

# *P-660H/HW/W-T Series*

*ADSL 2+ Gateway*

## ***User's Guide***

Version 3.40  
7/2005

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 or depth.

# Copyright

Copyright © 2005 by ZyXEL Communications Corporation.

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

Published by ZyXEL Communications Corporation. All rights reserved.

## **Disclaimer**

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

## **Trademarks**

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

# Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation

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

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

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

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

## **FCC Caution**

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

## **IMPORTANT NOTE: FCC Radiation Exposure Statement**

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

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

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

## Certifications

Go to [www.zyxel.com](http://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 <sup>A</sup>	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 Niils 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		

<b>METHOD</b>	<b>SUPPORT E-MAIL</b>	<b>TELEPHONE<sup>A</sup></b>	<b>WEB SITE</b>	<b>REGULAR MAIL</b>
<b>LOCATION</b>	<b>SALES E-MAIL</b>	<b>FAX</b>	<b>FTP SITE</b>	
<b>UNITED KINGDOM</b>	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

<b>Copyright</b> .....	<b>2</b>
<b>Federal Communications Commission (FCC) Interference Statement</b> .....	<b>3</b>
<b>Safety Warnings</b> .....	<b>5</b>
<b>ZyXEL Limited Warranty</b> .....	<b>6</b>
<b>Customer Support</b> .....	<b>7</b>
<b>Table of Contents</b> .....	<b>10</b>
<b>List of Figures</b> .....	<b>24</b>
<b>List of Tables</b> .....	<b>32</b>
<b>Preface</b> .....	<b>38</b>
<b>Introduction to DSL</b> .....	<b>40</b>
<b>Chapter 1</b>	
<b>Getting To Know Your Prestige</b> .....	<b>42</b>
1.1 Introducing the Prestige .....	42
1.2 Features .....	42
1.2.1 Wireless Features (P-660HW/P-660W) .....	45
1.3 Applications for the Prestige .....	46
1.3.1 Protected Internet Access .....	46
1.3.2 LAN to LAN Application .....	46
1.4 Front Panel LEDs .....	46
1.5 Hardware Connection .....	47
<b>Chapter 2</b>	
<b>Introducing the Web Configurator</b> .....	<b>48</b>
2.1 Web Configurator Overview .....	48
2.1.1 Accessing the Web Configurator .....	48
2.1.2 Resetting the Prestige .....	49
2.1.2.1 Using the Reset Button .....	49
2.1.3 Navigating the Web Configurator .....	50
2.2 Change Login Password .....	52

<b>Chapter 3</b>	
<b>Wizard Setup for Internet Access .....</b>	<b>54</b>
3.1 Introduction .....	54
3.1.1 Internet Access Wizard Setup .....	54
<b>Chapter 4</b>	
<b>LAN Setup .....</b>	<b>62</b>
4.1 LAN Overview .....	62
4.1.1 LANs, WANs and the Prestige .....	62
4.1.2 DHCP Setup .....	63
4.1.2.1 IP Pool Setup .....	63
4.1.3 DNS Server Address .....	63
4.1.4 DNS Server Address Assignment .....	63
4.2 LAN TCP/IP .....	64
4.2.1 IP Address and Subnet Mask .....	64
4.2.1.1 Private IP Addresses .....	65
4.2.2 RIP Setup .....	65
4.2.3 Multicast .....	66
4.2.4 Any IP .....	66
4.2.4.1 How Any IP Works .....	67
4.3 Configuring LAN .....	68
<b>Chapter 5</b>	
<b>Wireless LAN .....</b>	<b>70</b>
5.1 Wireless LAN Introduction .....	70
5.2 Wireless Security Overview .....	70
5.2.1 Encryption .....	70
5.2.2 Authentication .....	70
5.2.3 Restricted Access .....	71
5.2.4 Hide Prestige Identity .....	71
5.3 The Main Wireless LAN Screen .....	71
5.4 Configuring the Wireless Screen .....	73
5.4.1 WEP Encryption .....	73
5.5 Configuring MAC Filters .....	75
5.6 Introduction to WPA .....	77
5.6.1 WPA-PSK Application Example .....	77
5.6.2 WPA with RADIUS Application Example .....	78
5.6.3 Wireless Client WPA Supplicants .....	79
5.7 Configuring IEEE 802.1x and WPA .....	79
5.7.1 No Access Allowed or Authentication .....	80
5.7.2 Authentication Required: 802.1x .....	80
5.7.3 Authentication Required: WPA .....	82
5.7.4 Authentication Required: WPA-PSK .....	84

5.8 Configuring Local User Authentication .....	85
5.9 Configuring RADIUS .....	87

## Chapter 6

### WAN Setup..... 90

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

## Chapter 7

### Network Address Translation (NAT) Screens..... 102

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

7.4 Selecting the NAT Mode .....	107
7.5 Configuring SUA Server Set .....	108
7.6 Configuring Address Mapping Rules .....	110
7.7 Editing an Address Mapping Rule .....	111
<b>Chapter 8</b>	
<b>Dynamic DNS Setup.....</b>	<b>114</b>
8.1 Dynamic DNS Overview .....	114
8.1.1 DYNDNS Wildcard .....	114
8.2 Configuring Dynamic DNS .....	114
<b>Chapter 9</b>	
<b>Time and Date.....</b>	<b>116</b>
9.1 Configuring Time and Date .....	116
<b>Chapter 10</b>	
<b>Firewalls.....</b>	<b>118</b>
10.1 Firewall Overview .....	118
10.2 Types of Firewalls .....	118
10.2.1 Packet Filtering Firewalls .....	118
10.2.2 Application-level Firewalls .....	119
10.2.3 Stateful Inspection Firewalls .....	119
10.3 Introduction to ZyXEL's Firewall .....	119
10.3.1 Denial of Service Attacks .....	120
10.4 Denial of Service .....	120
10.4.1 Basics .....	120
10.4.2 Types of DoS Attacks .....	121
10.4.2.1 ICMP Vulnerability .....	123
10.4.2.2 Illegal Commands (NetBIOS and SMTP) .....	123
10.4.2.3 Traceroute .....	124
10.5 Stateful Inspection .....	124
10.5.1 Stateful Inspection Process .....	125
10.5.2 Stateful Inspection and the Prestige .....	126
10.5.3 TCP Security .....	126
10.5.4 UDP/ICMP Security .....	127
10.5.5 Upper Layer Protocols .....	127
10.6 Guidelines for Enhancing Security with Your Firewall .....	127
10.6.1 Security In General .....	128
10.7 Packet Filtering Vs Firewall .....	129
10.7.1 Packet Filtering: .....	129
10.7.1.1 When To Use Filtering .....	129
10.7.2 Firewall .....	129
10.7.2.1 When To Use The Firewall .....	129

<b>Chapter 11</b>	
<b>Firewall Configuration .....</b>	<b>132</b>
11.1 Access Methods .....	132
11.2 Firewall Policies Overview .....	132
11.3 Rule Logic Overview .....	133
11.3.1 Rule Checklist .....	133
11.3.2 Security Ramifications .....	133
11.3.3 Key Fields For Configuring Rules .....	134
11.3.3.1 Action .....	134
11.3.3.2 Service .....	134
11.3.3.3 Source Address .....	134
11.3.3.4 Destination Address .....	134
11.4 Connection Direction .....	134
11.4.1 LAN to WAN Rules .....	134
11.4.2 Alerts .....	135
11.5 Configuring Default Firewall Policy .....	135
11.6 Rule Summary .....	136
11.6.1 Configuring Firewall Rules .....	138
11.7 Customized Services .....	141
11.8 Configuring A Customized Service .....	141
11.9 Example Firewall Rule .....	142
11.10 Predefined Services .....	146
11.11 Anti-Probing .....	148
11.12 DoS Thresholds .....	149
11.12.1 Threshold Values .....	150
11.12.2 Half-Open Sessions .....	150
11.12.2.1 TCP Maximum Incomplete and Blocking Time .....	150
11.12.3 Configuring Firewall Thresholds .....	151
<b>Chapter 12</b>	
<b>Content Filtering .....</b>	<b>154</b>
12.1 Content Filtering Overview .....	154
12.2 The Main Content Filter Screen .....	154
12.3 Configuring Keyword Blocking .....	155
12.4 Configuring the Schedule .....	156
12.5 Configuring Trusted Computers .....	156
<b>Chapter 13</b>	
<b>Remote Management Configuration .....</b>	<b>158</b>
13.1 Remote Management Overview .....	158
13.1.1 Remote Management Limitations .....	158
13.1.2 Remote Management and NAT .....	159
13.1.3 System Timeout .....	159

13.2 Telnet .....	159
13.3 FTP .....	160
13.4 Web .....	160
13.5 Configuring Remote Management .....	160
<b>Chapter 14</b>	
<b>Universal Plug-and-Play (UPnP) .....</b>	<b>162</b>
14.1 Introducing Universal Plug and Play .....	162
14.1.1 How do I know if I'm using UPnP? .....	162
14.1.2 NAT Traversal .....	162
14.1.3 Cautions with UPnP .....	163
14.2 UPnP and ZyXEL .....	163
14.2.1 Configuring UPnP .....	163
14.3 Installing UPnP in Windows Example .....	164
14.4 Using UPnP in Windows XP Example .....	168
<b>Chapter 15</b>	
<b>Logs Screens .....</b>	<b>176</b>
15.1 Logs Overview .....	176
15.1.1 Alerts and Logs .....	176
15.2 Configuring Log Settings .....	176
15.3 Displaying the Logs .....	178
15.4 SMTP Error Messages .....	179
15.4.1 Example E-mail Log .....	180
<b>Chapter 16</b>	
<b>Media Bandwidth Management Advanced Setup.....</b>	<b>182</b>
16.1 Media Bandwidth Management Overview .....	182
16.2 Bandwidth Classes and Filters .....	182
16.3 Proportional Bandwidth Allocation .....	183
16.4 Bandwidth Management Usage Examples .....	183
16.4.1 Application-based Bandwidth Management Example .....	183
16.4.2 Subnet-based Bandwidth Management Example .....	183
16.4.3 Application and Subnet-based Bandwidth Management Example .....	184
16.5 Scheduler .....	185
16.5.1 Priority-based Scheduler .....	185
16.5.2 Fairness-based Scheduler .....	185
16.6 Maximize Bandwidth Usage .....	185
16.6.1 Reserving Bandwidth for Non-Bandwidth Class Traffic .....	185
16.6.2 Maximize Bandwidth Usage Example .....	186
16.7 Bandwidth Borrowing .....	187
16.7.1 Maximize Bandwidth Usage With Bandwidth Borrowing .....	187
16.8 The Main Media Bandwidth Management Screen .....	188

16.9 Configuring Summary .....	188
16.10 Configuring Class Setup .....	190
16.10.1 Media Bandwidth Management Class Configuration .....	190
16.10.2 Media Bandwidth Management Statistics .....	193
16.11 Bandwidth Monitor .....	194
<b>Chapter 17</b>	
<b>Maintenance .....</b>	<b>196</b>
17.1 Maintenance Overview .....	196
17.2 System Status Screen .....	196
17.2.1 System Statistics .....	198
17.3 DHCP Table Screen .....	200
17.4 Any IP Table Screen .....	201
17.5 Wireless Screen .....	201
17.5.1 Association List .....	201
17.6 Diagnostic Screens .....	202
17.6.1 General Diagnostic .....	202
17.6.2 DSL Line Diagnostic .....	203
17.7 Firmware Upgrade .....	205
<b>Chapter 18</b>	
<b>Introducing the SMT .....</b>	<b>208</b>
18.1 SMT Introduction .....	208
18.1.1 Procedure for SMT Configuration via Telnet .....	208
18.1.2 Entering Password .....	208
18.1.3 Prestige SMT Menus Overview .....	209
18.2 Navigating the SMT Interface .....	210
18.2.1 System Management Terminal Interface Summary .....	211
18.3 Changing the System Password .....	212
<b>Chapter 19</b>	
<b>Menu 1 General Setup .....</b>	<b>214</b>
19.1 General Setup .....	214
19.2 Procedure To Configure Menu 1 .....	214
19.2.1 Procedure to Configure Dynamic DNS .....	215
<b>Chapter 20</b>	
<b>Menu 2 WAN Backup Setup .....</b>	<b>218</b>
20.1 Introduction to WAN Backup Setup .....	218
20.2 Configuring Dial Backup in Menu 2 .....	218
20.2.1 Traffic Redirect Setup .....	219



