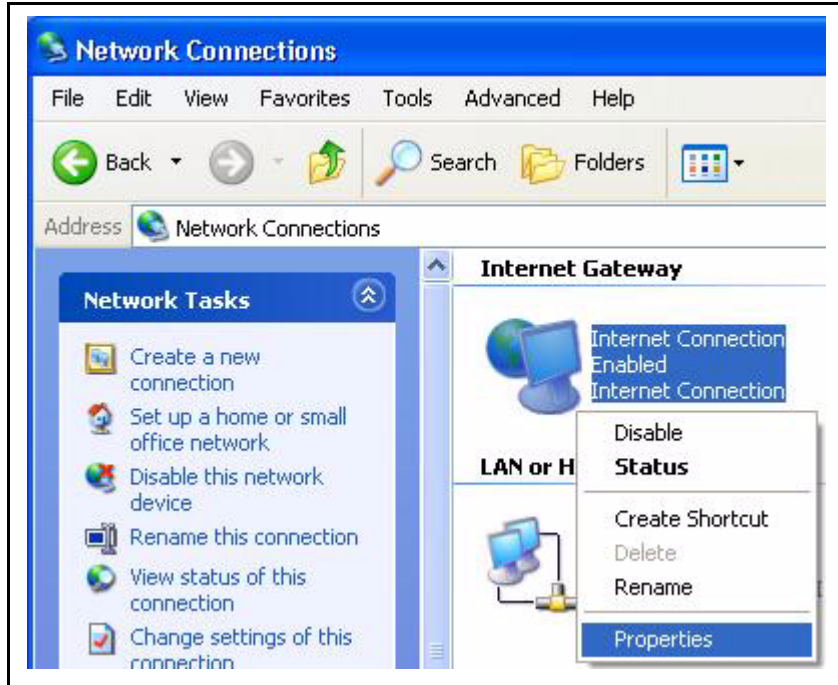
This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the Prestige.

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 46 Network Connections



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

Figure 47 Internet Connection Properties

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

Figure 48 Internet Connection Properties: Advanced Settings

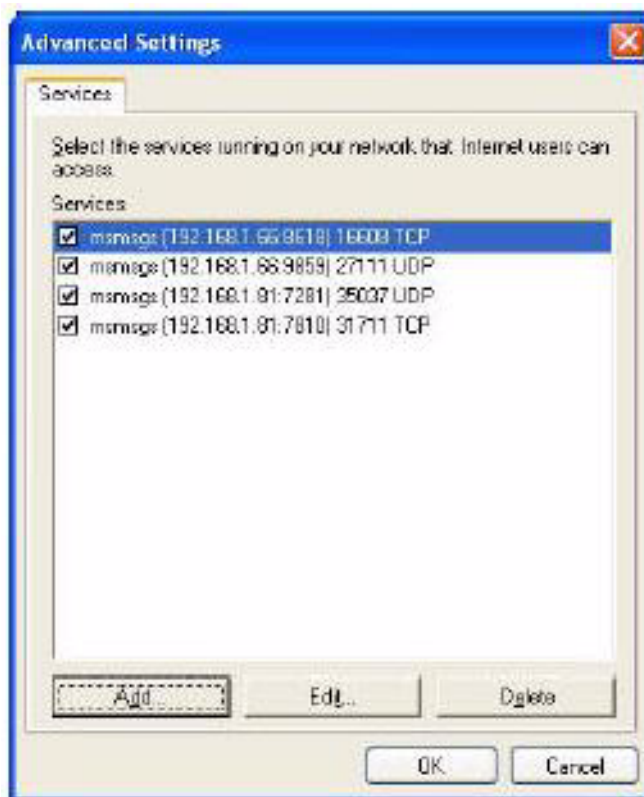
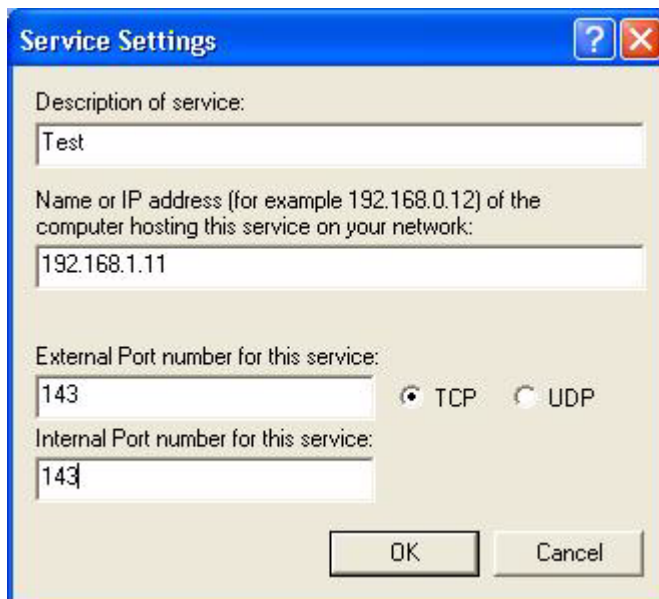


Figure 49 Internet Connection Properties: Advanced Settings: Add



- 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 50 System Tray Icon

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

Figure 51 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.

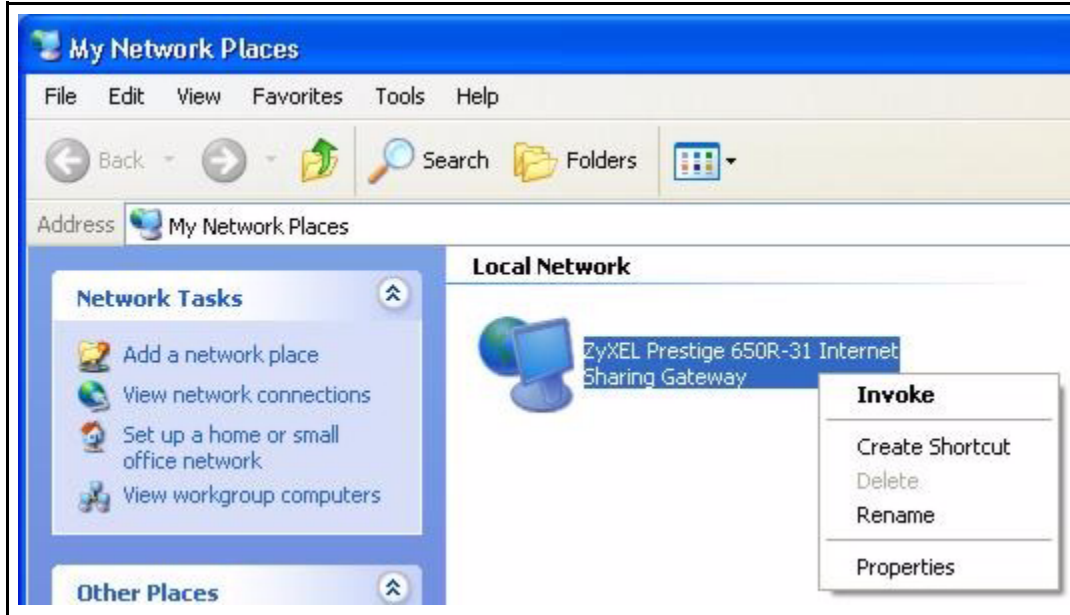
Follow the steps below to access the web configurator.

- 1 Click **Start** and then **Control Panel**.
- 2 Double-click **Network Connections**.
- 3 Select **My Network Places** under **Other Places**.

Figure 52 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 53 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 54 Network Connections: My Network Places: Properties: Example

CHAPTER 11

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.

11.1 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.

11.1.1 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.

11.2 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 11.2 on page 120](#)).

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 55 View Logs

#	Time	Message	Source	Destination	Notes
1	01/01/2000 00:44:11	SMT Session End			
2	01/01/2000 00:35:11	SMT Session Begin			

The following table describes the fields in this screen.

Table 27 View Logs

	DESCRIPTION
Back	Click Back to return to the previous screen
Refresh	Click Refresh to renew the log screen.
Clear Log	Click Clear Log to delete all the logs.
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.

CHAPTER 12

Maintenance

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

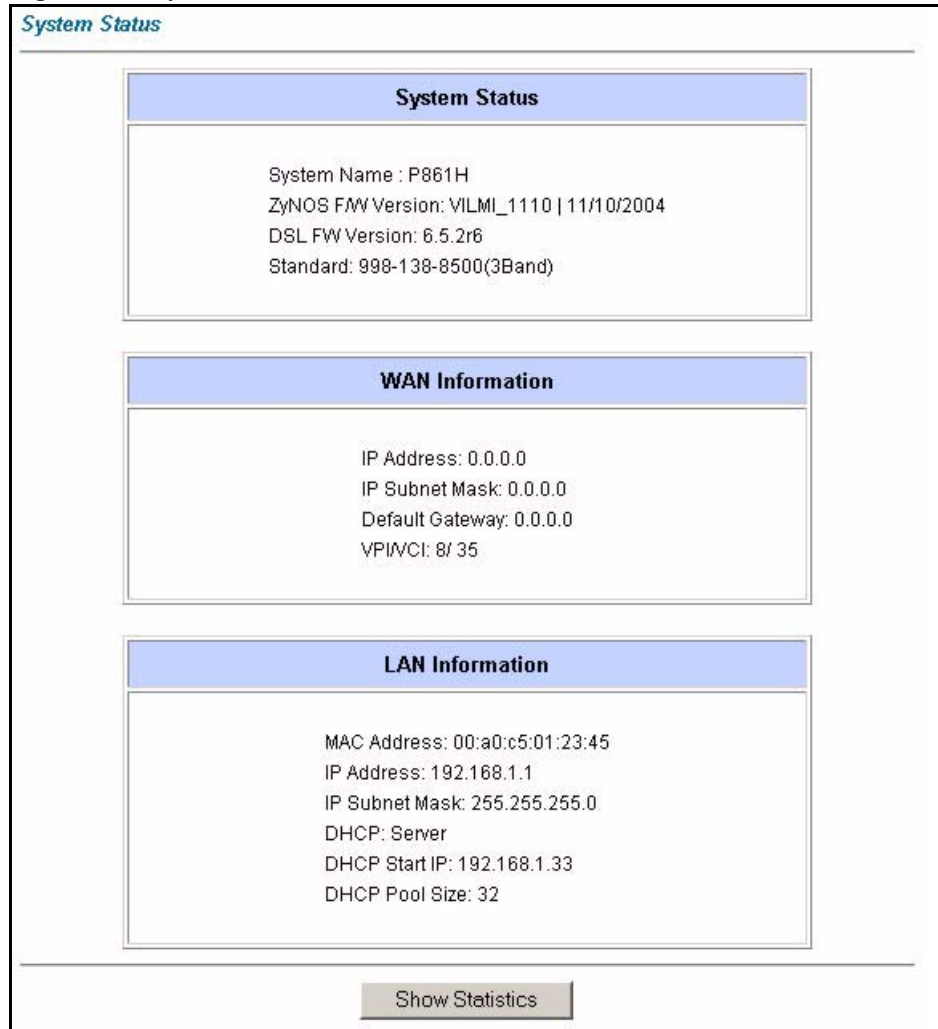
12.1 Maintenance Overview

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

12.2 System Status Screen

Click **System Status** to open the following screen, where you can use to monitor your Prestige. Note that these fields are READ-ONLY and only for diagnostic purposes.

Figure 56 System Status



The following table describes the fields in this screen.

Table 28 System Status

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

Table 28 System Status (continued)

LABEL	DESCRIPTION
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.
Show Statistics	Click Show Statistics to see the performance statistics such as number of packets sent and number of packets received for each port.

12.2.1 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 57 System Status: Show Statistics

System up Time: 22:19:19							
CPU Load: 0.00%							
WAN Port Statistics:							
Link Status: Down							
Upstream Speed: 0 kbps							
Downstream Speed: 0 kbps							
Node-Link	Status	TxPkts	RxPkts	Errors	Tx B/s	Rx B/s	Up Time
MyISP	N/A	0	0	0	0	0	0:00:00
MDWARE	N/A	0	0	0	0	0	0:00:00
IGMP	N/A	0	0	0	0	0	0:00:00
VIDEO-1	N/A	0	0	0	0	0	0:00:00
VIDEO-2	N/A	0	0	0	0	0	0:00:00
VIDEO-3	N/A	0	0	0	0	0	0:00:00
VIDEO-4	N/A	0	0	0	0	0	0:00:00
N/A	N/A	0	0	0	0	0	0:00:00
N/A	N/A	0	0	0	0	0	0:00:00
N/A	N/A	0	0	0	0	0	0:00:00
LAN Port Statistics:							
Interface:	Status	TxPkts	RxPkts				
Ethernet	Up	7156	6766				

The following table describes the fields in this screen.

Table 29 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.

Table 29 System Status: Show Statistics (continued)

LABEL	DESCRIPTION
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.
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.

12.3 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 58 DHCP Table

The screenshot shows a web interface titled "DHCP Table". Below the title is a table with three columns: "Host Name", "IP Address", and "MAC Address". The table contains one row of data: "tw11808-01", "192.168.1.5", and "00-85-A0-01-01-04".

Host Name	IP Address	MAC Address
tw11808-01	192.168.1.5	00-85-A0-01-01-04

The following table describes the fields in this screen.

Table 30 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.

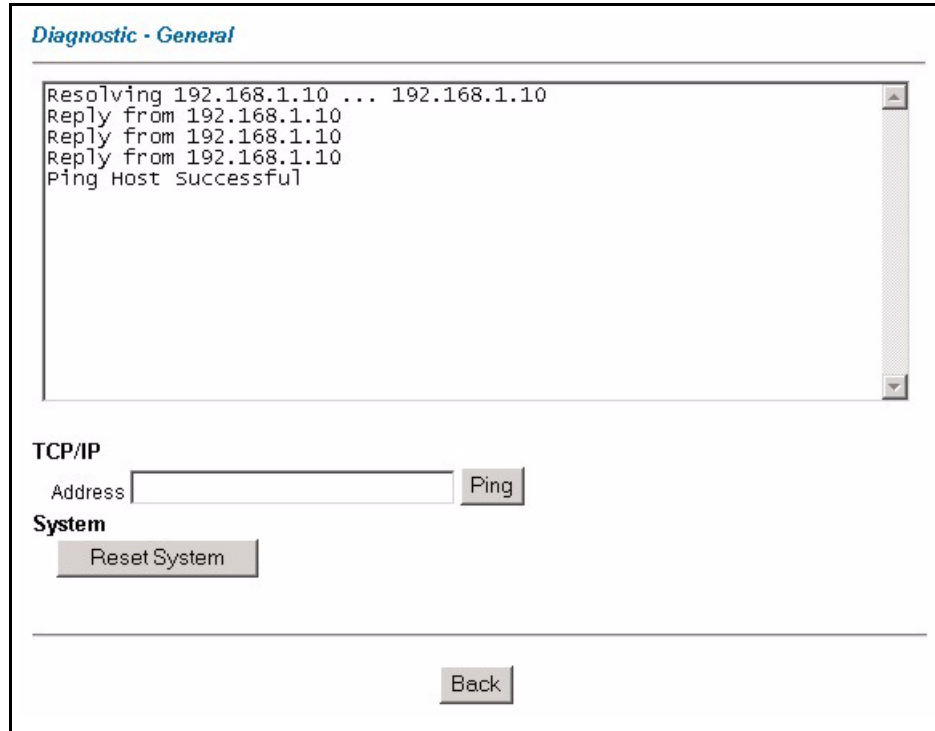
12.4 Diagnostic Screens

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

12.4.1 Diagnostic General Screen

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

Figure 59 Diagnostic: General



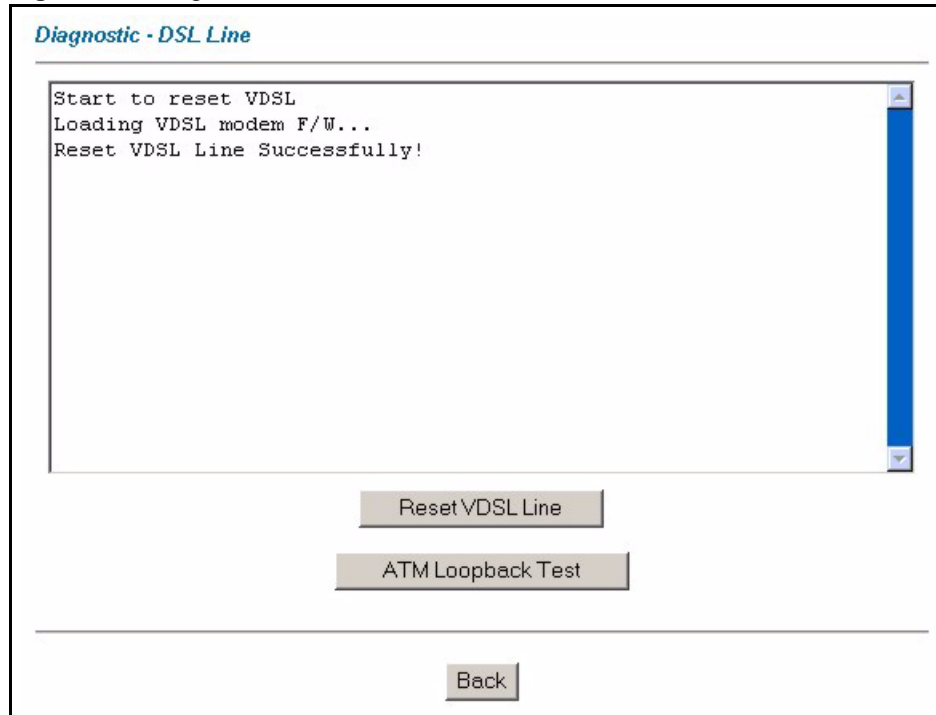
The following table describes the fields in this screen.

Table 31 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.

12.4.2 Diagnostic DSL Line Screen

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

Figure 60 Diagnostic: DSL Line

The following table describes the fields in this screen.

Table 32 Diagnostic: DSL Line

	DESCRIPTION
Reset VDSL Line	Click this button to reinitialize the VDSL line. The large text box above then displays the progress and results of this operation, for example: "Start to reset VDSL Loading VDSL modem F/W... Reset VDSL Line Successfully!"
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.
Back	Click this button to go back to the main Diagnostic screen.

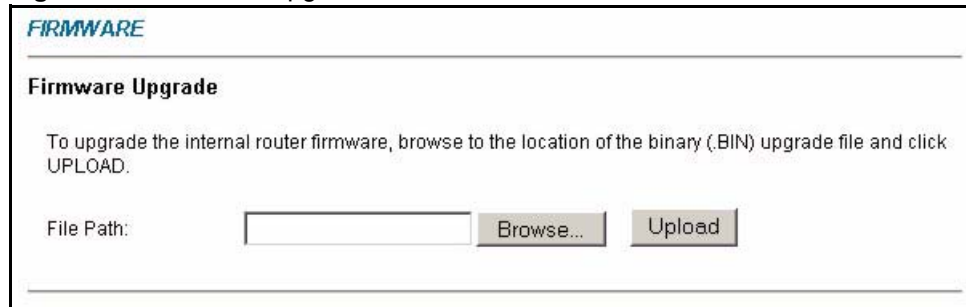
12.5 Firmware Screen

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 24 on page 214](#) 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 61 Firmware Upgrade



The following table describes the labels in this screen.

Table 33 Firmware Upgrade

	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.

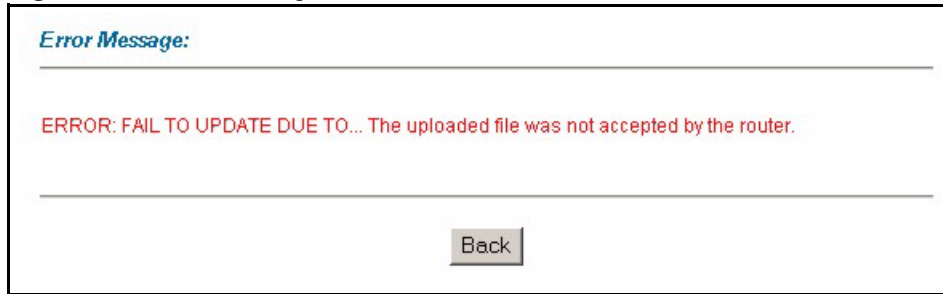
The Prestige automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 62 Network Temporarily Disconnected



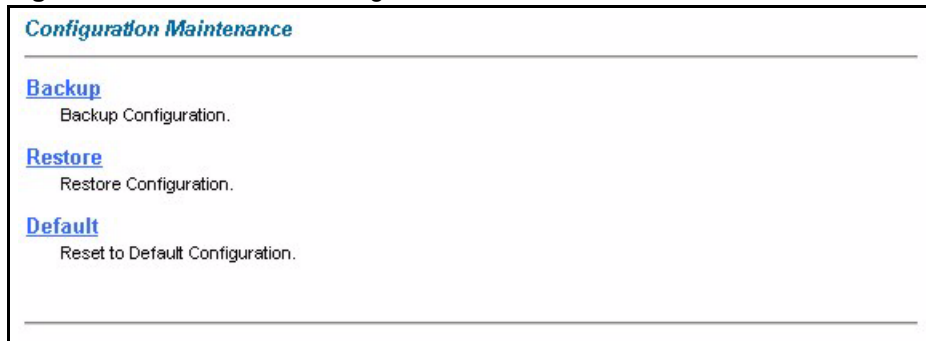
After two minutes, log in again and check your new firmware version in the **System Status** screen.

If the upload was not successful, the following screen will appear. Click **Back** to go back to the **Firmware** screen.

Figure 63 Error Message

12.6 Configuration Screen

Click **Maintenance**, and then the **Configuration** tab. Links to backup configuration, restoring configuration, and factory defaults appear as shown next.

