

# *P-2302R Series*

*VoIP Station Gateway*

## **User's Guide**

Version 3.60  
12/2005

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



# Copyright

Copyright © 2005 by ZyXEL Communications Corporation.

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

Published by ZyXEL Communications Corporation. All rights reserved.

## **Disclaimer**

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

## **Trademarks**

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

# Federal Communications Commission (FCC) Interference Statement

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

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

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

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

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

## Notice 1

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

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

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

## Certifications

- 1 Go to [www.zyxel.com](http://www.zyxel.com).
- 2 Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.
- 3 Select the certification you wish to view from this page.





# 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 or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

## Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact 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.

## Registration

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.

# 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 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	+33-4-72-52-97-97	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
		+33-4-72-52-19-20		
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		
HUNGARY	support@zyxel.hu	+36-1-3361649	www.zyxel.hu	ZyXEL Hungary 48, Zoldlomb Str. H-1025, Budapest Hungary
	info@zyxel.hu	+36-1-3259100		
KAZAKHSTAN	http://zyxel.kz/support	+7-3272-590-698	www.zyxel.kz	ZyXEL Kazakhstan 43, Dostyk ave., Office 414 Dostyk Business Centre 050010, Almaty Republic of Kazakhstan
	sales@zyxel.kz	+7-3272-590-689		
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		

METHOD	SUPPORT E-MAIL	TELEPHONE <sup>A</sup>	WEB SITE	REGULAR MAIL
LOCATION	SALES E-MAIL	FAX	FTP SITE	
POLAND	info@pl.zyxel.com	+48-22-5286603	www.pl.zyxel.com	ZyXEL Communications ul.Emilli Plater 53 00-113 Warszawa Poland
		+48-22-5206701		
RUSSIA	http://zyxel.ru/support	+7-095-542-89-29	www.zyxel.ru	ZyXEL Russia Ostrovityanova 37a Str. Moscow, 117279 Russia
	sales@zyxel.ru	+7-095-542-89-25		
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		
UKRAINE	support@ua.zyxel.com	+380-44-247-69-78	www.ua.zyxel.com	ZyXEL Ukraine 13, Pimonenko Str. Kiev, 04050 Ukraine
	sales@ua.zyxel.com	+380-44-494-49-32		
UNITED KINGDOM	support@zyxel.co.uk	+44-1344 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	+44-1344 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>22</b>
<b>List of Tables .....</b>	<b>28</b>
<b>Preface .....</b>	<b>32</b>
<b>Chapter 1</b>	
<b>Introducing the Prestige .....</b>	<b>34</b>
1.1 Prestige 2302R VoIP Station Gateway Series Overview .....	34
1.2 Prestige 2302RL VoIP Analog Telephone Adaptor with Lifeline .....	34
1.3 Features .....	34
1.4 LEDs .....	39
1.5 Applications .....	40
1.5.1 Make Calls via Internet Telephony Service Provider .....	40
1.5.2 Make Calls via IP-PBX .....	41
1.5.3 Make Peer-to-peer Calls .....	42
<b>Chapter 2</b>	
<b>Introducing the Web Configurator .....</b>	<b>44</b>
2.1 Web Configurator Overview .....	44
2.2 Accessing the Prestige Web Configurator .....	44
2.3 Resetting the Prestige .....	45
2.3.1 Procedure To Use The Reset Button .....	45
2.4 Navigating the Prestige Web Configurator .....	46
2.5 Common Screen Command Buttons .....	49
<b>Chapter 3</b>	
<b>Wizard Setup .....</b>	<b>50</b>
3.1 Wizard Setup Overview .....	50

3.2 Wizard 1: General Setup .....	50
3.2.1 Domain Name .....	50
3.3 Wizard 2: ISP Parameters for Internet Access .....	51
3.3.1 Ethernet .....	51
3.3.2 PPPoE Encapsulation .....	52
3.4 Wizard 3: WAN Setup .....	54
3.5 Wizard 4: SIP 1 Setup .....	56
3.6 Wizard Setup Complete .....	59
<b>Chapter 4</b>	
<b>System Screens .....</b>	<b>62</b>
4.1 System Overview .....	62
4.2 DNS Overview .....	62
4.3 General Screen .....	62
4.3.1 Domain Name .....	63
4.3.2 DNS Server Address Assignment .....	63
4.4 System General Configuration .....	63
4.5 Dynamic DNS .....	65
4.5.1 DynDNS Wildcard .....	65
4.6 Configuring Dynamic DNS .....	65
4.7 Configuring Password .....	67
4.8 Pre-defined NTP Time Servers List .....	68
4.9 Configuring Time Setting .....	68
4.9.1 Resetting the Time .....	70
<b>Chapter 5</b>	
<b>LAN Setup .....</b>	<b>72</b>
5.1 LAN Overview .....	72
5.2 IP Address and Subnet Mask .....	72
5.3 DHCP Setup .....	73
5.3.1 IP Pool Setup .....	73
5.4 LAN TCP/IP .....	73
5.4.1 Factory LAN Defaults .....	73
5.5 DNS Server Address .....	73
5.6 RIP Setup .....	74
5.7 Multicast .....	75
5.8 Any IP .....	75
5.8.0.1 How Any IP Works .....	76
5.9 Configuring LAN .....	77
5.10 Configuring IP Alias .....	79