<b>Chapter 21</b>	
<b>Menu 3 LAN Setup .....</b>	<b>222</b>
21.1 LAN Setup .....	222
21.1.1 General Ethernet Setup .....	222
21.2 Protocol Dependent Ethernet Setup .....	223
21.3 TCP/IP Ethernet Setup and DHCP .....	223
<b>Chapter 22</b>	
<b>Wireless LAN Setup .....</b>	<b>226</b>
22.1 Wireless LAN Overview .....	226
22.2 Wireless LAN Setup .....	226
22.2.1 Wireless LAN MAC Address Filter .....	227
<b>Chapter 23</b>	
<b>Internet Access .....</b>	<b>230</b>
23.1 Internet Access Overview .....	230
23.2 IP Policies .....	230
23.3 IP Alias .....	230
23.4 IP Alias Setup .....	231
23.5 Route IP Setup .....	232
23.6 Internet Access Configuration .....	233
<b>Chapter 24</b>	
<b>Remote Node Configuration .....</b>	<b>236</b>
24.1 Remote Node Setup Overview .....	236
24.2 Remote Node Setup .....	236
24.2.1 Remote Node Profile .....	236
24.2.2 Encapsulation and Multiplexing Scenarios .....	237
24.2.2.1 Scenario 1: One VC, Multiple Protocols .....	237
24.2.2.2 Scenario 2: One VC, One Protocol (IP) .....	237
24.2.2.3 Scenario 3: Multiple VCs .....	237
24.2.3 Outgoing Authentication Protocol .....	239
24.3 Remote Node Network Layer Options .....	240
24.3.1 My WAN Addr Sample IP Addresses .....	241
24.4 Remote Node Filter .....	242
24.5 Editing ATM Layer Options .....	243
24.5.1 VC-based Multiplexing (non-PPP Encapsulation) .....	243
24.5.2 LLC-based Multiplexing or PPP Encapsulation .....	243
24.5.3 Advance Setup Options .....	244
<b>Chapter 25</b>	
<b>Static Route Setup .....</b>	<b>246</b>
25.1 IP Static Route Overview .....	246

25.2 Configuration .....	246
<b>Chapter 26</b>	
<b>Bridging Setup .....</b>	<b>250</b>
26.1 Bridging in General .....	250
26.2 Bridge Ethernet Setup .....	250
26.2.1 Remote Node Bridging Setup .....	250
26.2.2 Bridge Static Route Setup .....	252
<b>Chapter 27</b>	
<b>Network Address Translation (NAT) .....</b>	<b>254</b>
27.1 Using NAT .....	254
27.1.1 SUA (Single User Account) Versus NAT .....	254
27.2 Applying NAT .....	254
27.3 NAT Setup .....	256
27.3.1 Address Mapping Sets .....	256
27.3.1.1 SUA Address Mapping Set .....	257
27.3.1.2 User-Defined Address Mapping Sets .....	258
27.3.1.3 Ordering Your Rules .....	259
27.4 Configuring a Server behind NAT .....	260
27.5 General NAT Examples .....	261
27.5.1 Example 1: Internet Access Only .....	262
27.5.2 Example 2: Internet Access with an Inside Server .....	262
27.5.3 Example 3: Multiple Public IP Addresses With Inside Servers .....	263
27.5.4 Example 4: NAT Unfriendly Application Programs .....	267
<b>Chapter 28</b>	
<b>Enabling the Firewall .....</b>	<b>270</b>
28.1 Remote Management and the Firewall .....	270
28.2 Access Methods .....	270
28.3 Enabling the Firewall .....	270
<b>Chapter 29</b>	
<b>Filter Configuration .....</b>	<b>272</b>
29.1 About Filtering .....	272
29.1.1 The Filter Structure of the Prestige .....	273
29.2 Configuring a Filter Set for the Prestige .....	274
29.3 Filter Rules Summary Menus .....	275
29.4 Configuring a Filter Rule .....	276
29.4.1 TCP/IP Filter Rule .....	277
29.4.2 Generic Filter Rule .....	279
29.5 Filter Types and NAT .....	281
29.6 Example Filter .....	281

29.7 Applying Filters and Factory Defaults .....	283
29.7.1 Ethernet Traffic .....	284
29.7.2 Remote Node Filters .....	284
<b>Chapter 30</b>	
<b>SNMP Configuration .....</b>	<b>286</b>
30.1 About SNMP .....	286
30.2 Supported MIBs .....	287
30.3 SNMP Configuration .....	287
30.4 SNMP Traps .....	288
<b>Chapter 31</b>	
<b>System Security .....</b>	<b>290</b>
31.1 System Security .....	290
31.1.1 System Password .....	290
31.1.2 Configuring External RADIUS Server .....	290
31.1.3 IEEE 802.1x .....	292
31.2 Creating User Accounts on the Prestige .....	294
<b>Chapter 32</b>	
<b>System Information and Diagnosis .....</b>	<b>296</b>
32.1 Overview .....	296
32.2 System Status .....	296
32.3 System Information .....	298
32.3.1 System Information .....	298
32.3.2 Console Port Speed .....	299
32.4 Log and Trace .....	300
32.4.1 Viewing Error Log .....	300
32.4.2 Syslog and Accounting .....	301
32.5 Diagnostic .....	303
<b>Chapter 33</b>	
<b>Firmware and Configuration File Maintenance .....</b>	<b>306</b>
33.1 Filename Conventions .....	306
33.2 Backup Configuration .....	307
33.2.1 Backup Configuration .....	307
33.2.2 Using the FTP Command from the Command Line .....	308
33.2.3 Example of FTP Commands from the Command Line .....	308
33.2.4 GUI-based FTP Clients .....	309
33.2.5 TFTP and FTP over WAN Management Limitations .....	309
33.2.6 Backup Configuration Using TFTP .....	310
33.2.7 TFTP Command Example .....	310
33.2.8 GUI-based TFTP Clients .....	310

33.3 Restore Configuration .....	311
33.3.1 Restore Using FTP .....	311
33.3.2 Restore Using FTP Session Example .....	312
33.4 Uploading Firmware and Configuration Files .....	313
33.4.1 Firmware File Upload .....	313
33.4.2 Configuration File Upload .....	313
33.4.3 FTP File Upload Command from the DOS Prompt Example .....	314
33.4.4 FTP Session Example of Firmware File Upload .....	315
33.4.5 TFTP File Upload .....	315
33.4.6 TFTP Upload Command Example .....	316
<b>Chapter 34</b>	
<b>System Maintenance.....</b>	<b>318</b>
34.1 Command Interpreter Mode .....	318
34.2 Call Control Support .....	319
34.2.1 Budget Management .....	319
34.3 Time and Date Setting .....	320
34.3.1 Resetting the Time .....	322
<b>Chapter 35</b>	
<b>Remote Management.....</b>	<b>324</b>
35.1 Remote Management Overview .....	324
35.2 Remote Management .....	324
35.2.1 Remote Management Setup .....	324
35.2.2 Remote Management Limitations .....	325
35.3 Remote Management and NAT .....	326
35.4 System Timeout .....	326
<b>Chapter 36</b>	
<b>IP Policy Routing.....</b>	<b>328</b>
36.1 IP Policy Routing Overview .....	328
36.2 Benefits of IP Policy Routing .....	328
36.3 Routing Policy .....	328
36.4 IP Routing Policy Setup .....	329
36.5 Applying an IP Policy .....	332
36.5.1 Ethernet IP Policies .....	332
36.6 IP Policy Routing Example .....	333
<b>Chapter 37</b>	
<b>Call Scheduling.....</b>	<b>338</b>
37.1 Introduction .....	338

<b>Chapter 38</b>	
<b>Troubleshooting .....</b>	<b>342</b>
38.1 Problems Starting Up the Prestige .....	342
38.2 Problems with the LAN .....	342
38.3 Problems with the WAN .....	343
38.4 Problems Accessing the Prestige .....	344
38.4.1 Pop-up Windows, JavaScripts and Java Permissions .....	344
38.4.1.1 Internet Explorer Pop-up Blockers .....	344
38.4.1.2 JavaScripts .....	347
38.4.1.3 Java Permissions .....	349
38.4.2 ActiveX Controls in Internet Explorer .....	351
<b>Appendix A</b>	
<b>Product Specifications .....</b>	<b>354</b>
<b>Appendix B</b>	
<b>Wall-mounting Instructions.....</b>	<b>358</b>
<b>Appendix C</b>	
<b>Setting up Your Computer's IP Address.....</b>	<b>360</b>
Windows 95/98/Me.....	360
Windows 2000/NT/XP .....	363
Macintosh OS 8/9.....	368
Macintosh OS X .....	370
Linux.....	371
<b>Appendix D</b>	
<b>IP Subnetting .....</b>	<b>376</b>
IP Addressing.....	376
IP Classes .....	376
Subnet Masks .....	377
Subnetting.....	377
Example: Two Subnets .....	378
Example: Four Subnets.....	380
Example Eight Subnets.....	381
Subnetting With Class A and Class B Networks.....	382
<b>Appendix E</b>	
<b>Boot Commands .....</b>	<b>384</b>
<b>Appendix F</b>	
<b>Command Interpreter.....</b>	<b>386</b>

Command Syntax.....	386
Command Usage .....	386
<b>Appendix G</b>	
<b>Firewall Commands .....</b>	<b>388</b>
<b>Appendix H</b>	
<b>NetBIOS Filter Commands .....</b>	<b>394</b>
Introduction .....	394
Display NetBIOS Filter Settings .....	394
NetBIOS Filter Configuration.....	395
<b>Appendix I</b>	
<b>Splitters and Microfilters .....</b>	<b>398</b>
Connecting a POTS Splitter .....	398
Telephone Microfilters .....	398
Prestige With ISDN .....	399
<b>Appendix J</b>	
<b>PPPoE .....</b>	<b>402</b>
PPPoE in Action.....	402
Benefits of PPPoE.....	402
Traditional Dial-up Scenario .....	402
How PPPoE Works .....	403
Prestige as a PPPoE Client .....	403
<b>Appendix K</b>	
<b>Log Descriptions.....</b>	<b>404</b>
Log Commands.....	418
Log Command Example.....	419
<b>Appendix L</b>	
<b>Wireless LANs .....</b>	<b>420</b>
Wireless LAN Topologies .....	420
Channel.....	422
RTS/CTS.....	422
Fragmentation Threshold .....	423
Preamble Type .....	424
IEEE 802.1x .....	425
RADIUS.....	425
Types of Authentication .....	426
WPA .....	428

Security Parameters Summary .....	429
<b>Appendix M</b>	
<b>Internal SPTGEN .....</b>	<b>430</b>
Internal SPTGEN Overview .....	430
The Configuration Text File Format.....	430
Internal SPTGEN FTP Download Example.....	431
Internal SPTGEN FTP Upload Example .....	432
Command Examples.....	453
<b>Index.....</b>	<b>456</b>

# List of Figures

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



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

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

Figure 125 Menu 11.1 Remote Node Profile .....	238
Figure 126 Menu 11.3 Remote Node Network Layer Options .....	240
Figure 127 Sample IP Addresses for a TCP/IP LAN-to-LAN Connection .....	242
Figure 128 Menu 11.5 Remote Node Filter (RFC 1483 or ENET Encapsulation) .....	242
Figure 129 Menu 11.5 Remote Node Filter (PPPoA or PPPoE Encapsulation) .....	243
Figure 130 Menu 11.6 for VC-based Multiplexing .....	243
Figure 131 Menu 11.6 for LLC-based Multiplexing or PPP Encapsulation .....	244
Figure 132 Menu 11.1 Remote Node Profile .....	244
Figure 133 Menu 11.8 Advance Setup Options .....	245
Figure 134 Sample Static Routing Topology .....	246
Figure 135 Menu 12 Static Route Setup .....	247
Figure 136 Menu 12.1 IP Static Route Setup .....	247
Figure 137 Menu 12.1.1 Edit IP Static Route .....	247
Figure 138 Menu 11.1 Remote Node Profile .....	251
Figure 139 Menu 11.3 Remote Node Network Layer Options .....	251
Figure 140 Menu 12.3.1 Edit Bridge Static Route .....	252
Figure 141 Menu 4 Applying NAT for Internet Access .....	255
Figure 142 Applying NAT in Menus 4 & 11.3 .....	255
Figure 143 Menu 15 NAT Setup .....	256
Figure 144 Menu 15.1 Address Mapping Sets .....	257
Figure 145 Menu 15.1.255 SUA Address Mapping Rules .....	257
Figure 146 Menu 15.1.1 First Set .....	258
Figure 147 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set .....	259
Figure 148 Menu 15.2 NAT Server Setup .....	260
Figure 149 Menu 15.2.1 NAT Server Setup .....	261
Figure 150 Multiple Servers Behind NAT Example .....	261
Figure 151 NAT Example 1 .....	262
Figure 152 Menu 4 Internet Access & NAT Example .....	262
Figure 153 NAT Example 2 .....	263
Figure 154 Menu 15.2.1 Specifying an Inside Server .....	263
Figure 155 NAT Example 3 .....	264
Figure 156 Example 3: Menu 11.3 .....	265
Figure 157 Example 3: Menu 15.1.1.1 .....	265
Figure 158 Example 3: Final Menu 15.1.1 .....	266
Figure 159 Example 3: Menu 15.2.1 .....	266
Figure 160 NAT Example 4 .....	267
Figure 161 Example 4: Menu 15.1.1.1 Address Mapping Rule .....	267
Figure 162 Example 4: Menu 15.1.1 Address Mapping Rules .....	268
Figure 163 Menu 21.2 Firewall Setup .....	271
Figure 164 Outgoing Packet Filtering Process .....	272
Figure 165 Filter Rule Process .....	273
Figure 166 Menu 21 Filter Set Configuration .....	274
Figure 167 NetBIOS_WAN Filter Rules Summary .....	274