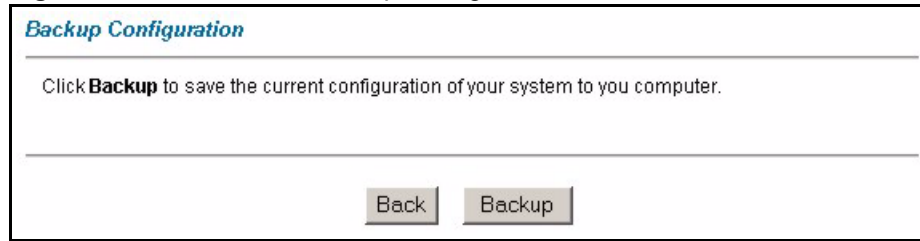
Figure 64 Maintenance Configuration

12.6.1 Backup Configuration

Backup configuration allows you to back up (save) the Prestige's current configuration to a file on your computer. Once your Prestige is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the Prestige's current configuration to your computer

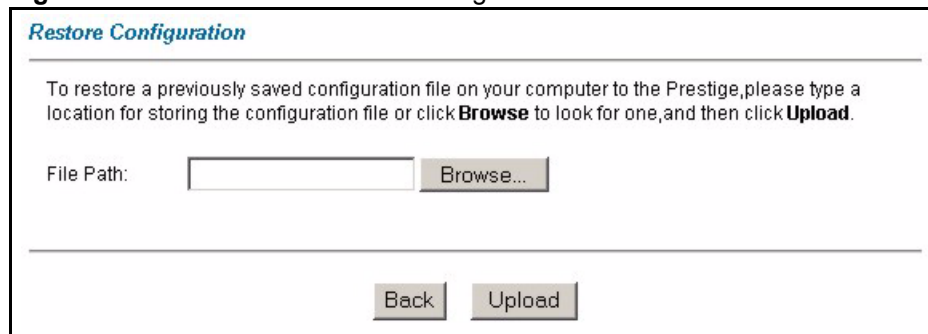
Figure 65 Maintenance Backup Configuration



12.6.2 Restore Configuration

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your Prestige.

Figure 66 Maintenance Restore Configuration



The following table describes the labels in this screen.

Table 34 Maintenance Restore Configuration

	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 file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Back	Click Back to return to the Configuration screen.
Upload	Click Upload to begin the upload process.

Note: Do not turn off the Prestige while configuration file upload is in progress.

After you see a “configuration upload successful” screen, you must then wait one minute 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 67 Temporarily Disconnected

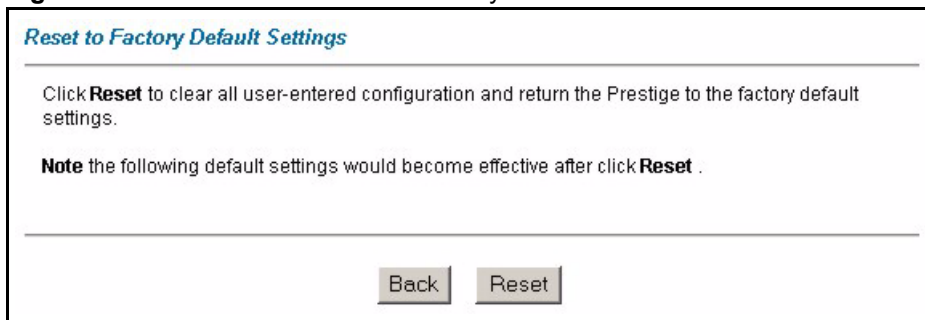
If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default Prestige IP address (192.168.1.1). See your Quick Start Guide for details on how to set up your computer's IP address.

If the upload was not successful, the following screen will appear. Click Back to return to the Configuration screen.

Figure 68 Error Message

12.6.3 Default Screen

Click **Maintenance**, **Configuration** and then **Default**. Pressing the **Reset** button in this section clears all user-entered configuration information and returns the Prestige to its factory defaults.

Figure 69 Maintenance Reset to Factory Defaults

CHAPTER 13

Introducing the SMT

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

13.1 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.

13.1.1 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.

13.1.2 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 70 Login Screen

Enter Password: ****

13.1.3 Prestige SMT Menu Overview

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

Table 35 SMT Menu Overview

MENUS	SUB MENUS		
1 General Setup	1.1 Configure Dynamic DNS		
3 LAN Setup	3.1 LAN Port Filter Setup		
	3.2 TCP/IP and DHCP Setup	3.2.1 IP Alias Setup	
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		
	12.3 Bridge Static Route	12.3.1 Edit Bridge Static Route	
15 NAT Setup	15.1 Address Mapping Sets	15.1.1 Address Mapping Rules	15.1.1.x Address Mapping Rule
	15.2 NAT Server Sets	15.2.x NAT Server Setup	
21 Filter Set Configuration	21.1 Filter Set Configuration	21.1 Filter Rules Summary	21.1.x.1 Generic Filter Rule
			21.1.x.1 TCP/IP Filter Rule
22 SNMP Configuration			
23 System Password	23.1 Change Password		

Table 35 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 Setup		

13.2 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 36 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 36 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 37 SMT Main Menu

Copyright (c) 1994 - 2004 ZyXEL Communications Corp.	
P861H Main Menu	
Getting Started 1. General Setup 3. Ethernet Setup 4. Internet Access Setup Advanced Applications 11. Remote Node Setup 12. Static Routing Setup 15. NAT Setup	Advanced Management 21. Filter Set Configuration 22. SNMP Configuration 23. System Password 24. System Maintenance 25. IP Routing Policy Setup 26. Schedule Setup 99. Exit
Enter Menu Selection Number:	

13.2.1 System Management Terminal Interface Summary

Table 38 Main Menu Summary

#	MENU TITLE	DESCRIPTION
1	General Setup	Use this menu to set up your general information.
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.

Table 38 Main Menu Summary

#	MENU TITLE	DESCRIPTION
12	Static Routing Setup	Use this menu to set up static routes.
15	NAT Setup	Use this menu to specify inside servers when NAT is enabled.
21	Filter Set Configuration	Use this menu to configure filters.
22	SNMP Configuration	Use this menu to set up SNMP related parameters.
23	System Password	Use this menu to 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.

13.3 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 71 Menu 23.1 Change Password

```

                                Menu 23 - System 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 14

Menu 1 General Setup

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

14.1 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.

14.2 Procedure To Configure Menu 1

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

Figure 72 Menu 1 General Setup

```

Menu 1 - General Setup

System Name= P861H
Location=
Contact Person's Name=

Edit Dynamic DNS= No

Route IP= Yes
Bridge= Yes
ILMI= 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 39 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. Note: The Prestige cannot be configured as a bridge and a router at the same time.

Table 39 Menu 1 General Setup

FIELD	DESCRIPTION
ILMI	<p>Use Integrated Local Management (ILMI) to automatically configure ATM permanent virtual circuits (PVCs) on the Prestige. This removes the need to dispatch a service technician to configure PVCs on the Prestige at the site where the Prestige is installed.</p> <p>ILMI operates between the network DSLAM and the VDSL device. ILMI uses SNMP and an ATM Management Information Database (MIB) to transfer configuration settings from the DSLAM to the Prestige. The configuration settings include Virtual Path Connections (VPC), Virtual Channel Connections (VCC), registered ATM network prefixes, registered ATM addresses and service registration information.</p> <p>Select Yes to turn ILMI on, select No to turn ILMI off.</p>
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.	

14.2.1 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 73 Menu 1.1 Configure Dynamic DNS

<pre> 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: </pre>
--

Follow the instructions in the next table to configure dynamic DNS parameters.

Table 40 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.

Table 40 Menu 1.1 Configure Dynamic DNS

FIELD	DESCRIPTION
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 15

Menu 3 LAN Setup

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

15.1 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 74 Menu 3 LAN Setup

```
Menu 3 - LAN Setup

1. LAN Port Filter Setup
2. TCP/IP and DHCP Setup

Enter Menu Selection Number:
```

15.1.1 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 75 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 21 on page 188](#) first, then return to this menu to define the filter sets.

15.2 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

15.3 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 76 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 41 DHCP Ethernet Setup

	DESCRIPTION
DHCP Setup	
DHCP	<p>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.</p> <p>If set to None, the DHCP server will be disabled.</p> <p>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.</p> <p>When DHCP server is used, the following items need to be set:</p>
Client IP Pool Starting Address	<p>This field specifies the first of the contiguous addresses in the IP address pool.</p> <p>Note: You can store a maximum of four IP addresses in the client IP pool.</p>
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 42 TCP/IP Ethernet Setup

	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 16

Internet Access

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

16.1 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.

16.2 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).

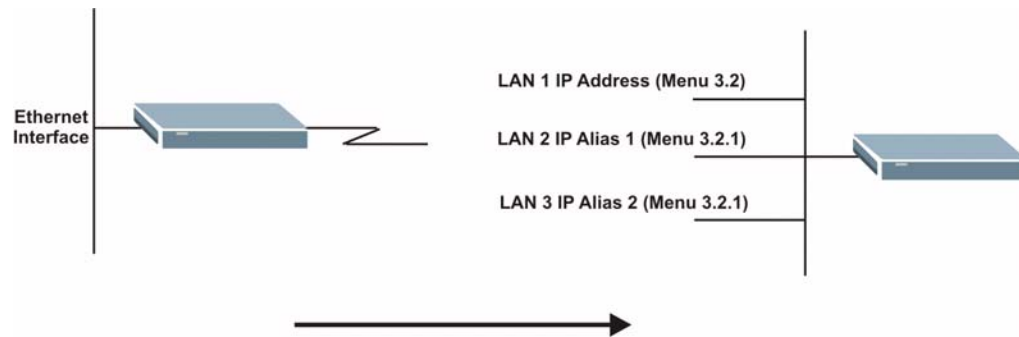
16.3 IP Alias

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 77 IP Alias Network Example

Use menu 3.2.1 to configure IP Alias on your Prestige.

16.4 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 78 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= Yes

Press ENTER to Confirm or ESC to Cancel:

```

Pressing [ENTER] displays **Menu 3.2.1 — IP Alias Setup**, as shown next.

Figure 79 Menu 3.2.1 IP Alias Setup

```

Menu 3.2.1 - IP Alias Setup

IP Alias 1= Yes
  IP Address= 192.168.2.1
  IP Subnet Mask= 255.255.255.0
  RIP Direction= None
  Version= RIP-1
  Incoming protocol filters=
  Outgoing protocol filters=
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 43 Menu 3.2.1 IP Alias Setup

	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.	

16.5 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 80 Menu 1 General Setup

```
Menu 1 - General Setup

System Name= P861H
Location=
Contact Person's Name=
Domain Name=
Edit Dynamic DNS= No

Route IP= Yes
Bridge= No
ILMI= No

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

16.6 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.

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 81 Menu 4 Internet Access Setup

```

Menu 4 - Internet Access Setup

ISP's Name= MyISP
Encapsulation= ENET ENCAP
Multiplexing= LLC-based
VPI #= 8
VCI #= 35
Service Name= N/A
My Login= N/A
My Password= N/A

NAT= Full Feature
  Address Mapping Set= 1
IP Address Assignment= Dynamic
  IP Address= N/A
ENET ENCAP Gateway= 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 44 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	This field displays the method of multiplexing used by your ISP.
VPI #	Enter the Virtual Path Identifier (VPI) assigned to you.
VCI #	Enter the Virtual Channel Identifier (VCI) assigned to you.
Service Name	Type a Service Name for PPPoE encapsulation only.
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.
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.
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.

Table 44 Menu 4 Internet Access Setup (continued)

FIELD	DESCRIPTION
ENET ENCAP Gateway	Enter the gateway IP address supplied by your ISP when you are using ENET ENCAP encapsulation.
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 17

Remote Node Configuration

This chapter covers remote node configuration.

17.1 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.

17.2 Remote Node Setup

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

17.2.1 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 82 Menu 11 Remote Node Setup

```
Menu 11 - Remote Node Setup

1. MyISP (ISP, NAT)
2. MDWARE
3. IGMP
4. VIDEO-1
5. VIDEO-2
6. VIDEO-3
7. VIDEO-4
8. _____
9. _____
10. _____

Enter Node # to Edit:
```

For more information on remote node setup see the WAN Setup chapter of this User's Guide.

17.2.2 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. Your prestige supports LLC method of multiplexing.

Figure 83 Menu 11.1 Remote Node Profile

```

Menu 11.1 - Remote Node Profile

Rem Node Name= MyISP           Route= IP
Active= Yes                    Bridge= No

Encapsulation= ENET ENCAP      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 45 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	This displays the method of multiplexing that your ISP uses.
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.

Table 45 Menu 11.1 Remote Node Profile (continued)

FIELD	DESCRIPTION
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. 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 28 on page 246 .
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 21 on page 188 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.	

17.2.3 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.

17.3 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 84 Menu 11.3 Remote Node Network Layer Options

```

Menu 11.3 - Remote Node Network Layer Options

IP Options:                               Bridge Options:
IP Address Assignment = Dynamic           Ethernet Addr Timeout(min)= N/A
Rem IP Addr = 0.0.0.0
Rem Subnet Mask= 0.0.0.0
My WAN Addr= N/A
NAT= Full Feature
    Address Mapping Set= 1
Metric= 2
Private= No
RIP Direction= None
    Version= RIP-1
Multicast= None
IP Policies=

Enter here to CONFIRM or ESC to CANCEL:

Press Space Bar to Toggle.

```

The next table explains fields in **Menu 11.3 – Remote Node Network Layer Options**.

Table 46 Menu 11.3 Remote Node Network Layer Options

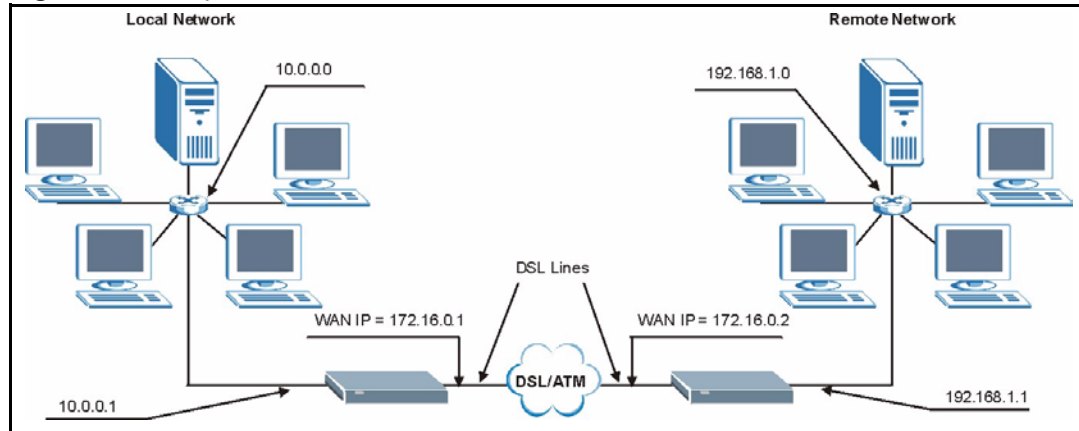
FIELD	DESCRIPTION
IP Address Assignment	Press [SPACE BAR] and then [ENTER] to select Dynamic if the remote node is using a dynamically assigned IP address or Static if it is using a static (fixed) IP address. You will only be able to configure this in the ISP node (also the one you configure in menu 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.

Table 46 Menu 11.3 Remote Node Network Layer Options (continued)

FIELD	DESCRIPTION
	Select SUA Only if you have just one public WAN IP address for your Prestige. The SMT uses Address Mapping Set 255 (see Figure 101 on page 175). Select None to disable NAT.
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 20 on page 172 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 20 on page 172 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 27 on page 236) 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.	

17.3.1 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 85 Sample IP Addresses for a TCP/IP LAN-to-LAN Connection

17.4 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 these fields. 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 86 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 87 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:

```

17.5 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**.

17.5.1 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 88 Menu 11.6 for LLC-based Multiplexing or PPP Encapsulation

```

Menu 11.6 - Remote Node ATM Layer Options
VPI/VCI (LLC-Multiplexing or PPP-Encapsulation)

VPI #= 8
VCI #= 35
ATM QoS Type= VBR-nRT
PCR= 4830
CDVT= 1
SCR= 604
MBS= 32
Application Type= Data
Ethernet Port 1= No
Ethernet Port 2= No
Ethernet Port 3= Yes
Ethernet Port 4= Yes

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).

17.5.2 Advance Setup Options

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

Figure 89 Menu 11.1 Remote Node Profile

```

Menu 11.1 - Remote Node Profile

Rem Node Name= MyISP                Route= IP
Active= Yes                          Bridge= Yes

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= admin                    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:

Press Space Bar to Toggle.

```

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 90 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 47 Menu 11.8 Advance Setup Options

FIELD	DESCRIPTION
PPPoE pass-through	<p>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.</p> <p>PPPoE pass through is an alternative to NAT for applications where NAT is not appropriate.</p> <p>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.</p>
<p>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.</p>	

CHAPTER 18

Static Route Setup

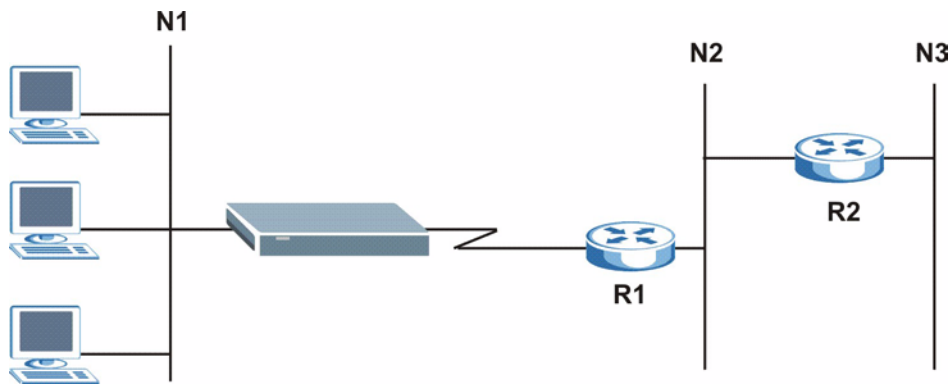
This chapter shows how to setup IP static routes.

18.1 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 91 Sample Static Routing Topology



18.2 Configuration

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

Figure 92 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 93 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 94 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 48 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 19

Bridging Setup

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

19.1 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.

19.2 Bridge Ethernet Setup

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

19.2.1 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 95 Menu 11.1 Remote Node Profile

```
Menu 11.1 - Remote Node Profile

Rem Node Name= MyISP                Route= IP
Active= Yes                          Bridge= Yes

Encapsulation= ENET ENCAP           Edit IP/Bridge= Yes
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:

Press Space Bar to Toggle.
```

- 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 96 Menu 11.3 Remote Node Network Layer Options

```

Menu 11.3 - Remote Node Network Layer Options

IP Options:                               Bridge Options:
IP Address Assignment = Dynamic           Ethernet Addr Timeout(min)= 0
Rem IP Addr = 0.0.0.0
Rem Subnet Mask= 0.0.0.0
My WAN Addr= N/A
NAT= Full Feature
    Address Mapping Set= 1
Metric= 2
Private= No
RIP Direction= None
    Version= RIP-1
Multicast= None
IP Policies=

Enter here to CONFIRM or ESC to CANCEL:

Press Space Bar to Toggle.

```

The following table describes the fields in this menu.

Table 49 Remote Node Network Layer Options: Bridge Fields

	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.

19.2.2 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 97 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 50 Menu 12.3.1 Edit Bridge Static Route

	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 20

Network Address Translation (NAT)

This chapter discusses how to configure NAT on the Prestige.

20.1 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.

20.1.1 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 20.3 on page 174](#) 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.

20.2 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 98 Menu 4 Applying NAT for Internet Access

```
Menu 4 - Internet Access Setup

ISP's Name= MyISP
Encapsulation= ENET ENCAP
Multiplexing= LLC-based
VPI #= 8
VCI #= 35
Service Name= N/A
My Login= N/A
My Password= N/A

NAT= SUA Only
  Address Mapping Set= N/A
  IP Address Assignment= Dynamic
  IP Address= N/A
  ENET ENCAP Gateway= N/A

  Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

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 99 Applying NAT in Menus 4 & 11.3

```

Menu 11.3 - Remote Node Network Layer Options

IP Options:                               Bridge Options:
IP Address Assignment = Dynamic           Ethernet Addr Timeout(min)= 0
Rem IP Addr = 0.0.0.0
Rem Subnet Mask= 0.0.0.0
My WAN Addr= N/A
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:

Press Space Bar to Toggle.

```

The following table describes the options for Network Address Translation.

Table 51 Applying NAT in Menus 4 & 11.3

FIELD	DESCRIPTION
NAT	Press [SPACE BAR] and then [ENTER] to select Full Feature if you have multiple public WAN IP addresses for your Prestige. The SMT uses the address mapping set that you configure and enter in the Address Mapping Set field (see Figure 101 on page 175).
	Select None to disable NAT.
	When you select SUA Only , the SMT uses Address Mapping Set 255 (see Figure 102 on page 176). Choose SUA Only if you have just one public WAN IP address for your Prestige.

20.3 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 100 Menu 15 NAT Setup

```
Menu 15 - NAT Setup

1. Address Mapping Sets

2. NAT Server Sets

Enter Menu Selection Number:
```

20.3.1 Address Mapping Sets

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

Figure 101 Menu 15.1 Address Mapping Sets

```
Menu 15.1 - Address Mapping Sets

1. ACL Default Set
2.
3.
4.
5.
6.
7.
8.
255. SUA (read only)

Enter Menu Selection Number:

Enter Menu Selection Number:
```

20.3.1.1 SUA Address Mapping Set

Enter 255 to display the next screen (see also [Section 20.1.1 on page 172](#)). The fields in this menu cannot be changed.

Figure 102 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 52 SUA Address Mapping Rules

	DESCRIPTION
Set Name	This is the name of the set you selected in menu 15.1 or enter the name of a new set you want to create.
Idx	This is the index or rule number.
Local Start IP	Local Start IP is the starting local IP address (ILA).
Local End IP	Local End IP is the ending local IP address (ILA). If the rule is for all local IPs, then the Start IP is 0.0.0.0 and the End IP is 255.255.255.255.
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.	

20.3.1.2 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 103 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.

20.3.1.3 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 53 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 104 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 54 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set

	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.	

20.4 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 105 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 106 Menu 15.2.1 NAT Server Setup

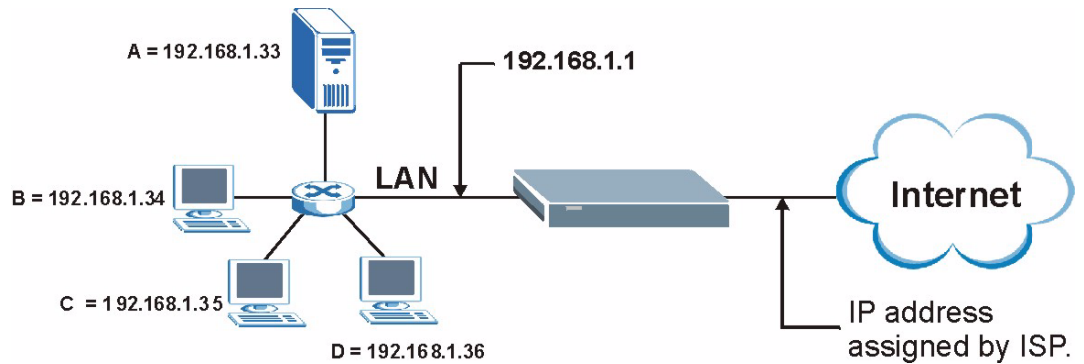
Menu 15.2 - NAT Server Setup			
Rule	Start Port No.	End Port No.	IP Address
1.	Default	Default	0.0.0.0
2.	21	21	192.168.1.33
3.	0	0	0.0.0.0
4.	0	0	0.0.0.0
5.	0	0	0.0.0.0
6.	0	0	0.0.0.0
7.	0	0	0.0.0.0
8.	0	0	0.0.0.0
9.	0	0	0.0.0.0
10.	0	0	0.0.0.0
11.	0	0	0.0.0.0
12.	0	0	0.0.0.0

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 107 Multiple Servers Behind NAT Example



20.5 General NAT Examples

The following are some examples of NAT configuration.