<b>Chapter 6</b>	
<b>WAN Screens</b> .....	<b>82</b>
6.1 WAN Overview .....	82
6.2 Configuring ISP .....	82
6.2.1 Ethernet Encapsulation .....	82
6.2.2 PPPoE Encapsulation .....	83
6.3 WAN IP Address Assignment .....	85
6.4 Configuring WAN IP .....	85
6.5 Configuring WAN MAC .....	88
<b>Chapter 7</b>	
<b>Introduction to VoIP</b> .....	<b>90</b>
7.1 VoIP Introduction .....	90
7.2 Introduction to SIP .....	90
7.2.1 SIP Identities .....	90
7.2.1.1 SIP Number .....	90
7.2.1.2 SIP Service Domain .....	91
7.2.2 SIP Call Progression .....	91
7.2.3 SIP Client Server .....	91
7.2.3.1 SIP User Agent .....	92
7.2.3.2 SIP Proxy Server .....	92
7.2.3.3 SIP Redirect Server .....	93
7.2.3.4 SIP Register Server .....	93
7.2.4 RTP .....	93
7.3 NAT .....	94
7.3.1 NAT Example .....	94
7.3.2 NAT Types .....	95
7.3.2.1 Full Cone NAT .....	96
7.3.2.2 Restricted Cone NAT .....	96
7.3.2.3 Port Restricted Cone NAT .....	97
7.3.2.4 Symmetric NAT .....	98
7.4 NAT and SIP .....	99
7.5 SIP ALG .....	99
7.6 Use NAT .....	99
7.7 STUN .....	100
7.8 Outbound Proxy .....	100
7.9 Voice Coding .....	100
7.9.1 Pulse Code Modulation .....	101
7.9.2 G.711 .....	101
7.9.3 G.729 .....	101
7.10 PSTN Call Setup Signaling .....	101
7.11 MWI (Message Waiting Indication) .....	101

<b>Chapter 8</b>	
<b>VoIP Screens.....</b>	<b>102</b>
8.1 VoIP Introduction .....	102
8.2 VoIP Configuration .....	102
8.3 Custom Tones (IVR) .....	104
8.3.0.1 Recording Custom Tones .....	105
8.3.0.2 Listening to Custom Tones .....	105
8.3.0.3 Deleting Custom Tones .....	105
8.4 Advanced VoIP Settings Configuration .....	105
8.5 Quality of Service (QoS) .....	109
8.5.1 Type Of Service (ToS) .....	110
8.5.2 DiffServ .....	110
8.5.2.1 DSCP and Per-Hop Behavior .....	110
8.5.3 VLAN .....	110
8.6 QoS Configuration .....	111
<b>Chapter 9</b>	
<b>Phone .....</b>	<b>112</b>
9.1 Phone Introduction .....	112
9.1.1 Voice Activity Detection/Silence Suppression .....	112
9.1.2 Comfort Noise Generation .....	112
9.1.3 Echo Cancellation .....	112
9.2 Phone Port Configuration .....	112
9.3 Supplementary Phone Services Overview .....	114
9.3.1 The Flash Key .....	114
9.3.2 Europe Type Supplementary Phone Services .....	114
9.3.2.1 European Call Hold .....	115
9.3.2.2 European Call Waiting .....	115
9.3.2.3 European Call Transfer .....	116
9.3.2.4 European Three-Way Conference .....	116
9.3.3 USA Type Supplementary Services .....	116
9.3.3.1 USA Call Hold .....	117
9.3.3.2 USA Call Waiting .....	117
9.3.3.3 USA Call Transfer .....	117
9.3.3.4 USA Three-Way Conference .....	117
9.4 Common Phone Configuration .....	117
<b>Chapter 10</b>	
<b>Phone Book .....</b>	<b>120</b>
10.1 Phone Book Introduction .....	120
10.1.1 Speed Dial .....	120
10.1.1.1 Peer-to-Peer Calls .....	120
10.1.2 Lifeline (Prestige 2302RL) .....	120

---

10.2 Speed Dial Configuration .....	120
10.3 Call Forward .....	122
10.4 Lifeline Configuration (Prestige 2302RL) .....	125
<b>Chapter 11</b>	
<b>Phone Usage .....</b>	<b>126</b>
11.1 Dialing a Telephone Number .....	126
11.2 Using Speed Dial to Dial a Telephone Number .....	126
11.3 Internal Calls .....	126
11.4 Checking the Prestige's IP Address .....	126
11.5 Auto Firmware Upgrade .....	127
<b>Chapter 12</b>	
<b>Network Address Translation (NAT) Screens .....</b>	<b>128</b>
12.1 NAT Overview .....	128
12.1.1 NAT Definitions .....	128
12.1.2 What NAT Does .....	129
12.1.3 How NAT Works .....	129
12.1.4 NAT Application .....	130
12.1.5 NAT Mapping Types .....	130
12.2 SUA (Single User Account) Versus NAT .....	131
12.3 SUA Server .....	131
12.3.1 Default Server IP Address .....	132
12.3.2 Port Forwarding: Services and Port Numbers .....	132
12.3.3 Configuring Servers Behind SUA (Example) .....	133
12.4 Configuring SUA Server .....	133
12.5 Configuring Address Mapping .....	135
12.5.1 Configuring Address Mapping .....	137
12.6 Trigger Port Forwarding .....	138
12.6.1 Trigger Port Forwarding Example .....	138
12.6.2 Two Points To Remember About Trigger Ports .....	139
12.7 Configuring Trigger Port Forwarding .....	139
<b>Chapter 13</b>	
<b>Static Route .....</b>	<b>142</b>
13.1 Static Route Overview .....	142
13.2 Configuring IP Static Route .....	142
13.2.1 Configuring a Static Route Entry .....	143
<b>Chapter 14</b>	
<b>Firewall .....</b>	<b>146</b>
14.1 Firewall Introduction .....	146
14.1.1 Stateful Inspection Firewall. ....	146