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

Figure 211 Menu 25 IP Routing Policy Setup .....	329
Figure 212 Menu 25.1 IP Routing Policy Setup .....	330
Figure 213 Menu 25.1.1 IP Routing Policy .....	331
Figure 214 Menu 3.2 TCP/IP and DHCP Ethernet Setup .....	333
Figure 215 Menu 11.3 Remote Node Network Layer Options .....	333
Figure 216 Example of IP Policy Routing .....	334
Figure 217 IP Routing Policy Example .....	335
Figure 218 IP Routing Policy Example .....	336
Figure 219 Applying IP Policies Example .....	336
Figure 220 Menu 26 Schedule Setup .....	338
Figure 221 Menu 26.1 Schedule Set Setup .....	339
Figure 222 Applying Schedule Set(s) to a Remote Node (PPPoE) .....	340
Figure 223 Pop-up Blocker .....	345
Figure 224 Internet Options .....	345
Figure 225 Internet Options .....	346
Figure 226 Pop-up Blocker Settings .....	347
Figure 227 Internet Options .....	348
Figure 228 Security Settings - Java Scripting .....	349
Figure 229 Security Settings - Java .....	350
Figure 230 Java (Sun) .....	351
Figure 231 Internet Options Security .....	352
Figure 232 Security Setting ActiveX Controls .....	353
Figure 233 Wall-mounting Example .....	358
Figure 234 Windows 95/98/Me: Network: Configuration .....	361
Figure 235 Windows 95/98/Me: TCP/IP Properties: IP Address .....	362
Figure 236 Windows 95/98/Me: TCP/IP Properties: DNS Configuration .....	363
Figure 237 Windows XP: Start Menu .....	364
Figure 238 Windows XP: Control Panel .....	364
Figure 239 Windows XP: Control Panel: Network Connections: Properties .....	365
Figure 240 Windows XP: Local Area Connection Properties .....	365
Figure 241 Windows XP: Internet Protocol (TCP/IP) Properties .....	366
Figure 242 Windows XP: Advanced TCP/IP Properties .....	367
Figure 243 Windows XP: Internet Protocol (TCP/IP) Properties .....	368
Figure 244 Macintosh OS 8/9: Apple Menu .....	369
Figure 245 Macintosh OS 8/9: TCP/IP .....	369
Figure 246 Macintosh OS X: Apple Menu .....	370
Figure 247 Macintosh OS X: Network .....	371
Figure 248 Red Hat 9.0: KDE: Network Configuration: Devices .....	372
Figure 249 Red Hat 9.0: KDE: Ethernet Device: General .....	372
Figure 250 Red Hat 9.0: KDE: Network Configuration: DNS .....	373
Figure 251 <b>Red Hat 9.0: KDE: Network Configuration: Activate</b> .....	373
Figure 252 Red Hat 9.0: Dynamic IP Address Setting in ifconfig-eth0 .....	374
Figure 253 Red Hat 9.0: Static IP Address Setting in ifconfig-eth0 .....	374

---

Figure 254 Red Hat 9.0: DNS Settings in resolv.conf .....	374
Figure 255 Red Hat 9.0: Restart Ethernet Card .....	375
Figure 256 Red Hat 9.0: Checking TCP/IP Properties .....	375
Figure 257 Option to Enter Debug Mode .....	384
Figure 258 Boot Module Commands .....	385
Figure 259 Connecting a POTS Splitter .....	398
Figure 260 Connecting a Microfilter .....	399
Figure 261 Prestige with ISDN .....	399
Figure 262 Single-Computer per Router Hardware Configuration .....	403
Figure 263 Prestige as a PPPoE Client .....	403
Figure 264 Displaying Log Categories Example .....	418
Figure 265 Displaying Log Parameters Example .....	418
Figure 266 Peer-to-Peer Communication in an Ad-hoc Network .....	420
Figure 267 Basic Service Set .....	421
Figure 268 Infrastructure WLAN .....	422
Figure 269 RTS/CTS .....	423
Figure 270 Configuration Text File Format: Column Descriptions .....	430
Figure 271 Invalid Parameter Entered: Command Line Example .....	431
Figure 272 Valid Parameter Entered: Command Line Example .....	431
Figure 273 Internal SPTGEN FTP Download Example .....	432
Figure 274 Internal SPTGEN FTP Upload Example .....	432



# List of Tables

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



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

Table 82 Menu 3.2.1 IP Alias Setup .....	232
Table 83 Menu 4 Internet Access Setup .....	234
Table 84 Menu 11.1 Remote Node Profile .....	238
Table 85 Menu 11.3 Remote Node Network Layer Options .....	240
Table 86 Menu 11.8 Advance Setup Options .....	245
Table 87 Menu 12.1.1 Edit IP Static Route .....	248
Table 88 Remote Node Network Layer Options: Bridge Fields .....	251
Table 89 Menu 12.3.1 Edit Bridge Static Route .....	252
Table 90 Applying NAT in Menus 4 & 11.3 .....	256
Table 91 SUA Address Mapping Rules .....	257
Table 92 Menu 15.1.1 First Set .....	259
Table 93 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set .....	260
Table 94 Abbreviations Used in the Filter Rules Summary Menu .....	275
Table 95 Rule Abbreviations Used .....	276
Table 96 Menu 21.1.x.1 TCP/IP Filter Rule .....	277
Table 97 Menu 21.1.5.1 Generic Filter Rule .....	280
Table 98 Filter Sets Table .....	283
Table 99 Menu 22 SNMP Configuration .....	288
Table 100 SNMP Traps .....	288
Table 101 Ports and Permanent Virtual Circuits .....	289
Table 102 Menu 23.2 System Security: RADIUS Server .....	291
Table 103 Menu 23.4 System Security: IEEE 802.1x .....	293
Table 104 Menu 14.1 Edit Dial-in User .....	295
Table 105 Menu 24.1 System Maintenance: Status .....	297
Table 106 Menu 24.2.1 System Maintenance: Information .....	299
Table 107 Menu 24.3.2 System Maintenance : Syslog and Accounting .....	301
Table 108 Menu 24.4 System Maintenance Menu: Diagnostic .....	304
Table 109 Filename Conventions .....	307
Table 110 General Commands for GUI-based FTP Clients .....	309
Table 111 General Commands for GUI-based TFTP Clients .....	311
Table 112 Menu 24.9.1 System Maintenance: Budget Management .....	320
Table 113 Menu 24.10 System Maintenance: Time and Date Setting .....	321
Table 114 Menu 24.11 Remote Management Control .....	325
Table 115 Menu 25.1 IP Routing Policy Setup .....	330
Table 116 Menu 25.1.1 IP Routing Policy .....	331
Table 117 Menu 26.1 Schedule Set Setup .....	339
Table 118 Troubleshooting Starting Up Your Prestige .....	342
Table 119 Troubleshooting the LAN .....	342
Table 120 Troubleshooting the WAN .....	343
Table 121 Troubleshooting Accessing the Prestige .....	344
Table 122 Device .....	354
Table 123 Firmware .....	355
Table 124 Classes of IP Addresses .....	376

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

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



# Preface

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

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

## About This User's Guide

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

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

## Syntax Conventions

- “Enter” means for you to type one or more characters. “Select” or “Choose” means for you to use one predefined choices.
- The SMT menu titles and labels are in **Bold Times New Roman** font. Predefined field choices are in **Bold Arial** font. Command and arrow keys are enclosed in square brackets. [ENTER] means the Enter, or carriage return key; [ESC] means the Escape key and [SPACE BAR] means the Space Bar.
- Mouse action sequences are denoted using a comma. For example, “click the Apple icon, **Control Panels** and then **Modem**” means first click the Apple icon, then point your mouse pointer to **Control Panels** and then click **Modem**.
- For brevity's sake, we will use “e.g.,” as a shorthand for “for instance”, and “i.e.,” for “that is” or “in other words” throughout this manual.
- The P-600H/HW/W T series may be referred to as the “Prestige” in this User's Guide.
- Application graphics and screen shoots shown are for the P-660W model unless otherwise specified.

## Related Documentation

- Supporting Disk  
Refer to the included CD for support documents.
- Quick Start Guide











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

- Web Configurator Online Help  
Embedded web help for descriptions of individual screens and supplementary information.
- ZyXEL Glossary and Web Site  
Please refer to [www.zyxel.com](http://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](mailto:techwriters@zyxel.com.tw) or send regular mail to The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Thank you.

### Graphics Icons Key

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

# Introduction to DSL

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

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

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

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

## Introduction to ADSL

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





# CHAPTER 1

## Getting To Know Your Prestige

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

### 1.1 Introducing the Prestige

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

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

Models ending in “1”, for example P-660W-T1, denote a device that works over the analog telephone system, POTS (Plain Old Telephone Service). Models ending in “3” denote a device that works over ISDN (Integrated Services Digital Network). Models ending in “7” denote a device that works over T-ISDN (UR-2).

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

The DSL RJ-11 (ADSL over POTS models) or RJ-45 (ADSL over ISDN models) connects to your ADSL-enabled telephone line. The Prestige is compatible with the ADSL/ADSL2/ADSL2+ standards. Maximum data rates attainable by the Prestige for each standard are shown in the next table.

**Table 1** ADSL Standards

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

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

### 1.2 Features

The following sections describe the features of the Prestige.

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

## **High Speed Internet Access**

Your Prestige ADSL/ADSL2/ADSL2+ router can support downstream transmission rates of up to 24Mbps and upstream transmission rates of 3.5Mbps. Actual speeds attained depend on the ADSL service you subscribed to, distance from your ISP, line quality, etc.

## **Zero Configuration Internet Access**

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

## **Any IP**

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

## **Firewall**

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

## **Content Filtering**

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

## **Traffic Redirect**

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

## **Media Bandwidth Management**

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

## Universal Plug and Play (UPnP)

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

## PPPoE (RFC2516)

PPPoE (Point-to-Point Protocol over Ethernet) emulates a dial-up connection. It allows your ISP to use their existing network configuration with newer broadband technologies such as ADSL. The PPPoE driver on the Prestige is transparent to the computers on the LAN, which see only Ethernet and are not aware of PPPoE thus saving you from having to manage PPPoE clients on individual computers. The Prestige also includes PPPoE idle time-out (the PPPoE connection terminates after a period of no traffic that you configure) and PPPoE Dial-on-Demand (the PPPoE connection is brought up only when an Internet access request is made).

## Network Address Translation (NAT)

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

## Dynamic DNS Support

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

## DHCP

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

## IP Alias

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

## IP Policy Routing (IPPR)

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

## Packet Filters

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

## Housing

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

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

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

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

#### Wireless LAN

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

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

#### Wi-Fi Protected Access

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

#### Antenna

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

#### Wireless LAN MAC Address Filtering

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

#### WEP Encryption

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

## 1.3 Applications for the Prestige

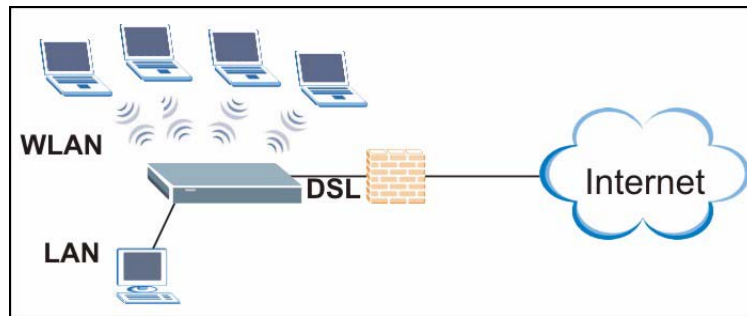
Here are some example uses for which the Prestige is well suited. Application graphics shown are for the P-660W.

### 1.3.1 Protected Internet Access

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

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

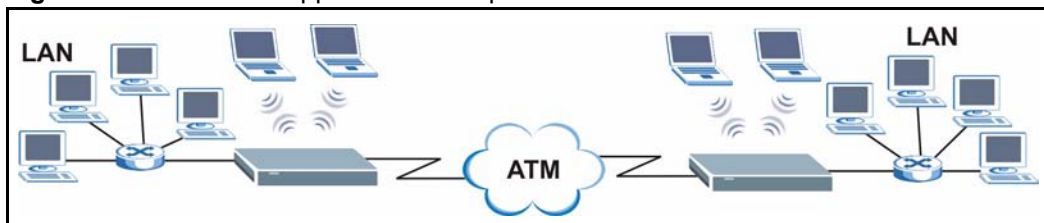
**Figure 1** Protected Internet Access Applications



### 1.3.2 LAN to LAN Application

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

**Figure 2** LAN-to-LAN Application Example



## 1.4 Front Panel LEDs

The following figure shows the front panel LEDs.