20.5.1 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 108 NAT Example 1

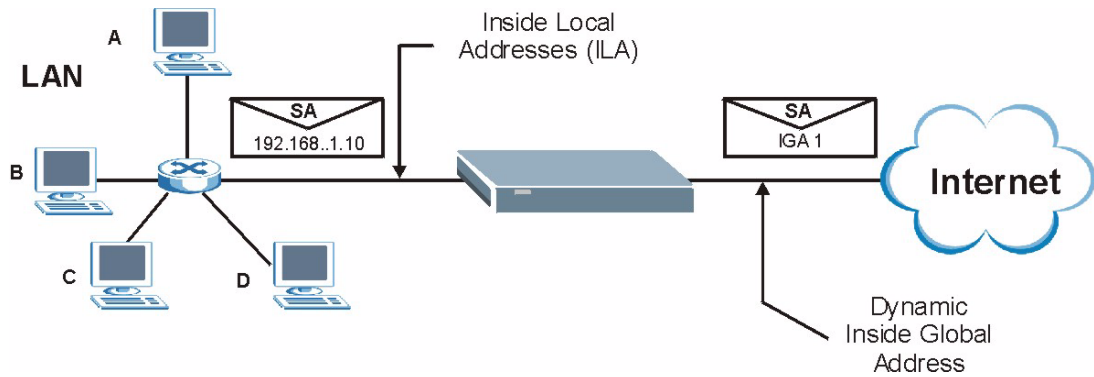


Figure 109 Menu 4 Internet Access & NAT Example

```

Menu 4 - Internet Access Setup

ISP's Name= MyISP
Encapsulation= ENET ENCAP
Multiplexing= LLC-based
VPI #= 8
VCI #= 35
Service Name= N/A
My Login= N/A
My Password= N/A

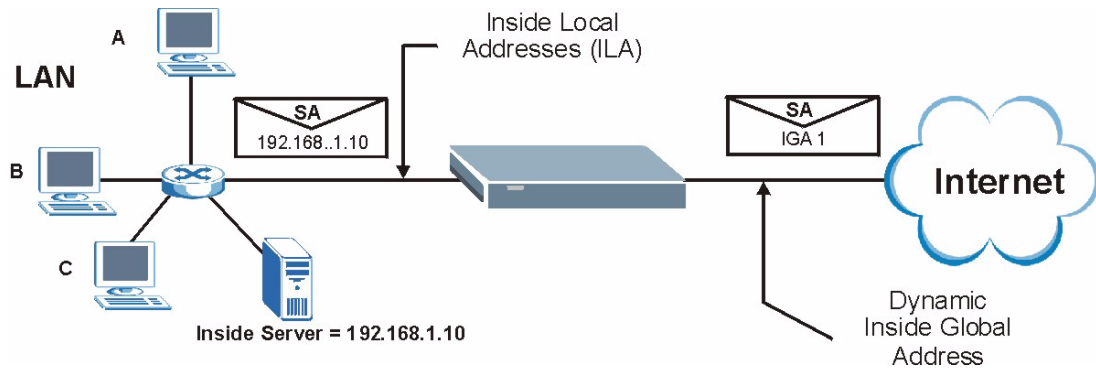
NAT= SUA Only
  Address Mapping Set= N/A
  IP Address Assignment= Dynamic
  IP Address= N/A
  ENET ENCAP Gateway= N/A

Press ENTER to Confirm or ESC to Cancel:
Press Space Bar to Toggle.
    
```

From menu 4, choose the **SUA Only** option from the **Network Address Translation** field. This is the **Many-to-One** mapping discussed in [Section 20.5 on page 180](#). 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.

20.5.2 Example 2: Internet Access with an Inside Server

Figure 110 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 111 Menu 15.2.1 Specifying an Inside Server

Menu 15.2 - NAT Server Setup

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:

20.5.3 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).

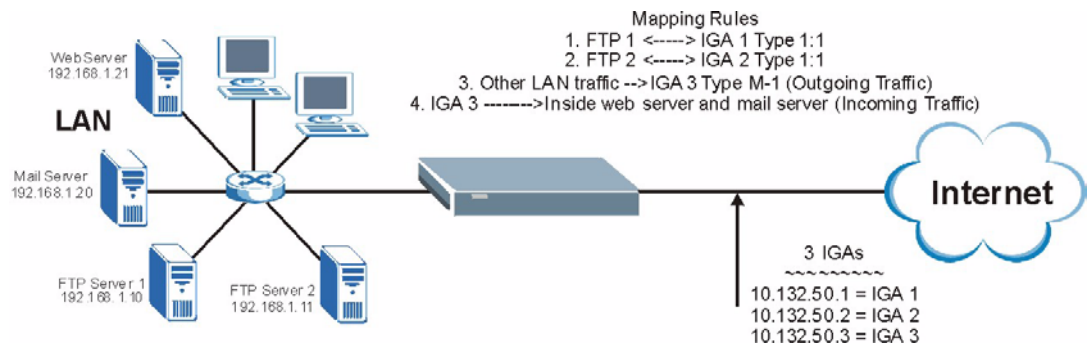
Map the second IGA to our second inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).

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 112 NAT Example 3



In this case you need to configure Address Mapping Set 1 from **Menu 15.1 - Address Mapping Sets**. Therefore you must choose the **Full Feature** option from the **Network Address Translation** field (in menu 4 or menu 11.3) in [Figure 113 on page 184](#).

- 1** Enter 15 from the main menu.
- 2** Enter 1 to configure the Address Mapping Sets.
- 3** Enter 1 to begin configuring this new set. Enter a Set Name, choose the **Edit Action** and then enter 1 for the **Select Rule** field. Press [ENTER] to confirm.
- 4** Select **Type** as **One-to-One** (direct mapping for packets going both ways), and enter the local **Start IP** as 192.168.1.10 (the IP address of FTP Server 1), the global **Start IP** as 10.132.50.1 (our first IGA). (See [Figure 114 on page 184](#)).
- 5** Repeat the previous step for rules 2 to 4 as outlined above.

Figure 113 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)= N/A
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= 1
Metric= 2
Private= No
RIP Direction= None
    Version= RIP-1
Multicast= None
IP Policies=

Enter here to CONFIRM or ESC to CANCEL:
```

The following figures show how to configure the first rule

Figure 114 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 115 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 116 Example 3: Menu 15.2.1

```

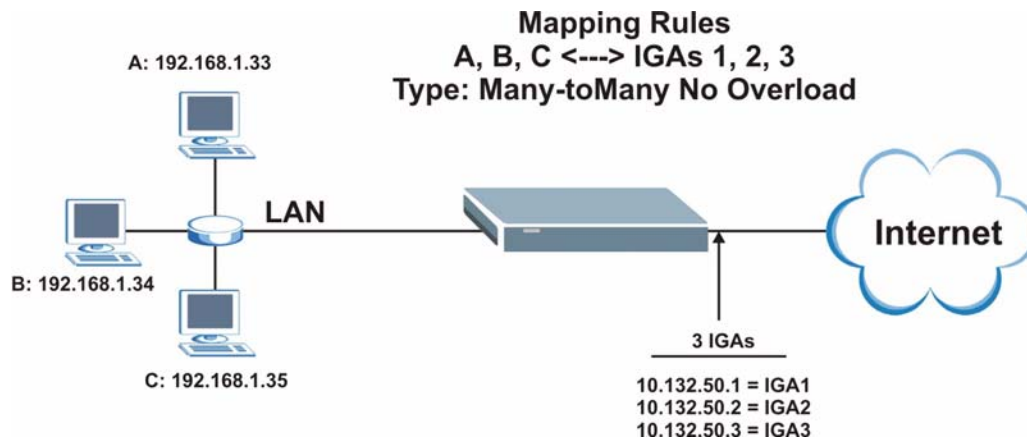
Menu 15.2.1 - NAT Server Setup
Rule  Start Port No.  End Port No.  IP Address
-----
 1.  Default          Default        0.0.0.0
 2.  80                80             192.168.1.21
 3.  25                25             192.168.1.20
 4.  0                  0              0.0.0.0
 5.  0                  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:
    
```

20.5.4 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 117 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 118 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 119 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 21

Filter Configuration

This chapter shows you how to create and apply filters.

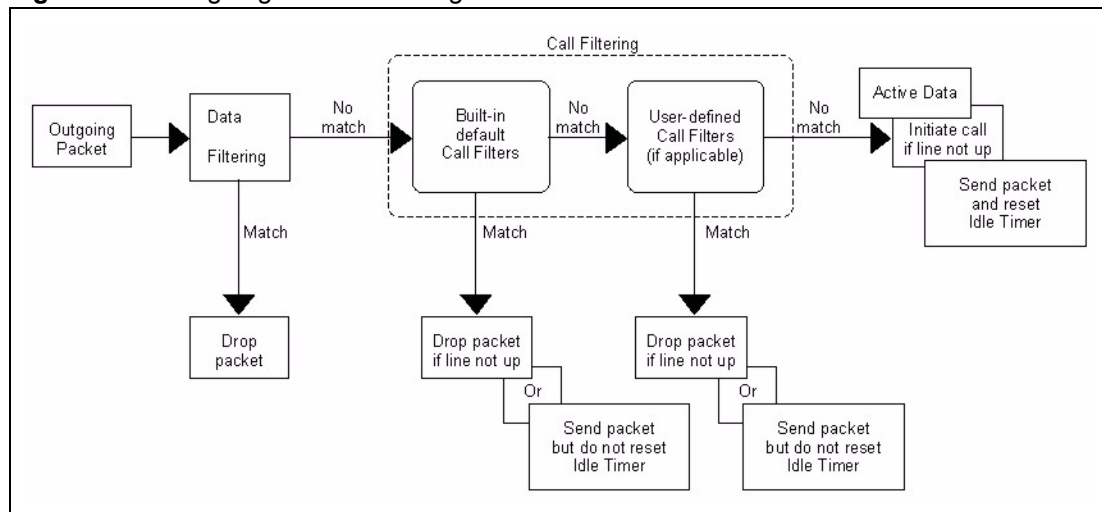
21.1 About Filtering

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.

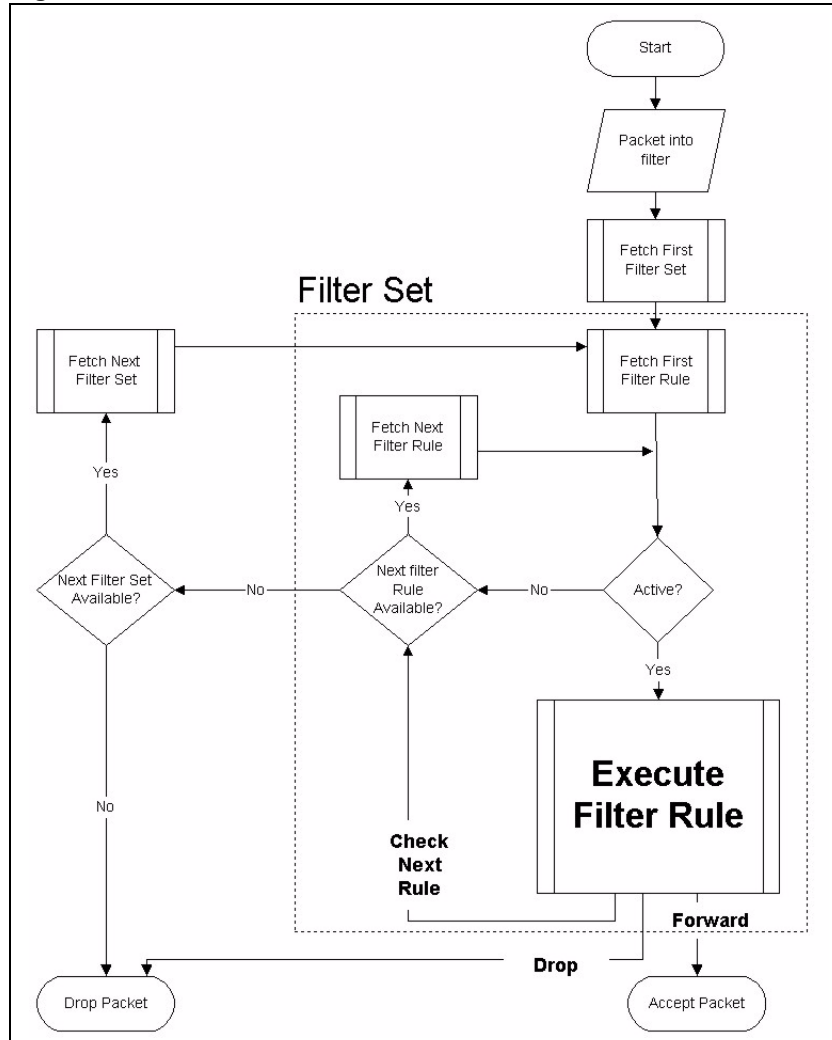
Outgoing packets must undergo data filtering before they encounter call filtering. Call filters are divided into two groups, the built-in call filters and user-defined call filters. Your Prestige has built-in call filters that prevent administrative, for example, RIP packets from triggering calls. These 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 120 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 121 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.

21.1.1 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.

21.2 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 Set Configuration**.
- 2 Enter 1 to display **Menu 21.1 – Filter Set Configuration** as shown next.

Figure 122 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 123 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 124 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 125 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:
    
```

21.3 Filter Rules Summary Menus

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

Table 55 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 55 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 56 Rule Abbreviations Used

	DESCRIPTION
IP	
	Protocol
SA	Source Address
SP	Source Port Number
DA	Destination Address
DP	Destination Port Number
GEN	
	Offset
Len	Length

21.4 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.

21.4.1 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 126 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 57 Menu 21.1.x.1 TCP/IP Filter Rule

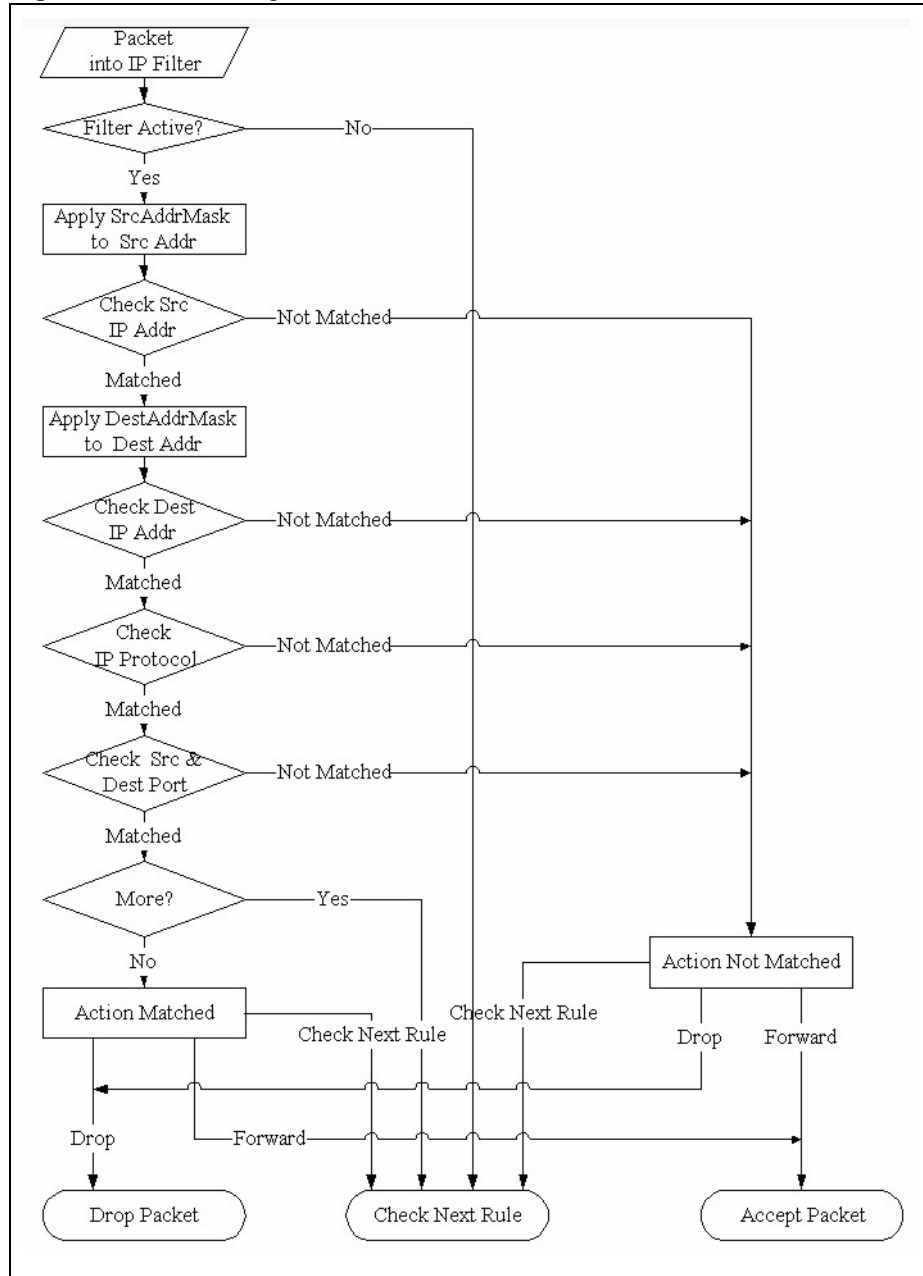
FIELD	DESCRIPTION
Filter #	This is the filter set, filter rule coordinates, for instance, 2, 3 refers to the second filter set and the third filter rule of that set.
Filter Type	Use [SPACE BAR] and then [ENTER] to choose a rule. Parameters displayed for each type will be different. Choices are TCP/IP 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 57 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 127 Executing an IP Filter



21.4.2 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 128 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 58 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 .

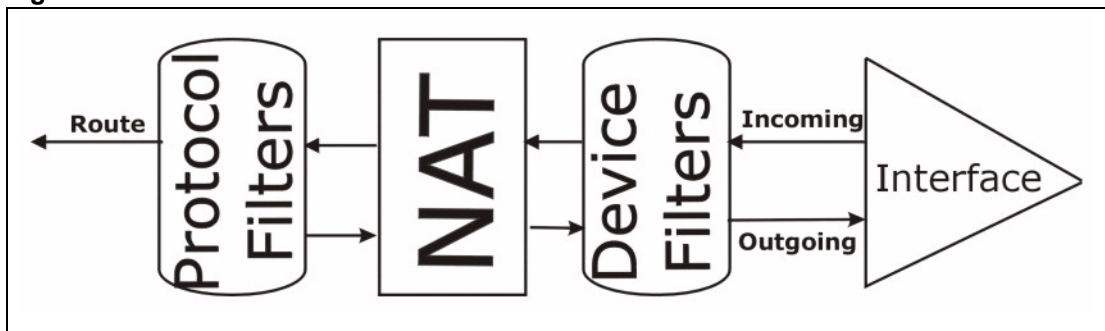
Table 58 Menu 21.1.5.1 Generic Filter Rule (continued)

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.	

21.5 Filter Types and NAT

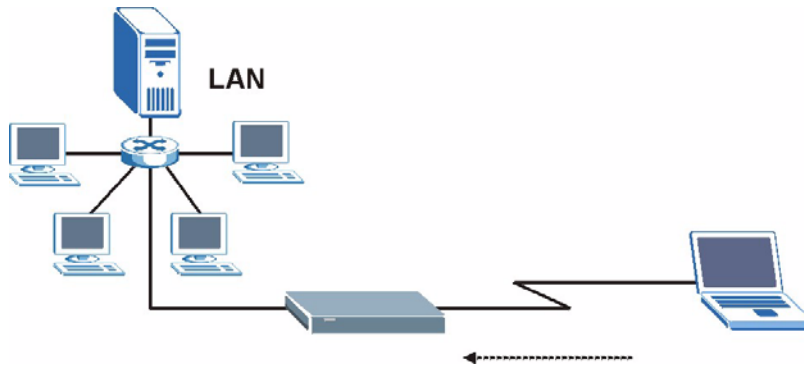
There are two classes of filter rules, **Generic Filter** Device rules and Protocol Filter (**TCP/IP**) rules. Generic Filter rules act on the raw data from/to LAN and WAN. Protocol Filter rules act on IP packets.

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 129 Protocol and Device Filter Sets

21.6 Example Filter

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

Figure 130 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 131 Menu 21.1.6.1 Sample Filter

```

Menu 21.2.2 - TCP/IP Filter Rule

Filter #: 2,2
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:
Press Space Bar to Toggle.

```

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 132 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
    
```

21.7 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 59 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.

21.7.1 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 133 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:

```

21.7.2 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 134 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 22

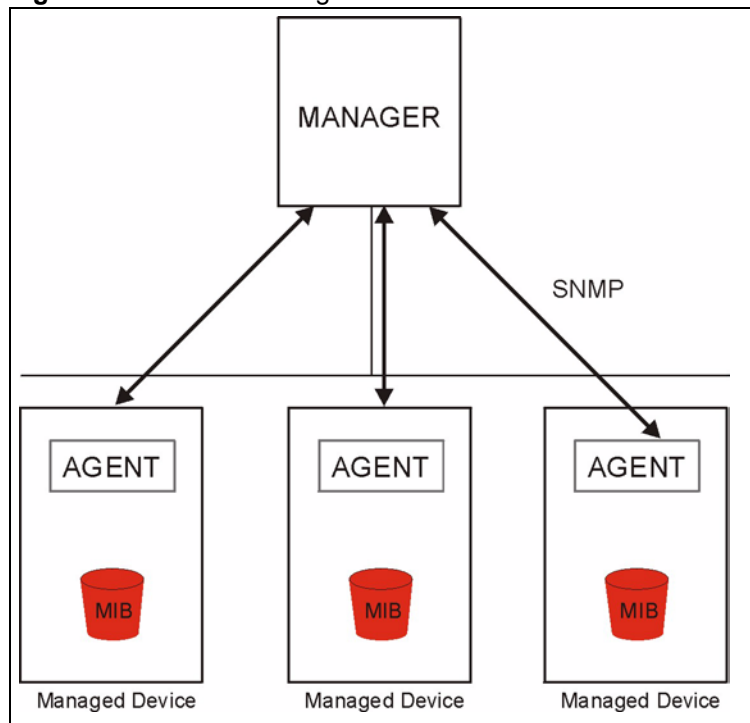
SNMP Configuration

This chapter explains SNMP Configuration menu 22.