14.1.2 About the Prestige Firewall .....	146
14.1.3 Guidelines For Enhancing Security With Your Firewall .....	147
14.2 Firewall Settings Screen .....	147
14.3 The Firewall, NAT and Remote Management .....	149
14.3.1 LAN-to-WAN rules .....	149
14.3.2 WAN-to-LAN rules .....	150
14.4 Services .....	150
<b>Chapter 15</b>	
<b>Content Filtering .....</b>	<b>154</b>
15.1 Introduction to Content Filtering .....	154
15.2 Restrict Web Features .....	154
15.3 Days and Times .....	154
15.4 Configure Content Filtering .....	154
<b>Chapter 16</b>	
<b>Remote Management Screens .....</b>	<b>158</b>
16.1 Remote Management Overview .....	158
16.1.1 Remote Management Limitations .....	158
16.1.2 Remote Management and NAT .....	159
16.1.3 System Timeout .....	159
16.2 Configuring Telnet .....	159
16.3 Configuring TELNET .....	159
16.4 Configuring FTP .....	160
16.5 Configuring WWW .....	161
16.6 SNMP .....	162
16.6.1 Supported MIBs .....	164
16.6.2 SNMP Traps .....	164
16.6.3 Configuring SNMP .....	165
16.7 Configuring DNS .....	167
16.8 Configuring Security .....	168
<b>Chapter 17</b>	
<b>Universal Plug-and-Play (UPnP) .....</b>	<b>170</b>
17.1 Introducing Universal Plug and Play .....	170
17.1.1 How do I know if I'm using UPnP? .....	170
17.1.2 NAT Traversal .....	170
17.1.3 Cautions with UPnP .....	170
17.2 UPnP and ZyXEL .....	171
17.2.1 Configuring UPnP .....	171
17.3 Installing UPnP in Windows Example .....	172
17.3.1 Installing UPnP in Windows Me .....	172
17.3.2 Installing UPnP in Windows XP .....	174

17.4 Using UPnP in Windows XP Example .....	176
17.4.1 Auto-discover Your UPnP-enabled Network Device .....	176
17.4.2 Web Configurator Easy Access .....	180
<b>Chapter 18</b>	
<b>Logs.....</b>	<b>184</b>
18.1 Configuring View Log .....	184
18.1.1 Log Message Descriptions .....	185
18.1.2 Syslog Logs .....	194
18.2 Configuring Log Settings .....	195
<b>Chapter 19</b>	
<b>Bandwidth Management.....</b>	<b>198</b>
19.1 Bandwidth Management Overview .....	198
19.2 Bandwidth Classes and Filters .....	198
19.3 Proportional Bandwidth Allocation .....	199
19.4 Application-based Bandwidth Management .....	199
19.5 Subnet-based Bandwidth Management .....	199
19.6 Application and Subnet-based Bandwidth Management .....	199
19.7 Scheduler .....	200
19.7.1 Priority-based Scheduler .....	200
19.7.2 Fairness-based Scheduler .....	200
19.8 Maximize Bandwidth Usage .....	200
19.8.1 Reserving Bandwidth for Non-Bandwidth Class Traffic .....	201
19.8.2 Maximize Bandwidth Usage Example .....	201
19.8.2.1 Priority-based Allotment of Unused and Unbudgeted Bandwidth	201
19.8.2.2 Fairness-based Allotment of Unused and Unbudgeted Bandwidth	202
19.9 Bandwidth Borrowing .....	202
19.9.1 Bandwidth Borrowing Example .....	203
19.9.2 Maximize Bandwidth Usage With Bandwidth Borrowing .....	203
19.10 Configuring Summary .....	203
19.11 Configuring Class Setup .....	205
19.11.1 Bandwidth Manager Class Configuration .....	206
19.11.2 Bandwidth Management Statistics .....	208
19.12 Configuring Monitor .....	209
<b>Chapter 20</b>	
<b>Maintenance .....</b>	<b>212</b>
20.1 Maintenance Overview .....	212
20.2 Status Screen .....	212
20.2.1 System Statistics .....	214
20.3 DHCP Table Screen .....	215