The following table describes the LEDs.

**Table 2** Front Panel LEDs

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

## 1.5 Hardware Connection

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

# CHAPTER 2

## Introducing the Web Configurator

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

### 2.1 Web Configurator Overview

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

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

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

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

#### 2.1.1 Accessing the Web Configurator

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

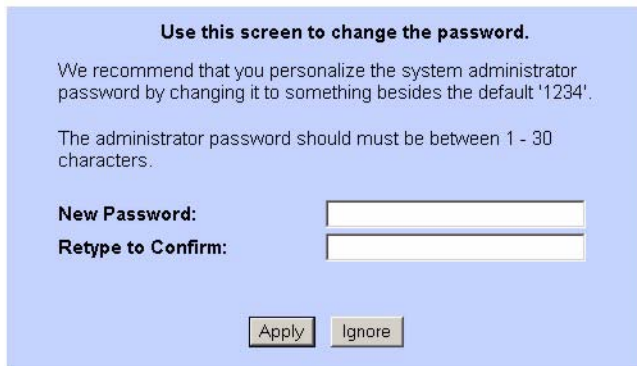
- 1** Make sure your Prestige hardware is properly connected (refer to the Quick Start Guide).
- 2** Prepare your computer/computer network to connect to the Prestige (refer to the Quick Start Guide).
- 3** Launch your web browser.
- 4** Type "192.168.1.1" as the URL.
- 5** A window displays as shown. The **Password** field already contains the default password "1234". Click **Login** to proceed to a screen asking you to change your password or click **Cancel** to revert to the default password.



**Figure 3** Password Screen

- 6 It is highly recommended you change the default password! Enter a new password between 1 and 30 characters, retype it to confirm and click **Apply**; alternatively click **Ignore** to proceed to the main menu if you do not want to change the password now.

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

**Figure 4** Change Password at Login

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

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

## 2.1.2 Resetting the Prestige

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

### 2.1.2.1 Using the Reset Button

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

## 2.1.3 Navigating the Web Configurator

The following summarizes how to navigate the web configurator from the **SITE MAP** screen. We use the Prestige 660W-T1 web screens in this guide as an example. Screens vary slightly for different Prestige models.

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

**Figure 5** Web Configurator: Site Map Screen



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

**Table 3** Web Configurator Screens Summary

LINK	SUB-LINK	FUNCTION
Wizard Setup	Connection Setup	Use these screens for initial configuration including general setup, ISP parameters for Internet Access and WAN IP/DNS Server/MAC address assignment.
	Media Bandwidth Mgmt	Use these screens to limit bandwidth usage by application.
Advanced Setup		
Password		Use this screen to change your password.
LAN		Use this screen to configure LAN DHCP and TCP/IP settings.

**Table 3** Web Configurator Screens Summary (continued)

LINK	SUB-LINK	FUNCTION
Wireless LAN (P-660W / P-660HW only)	Wireless	Use this screen to configure the wireless LAN settings.
	MAC Filter	Use this screen to change MAC filter settings on the Prestige.
	802.1x/WPA	Use this screen to configure WLAN authentication and security settings.
	Local User Database	Use this screen to set up built-in user profiles for wireless station authentication.
	RADIUS	Use this screen to specify the external RADIUS server for wireless station authentication.
WAN	WAN Setup	Use this screen to change the Prestige's WAN remote node settings.
	WAN Backup	Use this screen to configure your traffic redirect properties and WAN backup settings.
NAT	SUA Only	Use this screen to configure servers behind the Prestige.
	Full Feature	Use this screen to configure network address translation mapping rules.
Dynamic DNS		Use this screen to set up dynamic DNS.
Time and Date		Use this screen to change your Prestige's time and date.
Firewall	Default Policy	Use this screen to activate/deactivate the firewall and the direction of network traffic to which to apply the rule.
	Rule Summary	This screen shows a summary of the firewall rules, and allows you to edit/add a firewall rule.
	Anti Probing	Use this screen to change your anti-probing settings.
	Threshold	Use this screen to configure the threshold for DoS attacks.
Content Filter	Keyword	Use this screen to block sites containing certain keywords in the URL.
	Schedule	Use this screen to set the days and times for the Prestige to perform content filtering.
	Trusted	Use this screen to exclude a range of users on the LAN from content filtering on your Prestige.
Remote Management		Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet/FTP/Web to manage the Prestige.
UPnP		Use this screen to enable UPnP on the Prestige.
Logs	Log Settings	Use this screen to change your Prestige's log settings.
	View Log	Use this screen to view the logs for the categories that you selected.
Media Bandwidth Management	Summary	Use this screen to assign bandwidth limits to specific types of traffic.
	Class Setup	Use this screen to define a bandwidth class.
	Monitor	Use this screen to view bandwidth class statistics.
Maintenance		
System Status		This screen contains administrative and system-related information.

**Table 3** Web Configurator Screens Summary (continued)

LINK	SUB-LINK	FUNCTION
DHCP Table		This screen displays DHCP (Dynamic Host Configuration Protocol) related information and is READ-ONLY.
Any IP Table		Use this screen to view the IP and MAC addresses of LAN computers communicating with the Prestige.
Wireless LAN (P-660W / P-660HW only)	Association List	This screen displays the MAC address(es) of the wireless stations that are currently associating with the Prestige.
Diagnostic	General	These screens display information to help you identify problems with the Prestige general connection.
	DSL Line	These screens display information to help you identify problems with the DSL line.
Firmware		Use this screen to upload firmware to your Prestige
LOGOUT		Click <b>Logout</b> to exit the web configurator.

## 2.2 Change Login Password

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

**Figure 6** Password

*Password*

Old Password

New Password

Retype to confirm

**Please record your new password whenever you change it. The system will lock you out if you have forgotten your password.**

The following table describes the fields in this screen.

**Table 4** Password

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

# CHAPTER 3

## Wizard Setup for Internet Access

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

### 3.1 Introduction

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

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

#### 3.1.1 Internet Access Wizard Setup

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

**Figure 7** Internet Access Wizard Setup: ISP Parameters

*Wizard Setup - ISP Parameters for Internet Access*

<b>Mode</b>	Routing
<b>Encapsulation</b>	ENET ENCAP
<b>Multiplex</b>	LLC
<b>Virtual Circuit ID</b>	
VPI	0
VCI	100

Next

The following table describes the fields in this screen.

**Table 5** Internet Access Wizard Setup: ISP Parameters

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

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

**Figure 8** Internet Connection with PPPoE

The following table describes the fields in this screen.

**Table 6** Internet Connection with PPPoE

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

**Figure 9** Internet Connection with RFC 1483

*Connection Setup- ISP Parameters for Internet Access*

IP Address

**Network Address Translation**

▾

The following table describes the fields in this screen.

**Table 7** Internet Connection with RFC 1483

LABEL	DESCRIPTION
IP Address	This field is available if you select <b>Routing</b> in the <b>Mode</b> field. Type your ISP assigned IP address in this field.
Network Address Translation	Select <b>None</b> , <b>SUA Only</b> or <b>Full Feature</b> from the drop-down list box. Refer to the NAT chapter for more details.



**Table 7** Internet Connection with RFC 1483 (continued)

LABEL	DESCRIPTION
Back	Click <b>Back</b> to go back to the first wizard screen.
Next	Click <b>Next</b> to continue to the next wizard screen.

**Figure 10** Internet Connection with ENET ENCAP

The screenshot shows a wizard screen titled "Connection Setup-ISP Parameters for Internet Access". Under the "IP Address" section, there are two radio buttons: "Obtain an IP Address Automatically" (which is selected) and "Static IP Address". Below these are three text input fields: "IP Address" with "0.0.0.0", "Subnet Mask" with "0.0.0.0", and "ENET ENCAP Gateway" with "0.0.0.0". Under the "Network Address Translation" section, there is a dropdown menu currently set to "SUA Only". At the bottom of the screen are "Back" and "Next" buttons.

The following table describes the fields in this screen.

**Table 8** Internet Connection with ENET ENCAP

LABEL	DESCRIPTION
IP Address	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Select <b>Obtain an IP Address Automatically</b> if you have a dynamic IP address; otherwise select <b>Static IP Address</b> 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 <b>ENET ENCAP</b> in the <b>Encapsulation</b> field in the previous screen.
Network Address Translation	Select <b>None</b> , <b>SUA Only</b> or <b>Full Feature</b> from the drop-sown list box. Refer to the NAT chapter for more details.
Back	Click <b>Back</b> to go back to the first wizard screen.
Next	Click <b>Next</b> to continue to the next wizard screen.

**Figure 11** Internet Connection with PPPoA

The following table describes the fields in this screen.

**Table 9** Internet Connection with PPPoA

LABEL	DESCRIPTION
User Name	Enter the login name that your ISP gives you.
Password	Enter the password associated with the user name above.
IP Address	This option is available if you select <b>Routing</b> in the <b>Mode</b> 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 <b>Obtain an IP Address Automatically</b> if you have a dynamic IP address; otherwise click <b>Static IP Address</b> and type your ISP assigned IP address in the IP Address text box below.
Connection	Select <b>Connect on Demand</b> when you don't want the connection up all the time and specify an idle time-out (in seconds) in the <b>Max. Idle Timeout</b> field. The default setting selects <b>Connection on Demand</b> with 0 as the idle time-out, which means the Internet session will not timeout. Select <b>Nailed-Up Connection</b> 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 <b>Connection</b> settings.
Network Address Translation	This option is available if you select <b>Routing</b> in the <b>Mode</b> field. Select <b>None</b> , <b>SUA Only</b> or <b>Full Feature</b> from the drop-down list box. Refer to the NAT chapter for more details.
Back	Click <b>Back</b> to go back to the first wizard screen.
Next	Click <b>Next</b> to continue to the next wizard screen.

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

**Figure 12** Internet Access Wizard Setup: Third Screen

*Wizard Setup - ISP Parameters for Internet Access*

---

**WAN Information:**  
 Mode: **Routing**  
 Encapsulation: **ENET ENCAP**  
 Multiplexing: **LLC**  
 VPI/VCI: **0/100**  
 IP Address : **Obtain an IP Address Automatically**  
 Network Address Translation: **SUA Only**

**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**

Change LAN Configuration

---

Save Settings

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

**Figure 13** Internet Access Wizard Setup: LAN Configuration

*Connection 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

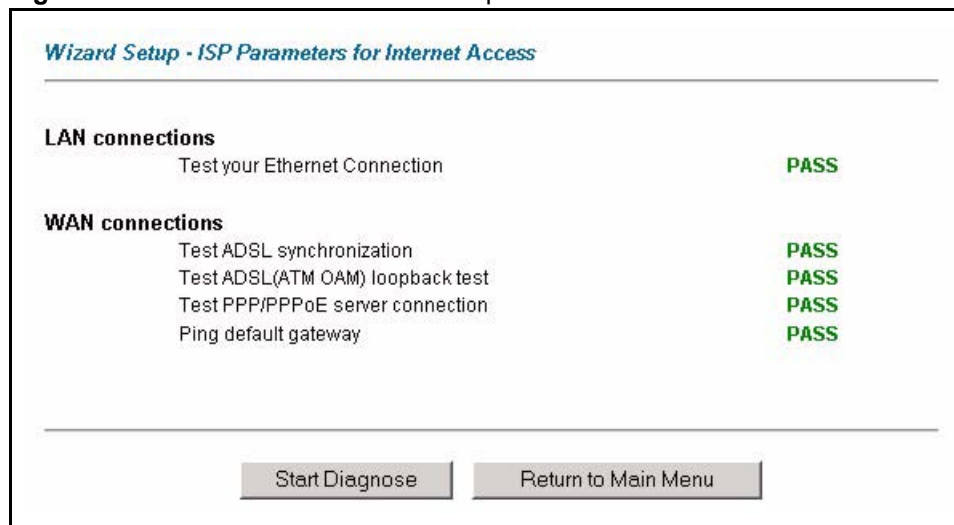
The following table describes the fields in this screen.

**Table 10** Internet Access Wizard Setup: LAN Configuration

LABEL	DESCRIPTION
LAN IP Address	Enter the IP address of your Prestige in dotted decimal notation, for example, 192.168.1.1 (factory default). If you changed the Prestige's LAN IP address, you must use the new IP address if you want to access the web configurator again.
LAN Subnet Mask	Enter a subnet mask in dotted decimal notation.
DHCP	
DHCP Server	From the <b>DHCP Server</b> drop-down list box, select <b>On</b> to allow your Prestige to assign IP addresses, an IP default gateway and DNS servers to computer systems that support the DHCP client. Select <b>Off</b> 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 <b>Back</b> to go back to the previous screen.
Finish	Click <b>Finish</b> to save the settings and proceed to the next wizard screen.