22.1 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 135 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.

22.2 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.

22.3 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 136 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 60 Menu 22 SNMP Configuration

FIELD	DESCRIPTION
SNMP:	
	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:	
	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.	

22.4 SNMP Traps

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

Table 61 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
1	coldStart (<i>defined in RFC-1215</i>)	A trap is sent after booting (power on).
2	warmStart (<i>defined in RFC-1215</i>)	A trap is sent after booting (software reboot).
3	linkDown (<i>defined in RFC-1215</i>)	A trap is sent with the port number when any of the links are down. See the following table.
4	linkUp (<i>defined in RFC-1215</i>)	A trap is sent with the port number.

Table 61 SNMP Traps (continued)

TRAP #	TRAP NAME	DESCRIPTION
5	authenticationFailure (<i>defined in RFC-1215</i>)	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 62 Ports and Permanent Virtual Circuits

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

CHAPTER 23

System Information and Diagnosis

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

23.1 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 137 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:
```

23.2 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 138 Menu 24.1 System Maintenance : Status

Menu 24.1 - System Maintenance - Status							
20:54:43							
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
2-1483	N/A	0	0	0	0	0	0:00:00
3-1483	N/A	0	0	0	0	0	0:00:00
4-1483	N/A	0	0	0	0	0	0:00:00
5-1483	N/A	0	0	0	0	0	0:00:00
6-1483	N/A	0	0	0	0	0	0:00:00
7-1483	N/A	0	0	0	0	0	0:00:00
	N/A	0	0	0	0	0	0:00:00
	N/A	0	0	0	0	0	0:00:00
	N/A	0	0	0	0	0	0:00:00
My WAN IP (from ISP): 0.0.0.0							
Ethernet:			WAN:				
Tx Pkts: 2510			Line Status: Down				
Rx Pkts: 0			Upstream Speed: 0 kbps				
CPU Load = 0.33%			Downstream Speed: 0 kbps				
Press Command:							
COMMANDS: 1-Reset Counters ESC-Exit							

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

Table 63 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.
WAN	This shows statistics for the WAN.

Table 63 Menu 24.1 System Maintenance: Status (continued)

FIELD	DESCRIPTION
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.

23.3 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 139 Menu 24.2 System Information and Console Port Speed

<pre> Menu 24.2 - System Information and Console Port Speed 1. System Information 2. Console Port Speed Please enter selection: </pre>
--

23.3.1 System Information

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

Figure 140 Menu 24.2.1 System Maintenance: Information

```

Menu 24.2.1 - System Maintenance - Information

Name: P861H
Routing: IP/BRIDGE
ZyNOS F/W Version: V3.40(RI.3) | 03/24/2005
VDSL Chipset Vendor: Ikanos, Version 6.5.2r6
Standard: 998-138-8500(3Band)

LAN
Ethernet Address: 00:a0:c5:01:23:45
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 64 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.
VDSL Chipset Vendor	Displays the vendor of the VDSL chipset and DSL version.
Standard	This refers to the operational protocol the Prestige and the DSLAM (Digital Subscriber Line Access Multiplexer) are using.
LAN	
	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.

23.3.2 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 141 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.

23.4 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.

23.4.1 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 142 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 143 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):

```

23.5 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 144 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 65 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 24

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.

24.1 Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the menus such as password, DHCP Setup, TCP/IP Setup, etc. It arrives from ZyXEL with a "rom" filename extension. Once you have customized the Prestige's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the "ras" file) is the system firmware and has a "bin" filename extension. With many FTP and TFTP clients, the filenames are similar to those seen next.

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

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file "firmware.bin" to the Prestige.

```
ftp> get rom-0 config.cfg
```

This is a sample FTP session saving the current configuration to the computer file "config.cfg".

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the Prestige only recognizes "rom-0" and "ras". Be sure you keep unaltered copies of both files for later use.

The following table is a summary. Please note that the internal filename refers to the filename on the Prestige and the external filename refers to the filename not on the Prestige, that is, on your computer, local network or FTP site and so the name (but not the extension) may vary. After uploading new firmware, see the **ZyNOS F/W Version** field in **Menu 24.2.1 – System Maintenance – Information** to confirm that you have uploaded the correct firmware version. The AT command is the command you enter after you press “y” when prompted in the SMT menu to go into debug mode.

Table 66 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

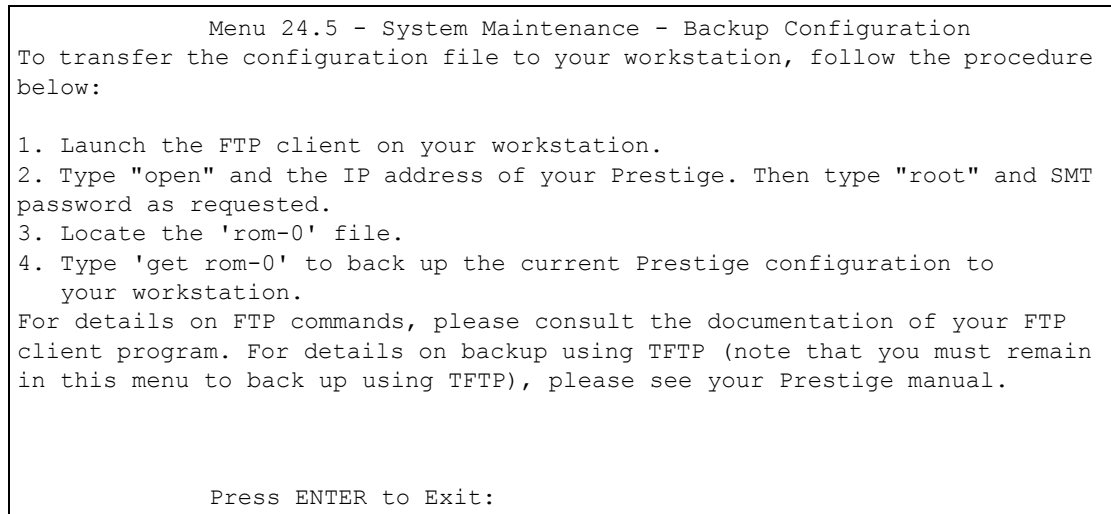
24.2 Backup Configuration

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.

24.2.1 Backup Configuration

Follow the instructions as shown in the next screen.

Figure 145 Telnet in Menu 24.5

24.2.2 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.

24.2.3 Example of FTP Commands from the Command Line

Figure 146 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

```

24.2.4 GUI-based FTP Clients

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

Table 67 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).

24.2.5 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.

24.2.6 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.

24.2.7 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`.

24.2.8 GUI-based TFTP Clients

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

Table 68 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 24.2.5 on page 217](#) to read about configurations that disallow TFTP and FTP over WAN.

24.3 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.

24.3.1 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 147 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.

24.3.2 Restore Using FTP Session Example

Figure 148 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 24.2.5 on page 217](#) to read about configurations that disallow TFTP and FTP over WAN.

24.4 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 24.2 on page 215](#) 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.

24.4.1 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 149 Telnet Into Menu 24.7.1 Upload System Firmware

```
Menu 24.7.1 - System Maintenance - Upload System Firmware

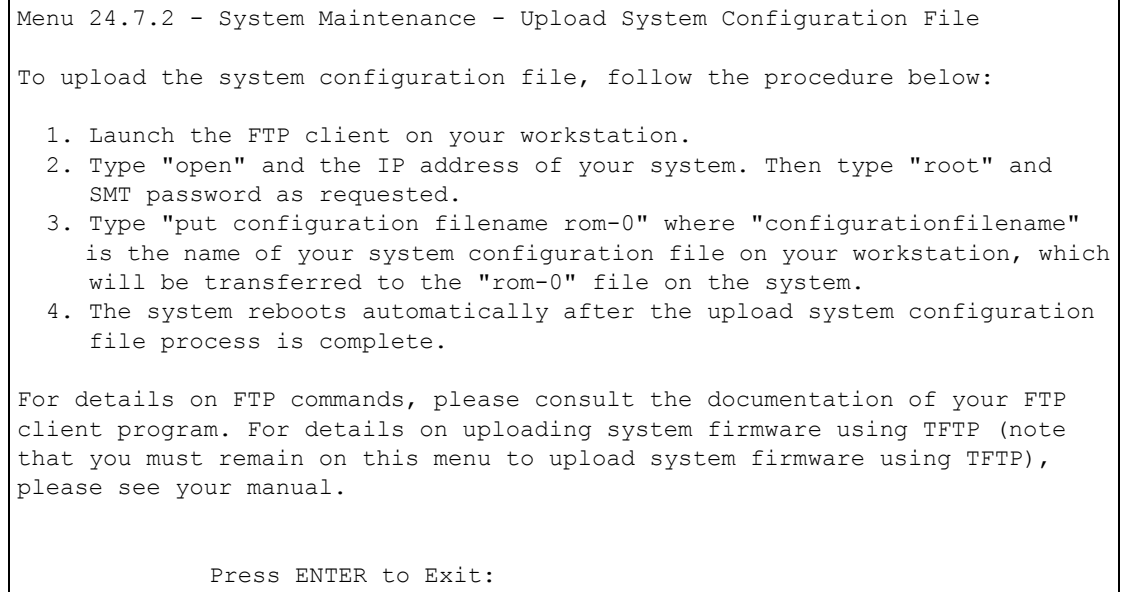
To upload the system firmware, follow the procedure below:
1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your system. Then type "root" and
   SMT password as requested.
3. Type "put firmware filename ras" where "firmwarefilename" is the name
   of your firmware upgrade 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:
```

24.4.2 Configuration File Upload

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

Figure 150 Telnet Into Menu 24.7.2 System Maintenance

To upload the firmware and the configuration file, follow these examples

24.4.3 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.

24.4.4 FTP Session Example of Firmware File Upload

Figure 151 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 24.2.5 on page 217](#) to read about configurations that disallow TFTP and FTP over WAN.

24.4.5 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.

24.4.6 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 25

System Maintenance

This chapter leads you through SMT menus 24.8 to 24.10.

25.1 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 152 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 153 Valid Commands

```
P861H> ?
Valid commands are:
sys          exit          ether          wan
ip           bridge         vdsl
P861H>
```

25.2 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 154 Menu 24.9 System Maintenance: Call Control

```
Menu 24.9 - System Maintenance - Call Control

1. Budget Management

Enter Menu Selection Number:
```

25.2.1 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 155 Menu 24.9.1 System Maintenance: Budget Management

Menu 24.9.1 - Budget Management			
Remote Node	Connection Time/Total Budget	Elapsed Time/Total Period	
1.MyISP	No Budget	No Budget	
2.MDWARE	No Budget	No Budget	
3.IGMP	No Budget	No Budget	
4.VIDEO-1	No Budget	No Budget	
5.VIDEO-2	No Budget	No Budget	
6.VIDEO-3	No Budget	No Budget	
7.VIDEO-4	No Budget	No Budget	
8.-----	---	---	
9.-----	---	---	
10.-----	---	---	
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 69 Menu 24.9.1 System Maintenance: Budget Management

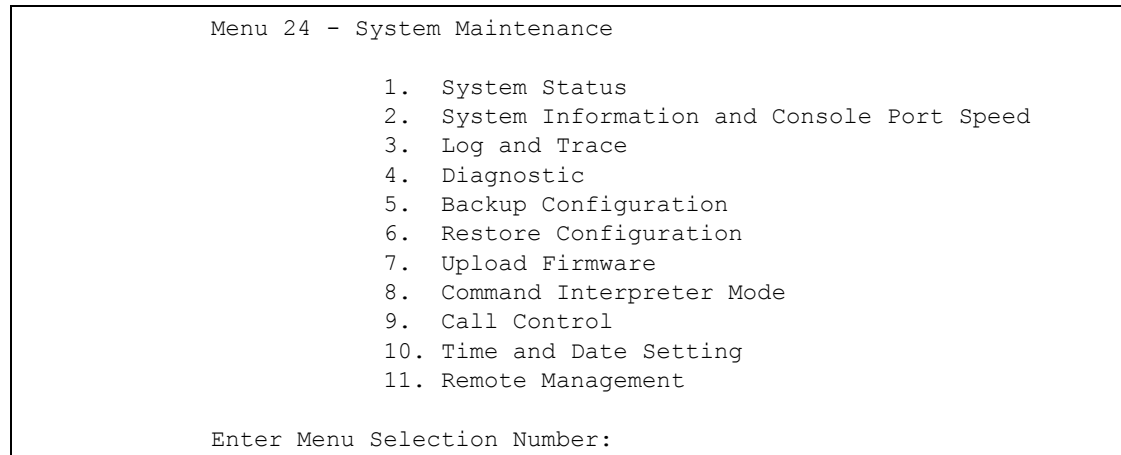
FIELD	DESCRIPTION
Remote Node	Enter the index number of the remote node you want to reset (just one in this case)
Connection Time/Total Budget	This is the total connection time that has gone by (within the allocated budget that you set in menu 11.1.
Elapsed Time/Total Period	The period is the time cycle 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.	

25.3 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 156 Menu 24 System Maintenance



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 157 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:                22 : 18 : 04
New Time (hh:mm:ss):        22 : 18 : 01

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:

Press Space Bar to Toggle.
    
```

Table 70 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.
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.	

25.3.1 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 26

Remote Management

This chapter covers remote management (SMT menu 24.11).

26.1 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.

26.2 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**.

26.2.1 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 158 Menu 24.11 Remote Management Control

```

Menu 24.11 - Remote Management Control

TELNET Server:
  Server Port = 23                Server Access = ALL
  Secured Client IP = 0.0.0.0

FTP Server:
  Server Port = 21                Server Access = ALL
  Secured Client IP = 0.0.0.0

Web Server:
  Server Port = 80                Server Access = ALL
  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 71 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.	

26.2.2 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.

26.3 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.

26.4 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 27

IP Policy Routing

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

27.1 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.

27.2 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.

27.3 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.

27.4 IP Routing Policy Setup

Menu 25 shows all the policies defined.

Figure 159 Menu 25 IP Routing Policy Setup

```

Menu 25 - IP Routing Policy Setup

Policy          Policy
Set #          Set #
-----          -----
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 160 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 72 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 161 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 73 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 Thrupt, 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 73 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.	

27.5 Applying an IP Policy

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

27.5.1 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 162 Menu 3.2 TCP/IP and DHCP Ethernet Setup

```
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= 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-2B
Multicast= IGMP-v2
IP Policies=
Edit IP Alias= No

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

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 163 Menu 11.3 Remote Node Network Layer Options

```
Menu 11.3 - Remote Node Network Layer Options

IP Options:                               Bridge Options:
IP Address Assignment = Dynamic           Ethernet Addr Timeout(min)= 0
Rem IP Addr = 0.0.0.0
Rem Subnet Mask= 0.0.0.0
My WAN Addr= N/A
NAT= Full Feature
    Address Mapping Set= 1
Metric= 2
Private= No
RIP Direction= None
    Version= RIP-1
Multicast= None
IP Policies=

Enter here to CONFIRM or ESC to CANCEL:

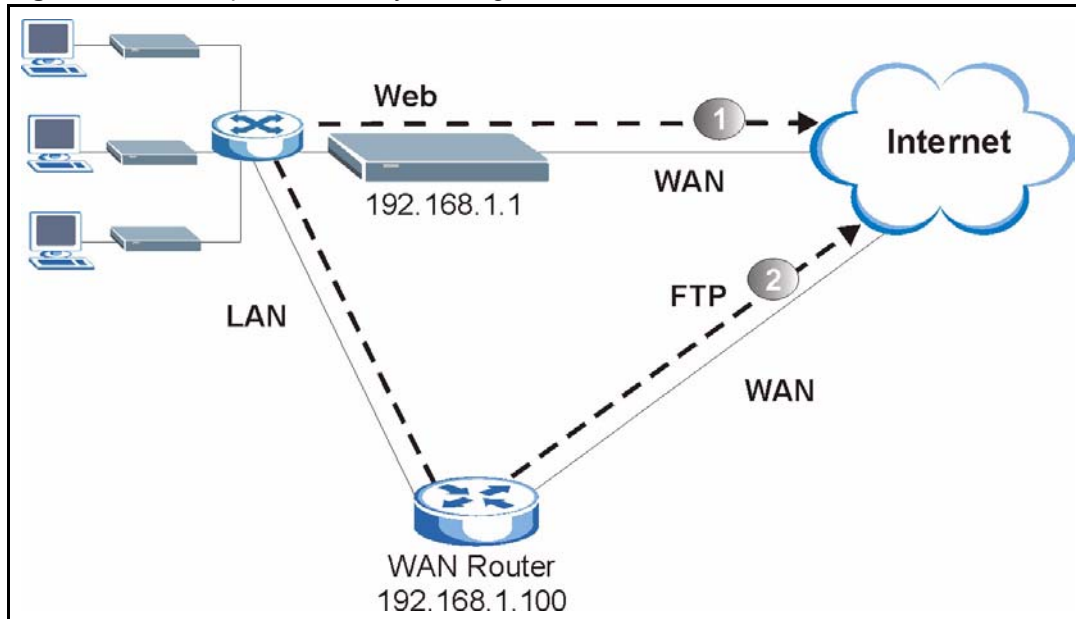
Press Space Bar to Toggle.
```

27.6 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 164 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 165 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:
    addr start= 192.168.1.2          end= 80
    port start= 0                    Log= No
  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 166 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:
  addr start= 0.0.0.0                             end= 21
  port start= 0                                   Log= No
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 167 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= 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-2B
Multicast= IGMP-v2
IP Policies= 1,2
Edit IP Alias= No

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

CHAPTER 28

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.

28.1 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 168 Menu 26 Schedule Setup

Menu 26 - Schedule Setup			
Schedule Set #	Name	Schedule 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 169 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:
Press Space Bar to Toggle.
    
```

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 74 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 74 Menu 26.1 Schedule Set Setup (continued)

FIELD	DESCRIPTION
Action	<p>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.</p> <p>Forced Down means that the connection is blocked whether or not there is a demand call on the line.</p> <p>Enable Dial-On-Demand means that this schedule permits a demand call on the line.</p> <p>Disable Dial-On-Demand means that this schedule prevents a demand call on the line.</p>
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 170 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 29

Introduction to CLI

This chapter introduces the line commands.

29.1 Command Line Interface Overview

In addition to the SMT, you can use line commands to configure the Prestige. It is recommended that you use the SMT for everyday management of the Prestige and that you use line commands for advanced Prestige diagnosis and troubleshooting. If you have problems with your Prestige, customer support may request that you issue some of these commands to assist them in troubleshooting.

29.1.1 Accessing the Command Line Interface

There are two ways to access the command line interface on the Prestige:

- Telnet to the Prestige
- Connect a computer to the console port and use terminal emulation software configured to the following parameters:
 - VT100 terminal emulation
 - 9600 bps
 - No parity, 8 data bits, 1 stop bit
 - No flow control

29.1.2 Command Conventions

The system uses a one-level command structure. You must type the full command every time, as follows.

```
P861H> <command>
```

For instance, the following example shows how to view the status of a VDSL port.

```
P861H> vdsl profile show
```

The conventions for typing in most CLI commands are shown next.

```
command <interface|device> subcommand [parameter]
```

```
command subcommand [parameter]
```

Note: Type all commands as displayed on the screen.

29.1.3 Command Syntax Conventions

Command keywords are in courier new font.

The | symbol means “or”.

Required fields in a command are enclosed in angle brackets <>. Use the following command to select a baud rate from 1 to 5.

```
sys baud <1|2|3|4|5>
```

Optional fields in a command are enclosed in square brackets [], for example, year; month and day are optional in the following command. This command just displays the date if you don't specify the year, month and day parameters.

```
sys date [year month day]
```

Commands can be abbreviated to the smallest unique string that differentiates the command. For example the “system date” command could be abbreviated to “s d”.

29.2 help Command

Type “help” or “?” to display a list of valid commands or type a command followed by “help” or “?” to display a list of associated subcommands. The following figure shows sample help information.

Figure 171 CLI Help : Sample Output

```
Copyright (c) 1994 - 2005 ZyXEL Communications Corp.