20.4 Any IP Table Screen .....	216
20.5 F/W Upload Screen .....	217
20.6 Configuration Screen .....	220
20.6.1 Backup Configuration .....	220
20.6.2 Restore Configuration .....	221
20.6.3 Back to Factory Defaults .....	222
20.7 Restart Screen .....	222
<b>Chapter 21</b>	
<b>Introducing the SMT .....</b>	<b>224</b>
21.1 SMT Introduction .....	224
21.2 Accessing the SMT via Telnet .....	224
21.3 Navigating the SMT Interface .....	224
21.3.1 System Management Terminal Interface Summary .....	226
21.3.2 Prestige SMT Menus Overview .....	227
21.4 Changing the System Password .....	228
<b>Chapter 22</b>	
<b>General Setup .....</b>	<b>230</b>
22.1 General Setup Introduction .....	230
22.2 General Setup Configuration .....	230
22.2.1 Procedure to Configure Dynamic DNS .....	231
<b>Chapter 23</b>	
<b>WAN Setup .....</b>	<b>234</b>
23.1 Introduction to WAN .....	234
23.2 WAN Setup .....	234
<b>Chapter 24</b>	
<b>LAN Setup .....</b>	<b>236</b>
24.1 LAN Setup .....	236
24.1.1 General Ethernet Setup .....	236
24.2 TCP/IP Ethernet Setup and DHCP .....	237
24.2.1 IP Alias Setup .....	239
<b>Chapter 25</b>	
<b>Internet Access .....</b>	<b>242</b>
25.1 Introduction to Internet Access Setup .....	242
25.2 Ethernet Encapsulation .....	242
25.3 Configuring the PPPoE Client .....	243
25.4 Basic Setup Complete .....	244

<b>Chapter 26</b>	
<b>Remote Node Configuration .....</b>	<b>246</b>
26.1 Introduction to Remote Node Setup .....	246
26.2 Remote Node Profile Setup .....	246
26.2.1 Ethernet Encapsulation .....	246
26.2.2 PPPoE Encapsulation .....	248
26.2.2.1 Outgoing Authentication Protocol .....	249
26.2.2.2 Nailed-Up Connection .....	249
26.3 Edit IP .....	250
26.4 Remote Node Filter .....	252
26.4.1 Traffic Redirect Setup .....	253
<b>Chapter 27</b>	
<b>Static Route Setup .....</b>	<b>256</b>
27.1 Static Route Introduction .....	256
27.2 IP Static Route Setup .....	256
<b>Chapter 28</b>	
<b>Network Address Translation (NAT) .....</b>	<b>258</b>
28.1 NAT Introduction .....	258
28.2 Applying NAT .....	258
28.3 NAT Setup .....	259
28.3.1 Address Mapping Sets .....	260
28.3.1.1 User-Defined Address Mapping Sets .....	261
28.3.1.2 Ordering Your Rules .....	262
28.4 Configuring a Server behind NAT .....	264
28.5 General NAT Examples .....	265
28.5.1 Example 1: Internet Access Only .....	265
28.5.2 Example 2: Internet Access with an Inside Server .....	266
28.5.3 Example 3: Multiple Public IP Addresses With Inside Servers .....	267
28.5.4 Example 4: NAT Unfriendly Application Programs .....	270
28.6 Configuring Trigger Port Forwarding .....	271
<b>Chapter 29</b>	
<b>Enabling the Firewall .....</b>	<b>274</b>
29.1 Remote Management and the Firewall .....	274
29.2 Access Methods .....	274
29.3 Enabling the Firewall .....	274
<b>Chapter 30</b>	
<b>Filter Configuration .....</b>	<b>276</b>
30.1 Introduction to Filters .....	276
30.1.1 The Filter Structure of the Prestige .....	277

30.2 Configuring a Filter Set .....	278
30.2.1 Configuring a Filter Rule .....	281
30.2.2 Configuring a TCP/IP Filter Rule .....	281
30.2.3 Configuring a Generic Filter Rule .....	284
30.3 Example Filter .....	286
30.4 Filter Types and NAT .....	288
30.5 Applying a Filter .....	288
30.5.1 Applying LAN Filters .....	289
30.5.2 Applying Remote Node Filters .....	289
<b>Chapter 31</b>	
<b>SNMP Configuration .....</b>	<b>290</b>
31.1 SNMP Introduction .....	290
31.2 SNMP Configuration .....	290
<b>Chapter 32</b>	
<b>System Information and Diagnosis .....</b>	<b>292</b>
32.1 System Status .....	292
32.2 System Information .....	294
32.2.1 System Information .....	294
32.2.2 Console Port Speed .....	295
32.3 Log and Trace .....	296
32.3.1 Syslog Logging .....	296
32.3.1.1 CDR .....	298
32.3.1.2 Packet triggered .....	298
32.3.1.3 Filter log .....	299
32.3.1.4 PPP log .....	299
32.3.2 Call-Triggering Packet .....	299
32.4 Diagnostic .....	300
32.4.1 WAN DHCP .....	301
<b>Chapter 33</b>	
<b>Firmware and Configuration File Maintenance .....</b>	<b>304</b>
33.1 Filename Conventions .....	304
33.2 Backup Configuration .....	305
33.2.1 Backup Configuration .....	305
33.2.2 Using the FTP Command from the Command Line .....	306
33.2.3 Example of FTP Commands from the Command Line .....	306
33.2.4 GUI-based FTP Clients .....	307
33.2.5 TFTP and FTP over WAN Management Limitations .....	307
33.2.6 Backup Configuration Using TFTP .....	307
33.2.7 TFTP Command Example .....	308
33.2.8 GUI-based TFTP Clients .....	308