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

**Figure 14** Internet Access Wizard Setup: Connection Tests



- 5 Launch your web browser and navigate to [www.zyxel.com](http://www.zyxel.com). Internet access is just the beginning. Refer to the rest of this guide for more detailed information on the complete range of Prestige features. If you cannot access the Internet, open the web configurator again to confirm that the Internet settings you configured in the Wizard Setup are correct.



# CHAPTER 4

## LAN Setup

This chapter describes how to configure LAN settings.

### 4.1 LAN Overview

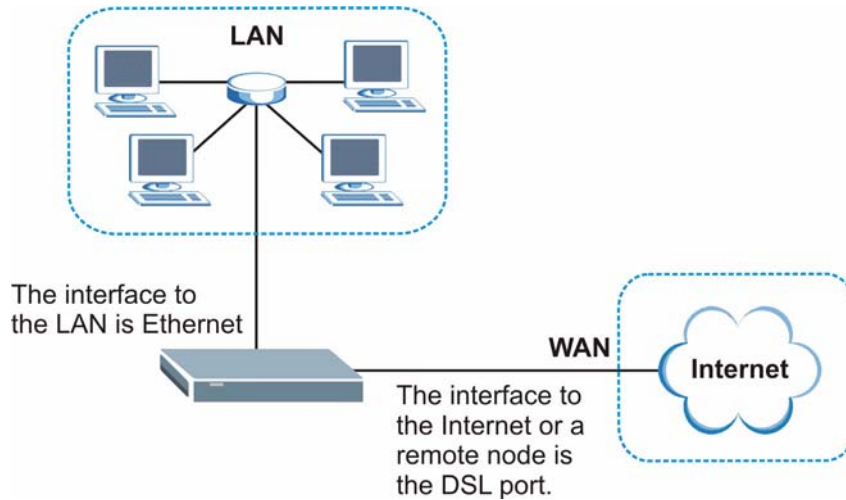
A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building. The LAN screens can help you configure a LAN DHCP server and manage IP addresses.

See [Section 4.3 on page 68](#) to configure the LAN screens.

#### 4.1.1 LANs, WANs and the Prestige

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

**Figure 15** LAN and WAN IP Addresses



## 4.1.2 DHCP Setup

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

### 4.1.2.1 IP Pool Setup

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

## 4.1.3 DNS Server Address

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

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

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

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

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

## 4.1.4 DNS Server Address Assignment

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

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

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

## 4.2 LAN TCP/IP

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

### 4.2.1 IP Address and Subnet Mask

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

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

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

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

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



### 4.2.1.1 Private IP Addresses

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

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

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

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

### 4.2.2 RIP Setup

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

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

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

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

### 4.2.3 Multicast

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

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

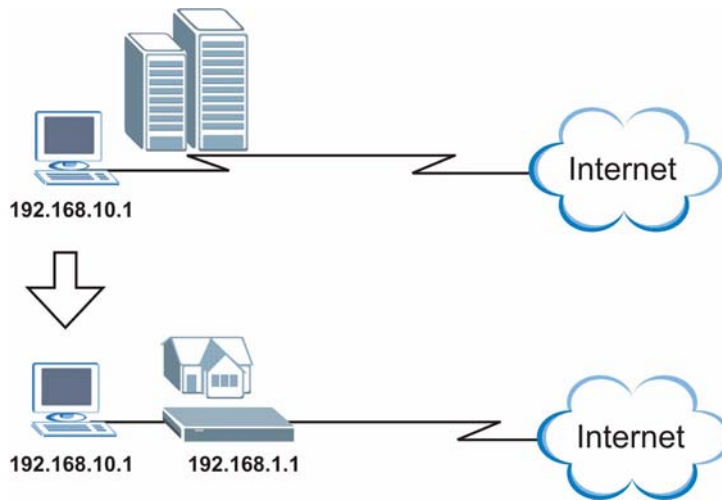
The Prestige supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the Prestige queries all directly connected networks to gather group membership. After that, the Prestige periodically updates this information. IP multicasting can be enabled/disabled on the Prestige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

### 4.2.4 Any IP

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

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

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

**Figure 16** Any IP Example

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

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

#### 4.2.4.1 How Any IP Works

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network. IP routing table is defined on IP Ethernet devices (the Prestige) to decide which hop to use, to help forward data along to its specified destination.

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

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

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

## 4.3 Configuring LAN

Click **LAN** to open the **LAN Setup** screen. See [Section 4.1 on page 62](#) for background information.

**Figure 17** LAN Setup

The screenshot shows the 'LAN - LAN Setup' window. It is divided into three sections: DHCP, TCP/IP, and Any IP Setup. At the bottom are 'Back', 'Apply', and 'Cancel' buttons.

Section	Field	Value
DHCP	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	IP Address	192.168.1.1
	IP Subnet Mask	255.255.255.0
	RIP Direction	Both
	RIP Version	RIP-1
	Multicast	None
Any IP Setup	<input checked="" type="checkbox"/> Active	

The following table describes the fields in this screen.

**Table 11** LAN Setup

LABEL	DESCRIPTION
DHCP	
DHCP	<p>If set to <b>Server</b>, 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 <b>None</b>, the DHCP server will be disabled.</p> <p>If set to <b>Relay</b>, 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 <b>Remote DHCP Server</b> field in this case.</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.

**Table 11** LAN Setup (continued)

LABEL	DESCRIPTION
Size of Client IP Pool	This field specifies the size or count of the IP address pool.
Primary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Secondary DNS Server	As above.
Remote DHCP Server	If <b>Relay</b> is selected in the <b>DHCP</b> 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 <b>None</b> , <b>Both</b> , <b>In Only</b> and <b>Out Only</b> .
RIP Version	Select the RIP version from <b>RIP-1</b> , <b>RIP-2B</b> and <b>RIP-2M</b> .
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 ( <b>IGMP-v1</b> ) and <b>IGMP-v2</b> . Select <b>None</b> to disable it.
Any IP Setup	<p>Select the <b>Active</b> check box to enable the Any IP feature. This allows a computer to access the Internet without changing the network settings (such as IP address and subnet mask) of the computer, even when the IP addresses of the computer and the Prestige are not in the same subnet.</p> <p>When you disable the Any IP feature, only computers with dynamic IP addresses or static IP addresses in the same subnet as the Prestige's LAN IP address can connect to the Prestige or access the Internet through the Prestige.</p>
Apply	Click <b>Apply</b> to save your changes back to the Prestige.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

# CHAPTER 5

## Wireless LAN

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

### 5.1 Wireless LAN Introduction

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

Refer to [Section 5.3 on page 71](#) to configure wireless LAN settings.

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

### 5.2 Wireless Security Overview

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

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

#### 5.2.1 Encryption

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

#### 5.2.2 Authentication

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

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

### 5.2.3 Restricted Access

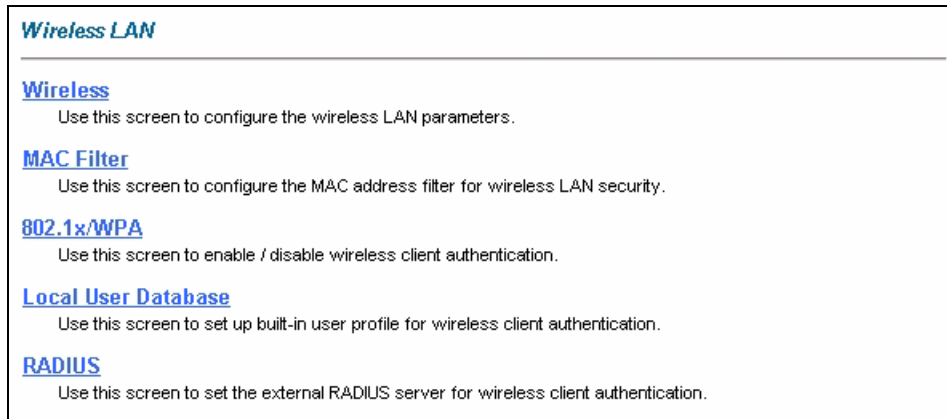
The **MAC Filter** screen allows you to configure the AP to give exclusive access to devices (**Allow Association**) or exclude them from accessing the AP (**Deny Association**).

### 5.2.4 Hide Prestige Identity

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

## 5.3 The Main Wireless LAN Screen

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

**Figure 18** Wireless LAN

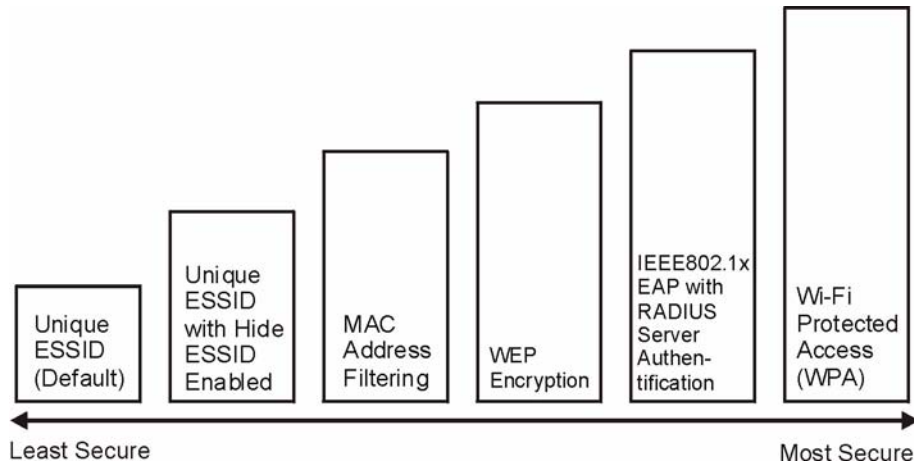
The following table describes the links in this screen.

**Table 12** Wireless LAN

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

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



**Figure 19** Wireless Security Methods

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

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

## 5.4 Configuring the Wireless Screen

### 5.4.1 WEP Encryption

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

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

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

**Figure 20** Wireless Screen

**Wireless LAN- Wireless**

Enable Wireless LAN

ESSID

Hide ESSID

Channel ID

RTS/CTS Threshold  (0 ~ 2432)

Fragmentation Threshold  (256 ~ 2432)

WEP Encryption

64-bit WEP: Enter 5 characters or 10 hexadecimal digits ("0-9", "A-F") preceded by 0x for each Key(1-4).  
 128-bit WEP: Enter 13 characters or 26 hexadecimal digits ("0-9", "A-F") preceded by 0x for each Key(1-4).  
 256-bit WEP: Enter 29 characters or 58 hexadecimal digits ("0-9", "A-F") preceded by 0x for each Key(1-4).

Key1

Key2

Key3

Key4

The following table describes the labels in this screen.

**Table 13** Wireless LAN

LABEL	DESCRIPTION
Enable Wireless LAN	You should configure some wireless security (see <a href="#">Figure 19 on page 73</a> ) when you enable the wireless LAN. Select the check box to enable the wireless LAN.
ESSID	The ESSID (Extended Service Set IDentification) is a unique name to identify the Prestige in the wireless LAN. Wireless stations associating to the Prestige must have the same ESSID. Enter a descriptive name of up to 32 printable characters (including spaces; alphabetic characters are case-sensitive).
Hide ESSID	Select <b>Yes</b> to hide the ESSID in so a station cannot obtain the ESSID through AP scanning. Select <b>No</b> to make the ESSID visible so a station can obtain the ESSID through AP scanning.
Channel ID	The radio frequency used by IEEE 802.11a, b or g wireless devices is called a channel. Select a channel from the drop-down list box.
RTS/CTS Threshold	The RTS (Request To Send) threshold (number of bytes) is for enabling RTS/CTS. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this value to be larger than the maximum MSDU (MAC service data unit) size turns off RTS/CTS. Setting this value to zero turns on RTS/CTS. Select the check box to change the default value and enter a new value between 0 and 2432.