P861H> help
Valid commands are:
sys                exit                ether                wan
ip                 bridge                vdsl
P861H>
```

29.3 exit Command

Syntax:

```
exit
```

This command ends the console or telnet session.

CHAPTER 30

System Commands

This chapter shows you the information about the system and gives a summary of commands available.

30.1 System Commands Overview

These are commands that you may use frequently in configuring and maintaining your switch.

30.2 System Configuring

The rest of this chapter shows commonly used command examples. System is a tool that can be used to monitor your Prestige. Specifically, it gives you information on your VDSL telephone line status, number of packets sent and received. Note that these fields are READ-ONLY and are meant to be used for diagnostic purposes.

30.3 sys Commands

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

Table 75 sys Command Summary

MODULE	COMMAND	SUB-COMMAND	ARGUMENTS	DESCRIPTION
sys	version			This command displays the RAS code.
	cpu	display		Displays the CPU's utilization.
		counter		This command displays the MAC and SAR counters from the CPU.
		clrctr		This command clears the CPU's MAC and SAR counters.
	spt	save		This command stores the configuration in the non-volatile memory.
	adjtime			Retrieves the date and time from the time server specified in SMT menu 24.10.
	callhist	display		Displays the call history.
		remove	<index>	Removes an entry from the call history.
	countrycode		[countrycode]	Sets or displays the country code.

Table 75 sys Command Summary

MODULE	COMMAND	SUB-COMMAND	ARGUMENTS	DESCRIPTION
	date		[year month date]	Sets or displays the system's current date.
	domainname			Displays the domain name that the device sends to the LAN DHCP clients.
	edit		<filename>	Edits the system preset text file such as autoexec.net.
	feature			Displays a list of the device's major features.
	hostname		[hostname]	Sets or displays the system name.
	logs	category	access [0:none/ 1:log/ 2:alert/ 3:both]	Records and/or sends alerts for access control logs.
			display	Displays the category settings.
			error [0:none/ 1:log/ 2:alert/ 3:both]	Records and/or sends alerts for system error logs.
			mten [0:none/ 1:log]	Records the system maintenance logs.
			upnp [0:none/ 1:log]	Records the UPnP logs.
			urlblocked [0:none/ 1:log/ 2:alert/ 3:both]	Records and/or sends alerts for web access blocked logs.
			urlforward [0:none/ 1:log]	Records web access forward logs.
		clear		Clears the log.
		display		Displays the log.
		load		Loads the log settings buffer. Use this command before you configure the log settings. Use sys logs save after you configure the log settings.
		mail	alertAddr [mail address]	Send alerts to this e-mail address.
			clearlog [0:no/1:yes]	Clears the logs.
			display	Displays the logs and alerts mail settings.
			logAddr [mail address]	Send logs to this e-mail address.

Table 75 sys Command Summary

MODULE	COMMAND	SUB-COMMAND	ARGUMENTS	DESCRIPTION
			schedule display	Displays the mail schedule.
			schedule hour [0-23]	Sets the hour to send logs.
			schedule minute [0-59]	Sets the minute to send the logs.
			schedule policy [0:full/ 1:hourly/ 2:daily/ 3:weekly/ 4:none]	Sets the mail schedule policy.
			schedule week [0:sun/1:mon/ 2:tue/3:wed/ 4:thu/5:fri/ 6:sat]	Sets the day of the week for sending weekly logs.
			server [domainName/ IP]	Sets the domain name or IP address of the mail server to which to send the logs.
			subject [mail subject]	Sets the log e-mail's subject.
			sendmail	
		save		Save the log settings from the buffer.
		syslog	active [0:no/ 1:yes]	Enables/disables syslog logging.
			display	Displays the syslog settings.
			facility [Local ID(1- 7)]	Specifies the file to which the device logs the syslog messages.
			server [domainName/ IP]	Specifies the domain name or IP address of the syslog server to which to send the syslogs.
	stdio		[minute]	Sets or displays the management terminal idle timeout value.
	time		[hour [min [sec]]]	Sets or displays the system time.
	trcdisp			
	trclog			
	trcpacket			
	view		<filename>	Displays the specified text file.
	wdog			
		switch	[on off]	Turns the watchdog firmware protection feature on or off.

Table 75 sys Command Summary

MODULE	COMMAND	SUB-COMMAND	ARGUMENTS	DESCRIPTION
		cnt	[value]	Sets (0-34463) or displays the current watchdog count (in 1.6 sec units).
	dreset			Resets node and mask.
	romreset			Restores the factory default configuration file.
	atsh			
	xmodemmode		[crc checksum]	Displays the mode that Xmodem uses.
	socket			Displays the system socket's ID #, type, control block address (PCB), IP address and port number of peer device connected to the socket (Remote Socket) and task control block (Owner).
	filter			
		netbios		
			disp	Displays the current NetBIOS filter modes.
			config <0:LAN to WAN, 1:WAN to LAN, 6:IPSec pass through><on off>	Sets NetBIOS filters.
	ddns	debug		Turns on/off the displaying of DDNS debug messages.
		display		Displays DDNS information.
		restart		Restarts DDNS.
		logout		This command has no effect.

30.4 sys Command Examples

These are some examples of the commands that belong to the sys (system) group of commands.

30.4.1 sys version

Syntax:

```
sys version
```

This command clears the system error log.

The following screen displays the RAS code, firmware version, system uptime and bootbase version

Table 76 sys version

```
P861H> sys version
ZyNOS version: V3.40(RD.1) | 08/19/2004
romRasSize: 1571276
system up time: 25:35:40 (8c9809 ticks)
bootbase version: V1.02(P861H) | 05/25/2004

P861H>
```

30.4.2 sys logs errlog disp

Syntax:

```
sys logs errlog disp
```

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

Table 77 sys logs errlog disp

```
P861H> sys logs errlog disp
 38 Sat Jan 1 00:33:22 2000 PINI ERROR Configuration restored
 39 Sat Jan 1 00:33:27 2000 PP08 INFO LAN promiscuous mode <1>
 40 Sat Jan 1 00:33:27 2000 PINI -WARN SNMP TRAP 1: warm start
 41 Sat Jan 1 00:33:27 2000 PINI -WARN Last errorlog repeat 1 Times
 42 Sat Jan 1 00:33:27 2000 PINI INFO main: init completed
 43 Sat Jan 1 00:33:33 2000 PP17 INFO adjtime task pause 1 day
 44 Sat Jan 1 00:33:51 2000 PP05 WARN MPOA Link Down
 45 Sat Jan 1 00:44:42 2000 PINI INFO SMT Session Begin
 46 Sat Jan 1 00:55:58 2000 PINI INFO SMT Session End
Clear Error Log (y/n):
```

30.4.3 sys logs errlog clear Command Example

Syntax:

```
sys logs errlog clear
```

This command clears the system error log.

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

CHAPTER 31

Ethernet, IP and WAN Commands

This chapter shows you information about the LAN and WAN interfaces and IP address details and gives a summary of commands available.

31.1 Ethernet Commands

The following chart lists and describes the ether commands. Each of these commands must be preceded by ether when you use them. For example, type `ether config` to display information on the LAN configuration.

Table 78 ether Command Summary

MODULE	COMMAND	SUB-COMMAND	ARGUMENTS	DESCRIPTION
ether	version			Displays the Ethernet device type.
	config			Displays information about the configuration block.
	driver	cnt	disp <name>	Displays the Ethernet driver counters.
		ioctl	<ch_name> <command> [arguments]	This command cannot be used currently.
		status	<ch_name>	Shows the LAN status.

31.2 IP Commands

The following chart lists and describes the ip commands. Each of these commands must be preceded by ip when you use them. For example, type `ip address` to display information on the host IP address.

These are the commonly used commands that belong to the ip group of commands.

Table 79 IP Command Summary

MODULE	COMMAND	SUB-COMMAND	ARGUMENTS	DESCRIPTION
ip	address		[addr]	Displays the host IP address.
	alias		<iface>	Sets an alias for the specified interface.

Table 79 IP Command Summary

MODULE	COMMAND	SUB-COMMAND	ARGUMENTS	DESCRIPTION
	aliasdis		<0 1>	Disables/enables the alias for the specified interface.
	arp	status	<iface>	Displays an interface's IP Address Resolution Protocol status.
	dhcp			
	dns	query		
		stats	clear	Clears DNS statistics.
			disp	Displays DNS statistics.
	icmp	status		Displays the ICMP statistics counter.
		discovery	<iface> [on off]	Sets the ICMP router discovery flag.
	ifconfig		[iface] [ipaddr] [broadcast<addr> mtu <value> dynamic]	This command configures a network interface.
	ping		<hostid>	Pings a remote host.
	route	status	[if]	Displays the routing table.
		add	<dest_addr default>[/ <bits>] <gateway> [<metric>]	Adds a route.
		addiface	<dest_addr default>[/ <bits>] <gateway> [<metric>]	Adds an entry to the routing table for the specified interface.
		addprivate	<dest_addr default>[/ <bits>] <gateway> [<metric>]	Adds a private route.
		drop	<host addr> [/<bits>]	Drops a route.
	smtp			
	status			Displays IP statistic counters.
	udp	status		Displays the UDP status.
	rip			
	tcp	status		Displays the TCP statistic counters.
	tftp			

Table 79 IP Command Summary

MODULE	COMMAND	SUB-COMMAND	ARGUMENTS	DESCRIPTION
	xparent		<join break >	
	urlfilter	reginfo		
		category		
		listUpdate		
		ftplist		
		listServerIP		
		listServerName		
		exemptZone	Display	Displays content filtering exempt zone information.
			actionFlags [type (1-3)] [enable/disable]	Enables/disables content filtering exempt zone action flags that determine to which IP addresses to apply content filtering.
			add [ip1] [ip2]	Sets a range of IP addresses to be in the exempt zone.
			delete [ip1] [ip2]	Removes a range of IP addresses from the exempt zone.
			clearAll	Returns the exempt zone settings to the previous configuration.
		customize		Use the customize commands to configure content filtering for trusted web sites, forbidden web sites and keyword blocking.
			display	Displays the content filtering customize action flags.
			actionFlags [act (1-7)] [enable/disable]	Sets the content filtering customize action flags.
			logFlags [type (1-3)] [enable/disable]	Sets the content filtering customize log flags.
			add [string] [trust/ untrust/ keyword]	Adds a trusted web site, forbidden web site or keyword blocking string.
			delete [string] [trust/ untrust/ keyword]	Deletes a trusted web site, forbidden web site or keyword blocking string.
			clearAll	Return to the default configuration.
	igmp	debug	[level]	Sets IGMP debug level.

Table 79 IP Command Summary

MODULE	COMMAND	SUB-COMMAND	ARGUMENTS	DESCRIPTION
		forwardall	[on off]	Activates/deactivates IGMP forwarding to all interfaces flag.
		querier	[on off]	Turns on/off IGMP stop query flag.
		iface	<iface> grouptm <timeout>	Sets IGMP group timeout for the specified interface.
			<iface> interval <interval>	Sets IGMP query interval for the specified interface.
			<iface> join <group>	Adds an interface to a group.
			<iface> leave <group>	Removes an interface from a group.
			<iface> query	Sends an IGMP query on the specified interface.
			<iface> rsptime [time]	Sets the IGMP response time.
			<iface> start	Turns on IGMP on the specified interface.
			<iface> stop	Turns off IGMP on the specified interface.
			<iface> ttl <threshold>	Sets the IGMP Time To Live threshold.
			<iface> v1compat [on off]	Turns on/off IGMP version 1 compatibility on the specified interface.
		robustness	<num>	Sets the IGMP robustness variable.
		status		Displays the IGMP status.
	pr			

31.3 ip Command Examples

These are some examples of the commands that belong to the ip (IP address) group of commands.

31.3.1 ip ping

Syntax:

```
ip ping <hostid>
```

This command pings a remote host. An example is shown next.

Figure 172 ip ping

```
P861H> ip ping 192.168.1.16

Resolving 192.168.1.16... 192.168.1.16
      sent      rcvd  rate   rtt    avg    mdev    max    min
        1         1  100    7     7     0      7     7
        2         2  100    4     7     1      7     4
        3         3  100    4     7     2      7     4
P861H>
```

31.3.2 ip route status

Syntax:

```
ip route status
```

This command displays the routing table. An example is shown next.

Figure 173 ip route status

```
P861H> ip route status
Dest          FF Len Device      Gateway      Metric stat Timer  Use
192.168.1.0   00 24  enet0       192.168.1.1  1    041b 0    3
172.16.0.0    00 16  swp00       192.168.1.2  2    801b 0    0
127.0.0.0     00 8   swp00       127.0.0.1    1    041b 0    0
P861H>
```

31.3.3 ip arp status

Syntax:

```
ip arp status
```

This command displays all interfaces' IP Address Resolution Protocol (ARP) status. An example is shown next.

Figure 174 ip arp status

```

P861H> ip arp status
received 0 badtype 0 bogus addr 0 reqst in 0 replies 0 reqst out 1
cache hit 2 (40%), cache miss 3 (60%)
IP-addr      Type      Time  Addr      stat iface
192.168.1.255  10 Mb Ethernet 0      ff:ff:ff:ff:ff:ff 43  NULL
num of arp entries= 1
P861H>

```

31.4 WAN Commands

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

Table 80 WAN Command Summary

MODULE	COMMAND	SUB-COMMAND	ARGUMENTS	DESCRIPTION
wan	hwsar	oam	<vpi> <vci> <Option1> <Option2> <Type>	Use this command to perform an oam test where <Option1>: 0 (F4), 1 (F5) <Option2>: 0 (Segment-To-Segment), 1 (End-To-End) <Type>: 0 (AIS), 1 (RDI), 2 (LoopBack)
		loopback	<option>	Use this command to perform a loopback test where <option>: 0 (off), 1 (on)

CHAPTER 32

VDSL Commands

This chapter shows you how to configure VDSL using line interface commands.

32.1 VDSL Commands Overview

Line interface commands contain advanced configuration features that may be used for debugging and troubleshooting. Exercise caution when using commands as incorrect usage may damage your Prestige.

See [Table 81 on page 264](#) for an overview of VDSL commands.

32.2 Command Summary

The following tables are summaries of the commands available in the Prestige together with a brief description of each command. See the related section in the User's Guide for more background information.

32.2.1 vdsl Commands

Valid commands are:

Table 81 vdsl Command Summary

MODULE	COMMAND	SUB-COMMAND	ARGUMENTS	DESCRIPTION
vdsl	port	clrcntr		Clears the current performance counter.
		counter		Gets the current performance counter from the VDSL modem.
		snr		If the VDSL line is not up, no output is displayed. Otherwise it displays the SNR ratio of the current connection.
		speed		If the VDSL line is up, then it will display the line rate and payload rate. Otherwise a row of zeros is displayed. The transmit power is also displayed.

Table 81 vdsl Command Summary

MODULE	COMMAND	SUB-COMMAND	ARGUMENTS	DESCRIPTION
	profile	actv		This command sends the current selected profile to BME (VDSL modem). It downloads modem code into BME and also sends system and port provisioning data to BME. BME then starts a linkup attempt with the VDSL line. The command will have no effect if the current used profile has the same settings as the current running profile settings.
		default		Reset profile setting to factory defaults.
		show		Display all detailed attributes of the current or default profile.
	pvc	list		Display all detailed attributes of the current or default profile.
	version			This command displays the driver version.

32.3 VDSL Default Values

The default values for the following VDSL parameters are shown in the next table.

Table 82 VDSL Default Values

	DEFAULT VALUE
VDSL Active	on
VDSL Upstream Power Backoff(UPBO) Option	disable
VDSL Channel Type (Latency Mode)	interleave
Upstream Max interleave delay	10ms
Downstream Max interleave delay	10ms
VDSL Band Modifier	0x11 (The lowest DS frequency starts from 138KHz)

32.3.1 Service Categories

Service categories ensure that high priority transmissions get the bandwidth they need.

CBR (Constant Bit Rate) provides a fixed amount of bandwidth that is always available even if no data is being sent. A PCR is specified and if traffic exceeds this rate, cells may be dropped. An example application is a T1 circuit.

rt-VBR (real-time Variable Bit Rate) also provides a fixed amount of bandwidth (a PCR is specified) but is only available when data is being sent. An example application is real-time videoconferencing.

nrt-VBR (non-real-time Variable Bit Rate) is commonly used for “bursty” traffic typical on LANs. PCR and MBS define the burst levels, SCR defines the minimum level. An example application is multimedia e-mail.

Unspecified Bit Rate (UBR) does not guarantee bandwidth or throughput. Cells are dropped if there is not enough bandwidth. Only the PCR is set. An example application is background file transfer.

Table 83 Service Characteristic

CHARACTERISTIC	CBR	RT-VBR	NRT-VBR	UBR
Guaranteed Bandwidth	Yes	Yes	Yes	No
Good for Real-Time Traffic	Yes	Yes	No	No
Suitable for Bursty Traffic	No	No	Yes	Yes

32.4 Interleave Delay

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

An interleave delay of “0” means no interleaving takes place and transmission is faster (a “fast channel”). This would be suitable if you have a good line where little error correction is necessary.

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

32.5 SNR (Signal-to-Noise-Ratio)

The Prestige uses SNR(Signal-to-Noise-Ratio) to determine line quality. SNR is the ratio of the amplitude of the actual signal to the amplitude of noise signals at a given point in time. A slow SNR indicates poor line quality. When SNR (upstream or downstream) falls below a pre-determined threshold, the Prestige then uses rate adaptation.

32.6 VDSL Command Examples

You must type the main command first and then the sub-commands, as follows:

```
P861H> vdsl
vdsl> port snr
```

The rest of this chapter shows commonly used VDSL sub-command examples.

32.6.1 VDSL Port Command

Syntax:

```
vdsl port snr
vdsl port speed
vdsl port counter
vdsl port clrcntr
```

This command displays the information on your VDSL port SNR(Signal-to-Noise-Ratio), speed and counter. You can also clear the port counter.

The examples are shown next

Figure 175 VDSL Port Speed Commands Example (Link Down)

```
P861H> vdsl port speed
VDSL status : DOWN
P861H>
```

Figure 176 VDSL Port Speed Commands Example (Link Up)

```
P861H> vdsl port speed
VDSL status : UP
Downstream line rate : 72384 kbps
Upstream line rate : 44928 kbps
Fast Downstream payload rate : 0 kpbs
Slow Downstream payload rate : 60864 kpbs
Fast Upstream payload rate : 0 kpbs
Slow Upstream payload rate : 37440 kpbs
Downstream delay : 3.8 ms
Upstream delay : 6.2 ms
Tx total power 5.9 dbm
vdsl>
```

The following table explains these parameters.

Table 84 VDSL Port Speed Commands

	DESCRIPTION
VDSL Status	This displays whether the VDSL connection is down.
Downstream line rate	This displays the downstream line speed in Kbps.
Upstream line rate	This displays the upstream line speed in Kbps.
Fast Downstream payload rate	This displays the downstream transfer rate in fast channel mode. When the VDSL link is up in fast channel mode, the slow downstream payload rate displays zero.
Slow Downstream payload rate	This displays the downstream transfer rate in slow channel mode.
Fast Upstream payload rate	This displays the upstream transfer rate in fast channel mode. When the VDSL link is up in fast channel mode, the slow upstream payload rate displays zero.
Slow Upstream payload rate	This displays the upstream transfer rate in slow channel mode.
Downstream delay	This displays the downstream delay.
Upstream delay	This displays the upstream delay.
Tx total power	This displays transmission power information in dBm.

32.6.2 VDSL Clear Port Clear Counter

Figure 177 VDSL Clear Port Counter Command Example

```
P861H> vdsl port clrcntr
P861H>
```

32.6.3 PVC List Command

Syntax:

```
vdsl pvclist
```

This command lists the PVC (Permanent Virtual Circuit) channel. An example is shown next

Figure 178 vdsl pvc list Command Example

```

P861H> vdsl pvc list
===== PVC =====
pvc  act  vpi/vci      qos      pcr  cdvt      scr  mbs   app      ether  encap  ip
-----
 0   Y    835         vbrnr    4830   1      604   32   data     3 4    ENET  IP
 1   Y    032         vbrrt    360    1      360   32   mdware   1 2    1483  BDG
 2   Y    132         cbr      360    1      NA    NA    igmp     1 2    1483  BDG
 3   Y    133         cbr      NA     NA     NA    NA    video    1 2    1483  BDG
 4   Y    134         cbr      NA     NA     NA    NA    video    1 2    1483  BDG
 5   Y    135         cbr      NA     NA     NA    NA    video    1 2    1483  BDG
 6   Y    136         cbr      NA     NA     NA    NA    video    1 2    1483  BDG
=====
P861H>
    
```

The following table explains these parameters.

Table 85 PVC List

	DESCRIPTION
pvc	This displays the Permanent Virtual Circuit (PVC) index number.
act	This displays whether this PVC is active or not.
vpi/vci	This displays the Virtual Path Identifier and Virtual Channel Identifier.
qos	This displays the ATM QoS type.
pcr	This displays the maximum rate at which the sender can send cells (cells per second).
cdvt	This displays the acceptable range of the Cell Delay Variation (cells per second).
scr	This displays the mean cell rate of each bursty traffic source (cells per second).
mbs	This displays the maximum number of cells that can be sent to the PCR (cells per second).
app	This displays the name of an application on a PVC.
ether	This displays which Ethernet port a PVC can use.
encap	This displays the method of encapsulation used by your ISP. Choices vary depending on the operating mode of each remote node. If the operating mode is set as a bridge, this field displays either PPPoA or RFC 1483 . If the operating mode is set as routing, this field displays PPPoA , RFC 1483 , ENET ENCAP or PPPoE .
ip	This field displays whether the remote node is configured as a router (IP) or as a bridge (BDG).

32.6.4 Activate the VDSL Current Port Profile

Syntax:

```
vdsl profile actv
```

This command activates the VDSL current port profile.

It sends the current selected profile to the Prestige. It also sends system and port provisioning data to the Prestige. The Prestige then initiates the profile.

32.6.5 Reset VDSL Profile

Syntax:

```
vdsl profile default
```

This command resets the VDSL profile to be the default settings

Figure 179 Reset VDSL Profile

```
P861H> vdsl profile default
Profile reset OK!
P861H>
```

32.6.6 Band Plans

Each VDSL mode operates in a different frequency band allocation, resulting in different upstream and downstream speeds. The following table summarizes frequency ranges for each VDSL mode supported by the Prestige.

Table 86 VDSL Mode and Frequency Ranges

	BAND PLAN	FREQ. RANGE (HZ)			
		Upstream_1	Downstream_1	Upstream_1	Downstream_2
ANSI/ETSI Plan 998	998-138-8500	0.138M ~ 3.75M	3.75M ~ 5.20M	5.20M ~ 8.50M	
	998-138-12000	0.138M ~ 3.75M	3.75M ~ 5.20M	5.20M ~ 8.50M	8.50M ~ 12.00M
ETSI Plan 997	997-138-8500	0.138M ~ 3.00M	3.00M ~ 5.10M	5.10M ~ 7.05M	7.05M ~ 8.50M
	998-137-4400	0.138M ~ 3.00M	3.00M ~ 4.40M		

32.6.7 Show Profile Command

Syntax:

```
vdsl profile show
```

This command displays band plan, UPBO option, channel type, band plan and band modifier. Maximum upstream and downstream delays are only available in the interleaved/slow channel mode. An example is shown next.

Figure 180 VDSL Profile Show Command Example

```
P861H> vdsl profile show
Profile settings
  channel type : slow
    band plan : 998-138-8500
  band modifier : 0x11
    UPBO : disable
  Max DS Delay : 10.0 ms
  Max US Delay : 10.0 ms
P861H>
```

32.6.8 VDSL Version Command

Syntax:

```
vdsl version
```

This command shows the VDSL chip firmware version. An example is shown next.

Figure 181 DSL Version Command Example