33.3 Restore Configuration .....	309
33.3.1 Restore Using FTP .....	309
33.3.2 Restore Using FTP Session Example .....	310
33.4 Uploading Firmware and Configuration Files .....	310
33.4.1 Firmware File Upload .....	310
33.4.2 Configuration File Upload .....	311
33.4.3 FTP File Upload Command from the DOS Prompt Example .....	311
33.4.4 FTP Session Example of Firmware File Upload .....	312
33.4.5 TFTP File Upload .....	312
33.4.6 TFTP Upload Command Example .....	313
<b>Chapter 34</b>	
<b>System Maintenance.....</b>	<b>314</b>
34.1 Command Interpreter Mode .....	314
34.1.1 Command Syntax .....	314
34.1.2 Command Usage .....	315
34.2 Call Control Support .....	315
34.2.1 Budget Management .....	315
34.2.2 Call History .....	316
34.3 Time and Date Setting .....	317
<b>Chapter 35</b>	
<b>Remote Management.....</b>	<b>320</b>
<b>Chapter 36</b>	
<b>Call Scheduling .....</b>	<b>322</b>
<b>Chapter 37</b>	
<b>Troubleshooting .....</b>	<b>326</b>
37.1 Problems Starting Up the Prestige .....	326
37.2 Problems with the LAN Interface .....	326
37.3 Problems with the WAN Interface .....	327
37.4 Problems with Internet Access .....	327
37.5 Problems with the Password .....	327
37.6 Problems with the Web Configurator .....	328
37.7 Problems with a Telephone or the Telephone Port .....	328
37.8 Problems with Voice Service .....	329
37.9 Pop-up Windows, JavaScripts and Java Permissions .....	329
37.9.1 Internet Explorer Pop-up Blockers .....	329
37.9.1.1 Disable Pop-up Blockers .....	329
37.9.1.2 Enable Pop-up Blockers with Exceptions .....	330
37.9.2 JavaScripts .....	332
37.9.3 Java Permissions .....	334
37.9.3.1 JAVA (Sun) .....	335

<b>Appendix A</b> <b>Product Specifications .....</b>	<b>338</b>
<b>Appendix B</b> <b>Wall-mounting Instructions.....</b>	<b>342</b>
<b>Appendix C</b> <b>Setting up Your Computer's IP Address.....</b>	<b>344</b>
<b>Appendix D</b> <b>IP Subnetting .....</b>	<b>356</b>
<b>Appendix E</b> <b>PPPoE .....</b>	<b>364</b>
<b>Appendix F</b> <b>Triangle Route .....</b>	<b>366</b>
<b>Appendix G</b> <b>SIP Passthrough .....</b>	<b>370</b>
<b>Index.....</b>	<b>372</b>

# List of Figures

Figure 1 LEDs .....	40
Figure 2 Internet Telephony Service Provider Application .....	41
Figure 3 IP-PBX Application .....	42
Figure 4 Peer-to-peer Calling .....	42
Figure 5 Web Site Address .....	44
Figure 6 Enter Password .....	45
Figure 7 Change Password .....	45
Figure 8 Web Configurator .....	47
Figure 9 Wizard 1: General Setup .....	51
Figure 10 Wizard 2: Ethernet Encapsulation .....	52
Figure 11 Wizard 2: PPPoE Encapsulation .....	53
Figure 12 Wizard 3: WAN Setup .....	54
Figure 13 Wizard 4: SIP 1 Setup .....	57
Figure 14 Wizard Finish .....	60
Figure 15 System General .....	64
Figure 16 DDNS .....	66
Figure 17 Password .....	67
Figure 18 Time Setting .....	69
Figure 19 Any IP Example .....	76
Figure 20 LAN IP .....	77
Figure 21 Physical Network & Partitioned Logical Networks .....	79
Figure 22 LAN IP Alias .....	80
Figure 23 Ethernet Encapsulation .....	83
Figure 24 PPPoE Encapsulation .....	84
Figure 25 WAN: IP .....	86
Figure 26 MAC Setup .....	89
Figure 27 SIP User Agent .....	92
Figure 28 SIP Proxy Server .....	92
Figure 29 SIP Redirect Server .....	93
Figure 30 NAT: Outgoing .....	94
Figure 31 NAT: Incoming .....	95
Figure 32 Full Cone NAT Example .....	96
Figure 33 Restricted Cone NAT Example .....	97
Figure 34 Port Restricted Cone NAT Example .....	98
Figure 35 Symmetric NAT .....	99
Figure 36 STUN .....	100
Figure 37 VoIP .....	103
Figure 38 VoIP Advanced .....	106