**Table 13** Wireless LAN (continued)

LABEL	DESCRIPTION
Fragmentation Threshold	This is the threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Select the check box to change the default value and enter a value between 256 and 2432.
You won't see the following WEP-related fields if you have <b>WPA</b> or <b>WPA-PSK</b> enabled.	
Passphrase	Enter a "passphrase" (password phrase) of up to 63 case-sensitive printable characters and click <b>Generate</b> to have the Prestige create four different WEP keys. At the time of writing, you cannot use passphrase to generate 256-bit WEP keys.
Generate	After you enter the passphrase, click <b>Generate</b> to have the Prestige generate four different WEP keys automatically. The keys display in the fields below.
WEP Encryption	WEP (Wired Equivalent Privacy) encrypts data frames before transmitting over the wireless network. Select <b>Disable</b> to allow all wireless stations to communicate with the access points without any data encryption. Select <b>64-bit WEP</b> , <b>128-bit WEP</b> or <b>256-bit WEP</b> to use data encryption.
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the Prestige and the wireless stations must use the same WEP key for data transmission. If you want to manually set the WEP keys, enter the key in the field provided. If you chose <b>64-bit WEP</b> , then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose <b>128-bit WEP</b> , then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). If you chose <b>256-bit WEP</b> , then enter 29 ASCII characters or 58 hexadecimal characters ("0-9", "A-F"). The values for the WEP keys must be set up exactly the same on all wireless devices in the same wireless LAN. You must configure all four keys, but only one key can be used at any one time. The default key is key 1.
Back	Click <b>Back</b> to go to the main wireless LAN setup screen.
Apply	Click <b>Apply</b> to save your changes back to the Prestige.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

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

## 5.5 Configuring MAC Filters

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC addresses of the devices to configure this screen. To change your Prestige's MAC filter settings, click **Wireless LAN**, **MAC Filter** to open the **MAC Filter** screen. The screen appears as shown.

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

**Figure 21** MAC Filter

*Wireless LAN- MAC Filter*

Active

Action

MAC Address	
1	<input type="text" value="00:00:00:00:00:00"/>
2	<input type="text" value="00:00:00:00:00:00"/>
3	<input type="text" value="00:00:00:00:00:00"/>
4	<input type="text" value="00:00:00:00:00:00"/>
5	<input type="text" value="00:00:00:00:00:00"/>
6	<input type="text" value="00:00:00:00:00:00"/>
7	<input type="text" value="00:00:00:00:00:00"/>
8	<input type="text" value="00:00:00:00:00:00"/>
9	<input type="text" value="00:00:00:00:00:00"/>
10	<input type="text" value="00:00:00:00:00:00"/>
11	<input type="text" value="00:00:00:00:00:00"/>
12	<input type="text" value="00:00:00:00:00:00"/>
13	<input type="text" value="00:00:00:00:00:00"/>
14	<input type="text" value="00:00:00:00:00:00"/>
15	<input type="text" value="00:00:00:00:00:00"/>
16	<input type="text" value="00:00:00:00:00:00"/>
17	<input type="text" value="00:00:00:00:00:00"/>
18	<input type="text" value="00:00:00:00:00:00"/>
19	<input type="text" value="00:00:00:00:00:00"/>
20	<input type="text" value="00:00:00:00:00:00"/>
21	<input type="text" value="00:00:00:00:00:00"/>
22	<input type="text" value="00:00:00:00:00:00"/>
23	<input type="text" value="00:00:00:00:00:00"/>
24	<input type="text" value="00:00:00:00:00:00"/>
25	<input type="text" value="00:00:00:00:00:00"/>
26	<input type="text" value="00:00:00:00:00:00"/>
27	<input type="text" value="00:00:00:00:00:00"/>
28	<input type="text" value="00:00:00:00:00:00"/>
29	<input type="text" value="00:00:00:00:00:00"/>
30	<input type="text" value="00:00:00:00:00:00"/>
31	<input type="text" value="00:00:00:00:00:00"/>
32	<input type="text" value="00:00:00:00:00:00"/>

The following table describes the fields in this menu.

**Table 14** MAC Filter

LABEL	DESCRIPTION
Active	Select <b>Yes</b> from the drop down list box to enable MAC address filtering.
Action	Define the filter action for the list of MAC addresses in the <b>MAC Address</b> table. Select <b>Deny Association</b> to block access to the router, MAC addresses not listed will be allowed to access the Prestige. Select <b>Allow Association</b> to permit access to the router, MAC addresses not listed will be denied access to the Prestige.

**Table 14** MAC Filter (continued)

LABEL	DESCRIPTION
MAC Address	Enter the MAC addresses in a valid MAC address format, that is, six hexadecimal character pairs, for example, 12:34:56:78:9a:bc of the wireless stations that are allowed or denied access to the Prestige in these address fields.
Back	Click <b>Back</b> to go to the main wireless LAN setup screen.
Apply	Click <b>Apply</b> to save your changes back to the Prestige.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 5.6 Introduction to WPA

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

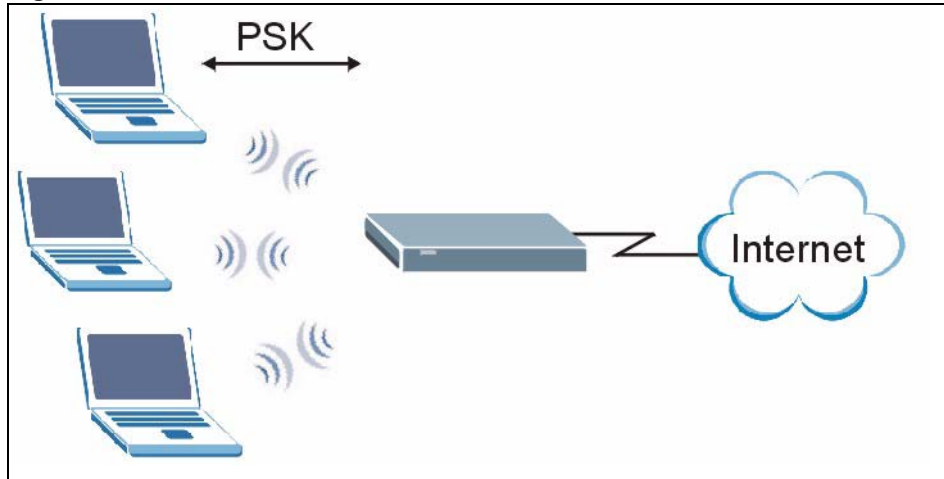
If you don't have an external RADIUS server, you should use WPA-PSK (WPA -Pre-Shared Key). WPA-PSK only requires a single (identical) password entered into each WLAN member. As long as the passwords match, a client will be granted access to a WLAN.

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

### 5.6.1 WPA-PSK Application Example

A WPA-PSK application looks as follows.

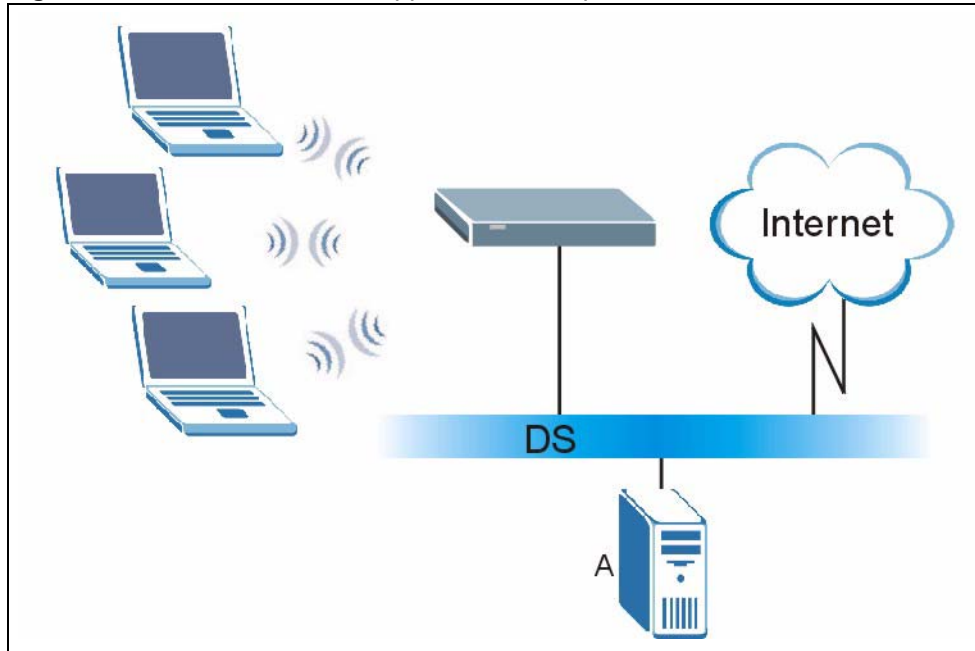
- 1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must be between 8 and 63 printable characters (including spaces; alphabetic characters are case-sensitive).
- 2 The AP checks each client's password and (only) allows it to join the network if the passwords match.
- 3 The AP derives and distributes keys to the wireless clients.
- 4 The AP and wireless clients use the TKIP encryption process to encrypt data exchanged between them.

**Figure 22** WPA - PSK Authentication

### 5.6.2 WPA with RADIUS Application Example

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

- 1 The AP passes the wireless client's authentication request to the RADIUS server.
- 2 The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
- 3 The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly transmitted between the AP and the wireless clients

**Figure 23** WPA with RADIUS Application Example2

### 5.6.3 Wireless Client WPA Supplicants

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

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

See [Section 5.7.3 on page 82](#) and [Section 5.7.4 on page 84](#) for configuration instruction.

## 5.7 Configuring IEEE 802.1x and WPA

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

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

## 5.7.1 No Access Allowed or Authentication

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

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

The screenshot shows a configuration window titled "Wireless LAN - 802.1x/WPA". Under the "802.1x Authentication" section, the "Wireless Port Control" dropdown menu is set to "No Access Allowed". At the bottom of the window are three buttons: "Back", "Apply", and "Cancel".

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

The screenshot shows a configuration window titled "Wireless LAN - 802.1x/WPA". Under the "802.1x Authentication" section, the "Wireless Port Control" dropdown menu is set to "No Authentication Required". At the bottom of the window are three buttons: "Back", "Apply", and "Cancel".

The following table describes the label in these screens.

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

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

## 5.7.2 Authentication Required: 802.1x

You need the following for IEEE 802.1x authentication.



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

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

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

The screenshot shows a configuration window titled "Wireless LAN - 802.1x/WPA". Under the "802.1x Authentication" section, the "Wireless Port Control" dropdown is set to "Authentication Required". The "ReAuthentication Timer" is set to 1800 seconds, and the "Idle Timeout" is set to 3600 seconds. In the "Key Management Protocol" section, the dropdown is set to "802.1x", which is circled in red. The "Dynamic WEP Key Exchange" dropdown is set to "Disable". The "Authentication Databases" dropdown is set to "Local User Database Only". At the bottom, there are "Back", "Apply", and "Cancel" buttons.

The following table describes the labels in this screen.

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

LABEL	DESCRIPTION
Wireless Port Control	To control wireless station access to the wired network, select a control method from the drop-down list box. Choose from <b>No Authentication Required</b> , <b>Authentication Required</b> and <b>No Access Allowed</b> . The following fields are only available when you select <b>Authentication Required</b> .
ReAuthentication Timer (in Seconds)	Specify how often wireless stations have to reenter usernames and passwords in order to stay connected. This field is activated only when you select <b>Authentication Required</b> in the <b>Wireless Port Control</b> field. Enter a time interval between 10 and 9999 seconds. The default time interval is <b>1800</b> seconds (30 minutes).  <b>Note:</b> If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.

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

LABEL	DESCRIPTION
Idle Timeout (in Seconds)	The Prestige automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the username and password again before access to the wired network is allowed.  This field is activated only when you select <b>Authentication Required</b> in the <b>Wireless Port Control</b> field. The default time interval is <b>3600</b> seconds (or 1 hour).
Key Management Protocol	Choose <b>802.1x</b> from the drop-down list.
Dynamic WEP Key Exchange	This field is activated only when you select <b>Authentication Required</b> in the <b>Wireless Port Control</b> field. Also set the <b>Authentication Databases</b> field to <b>RADIUS Only</b> . Local user database may not be used.  Select <b>Disable</b> to allow wireless stations to communicate with the access points without using dynamic WEP key exchange.  Select <b>64-bit WEP</b> , <b>128-bit WEP</b> or <b>256-bit WEP</b> to enable data encryption.  Up to 32 stations can access the Prestige when you configure dynamic WEP key exchange.  This field is not available when you set <b>Key Management Protocol</b> to <b>WPA</b> or <b>WPA-PSK</b> .
Authentication Databases	The authentication database contains wireless station login information. The local user database is the built-in database on the Prestige. The RADIUS is an external server. Use this drop-down list box to select which database the Prestige should use (first) to authenticate a wireless station.  Before you specify the priority, make sure you have set up the corresponding database correctly first.  Select <b>Local User Database Only</b> to have the Prestige just check the built-in user database on the Prestige for a wireless station's username and password.  Select <b>RADIUS Only</b> to have the Prestige just check the user database on the specified RADIUS server for a wireless station's username and password.  Select <b>Local first, then RADIUS</b> to have the Prestige first check the user database on the Prestige for a wireless station's username and password. If the user name is not found, the Prestige then checks the user database on the specified RADIUS server.  Select <b>RADIUS first, then Local</b> to have the Prestige first check the user database on the specified RADIUS server for a wireless station's username and password. If the Prestige cannot reach the RADIUS server, the Prestige then checks the local user database on the Prestige. When the user name is not found or password does not match in the RADIUS server, the Prestige will not check the local user database and the authentication fails.
Back	Click <b>Back</b> to go to the main wireless LAN setup screen.
Apply	Click <b>Apply</b> to save your changes back to the Prestige.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

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

### 5.7.3 Authentication Required: WPA

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

See [Section 5.6 on page 77](#) for more information.