```
P861H> vdsl version
Firmware-VTU-R:6.5.2r6 Time Apr 21 2004, 12:54:16, RTOS 5.4
BME R:48 AFE<num, ver> <0:910>
IFE<num:Dev.Rev> <0:2.4>
BME ID: 0x30
P861H>
```

CHAPTER 33

Troubleshooting

This chapter covers potential problems and the corresponding remedies.

33.1 Problems Starting Up the Prestige

Table 87 Troubleshooting Starting Up Your Prestige

PROBLEM	CORRECTIVE ACTION
None of the LEDs turn on when I turn on the Prestige.	<p>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.</p> <p>Turn the Prestige off and on.</p> <p>If the error persists, you may have a hardware problem. In this case, you should contact your vendor.</p>

33.2 Problems with the LAN

Table 88 Troubleshooting the LAN

PROBLEM	CORRECTIVE ACTION
The LAN LEDs do not turn on.	<p>Check your Ethernet cable connections (refer to the Quick Start Guide for details). Check for faulty Ethernet cables.</p>
	<p>Make sure your computer's Ethernet Card is working properly.</p>

33.3 Problems with the WAN

Table 89 Troubleshooting the WAN

PROBLEM	CORRECTIVE ACTION
The VDSL LED is off.	<p>Check the telephone wire and connections between the Prestige DSL port and the wall jack.</p> <p>Make sure that the telephone company has checked your phone line and set it up for DSL service.</p> <p>Make sure the distance from the Prestige to the DSLAM does not exceed 1.25 km (3750 feet). Rates deteriorate the further away the DSLAM is from the modem.</p> <p>Check with your telephone company that the telephone line quality is good enough for VDSL transmission. If G.hs is disabled in the Prestige, then make sure the Prestige and the remote DSLAM have the same VDSL parameters. Use the CI commands (refer to the chapter on VDSL commands) to check your VDSL parameters such as band plan, band modifier, channel type, encapsulation mode, VPI/VCI numbers, QoS parameters and service categories.</p> <p>Reset your VDSL line to reinitialize your link to the DSLAM. For details, refer to the Table 32 on page 128 (web configurator) or Table 65 on page 212 (SMT).</p>
I cannot get a WAN IP address from the ISP.	<p>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.</p> <p>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).</p>
I cannot access the Internet.	<p>Make sure the Prestige is turned on and connected to the network.</p> <p>Verify your WAN settings. Refer to the chapter on WAN setup (web configurator) or the section on Internet Access (SMT).</p> <p>Make sure you entered the correct user name and password.</p> <p>If you use PPPoE pass through, make sure that bridge mode is turned on.</p>
The Internet connection disconnects.	<p>Check the schedule rules. Refer to Chapter 28 on page 246 (SMT).</p> <p>If you use PPPoA or PPPoE encapsulation, check the idle time-out setting. Refer to the Chapter 5 on page 70 (web configurator) or Chapter 17 on page 154 (SMT).</p> <p>Contact your ISP.</p>

33.4 Problems Accessing the Prestige

Table 90 Troubleshooting Accessing the Prestige

PROBLEM	CORRECTIVE ACTION
I cannot access the Prestige.	<p>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.</p> <p>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.</p>
I cannot access the web configurator.	<p>Make sure that there is not an SMT console session running.</p> <p>Use the Prestige's WAN IP address when configuring from the WAN. Refer to the instructions on checking your WAN connection.</p> <p>Use the Prestige's LAN IP address when configuring from the LAN. Refer to for instructions on checking your LAN connection.</p> <p>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.</p> <p>Your computer's and the Prestige's IP addresses must be on the same subnet for LAN access.</p> <p>If you changed the Prestige's LAN IP address, then enter the new one as the URL.</p> <p>Remove any filters in SMT menu 3.1 (LAN) or menu 11.5 (WAN) that block web service.</p> <p>See the following section to check that pop-up windows, JavaScripts and Java permissions are allowed.</p>

33.4.1 Pop-up Windows, JavaScripts

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

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

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

33.4.1.1 Internet Explorer Pop-up Blockers

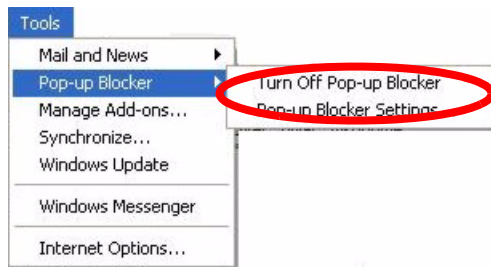
You may have to disable pop-up blocking to log into your device.

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.

33.4.1.1.1 Disable pop-up Blockers

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

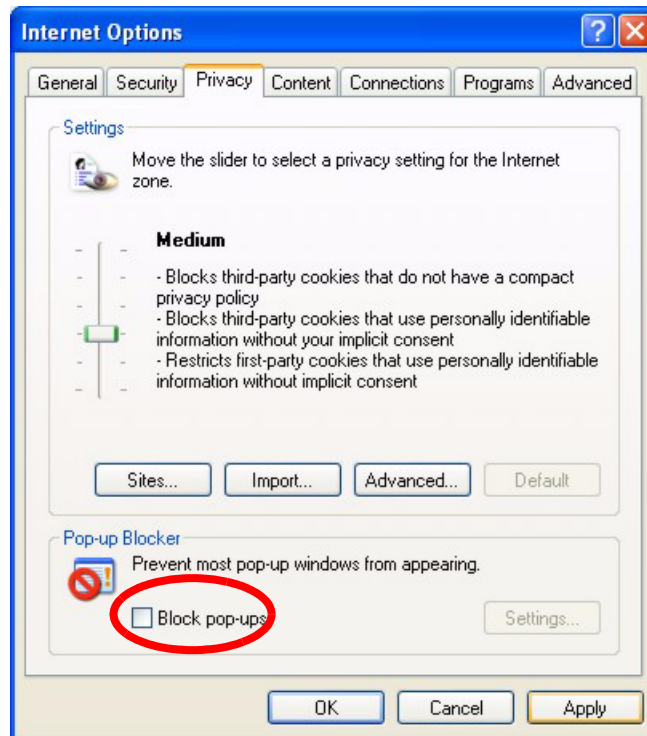
Figure 182 Pop-up Blocker



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 183 Internet Options

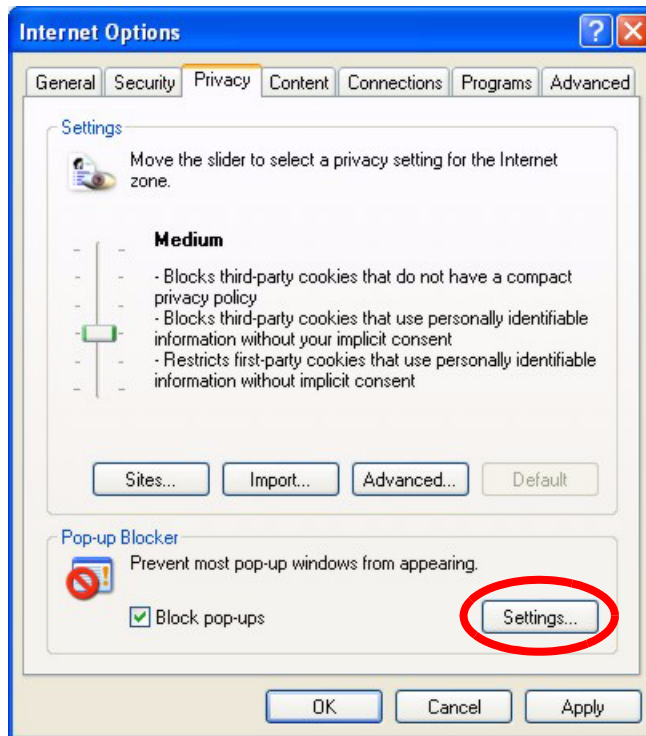


- 3** Click **Apply** to save this setting.

33.4.1.1.2 Enable pop-up Blockers with Exceptions

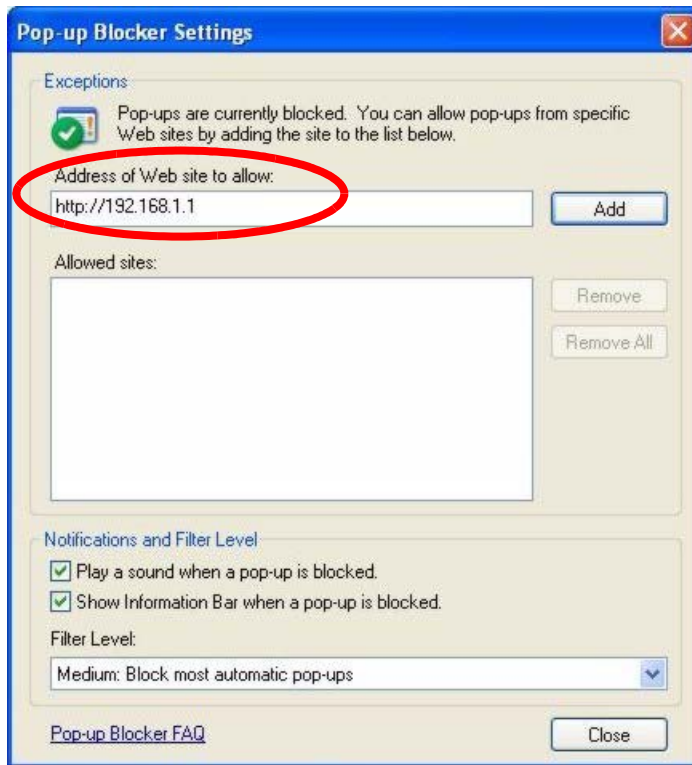
Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

- 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 184 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 185 Pop-up Blocker Settings



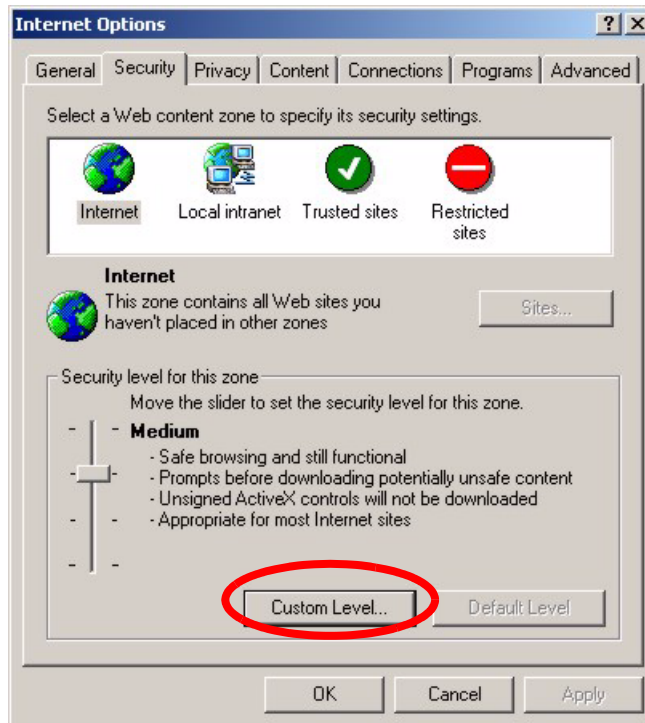
5 Click **Close** to return to the **Privacy** screen.

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

33.4.1.2 JavaScripts

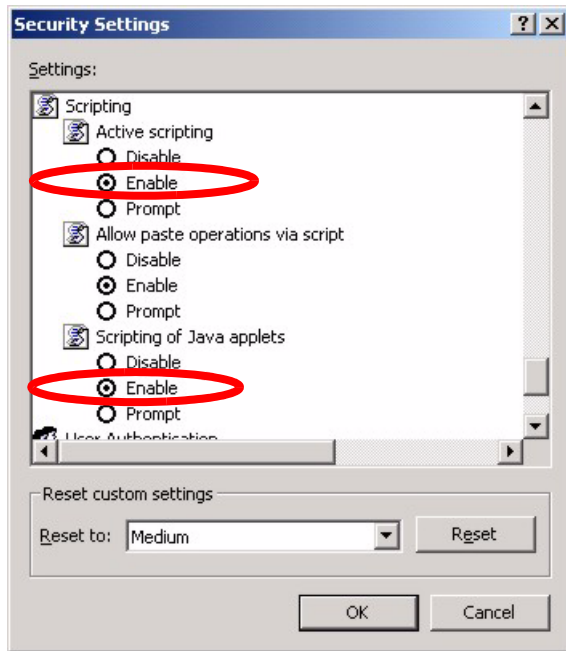
If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

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

Figure 186 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 187 Security Settings - Java Scripting



Appendix A

Product Specifications

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

Specification Tables

Table 91 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
	(260 W) x (161 D) x (51 H) mm
Weight	500g
Power Specification	12VAC 1.25A
Built-in Switch	Four auto-negotiating, auto MDI/MDI-X 10/100 Mbps RJ-45 Ethernet ports
Operation Temperature	0° C ~ 50° C
Operation Humidity	10% ~ 90% RH

Table 92 Firmware

<p>VDSL Standards</p>	<p>Band Plan Rates: 998 4 Band (without optional band) Max Downstream Rate: 60 Mbps Max Upstream Rate: 34 Mbps 997 4 Band (without optional band) Max Downstream Rate: 43 Mbps Max Upstream Rate: 27 Mbps 997 4 Band (without optional band) SRA (Seamless Rate Adaptation) Auto-negotiating rate adaptation VDSL 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) LLC-based multiplexing Up to 8 PVCs (Permanent Virtual Circuits) I.610 F4/F5 OAM</p>
<p>Other Protocol Support</p>	<p>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</p>
<p>Management</p>	<p>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, VDSL circuitry, RAM and LAN port Syslog</p>
<p>NAT/SUA</p>	<p>Port Forwarding 1024 NAT sessions Multimedia application. PPTP under NAT/SUA. IPSec passthrough SIP ALG passthrough.</p>

Table 92 Firmware (continued)

Static Routes	16 IP and 4 Bridge
Other Features	Dynamic DNS IP Alias IP Policy Routing VLAN ID 1 ~ 16

Appendix B

Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

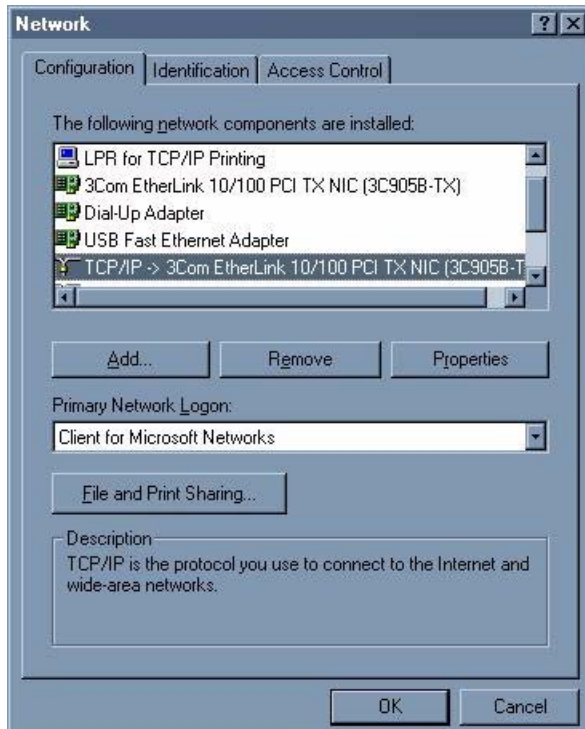
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

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

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the Prestige's LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.

Figure 188 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:

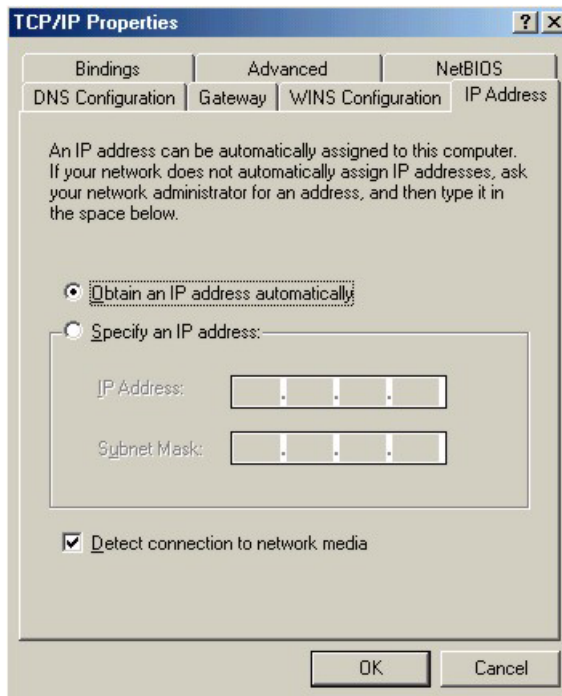
- 1 Click **Add**.
- 2 Select **Client** and then click **Add**.

- 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.

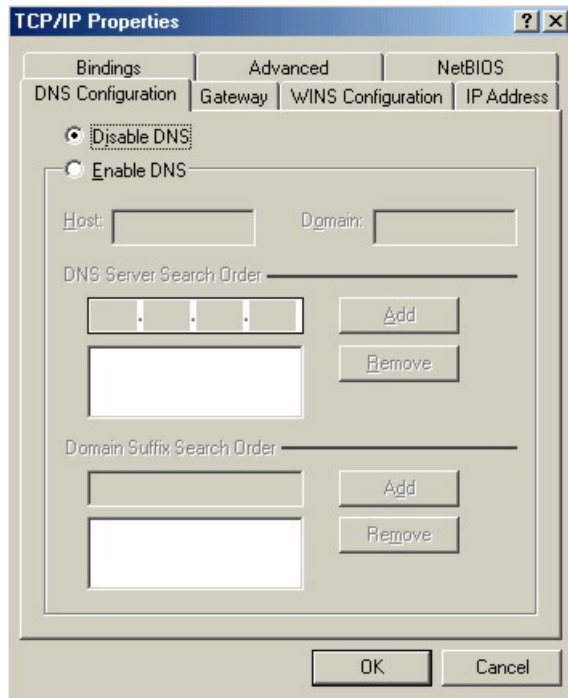
Configuring

- 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 189 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 190 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.

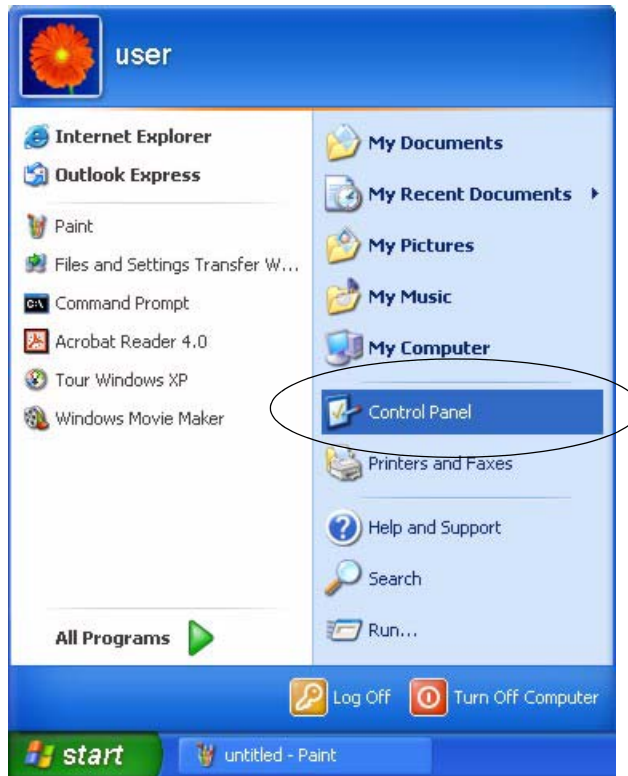
Verifying Settings

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**.

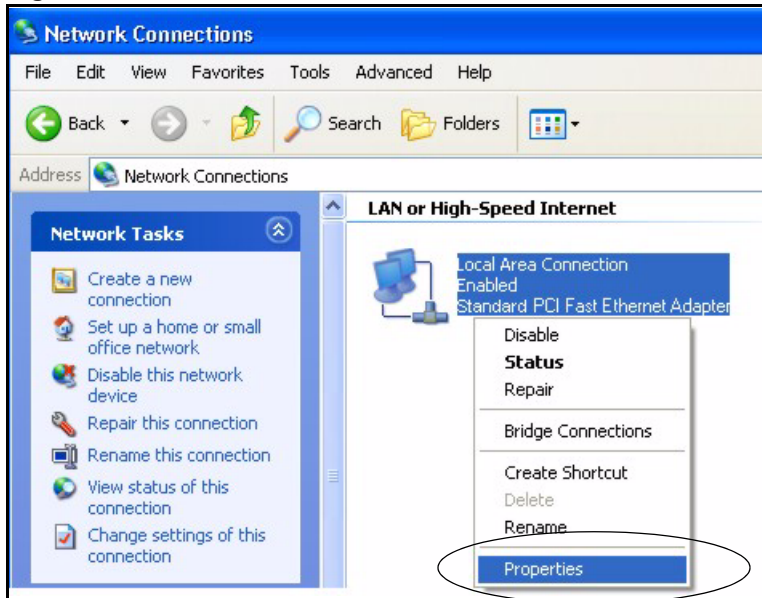
Figure 191 Windows XP: Start Menu

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

Figure 192 Windows XP: Control Panel

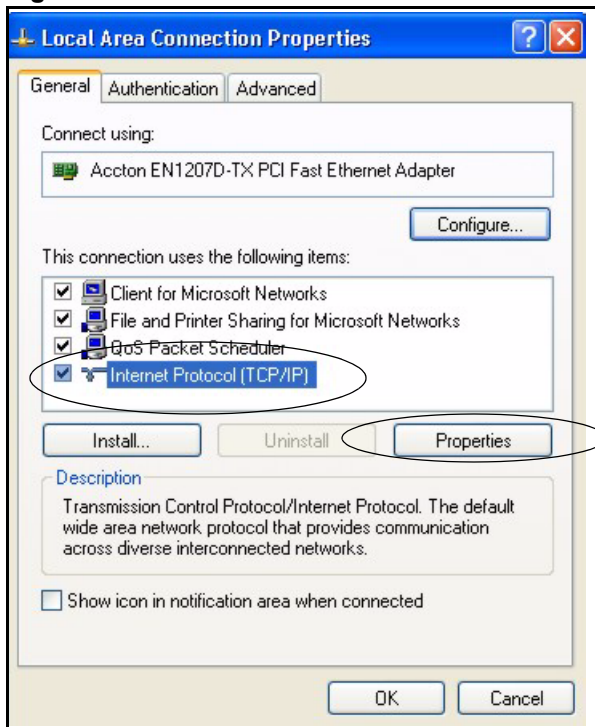
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 193 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 194 Windows XP: Local Area Connection Properties

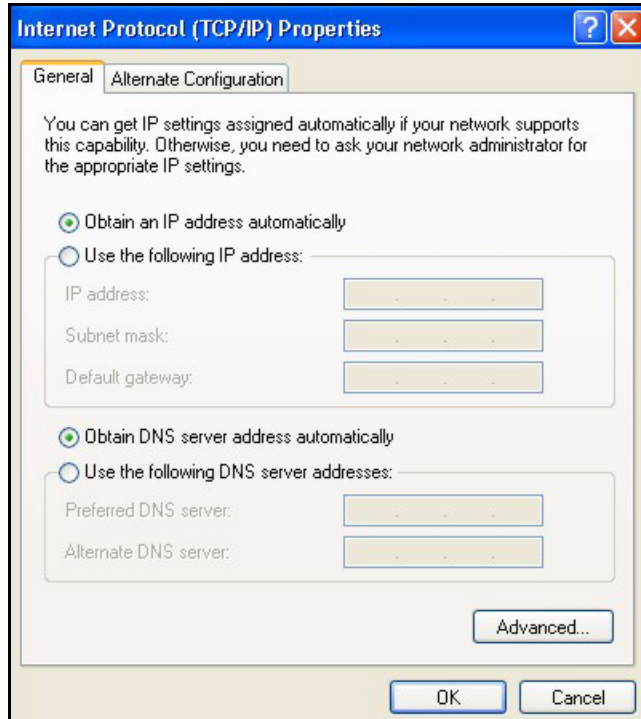


5 The **Internet Protocol TCP/IP Properties** window opens (the **General** tab in Windows XP).

- 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**.

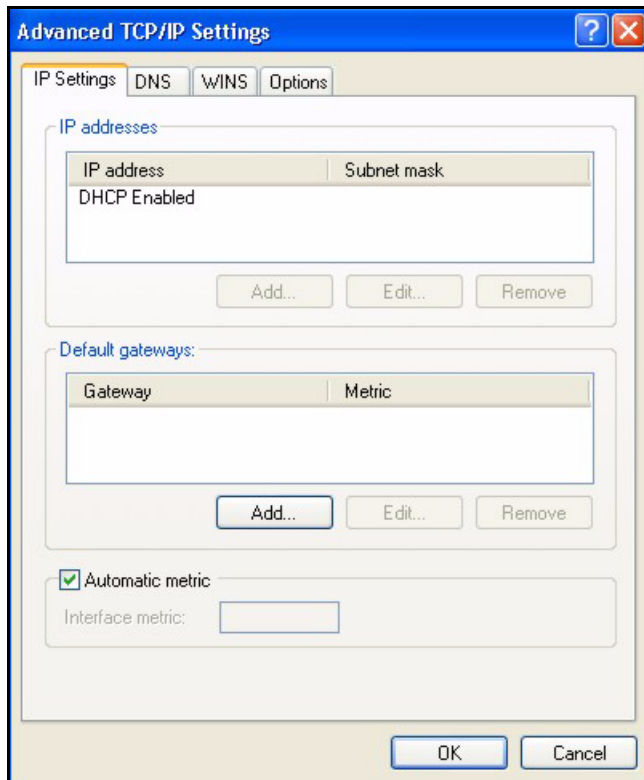
Figure 195 Windows XP: Internet Protocol (TCP/IP) Properties



- 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:

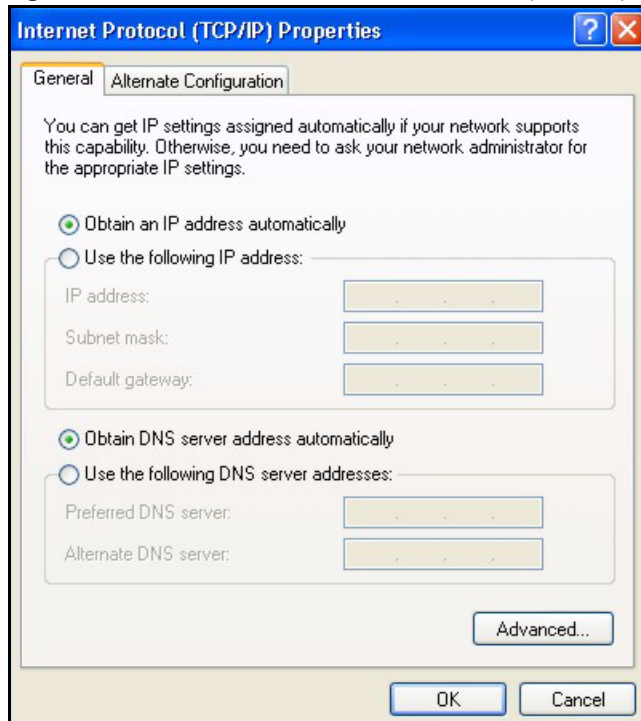
- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP 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 196 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 197 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).

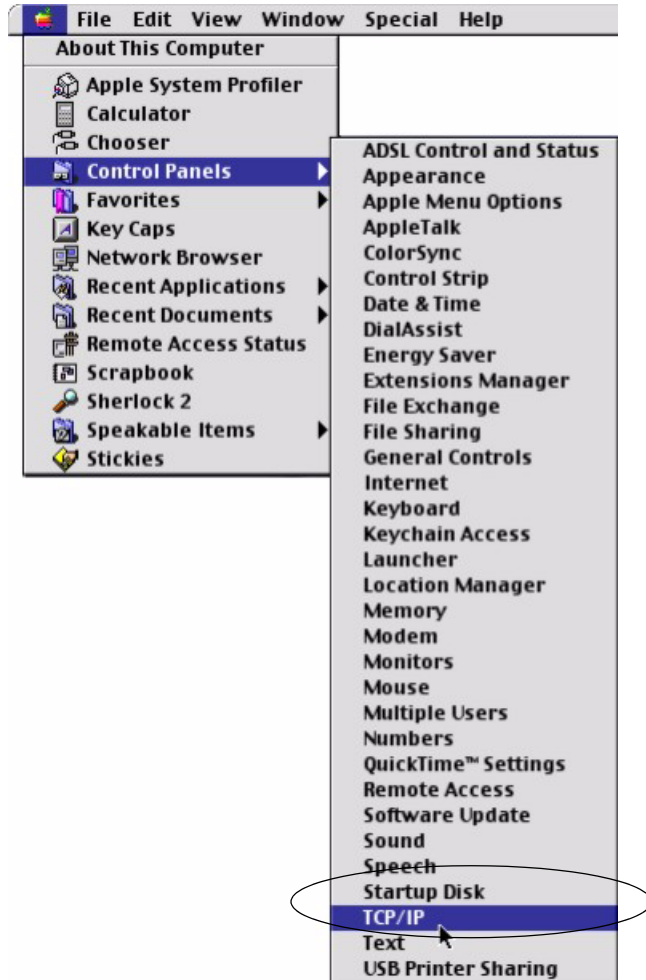
Verifying Settings

- 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

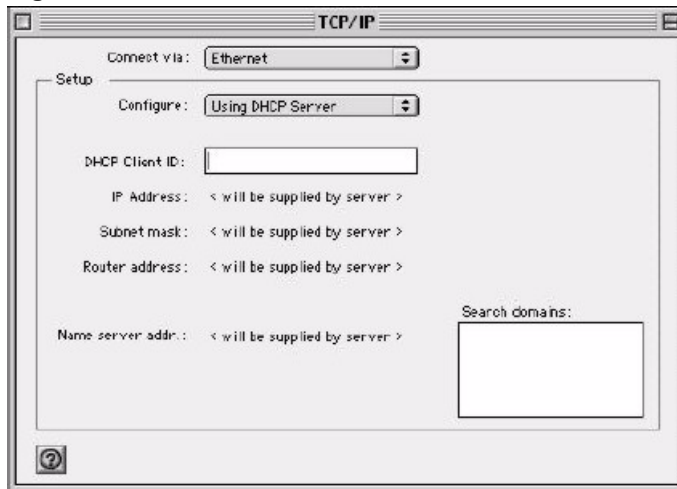
- 1** Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 198 Macintosh OS 8/9: Apple Menu



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

Figure 199 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).

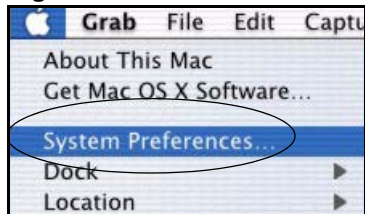
Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

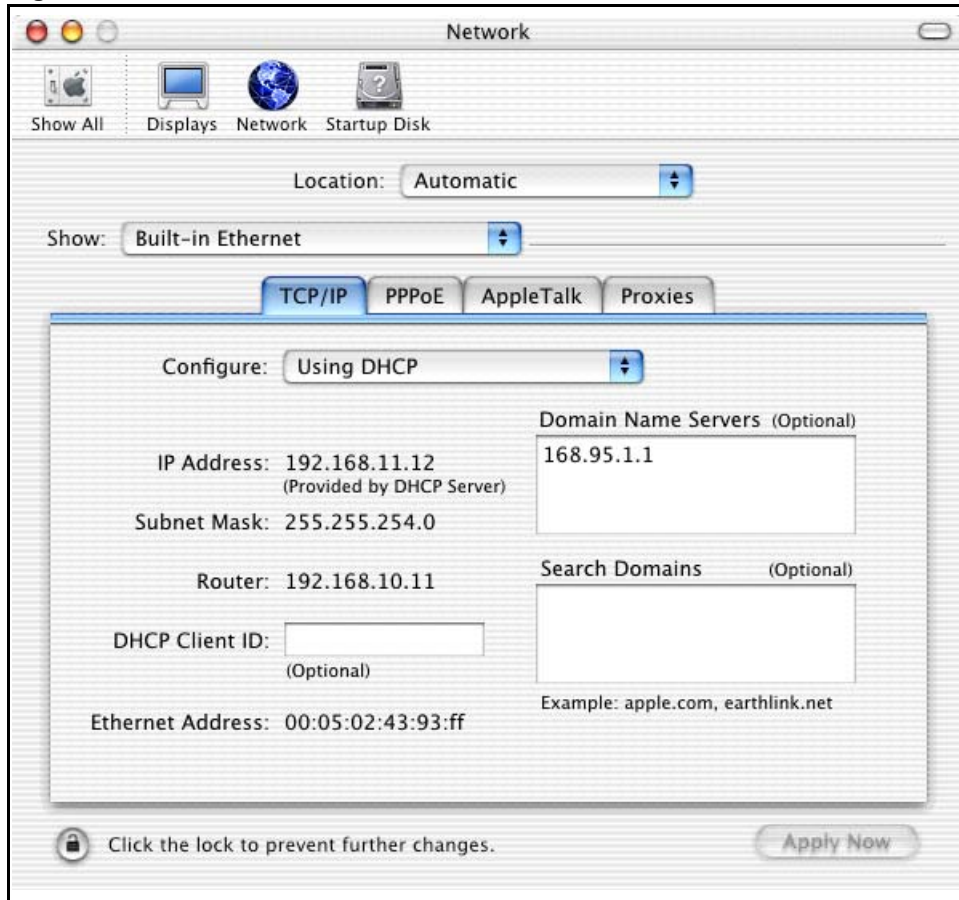
Macintosh OS X

- 1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 200 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 201 Macintosh OS X: Network

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your Prestige in the **Router address** box.

5 Click **Apply Now** and close the window.

6 Turn on your Prestige and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

Appendix C

IP Subnetting

IP Addressing

Routers “route” based on the network number. The router that delivers the data packet to the correct destination host uses the host ID.

IP Classes

An IP address is made up of four octets (eight bits), written in dotted decimal notation, for example, 192.168.1.1. IP addresses are categorized into different classes. The class of an address depends on the value of its first octet.

- Class “A” addresses have a 0 in the left most bit. In a class “A” address the first octet is the network number and the remaining three octets make up the host ID.
- Class “B” addresses have a 1 in the left most bit and a 0 in the next left most bit. In a class “B” address the first two octets make up the network number and the two remaining octets make up the host ID.
- Class “C” addresses begin (starting from the left) with 1 1 0. In a class “C” address the first three octets make up the network number and the last octet is the host ID.
- Class “D” addresses begin with 1 1 1 0. Class “D” addresses are used for multicasting. (There is also a class “E” address. It is reserved for future use.)

Table 93 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 94 Allowed IP Address Range By Class

CLASS	ALLOWED RANGE OF FIRST OCTET (BINARY)	ALLOWED RANGE OF FIRST OCTET (DECIMAL)
Class A	00000000 to 01111111	0 to 127
Class B	10000000 to 10111111	128 to 191
Class C	11000000 to 11011111	192 to 223
Class D	11100000 to 11101111	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 95 “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 96 Alternative Subnet Mask Notation

SUBNET MASK IP ADDRESS	SUBNET MASK “1” BITS	LAST OCTET BIT VALUE
255.255.255.0	/24	0000 0000
255.255.255.128	/25	1000 0000
255.255.255.192	/26	1100 0000
255.255.255.224	/27	1110 0000
255.255.255.240	/28	1111 0000
255.255.255.248	/29	1111 1000
255.255.255.252	/30	1111 1100

The first mask shown is the class “C” natural mask. Normally if no mask is specified it is understood that the natural mask is being used.

Example: Two Subnets

As an example, you have a class “C” address 192.168.1.0 with subnet mask of 255.255.255.0.

Table 97 Two Subnets Example

	NETWORK NUMBER	HOST ID
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask	255.255.255.	0
Subnet Mask (Binary)	11111111.11111111.11111111.	00000000

The first three octets of the address make up the network number (class “C”). You want to have two separate networks.

Divide the network 192.168.1.0 into two separate subnets by converting one of the host ID bits of the IP address to a network number bit. The “borrowed” host ID bit can be either “0” or “1” thus giving two subnets; 192.168.1.0 with mask 255.255.255.128 and 192.168.1.128 with mask 255.255.255.128.

Note: In the following charts, shaded/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 98 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	10000000
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 99 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	10000000
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 (11111111.11111111.11111111.11000000) 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 100 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
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 101 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	01000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
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 102 Subnet 3

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
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 103 Subnet 4

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	11000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
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 104 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 105 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 93 on page 296](#)) available for subnetting.

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

Table 106 Class B Subnet Planning

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Appendix D

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 202 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 203 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 E

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