Figure 39 DiffServ: Differentiated Service Field .....	110
Figure 40 QoS .....	111
Figure 41 Phone Port .....	113
Figure 42 Phone Port Common .....	118
Figure 43 Speed Dial .....	121
Figure 44 Call Forward .....	123
Figure 45 Lifeline .....	125
Figure 46 How NAT Works .....	129
Figure 47 NAT Application With IP Alias .....	130
Figure 48 Multiple Servers Behind NAT Example .....	133
Figure 49 SUA/NAT Setup .....	134
Figure 50 Address Mapping .....	136
Figure 51 Address Mapping Edit .....	137
Figure 52 Trigger Port Forwarding Process: Example .....	139
Figure 53 Trigger Port .....	140
Figure 54 Example of Static Routing Topology .....	142
Figure 55 IP Static Route .....	143
Figure 56 Edit IP Static Route .....	144
Figure 57 Firewall: Settings .....	148
Figure 58 Firewall Rule Directions .....	149
Figure 59 Firewall: Service .....	151
Figure 60 Content Filter .....	155
Figure 61 Telnet Configuration on a TCP/IP Network .....	159
Figure 62 Remote Management: Telnet .....	160
Figure 63 Remote Management: FTP .....	161
Figure 64 Remote Management: WWW .....	162
Figure 65 SNMP Management Model .....	163
Figure 66 Remote Management: SNMP .....	166
Figure 67 Remote Management: DNS .....	167
Figure 68 Security .....	168
Figure 69 Configuring UPnP .....	171
Figure 70 Add/Remove Programs: Windows Setup: Communication .....	173
Figure 71 Add/Remove Programs: Windows Setup: Communication: Components .....	173
Figure 72 Network Connections .....	174
Figure 73 Windows Optional Networking Components Wizard .....	175
Figure 74 Networking Services .....	176
Figure 75 Network Connections .....	177
Figure 76 Internet Connection Properties .....	178
Figure 77 Internet Connection Properties: Advanced Settings .....	179
Figure 78 Internet Connection Properties: Advanced Settings: Add .....	179
Figure 79 System Tray Icon .....	180
Figure 80 Internet Connection Status .....	180
Figure 81 Network Connections .....	181

Figure 82 Network Connections: My Network Places .....	182
Figure 83 Network Connections: My Network Places: Properties: Example .....	183
Figure 84 View Log .....	184
Figure 85 Log Settings .....	196
Figure 86 Subnet-based Bandwidth Management Example .....	199
Figure 87 Bandwidth Manager: Summary .....	204
Figure 88 Bandwidth Manager: Class Setup .....	205
Figure 89 Bandwidth Manager: Edit Class .....	206
Figure 90 Bandwidth Management Statistics .....	208
Figure 91 Bandwidth Manager Monitor .....	209
Figure 92 System Status .....	213
Figure 93 Maintenance System Statistics .....	214
Figure 94 Maintenance DHCP Table .....	216
Figure 95 Any IP Table .....	217
Figure 96 Firmware Upload .....	218
Figure 97 Firmware Upload In Process .....	219
Figure 98 Network Temporarily Disconnected .....	219
Figure 99 Firmware Upload Error .....	219
Figure 100 Configuration .....	220
Figure 101 Configuration Upload Successful .....	221
Figure 102 Network Temporarily Disconnected .....	221
Figure 103 Reset Warning Message .....	222
Figure 104 Restart Screen .....	223
Figure 105 Login Screen .....	224
Figure 106 SMT Main Menu .....	226
Figure 107 Menu 23 System Password .....	229
Figure 108 Menu 1 General Setup. ....	230
Figure 109 Menu 1.1 Configure Dynamic DNS .....	232
Figure 110 Menu 2 WAN Setup .....	234
Figure 111 Menu 3 LAN Setup .....	236
Figure 112 Menu 3.1 LAN Port Filter Setup. ....	236
Figure 113 Menu 3.2 TCP/IP and DHCP Ethernet Setup .....	237
Figure 114 Menu 3.2.1: IP Alias Setup .....	239
Figure 115 Menu 4 Internet Access Setup .....	242
Figure 116 Internet Access Setup (PPPoE) .....	244
Figure 117 Menu 11.1 Remote Node Profile for Ethernet Encapsulation .....	247
Figure 118 Menu 11.1 Remote Node Profile for PPPoE Encapsulation .....	249
Figure 119 Menu 11.3 Remote Node Network Layer Options for Ethernet Encapsulation .	251
Figure 120 Menu 11.5: Remote Node Filter (Ethernet Encapsulation) .....	253
Figure 121 Menu 11.5: Remote Node Filter (PPPoE Encapsulation) .....	253
Figure 122 Menu 11.6: Traffic Redirect Setup .....	254
Figure 123 Menu 12 IP Static Route Setup .....	256
Figure 124 Menu12.1 Edit IP Static Route .....	257