**Figure 27** Wireless LAN: 802.1x/WPA: WPA

**Wireless LAN - 802.1x/WPA**

**802.1x Authentication**

Wireless Port Control: Authentication Required

ReAuthentication Timer: 1800 (In Seconds)

Idle Timeout: 3600 (In Seconds)

Key Management Protocol: **WPA**

WPA Mixed Mode

Group Data Privacy: TKIP

WPA Group Key Update Timer: 1800 (In Seconds)

Authentication Databases: RADIUS Only

Buttons: Back, Apply, Cancel

The following table describes the labels not previously discussed.

**Table 17** Wireless LAN: 802.1x/WPA: WPA

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

## 5.7.4 Authentication Required: WPA-PSK

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

See [Section 5.6 on page 77](#) for more information.

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

The screenshot shows the configuration interface for Wireless LAN: 802.1x/WPA. The '802.1x Authentication' section includes 'Wireless Port Control' (set to 'Authentication Required'), 'ReAuthentication Timer' (1800), and 'Idle Timeout' (3600). The 'Key Management Protocol' dropdown is highlighted with a red circle and set to 'WPA-PSK'. Below it is the 'Pre-Shared Key' field, a 'WPA Mixed Mode' checkbox, 'Group Data Privacy' (TKIP), and 'WPA Group Key Update Timer' (1800). At the bottom are 'Back', 'Apply', and 'Cancel' buttons.

The following table describes the labels not previously discussed.

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

LABEL	DESCRIPTION
Key Management Protocol	Choose <b>WPA-PSK</b> in this field.
Pre-Shared Key	The encryption mechanisms used for <b>WPA</b> and <b>WPA-PSK</b> are the same. The only difference between the two is that <b>WPA-PSK</b> uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 printable characters (including spaces; alphabetic characters are case-sensitive).
WPA Mixed Mode	The Prestige can operate in <b>WPA Mixed Mode</b> , which supports both clients running WPA and clients running dynamic WEP key exchange with 802.1x in the same Wi-Fi network. Select the check box to activate WPA mixed mode. Otherwise, clear the check box and configure the <b>Group Data Privacy</b> field.

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

LABEL	DESCRIPTION
Group Data Privacy	<b>Group Data Privacy</b> allows you to choose <b>TKIP</b> (recommended) or <b>WEP</b> for broadcast and multicast ("group") traffic if the <b>Key Management Protocol</b> is <b>WPA</b> and <b>WPA Mixed Mode</b> is disabled. <b>WEP</b> is used automatically if you have enabled <b>WPA Mixed Mode</b> . All unicast traffic is automatically encrypted by <b>TKIP</b> when <b>WPA</b> or <b>WPA-PSK Key Management Protocol</b> is selected.
Authentication Databases	This field is only visible when <b>WPA Mixed Mode</b> is enabled.


## 5.8 Configuring Local User Authentication

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

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

**Figure 29** Local User Database

*Wireless LAN - Local User Database*

#	Active	User Name	Password
1	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
2	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
3	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
4	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
5	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
6	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
7	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
8	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
9	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
			
29	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
30	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
31	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
32	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

The following table describes the fields in this screen.

**Table 19** Local User Database

LABEL	DESCRIPTION
#	This is the index number of a local user account.
Active	Select this check box to enable the user profile.
User Name	Enter a user name of up to 31 alphanumeric characters (case-sensitive), hyphens ('-') and underscores ('_') if you're using MD5 encryption and maximum 14 if you're using PEAP.
Password	Enter a password of up to 31 printable characters (including spaces; alphabetic characters are case-sensitive) if you're using MD5 encryption and maximum 14 if you're using PEAP.
Back	Click <b>Back</b> to go to the main wireless LAN setup screen.
Apply	Click <b>Apply</b> to save these settings back to the Prestige.
Cancel	Click <b>Cancel</b> to begin configuring this screen again.

## 5.9 Configuring RADIUS

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

**Figure 30** RADIUS

**Wireless LAN - RADIUS**

**Authentication Server**

Active: Yes

Server IP Address: 0.0.0.0

Port Number: 1812

Shared Secret: [Empty]

**Accounting Server**

Active: No

Server IP Address: 0.0.0.0

Port Number: 1813

Shared Secret: [Empty]

Buttons: Back, Apply, Cancel

The following table describes the fields in this screen.

**Table 20** RADIUS

LABEL	DESCRIPTION
Authentication Server	
Active	Select <b>Yes</b> from the drop-down list box to enable user authentication through an external authentication server.
Server IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	The default port of the RADIUS server for authentication is <b>1812</b> . You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the access points. The key is not sent over the network. This key must be the same on the external authentication server and Prestige.
Accounting Server	
Active	Select <b>Yes</b> from the drop-down list box to enable user authentication through an external accounting server.
Server IP Address	Enter the IP address of the external accounting server in dotted decimal notation.

**Table 20** RADIUS (continued)

LABEL	DESCRIPTION
Port Number	The default port of the RADIUS server for accounting is <b>1813</b> . You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the access points. The key is not sent over the network. This key must be the same on the external accounting server and the Prestige.
Back	Click <b>Back</b> to go to the main wireless LAN setup screen.
Apply	Click <b>Apply</b> to save these settings back to the Prestige.
Cancel	Click <b>Cancel</b> to begin configuring this screen again.





# CHAPTER 6

## WAN Setup

This chapter describes how to configure WAN settings.

### 6.1 WAN Overview

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

#### 6.1.1 Encapsulation

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

##### 6.1.1.1 ENET ENCAP

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

##### 6.1.1.2 PPP over Ethernet

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

##### 6.1.1.3 PPPoA

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

#### 6.1.1.4 RFC 1483

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

### 6.1.2 Multiplexing

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

#### 6.1.2.1 VC-based Multiplexing

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

#### 6.1.2.2 LLC-based Multiplexing

In this case one VC carries multiple protocols with protocol identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol, for example, if charging heavily depends on the number of simultaneous VCs.

### 6.1.3 VPI and VCI

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

### 6.1.4 IP Address Assignment

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

#### 6.1.4.1 IP Assignment with PPPoA or PPPoE Encapsulation

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

### 6.1.4.2 IP Assignment with RFC 1483 Encapsulation

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

### 6.1.4.3 IP Assignment with ENET ENCAP Encapsulation

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

### 6.1.5 Nailed-Up Connection (PPP)

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

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

### 6.1.6 NAT

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

## 6.2 Metric

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

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

- Normal route: designated by the ISP (see [Section 6.7 on page 95](#))
- Traffic-redirect route (see [Section 6.8 on page 98](#))
- WAN-backup route, also called dial-backup (see [Section 6.9 on page 99](#))

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

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

IP Policy Routing overrides the default routing behavior and takes priority over all of the routes mentioned above.

## 6.3 PPPoE Encapsulation

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

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

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

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

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

## 6.4 Traffic Shaping

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

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

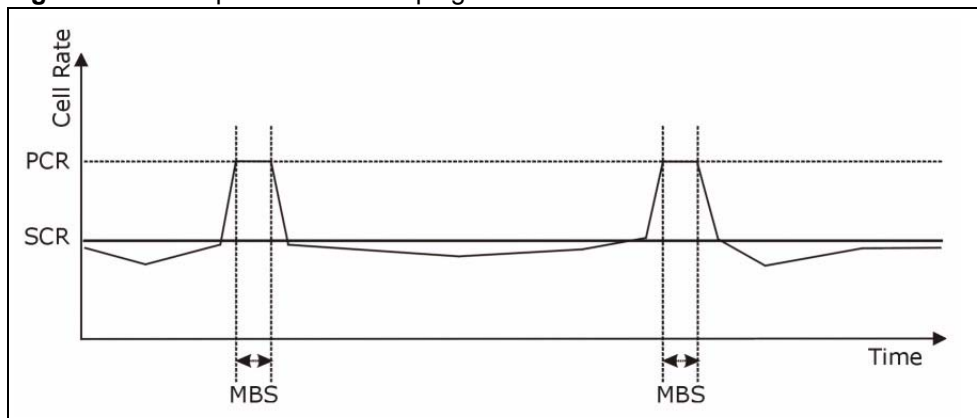
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

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

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

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

**Figure 31** Example of Traffic Shaping



## 6.5 Zero Configuration Internet Access

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

Zero configuration for Internet access is disable when

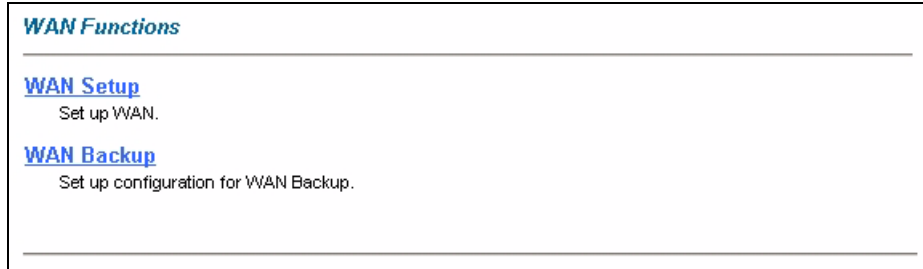
- the Prestige is in bridge mode
- you set the Prestige to use a static (fixed) WAN IP address.

## 6.6 The Main WAN Screen

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

See [Section 6.1 on page 90](#) for more information.

**Figure 32** WAN



The following table describes the links in this screen.

**Table 21** WAN

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

## 6.7 Configuring WAN Setup

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

See [Section 6.1 on page 90](#) for more information.

**Figure 33** WAN Setup (PPPoE)

**WAN - WAN Setup**

---

**Name**

**Mode**

**Encapsulation**

**Multiplex**

**Virtual Circuit ID**

VPI

VCI

**ATM QoS Type**

**Cell Rate**

Peak Cell Rate  cell/sec

Sustain Cell Rate  cell/sec

Maximum Burst Size

**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**

**Zero Configuration**

---

The following table describes the fields in this screen.

**Table 22** WAN Setup

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



**Table 22** WAN Setup (continued)

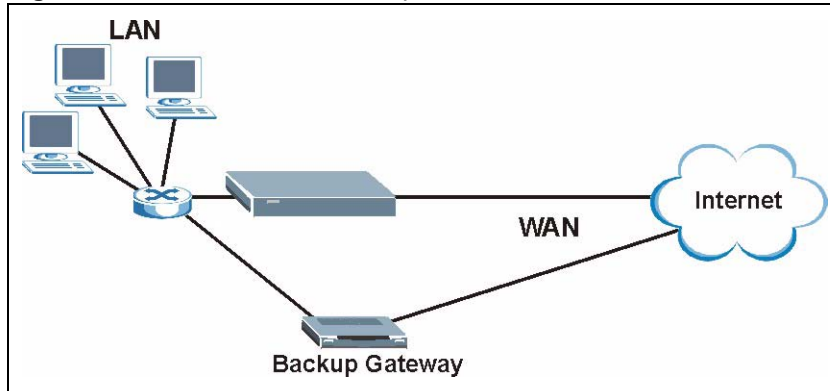
LABEL	DESCRIPTION
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. Choices vary depending on the mode you select in the <b>Mode</b> field. If you select <b>Bridge</b> in the <b>Mode</b> field, select either <b>PPPoA</b> or <b>RFC 1483</b> . If you select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

**Table 22** WAN Setup (continued)

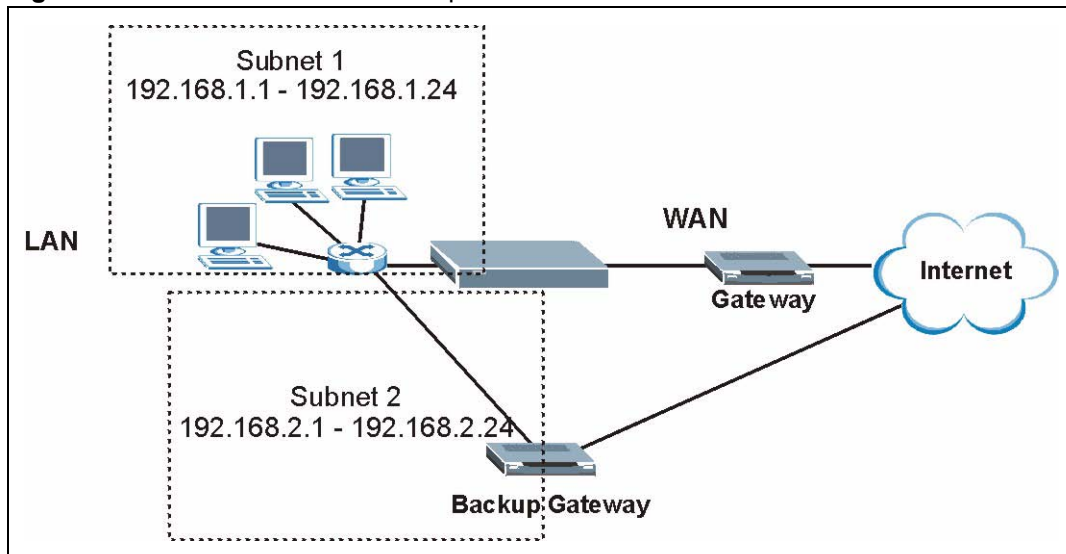
LABEL	DESCRIPTION
Connect on Demand	Select <b>Connect on Demand</b> when you don't want the connection up all the time and specify an idle time-out in the <b>Max Idle Timeout</b> field.
Max Idle Timeout	Specify an idle time-out in the <b>Max Idle Timeout</b> field when you select <b>Connect on Demand</b> . 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 <b>PPPoE</b> 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>
ENET ENCAP Gateway (ENET ENCAP encapsulation only)	You must specify a gateway IP address (supplied by your ISP) when you select <b>ENET ENCAP</b> in the <b>Encapsulation</b> field
Zero Configuration	<p>This feature is not applicable/available when you configure the Prestige to use a static WAN IP address or in bridge mode.</p> <p>Select <b>Yes</b> to set the Prestige to automatically detect the Internet connection settings (such as the VCI/VPI numbers and the encapsulation method) from the ISP and make the necessary configuration changes.</p> <p>Select <b>No</b> to disable this feature. You must manually configure the Prestige for Internet access.</p>
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save the changes.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 6.8 Traffic Redirect

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

**Figure 34** Traffic Redirect Example

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

**Figure 35** Traffic Redirect LAN Setup

## 6.9 Configuring WAN Backup

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

**Figure 36** WAN Backup

The following table describes the fields in this screen.