```
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 107 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` This command blocks IPSec NetBIOS packets.
`config 3 on`

`sys filter netbios` This command stops NetBIOS commands from initiating calls.
`config 4 off`

Appendix F

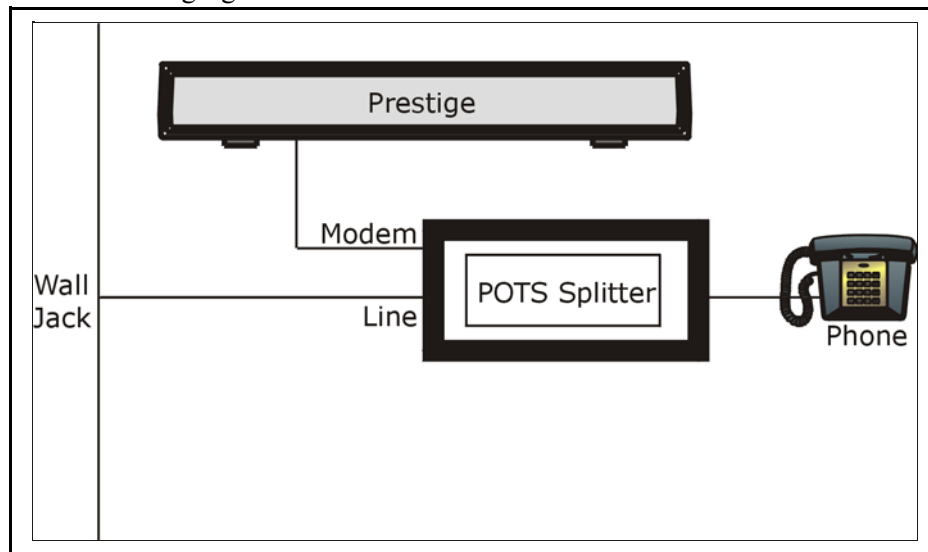
Splitters and Microfilters

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

Connecting a POTS Splitter

When you use the VDSL standard, you can use a POTS (Plain Old Telephone Service) splitter to separate the telephone and VDSL 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.



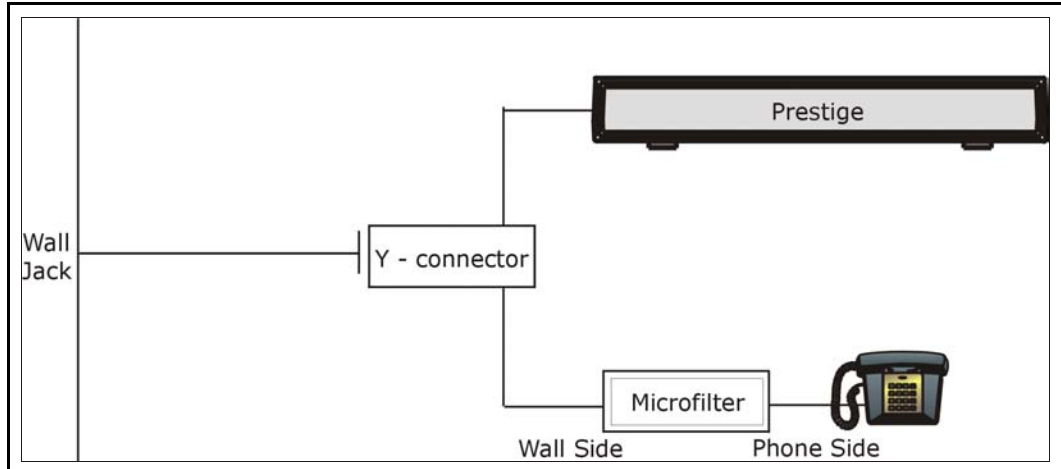
- 1 Connect the side labeled “Phone” to your telephone.
- 2 Connect the side labeled “Modem” to your Prestige.
- 3 Connect the side labeled “Line” to the telephone wall jack.

Telephone Microfilters

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

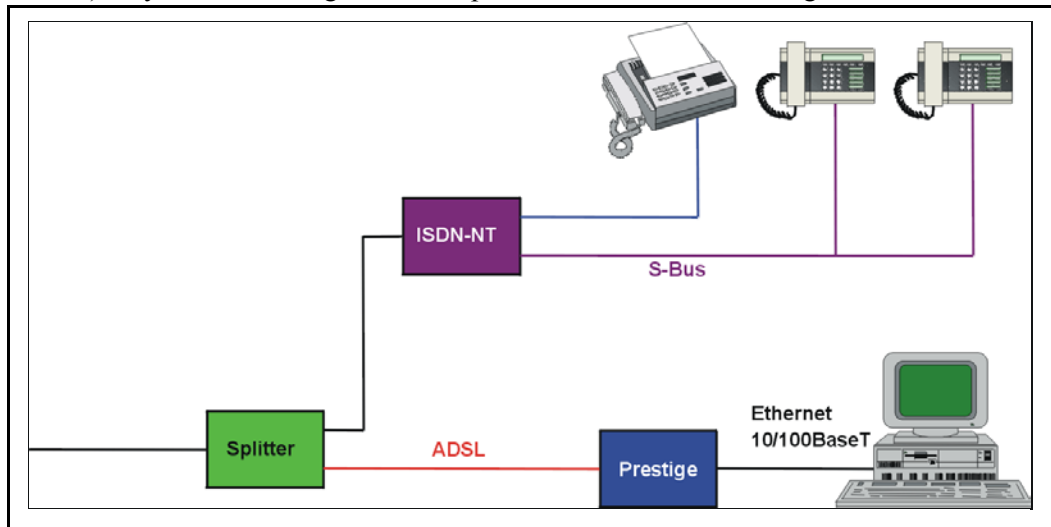
- 1 Connect a phone cable from the wall jack to the single jack end of the Y- Connector.

- 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.



Prestige With ISDN

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



Appendix G

PPPoE

PPPoE in Action

An VDSL 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 204 on page 313](#)). 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.

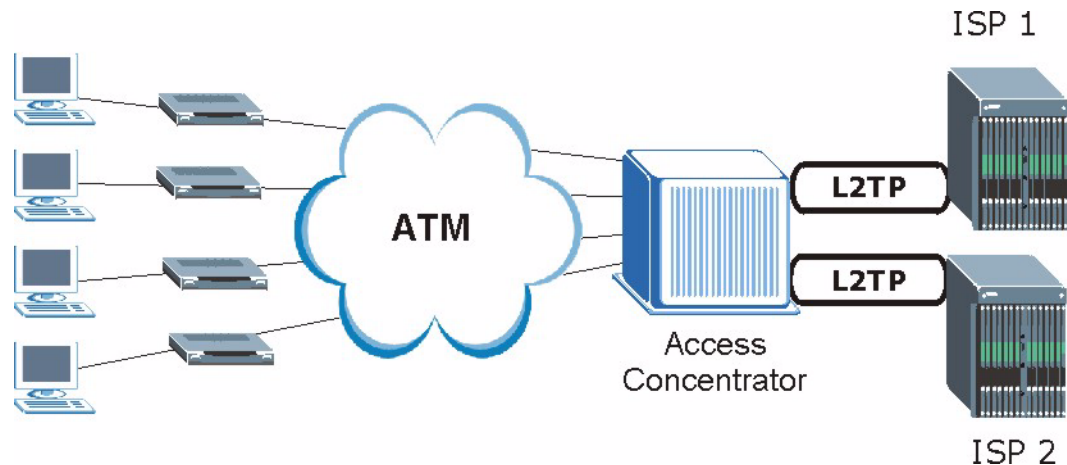
It lessens the burden on the carriers of provisioning virtual circuits all the way to the ISP on multiple switches for thousands of users. For GSTN (PSTN and ISDN), the switching fabric is already in place.

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 204 Single-Computer per Router Hardware Configuration



How PPPoE Works

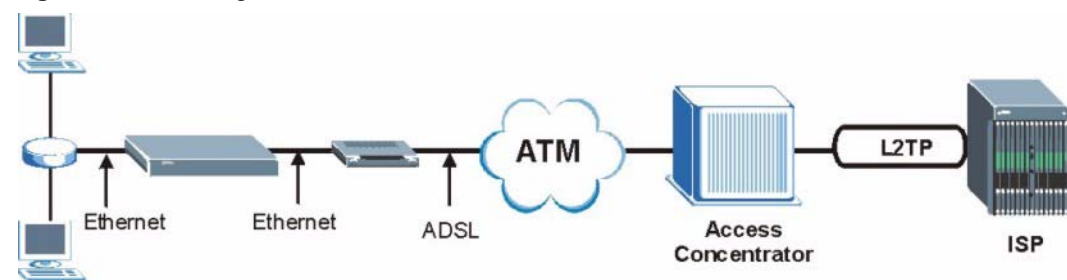
The PPPoE driver makes the Ethernet appear as a serial link to the computer and the computer runs PPP over it, while the modem bridges the Ethernet frames to the Access Concentrator (AC). Between the AC and an ISP, the AC is acting as a L2TP (Layer 2 Tunneling Protocol) LAC (L2TP Access Concentrator) 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 205 Prestige as a PPPoE Client



Appendix H

Log Descriptions

This appendix provides descriptions of example log messages.