Figure 125 Menu 4 Applying NAT for Internet Access .....	258
Figure 126 Menu 11.3 Applying NAT to the Remote Node .....	259
Figure 127 Menu 15 NAT Setup .....	260
Figure 128 Menu 15.1 Address Mapping Sets .....	260
Figure 129 Menu 15.1.255 SUA Address Mapping Rules .....	260
Figure 130 Menu 15.1.1 First Set .....	262
Figure 131 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set .....	263
Figure 132 Menu 15.2 NAT Server Setup .....	264
Figure 133 Multiple Servers Behind NAT Example .....	265
Figure 134 NAT Example 1 .....	265
Figure 135 Menu 4 Internet Access & NAT Example .....	266
Figure 136 NAT Example 2 .....	266
Figure 137 Menu 15.2 Specifying an Inside Server .....	267
Figure 138 NAT Example 3 .....	268
Figure 139 NAT Example 3: Menu 11.3 .....	268
Figure 140 Example 3: Menu 15.1.1.1 .....	269
Figure 141 Example 3: Final Menu 15.1.1 .....	269
Figure 142 Example 3: Menu 15.2 .....	270
Figure 143 NAT Example 4 .....	270
Figure 144 Example 4: Menu 15.1.1.1 Address Mapping Rule. ....	271
Figure 145 Example 4: Menu 15.1.1 Address Mapping Rules .....	271
Figure 146 Menu 15.3 Trigger Port Setup .....	272
Figure 147 Menu 21: Filter and Firewall Setup .....	274
Figure 148 Menu 21.2 Firewall Setup .....	275
Figure 149 Outgoing Packet Filtering Process .....	276
Figure 150 Filter Rule Process .....	278
Figure 151 Menu 21: Filter and Firewall Setup .....	279
Figure 152 Menu 21.1: Filter Set Configuration .....	279
Figure 153 Menu 21.1.x: Filter Rules Summary .....	280
Figure 154 Menu 21.1.x.x: TCP/IP Filter Rule .....	282
Figure 155 Executing an IP Filter .....	284
Figure 156 Menu 21.1.x.x: Generic Filter Rule .....	285
Figure 157 Telnet Filter Example .....	286
Figure 158 Example Filter: Menu 21.1.3.1 .....	287
Figure 159 Example Filter Rules Summary: Menu 21.1.3 .....	287
Figure 160 Protocol and Device Filter Sets .....	288
Figure 161 Filtering LAN Traffic .....	289
Figure 162 Filtering Remote Node Traffic .....	289
Figure 163 Menu 22 SNMP Configuration .....	290
Figure 164 Menu 24 System Maintenance .....	292
Figure 165 Menu 24.1 System Maintenance: Status .....	293
Figure 166 Menu 24.2 System Information and Console Port Speed .....	294
Figure 167 Menu 24.2.1 System Maintenance: Information .....	295

Figure 168 Menu 24.2.2 System Maintenance: Change Console Port Speed .....	296
Figure 169 Menu 24.2 System Information and Console Port Speed .....	296
Figure 170 Menu 24.3.2 System Maintenance: Syslog Logging .....	297
Figure 171 Call-Triggering Packet Example .....	300
Figure 172 Menu 24.4 System Maintenance: Diagnostic .....	301
Figure 173 LAN & WAN DHCP .....	301
Figure 174 Telnet in Menu 24.5 .....	306
Figure 175 FTP Session Example .....	306
Figure 176 Telnet into Menu 24.6. ....	309
Figure 177 Restore Using FTP Session Example .....	310
Figure 178 Telnet Into Menu 24.7.1 Upload System Firmware .....	311
Figure 179 Telnet Into Menu 24.7.2 System Maintenance .....	311
Figure 180 FTP Session Example of Firmware File Upload .....	312
Figure 181 Command Mode in Menu 24 .....	314
Figure 182 Valid Commands Example .....	315
Figure 183 Menu 24.9 System Maintenance: Call Control .....	315
Figure 184 Menu 24.9.1 Budget Management .....	316
Figure 185 Menu 24.9.2 - Call History .....	317
Figure 186 Menu 24: System Maintenance .....	318
Figure 187 Menu 24.10 System Maintenance: Time and Date Setting .....	318
Figure 188 Menu 24.11 – Remote Management Control .....	320
Figure 189 Menu 26 Schedule Setup .....	322
Figure 190 Menu 26.1 Schedule Set Setup .....	323
Figure 191 Applying Schedule Set(s) to a Remote Node (PPPoE) .....	324
Figure 192 Pop-up Blocker .....	330
Figure 193 Internet Options .....	330
Figure 194 Internet Options .....	331
Figure 195 Pop-up Blocker Settings .....	332
Figure 196 Internet Options .....	333
Figure 197 Security Settings - Java Scripting .....	334
Figure 198 Security Settings - Java .....	335
Figure 199 Java (Sun) .....	336
Figure 200 Windows 95/98/Me: Network: Configuration .....	345
Figure 201 Windows 95/98/Me: TCP/IP Properties: IP Address .....	346
Figure 202 Windows 95/98/Me: TCP/IP Properties: DNS Configuration .....	347
Figure 203 Windows XP: Start Menu .....	348
Figure 204 Windows XP: Control Panel .....	348
Figure 205 Windows XP: Control Panel: Network Connections: Properties .....	349
Figure 206 Windows XP: Local Area Connection Properties .....	349
Figure 207 Windows XP: Internet Protocol (TCP/IP) Properties .....	350
Figure 208 Windows XP: Advanced TCP/IP Properties .....	351
Figure 209 Windows XP: Internet Protocol (TCP/IP) Properties .....	352
Figure 210 Macintosh OS 8/9: Apple Menu .....	353

Figure 211 Macintosh OS 8/9: TCP/IP .....	353
Figure 212 Macintosh OS X: Apple Menu .....	354
Figure 213 Macintosh OS X: Network .....	355
Figure 214 Single-Computer per Router Hardware Configuration .....	365
Figure 215 Prestige as a PPPoE Client .....	365
Figure 216 Ideal Setup .....	366
Figure 217 "Triangle Route" Problem .....	367
Figure 218 IP Alias .....	368
Figure 219 Gateways on the WAN Side .....	368