**Table 23** WAN Backup

LABEL	DESCRIPTION
Backup Type	Select the method that the Prestige uses to check the DSL connection. Select <b>DSL Link</b> to have the Prestige check if the connection to the DSLAM is up. Select <b>ICMP</b> to have the Prestige periodically ping the IP addresses configured in the <b>Check WAN IP Address</b> fields.
Check WAN IP Address1-3	Configure this field to test your Prestige's WAN accessibility. Type the IP address of a reliable nearby computer (for example, your ISP's DNS server address).  <b>Note:</b> If you activate either traffic redirect or dial backup, you must configure at least one IP address here.  When using a WAN backup connection, the Prestige periodically pings the addresses configured here and uses the other WAN backup connection (if configured) if there is no response.
Fail Tolerance	Type the number of times (2 recommended) that your Prestige may ping the IP addresses configured in the <b>Check WAN IP Address</b> field without getting a response before switching to a WAN backup connection (or a different WAN backup connection).
Recovery Interval	When the Prestige is using a lower priority connection (usually a WAN backup connection), it periodically checks to whether or not it can use a higher priority connection.  Type the number of seconds (30 recommended) for the Prestige to wait between checks. Allow more time if your destination IP address handles lots of traffic.

**Table 23** WAN Backup (continued)

LABEL	DESCRIPTION
Timeout	Type the number of seconds (3 recommended) for your Prestige to wait for a ping response from one of the IP addresses in the <b>Check WAN IP Address</b> field before timing out the request. The WAN connection is considered "down" after the Prestige times out the number of times specified in the <b>Fail Tolerance</b> field. Use a higher value in this field if your network is busy or congested.
Traffic Redirect	Traffic redirect forwards traffic to a backup gateway when the Prestige cannot connect to the Internet.
Active	Select this check box to have the Prestige use traffic redirect if the normal WAN connection goes down.  <b>Note:</b> If you activate traffic redirect, you must configure at least one Check WAN IP Address.
Metric	This field sets this route's priority among the routes the Prestige uses. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".
Backup Gateway	Type the IP address of your backup gateway in dotted decimal notation. The Prestige automatically forwards traffic to this IP address if the Prestige's Internet connection terminates.
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save the changes.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

# CHAPTER 7

## Network Address Translation (NAT) Screens

This chapter discusses how to configure NAT on the Prestige.

### 7.1 NAT Overview

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

#### 7.1.1 NAT Definitions

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

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

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

**Table 24** NAT Definitions

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

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

## 7.1.2 What NAT Does

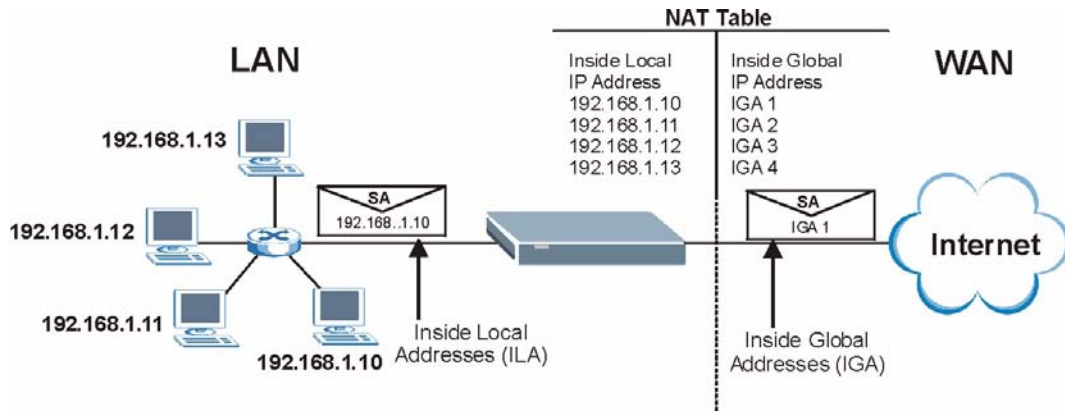
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address)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

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping – see [Table 25 on page 105](#)), NAT offers the additional benefit of firewall protection. With no servers defined, your Prestige filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631, The IP Network Address Translator (NAT)*.

## 7.1.3 How NAT Works

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

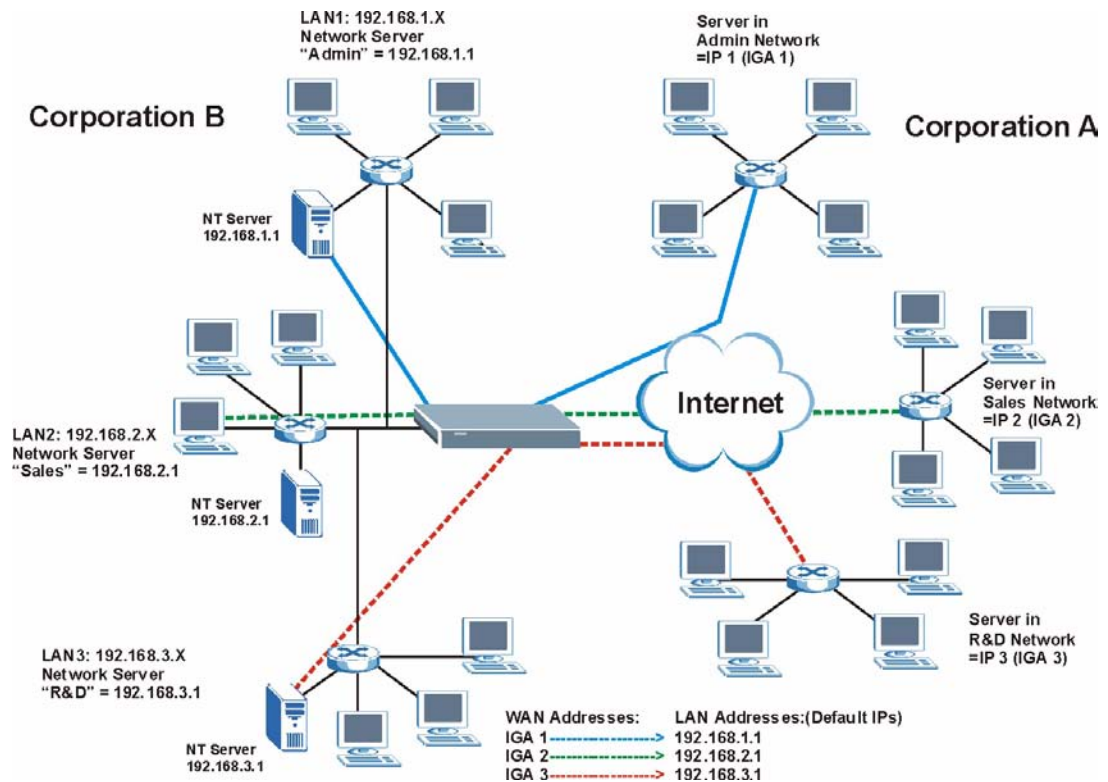
Figure 37 How NAT Works



### 7.1.4 NAT Application

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

Figure 38 NAT Application With IP Alias





## 7.1.5 NAT Mapping Types

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

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

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

The following table summarizes these types.

**Table 25** NAT Mapping Types

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

## 7.2 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. The Prestige also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types as outlined in [Table 25 on page 105](#).

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

## 7.3 SUA Server

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

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

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

### 7.3.1 Default Server IP Address

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

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

### 7.3.2 Port Forwarding: Services and Port Numbers

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

**Table 26** Services and Port Numbers

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

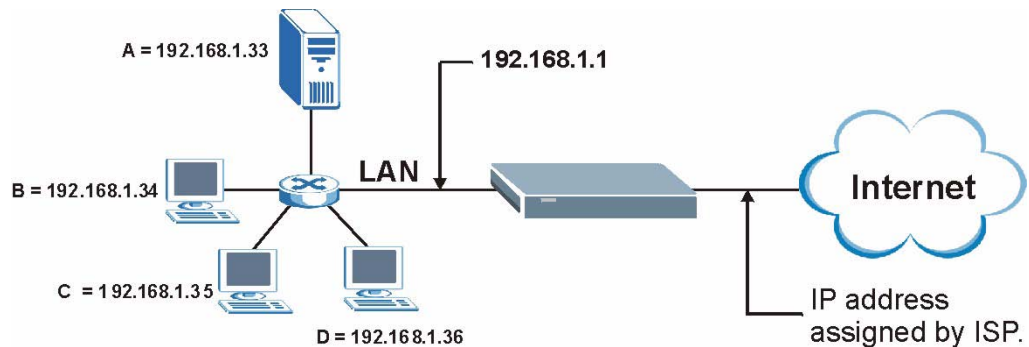
**Table 26** Services and Port Numbers (continued)

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

### 7.3.3 Configuring Servers Behind SUA (Example)

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

IP address assigned by ISP.

**Figure 39** Multiple Servers Behind NAT Example

## 7.4 Selecting the NAT Mode

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

**Figure 40** NAT Mode

**NAT - Mode**

---

Network Address Translation

None

SUA Only [Edit Details](#)

Full Feature [Edit Details](#)

---

The following table describes the labels in this screen.

**Table 27** NAT Mode

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

## 7.5 Configuring SUA Server Set

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

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

See [Section 7.3 on page 106](#) for more information. See [Table 26 on page 106](#) for port numbers commonly used for particular services.

**Figure 41** Edit SUA/NAT Server Set

	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

The following table describes the fields in this screen.

**Table 28** Edit SUA/NAT Server Set

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

## 7.6 Configuring Address Mapping Rules

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

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

**Figure 42** Address Mapping Rules

	Local Start IP	Local End IP	Global Start IP	Global End IP	Type
<a href="#">Rule 1</a>	...	...	...	0.0.0.0	-
<a href="#">Rule 2</a>	...	...	...	0.0.0.0	-
<a href="#">Rule 3</a>	...	...	...	0.0.0.0	-
<a href="#">Rule 4</a>	...	...	...	0.0.0.0	-
<a href="#">Rule 5</a>	...	...	...	0.0.0.0	-
<a href="#">Rule 6</a>	...	...	...	0.0.0.0	-
<a href="#">Rule 7</a>	...	...	...	0.0.0.0	-
<a href="#">Rule 8</a>	...	...	...	0.0.0.0	-
<a href="#">Rule 9</a>	...	...	...	0.0.0.0	-
<a href="#">Rule 10</a>	...	...	...	0.0.0.0	-

Back

The following table describes the fields in this screen.

**Table 29** Address Mapping Rules

LABEL	DESCRIPTION
Local Start IP	This is the starting Inside Local IP Address (ILA). Local IP addresses are <b>N/A</b> for <b>Server</b> 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 <b>Local Start IP</b> address and 255.255.255.255 as the <b>Local End IP</b> address. This field is <b>N/A</b> for <b>One-to-one</b> and <b>Server</b> 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 <b>Many-to-One</b> and <b>Server</b> mapping types.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is <b>N/A</b> for <b>One-to-one</b> , <b>Many-to-One</b> and <b>Server</b> mapping types.