Table 108 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 108 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 109 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 110 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 111 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 CLI command: "sys firewall tcprst").

Table 112 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 113 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 125 on page 326 .
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 125 on page 326 .
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 114 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 115 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 115 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 116 UPnP Logs

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

Table 117 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 117 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 118 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 125 on page 326 .
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 125 on page 326 .
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 125 on page 326 .
icmp echo: ICMP (type:%d, code:%d)	The firewall detected an ICMP echo attack. For type and code details, see Table 125 on page 326 .
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 125 on page 326 .
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 125 on page 326 .
traceroute ICMP (type:%d, code:%d)	The firewall detected an ICMP traceroute attack. For type and code details, see Table 125 on page 326 .

Table 119 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" CLI 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 120 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 120 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 120 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 1 verification 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 120 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 121 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 121 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 122 on page 324 for the corresponding descriptions of the codes.

Table 122 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 122 Certificate Path Verification Failure Reason Codes (continued)

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

Table 123 802.1X 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 method.	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 124 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 125 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 125 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 126 Syslog Logs

LOG MESSAGE	DESCRIPTION
<pre><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>"</pre>	<p>"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.</p>

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 127 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 127 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 206 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 207 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.

- 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 I

Loop Reach

Testing Conditions

Loop Simulator : DLS 8100
Loop Wire : 26AWG

Note: These are by no means guaranteed values. These rates were achieved under laboratory conditions.

Band Plan : 998_138_12000(4B)

Table 128 Band Plan : 998_138_12000(4B)

NO.	LOOP LENGTH (FEET)	DOWNSTREAM LINE RATE (KBPS)	UPSTREAM LINE RATE (KBPS)	DOWNSTREAM PAYLOAD (KBPS)	UPSTREAM PAYLOAD RATE (KBPS)
1	0	74496	45504	65728	40128
2	1000	70336	41344	62528	36288
3	2000	54528	8704	47360	7488
4	3000	31424	3392	27008	2688

Band Plan : 998_138_8500(3B)

Table 129 Band Plan : 998_138_8500(3B)

NO.	LOOP LENGTH (FEET)	DOWNSTREAM LINE RATE (KBPS)	UPSTREAM LINE RATE (KBPS)	DOWNSTREAM PAYLOAD (KBPS)	UPSTREAM PAYLOAD RATE (KBPS)
1	0	73856	13824	64960	12224
2	1000	70784	13696	62656	12096
3	2000	54080	8704	46912	7488
4	3000	31552	3584	27136	2816

Band Plan : 997_138_8500(4B)

Table 130 Band Plan : 997_138_8500(4B)

NO.	LOOP LENGTH (FEET)	DOWNSTREAM LINE RATE (KBPS)	UPSTREAM LINE RATE (KBPS)	DOWNSTREAM PAYLOAD (KBPS)	UPSTREAM PAYLOAD RATE (KBPS)
1	0	44864	37888	39616	33472
2	1000	43776	36864	38592	32512
3	2000	33088	20480	28800	17344
4	3000	17472	6848	15104	5760

Appendix J

ASCII Characters

This appendix tells you about ASCII (American Standard Code for Information Interchange) characters.

ASCII Code

Computers use ASCII code to represent binary (0 or 1) as letters and other characters.

The ASCII code is a list that contains all the letters in the alphabet plus other additional characters. In this code the same order number always represents each character. For example, in ASCII code the capital letter A is always represented by the order number 65, which is easily represented using 0's and 1's in binary (1000001).

The standard ASCII code defines 128 character codes (from 0 to 127), of which, the first 32 are control codes (non-printable), and the other 96 are representable (printable) characters:

*	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	NUL	SOH	STX	ETX	EOT	ENQ	ACK	BEL	BS	TAB	LF	VT	FF	CR	SO	SI
1	DLE	DC1	DC2	DC3	DC4	NAK	SYN	ETB	CAN	EM	SUB	ESC	FS	GS	RS	US
2		!	"	#	\$	%	&	'	()	*	+	,	-	.	/
3	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5	P	Q	R	S	T	U	V	W	X	Y	Z	[\]	^	_
6	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7	p	q	r	s	t	u	v	w	x	y	z	{		}	~	

*This panel is organized in hexadecimal: row numbers represent the first digit and the column numbers represent the second digit. For example, the **A** character is located at the **4th** row and the **1st** column, which is represented in hexadecimal as **0x41 (65)**.

Index **C**

Numerics

110V AC [5](#)
230V AC [5](#)

A

Abnormal Working Conditions [6](#)
AC [5](#)
Accessories [5](#)
Acts of God [6](#)
Address Assignment [63](#)
Address mapping [92](#)
ADSL, what is it? [34](#)
Airflow [5](#)
Alternative Subnet Mask Notation [298](#)
American Wire Gauge [5](#)
applications
 Internet access [38](#)
Applications [39](#)
AT command [215](#)
ATM Adaptation Layer 5 (AAL5) [70](#)
ATM layer options [161](#)
Authentication [157](#)
Authentication protocol [157](#)
Authority [3](#)
auto-negotiation [36](#)
AWG [5](#)

B

Backup [215](#)
Basement [5](#)
Bridging [157, 168](#)
 Ether Address [171](#)
 Ethernet [168](#)
 Ethernet Addr Timeout [170](#)
 Remote Node [168](#)
 Static Route Setup [170](#)
bridging [141](#)
Budget Management [227, 228](#)

Cables, Connecting [5](#)
Call filtering [188](#)
Call filters
 Built-in [188](#)
 User-defined [188](#)
Call Scheduling [246](#)
 Maximum Number of Schedule Sets [246](#)
 PPPoE [248](#)
 Precedence [246](#)
 Precedence Example [246](#)
Certifications [3](#)
Changes or Modifications [3](#)
CHAP [157](#)
Charge [6](#)
Circuit [3](#)
Class B [3](#)
Command Interpreter Mode [226](#)
Communications [3](#)
Community [203](#)
compact [38](#)
compact guide [44](#)
Compliance, FCC [3](#)
Components [6](#)
Computer Name [140](#)
Condition [6](#)
Conditions that prevent TFTP and FTP from working
 over WAN [217](#)
Configuration [62, 126](#)
configuration file [214](#)
Connecting Cables [5](#)
Consequential Damages [6](#)
Contact Information [7](#)
Contacting Customer Support [7](#)
Copyright [2](#)
Correcting Interference [3](#)
Corrosive Liquids [5](#)
Cost Of Transmission [159, 166](#)
Country Code [209](#)
Covers [5](#)
CPU Load [208](#)
Customer Support [7](#)

D

Damage [5](#)
Dampness [5](#)
Danger [5](#)

Data Filtering [188](#)
Dealer [3](#)
default LAN IP address [44](#)
Defective [6](#)
Denmark, Contact Information [7](#)
Device Filter rules [197](#)
device model number [129](#)
Device rule [197](#)
DHCP [37](#), [62](#), [64](#), [96](#), [126](#), [146](#), [209](#)
DHCP client [37](#)
DHCP relay [37](#)
DHCP server [37](#), [126](#), [146](#)
DHCP table [126](#)
diagnostic [127](#)
Diagnostic Tools [206](#)
Disclaimer [2](#)
Discretion [6](#)
DNS [146](#)
Domain Name [63](#), [89](#)
domain name [140](#)
Domain Name System [63](#)
DSL (Digital Subscriber Line) [34](#)
DSL line, reinitialize [128](#)
DSL, What Is It? [34](#)
Dust [5](#)
Dynamic DNS [37](#), [96](#), [141](#)
dynamic DNS [37](#), [142](#)
Dynamic Host Configuration Protocol [37](#)
DYNDNS Wildcard [96](#)

E

ECHO [88](#)
Electric Shock [5](#)
Electrical Pipes [5](#)
Electrocution [5](#)
embedded help [46](#)
Encapsulated Routing Link Protocol (ENET ENCAP) [70](#)
Encapsulation [70](#), [152](#), [155](#)
 ENET ENCAP [70](#)
 PPP over Ethernet [70](#)
 PPPoA [70](#)
 RFC 1483 [71](#)
Equal Value [6](#)
Error Log [210](#)
Ethernet [281](#)
Europe [5](#)
Exposure [5](#)

F

Failure [6](#)
FCC [3](#)
 Compliance [3](#)
 Rules, Part 15 [3](#)
FCC Rules [3](#)
Federal Communications Commission [3](#)
Filename Conventions [214](#)
filename conventions [215](#)
Filter [144](#), [188](#)
 Applying Filters [199](#)
 Ethernet Traffic [200](#)
 Ethernet traffic [200](#)
 Filter Rules [191](#)
 Filter structure [189](#)
 Generic Filter Rule [195](#)
 Remote Node [160](#)
 Remote Node Filter [160](#)
 Remote Node Filters [200](#)
 Sample [198](#)
 SUA [197](#)
 TCP/IP Filter Rule [193](#)
Filter Rule Process [189](#)
Filter Rule Setup [192](#)
Filter Set
 Class [192](#)
Filtering [188](#), [192](#)
Filtering Process
 Outgoing Packets [188](#)
Finger [89](#)
Finland, Contact Information [7](#)
firmware [128](#), [214](#)
 upgrade [129](#)
 upload [128](#)
 upload error [129](#)
Fitness [6](#)
France, Contact Information [7](#)
FTP [88](#), [100](#), [233](#)
 Restrictions [233](#)
FTP File Transfer [221](#)
FTP Restrictions [100](#), [217](#)
FTP Server [183](#)
Functionally Equivalent [6](#)

G

Gas Pipes [5](#)
Gateway [166](#)
Gateway Node [171](#)
General Setup [140](#)

Generic filter [197](#)
 Germany, Contact Information [7](#)
 God, act of [6](#)

H

Harmful Interference [3](#)
 Hidden Menus [136](#)
 High Definition Television [39](#)
 High Voltage Points [5](#)
 Home Gateway [39](#)
 Hop Count [159](#), [166](#)
 Host [47](#)
 Host IDs [296](#)
 HTTP [89](#)
 HTTP (Hypertext Transfer Protocol) [128](#)

I

IANA [64](#), [65](#)
 Idle timeout [157](#)
 IGMP [65](#), [66](#)
 IGMP support [159](#)
 Indirect Damages [6](#)
 Install UPnP [108](#)
 Windows Me [108](#)
 Windows XP [110](#)
 Insurance [6](#)
 Interactive Applications [236](#)
 Interference [3](#)
 Interference Correction Measures [3](#)
 Interference Statement [3](#)
 Internet Access [37](#), [148](#), [151](#), [152](#)
 Internet access [48](#), [148](#)
 Internet Access Setup [172](#), [273](#)
 Internet access wizard setup [48](#)
 Internet Assigned Numbers AuthoritySee IANA [64](#)
 IP Address [64](#), [88](#), [126](#), [146](#), [166](#), [171](#), [194](#), [209](#), [212](#),
[238](#)
 IP Address Assignment [71](#)
 ENET ENCAP [72](#)
 PPPoA or PPPoE [71](#)
 RFC 1483 [71](#)
 IP Addressing [296](#)
 IP alias [37](#), [148](#)
 IP Alias Setup [149](#)
 IP Classes [296](#)

IP Filter [195](#)
 Logic Flow [194](#)
 IP mask [193](#)
 IP Packet [195](#)
 IP Policies [240](#)
 IP policy [148](#)
 IP policy routing [236](#)
 IP Policy Routing (IPPR) [38](#), [148](#)
 Applying an IP Policy [240](#)
 Ethernet IP Policies [240](#)
 Gateway [240](#)
 IP Pool Setup [63](#)
 IP Protocol [239](#)
 IP protocol [236](#)
 IP Routing Policy (IPPR) [236](#)
 Benefits [236](#)
 Cost Savings [236](#)
 Criteria [236](#)
 Load Sharing [236](#)
 Setup [237](#)
 IP Static Route [164](#)
 IP Static Route Setup [165](#)

L

Labor [6](#)
 LAN [207](#)
 LAN Setup [62](#), [70](#)
 LAN TCP/IP [64](#)
 Legal Rights [6](#)
 Liability [2](#)
 License [2](#)
 Lightning [5](#)
 Link type [207](#)
 Liquids, Corrosive [5](#)
 LLC-based Multiplexing [161](#)
 Log and Trace [210](#)
 Logging Option [194](#), [197](#)
 Logical networks [148](#)
 Login [156](#)
 Logs [120](#)

M

MAC (Media Access Control) [126](#)
 MAC address [171](#)
 Main Menu [137](#)

- maintenance [122](#)
- management idle timeout period [45](#)
- Management Information Base (MIB) [203](#)
- Materials [6](#)
- Maximum Burst Size (MBS) [80](#)
- Media Access Control [168](#)
- Merchantability [6](#)
- Message Logging [210](#)
- Metric [159](#), [166](#)
- Middleware [38](#)
- Modifications [3](#)
- Multicast [65](#), [159](#)
- Multiplexing [152](#), [155](#)
- multiplexing
 - LLC-based [71](#)
 - VC-based [71](#)
- Multiprotocol Encapsulation [71](#)
- My WAN Address [158](#)

N

- Nailed-Up Connection [72](#)
- NAT [64](#), [88](#), [89](#), [197](#)
 - Address mapping rule [93](#)
 - Application [86](#)
 - Applying NAT in the SMT Menus [172](#)
 - Configuring [174](#)
 - Definitions [84](#)
 - Examples [180](#)
 - How it works [85](#)
 - Mapping Types [87](#)
 - Non NAT Friendly Application Programs [186](#)
 - Ordering Rules [177](#)
 - What it does [85](#)
 - What NAT does [85](#)
- NAT (Network Address Translation) [84](#)
- NAT mode [90](#)
- NAT Traversal [106](#)
- navigating the web configurator [45](#)
- Network Address Translation [152](#)
- Network Address Translation (NAT) [37](#), [172](#)
- Network Management [89](#)
- New [6](#)
- NNTP [89](#)
- North America [5](#)
- North America Contact Information [7](#)
- Norway, Contact Information [7](#)

O

- Opening [5](#)
- Operating Condition [6](#)
- Out-dated Warranty [6](#)
- Outlet [3](#)

P

- Packet
 - Error [207](#)
 - Received [207](#)
 - Transmitted [207](#)
- Packets [207](#)
- PAP [157](#)
- Parts [6](#)
- Password [134](#), [138](#), [156](#), [203](#)
- password [134](#)
- Patent [2](#)
- Peak Cell Rate (PCR) [80](#)
- Permission [2](#)
- Photocopying [2](#)
- Ping [212](#)
- Pipes [5](#)
- Point to Point Protocol over ATM Adaptation Layer 5 (AAL5) [70](#)
- Point-to-Point [34](#)
- Point-to-Point Tunneling Protocol [89](#)
- policy-based routing [236](#)
- Pool [5](#)
- POP3 [89](#)
- Port Numbers [88](#)
- Postage Prepaid. [6](#)
- Power Adaptor [5](#)
- Power Cord [5](#)
- Power Outlet [5](#)
- Power Supply [5](#)
- Power Supply, repair [5](#)
- PPP Encapsulation [161](#)
- PPP session over Ethernet (PPP over Ethernet, RFC 2516) [70](#)
- PPPoE [72](#), [312](#)
 - Benefits [72](#)
- PPPoE (Point-to-Point Protocol over Ethernet) [37](#), [72](#)
- PPPoE pass-through [163](#)
- PPTP [89](#)
- Precedence [236](#), [239](#)
- Prestige model [214](#)

Private [159, 166](#)
 Product Model [7](#)
 Product Page [4](#)
 Product Serial Number [7](#)
 Products [6](#)
 Proof of Purchase [6](#)
 Proper Operating Condition [6](#)
 Protocol [193](#)
 Protocol filter [197](#)
 Protocol Filter Rules [197](#)
 Purchase, Proof of [6](#)
 Purchaser [6](#)
 PVC (Permanent Virtual Circuit) [70](#)

Q

Qualified Service Personnel [5](#)
 Quality of Service [236](#)
 Quick Start Guide [33](#)

R

Radio Communications [3](#)
 Radio Frequency Energy [3](#)
 Radio Interference [3](#)
 Radio Reception [3](#)
 Radio Technician [3](#)
 RAS [209, 237](#)
 Rate
 Receiving [207](#)
 Transmission [207](#)
 Rear Panel [42](#)
 Receiving Antenna [3](#)
 Registered [2](#)
 Registered Trademark [2](#)
 Regular Mail [7](#)
 reinitialize the ADSL line [128](#)
 Related Documentation [32](#)
 Relocate [3](#)
 Re-manufactured [6](#)
 Remote DHCP Server [146](#)
 Remote Management and NAT [101](#)
 Remote Management Limitations [100, 233](#)
 Remote Management Setup [232](#)
 Remote Node [154, 207](#)
 Remote Node Profile [156](#)
 Remote Node Setup [154](#)

Remote node [154](#)
 Remote Node Index Number [207](#)
 Removing [5](#)
 Reorient [3](#)
 Repair [5, 6](#)
 Replace [6](#)
 Replacement [6](#)
 Reproduction [2](#)
 Required fields [137](#)
 Reset [42](#)
 Reset button, the [42](#)
 resetting the Prestige [42](#)
 Restore [6](#)
 Restore Configuration [219](#)
 Return Material Authorization (RMA) Number [6](#)
 Returned Products [6](#)
 Returns [6](#)
 RFC 1483 [71](#)
 RFC 1631 [84](#)
 RFC-2364 [156](#)
 RFC2516 [37](#)
 Rights [2](#)
 Rights, Legal [6](#)
 RIP [146, 159](#)
 RIPSee Routing Information Protocol [65](#)
 Risk [5](#)
 Risks [5](#)
 RMA [6](#)
 romfile [214](#)
 Routing [148](#)
 Routing Information Protocol [65](#)
 Direction [65](#)
 Version [65](#)
 Routing Policy [236](#)

S

Safety Warnings [5](#)
 Sample IP Addresses [159](#)
 Schedule Sets
 Duration [247](#)
 Separation Between Equipment and Receiver [3](#)
 Serial Number [7](#)
 Server [87, 174, 176, 178, 179, 181, 182, 183, 230](#)
 Server behind NAT [179](#)
 Service [5, 6](#)
 Service Personnel [5](#)
 Service Type [273](#)

Services [88](#)
 Set top box [39](#)
 setup a schedule [247](#)
 Shipping [6](#)
 Shock, Electric [5](#)
 SMT Menu Overview [135](#)
 SMTP [89](#)
 SNMP [89](#)

- Community [204](#)
- Configuration [203](#)
- Get [203](#)
- GetNext [203](#)
- Manager [202](#)
- MIBs [203](#)
- Set [203](#)
- Trap [203](#)
- Trusted Host [204](#)

 Source-Based Routing [236](#)
 Spain, Contact Information [7](#)
 Static route [164](#)
 Static Routing Topology [164](#)
 SUA [88, 89](#)
 SUA (Single User Account) [88, 172](#)
 SUA server [88, 90](#)

- Default server set [88](#)

 SUA vs NAT [88](#)
 SUA/NAT Server Set [91](#)
 Subnet Mask [64, 146, 158, 166, 209](#)
 Subnet Masks [297](#)
 Subnetting [297](#)
 Supply Voltage [5](#)
 Support E-mail [7](#)
 Supporting Disk [32](#)
 Sustain Cell Rate (SCR) [80](#)
 Sweden, Contact Information [7](#)
 Swimming Pool [5](#)
 Syntax Conventions [32](#)
 System

- Console Port Speed [209](#)
- Diagnostic [211](#)
- Log and Trace [210](#)
- System Information [208](#)
- System Status [206](#)

 System Information [208](#)
 System Information & Diagnosis [206](#)
 System Maintenance [206, 208, 215, 218, 223, 226, 227, 230](#)
 System Management Terminal [136](#)
 System Status [207](#)
 System Timeout [101, 234](#)

T

Tampering [6](#)
 TCP/IP [101, 197, 212](#)
 Telecommunication Line Cord. [5](#)
 Telephone [7](#)
 Television Interference [3](#)
 Television Reception [3](#)
 Telnet [101, 134](#)
 Telnet Configuration [101](#)
 TFTP

- Restrictions [233](#)

 TFTP File Transfer [223](#)
 TFTP Restrictions [100, 217](#)
 Thunderstorm [5](#)
 Time and Date Setting [228, 229](#)
 Time Zone [230](#)
 TOS (Type of Service) [236](#)
 Trace Records [210](#)
 Trademark [2](#)
 Trademark Owners [2](#)
 Trademarks [2](#)
 Traffic shaping [73](#)
 Translation [2](#)
 TV Technician [3](#)
 Type of Service [236, 238, 239, 240](#)

U

Undesired Operations [3](#)
 Universal Plug and Play [106](#)

- Application [106](#)
- Security issues [106](#)

 Universal Plug and Play (UPnP) [37](#)
 Universal Plug and Play Forum [107](#)
 UNIX Syslog [210](#)
 Upload Firmware [221](#)
 UPnP [106](#)
 User Name [97](#)

V

Value [6](#)
 Vendor [5](#)
 Ventilation Slots [5](#)
 Viewing Certifications [3, 4](#)

Virtual Channel Identifier (VCI) [71](#)
virtual circuit (VC) [71](#)
Virtual Path Identifier (VPI) [71](#)
Voltage Supply [5](#)
Voltage, High [5](#)
VPI & VCI [71](#)

W

Wall Mount [5](#)
WAN (Wide Area Network) [70](#)
Warnings [5](#)
Warranty [6](#)
Warranty Information [7](#)
Warranty Period [6](#)
Water [5](#)
Water Pipes [5](#)
Web Configurator [44](#), [45](#), [46](#)
web configurator screen summary [46](#)
Web Site [7](#)
Wet Basement [5](#)
Workmanship [6](#)
Worldwide Contact Information [7](#)
Written Permission [2](#)

X

XMODEM protocol [215](#)

Z

ZyNOS [2](#), [215](#)
ZyNOS (ZyXEL Network Operating System) [214](#)
ZyNOS F/W Version [215](#)
ZyXEL Communications Corporation [2](#)
ZyXEL Home Page [4](#)
ZyXEL Limited Warranty
 Note [6](#)
ZyXEL Network Operating System [2](#)