# List of Tables

Table 1 LED Descriptions .....	40
Table 2 Web Configurator Screens Summary .....	47
Table 3 Common Screen Command Buttons .....	49
Table 4 Wizard 2: Ethernet Encapsulation .....	52
Table 5 Wizard 2: PPPoE Encapsulation .....	53
Table 6 Wizard 3: WAN Setup .....	54
Table 7 Wizard 4: SIP 1 Setup .....	57
Table 8 System General .....	64
Table 9 DDNS .....	66
Table 10 Password .....	67
Table 11 Pre-defined NTP Time Servers .....	68
Table 12 Time Setting .....	69
Table 13 LAN IP .....	78
Table 14 LAN IP Alias .....	80
Table 15 Ethernet Encapsulation .....	83
Table 16 PPPoE Encapsulation .....	84
Table 17 Private IP Address Ranges .....	85
Table 18 WAN: IP .....	86
Table 19 SIP Call Progression .....	91
Table 20 NAT Types .....	95
Table 21 VoIP .....	103
Table 22 Custom Tones Details .....	104
Table 23 VoIP Advanced .....	107
Table 24 QoS .....	111
Table 25 Phone Port .....	113
Table 26 European Type Flash Key Commands .....	115
Table 27 USA Type Flash Key Commands .....	116
Table 28 Phone Common .....	118
Table 29 Speed Dial .....	121
Table 30 Call Forward .....	124
Table 31 Lifeline .....	125
Table 32 NAT Definitions .....	128
Table 33 NAT Mapping Types .....	131
Table 34 Services and Port Numbers .....	132
Table 35 SUA/NAT Setup .....	134
Table 36 Address Mapping .....	136
Table 37 Address Mapping Edit .....	137
Table 38 Trigger Port .....	140

Table 39 IP Static Route .....	143
Table 40 Edit IP Static Route .....	144
Table 41 Firewall: Settings .....	148
Table 42 Firewall: Service .....	151
Table 43 Content Filter .....	155
Table 44 Remote Management: Telnet .....	160
Table 45 Remote Management: FTP .....	161
Table 46 Remote Management: WWW .....	162
Table 47 SNMPv1 Traps .....	164
Table 48 SNMPv2 Traps .....	164
Table 49 SNMP Interface Index to Physical Port Mapping .....	165
Table 50 Remote Management: SNMP .....	166
Table 51 Remote Management: DNS .....	167
Table 52 Security .....	169
Table 53 Configuring UPnP .....	172
Table 54 View Log .....	185
Table 55 System Error Logs .....	185
Table 56 System Maintenance Logs .....	185
Table 57 Access Control Logs .....	186
Table 58 TCP Reset Logs .....	187
Table 59 Packet Filter Logs .....	187
Table 60 ICMP Logs .....	188
Table 61 CDR Logs .....	188
Table 62 PPP Logs .....	188
Table 63 UPnP Logs .....	189
Table 64 Content Filtering Logs .....	189
Table 65 Attack Logs .....	190
Table 66 Remote Management Logs .....	191
Table 67 ICMP Notes .....	191
Table 68 SIP Logs .....	192
Table 69 RTP Logs .....	193
Table 70 FSM Logs: Caller Side .....	193
Table 71 FSM Logs: Callee Side .....	193
Table 72 Lifeline Logs .....	193
Table 73 Syslog Logs .....	194
Table 74 RFC-2408 ISAKMP Payload Types .....	194
Table 75 Log Settings .....	197
Table 76 Application and Subnet-based Bandwidth Management Example .....	199
Table 77 Maximize Bandwidth Usage Example .....	201
Table 78 Priority-based Allotment of Unused and Unbudgeted Bandwidth Example .....	201
Table 79 Fairness-based Allotment of Unused and Unbudgeted Bandwidth Example .....	202
Table 80 Bandwidth Borrowing Example .....	203
Table 81 Bandwidth Manager: Summary .....	204

Table 82 Bandwidth Manager: Class Setup .....	205
Table 83 Bandwidth Manager: Edit Class .....	206
Table 84 Services and Port Numbers .....	208
Table 85 Bandwidth Management Statistics .....	209
Table 86 Bandwidth Manager Monitor .....	210
Table 87 System Status .....	213
Table 88 Maintenance System Statistics .....	215
Table 89 Maintenance DHCP Table .....	216
Table 90 Any IP Table .....	217
Table 91 Firmware Upload .....	218
Table 92 Restore Configuration .....	221
Table 93 Main Menu Commands .....	225
Table 94 Main Menu Summary .....	226
Table 95 SMT Menus Overview .....	227
Table 96 Menu 1 General Setup .....	230
Table 97 Menu 1.1 Configure Dynamic DNS .....	232
Table 98 Menu 2 WAN Setup .....	234
Table 99 DHCP Ethernet Setup Fields .....	237
Table 100 Menu 3.2: LAN TCP/IP Setup Fields .....	238
Table 101 Menu 3.2.1: IP Alias Setup .....	239
Table 102 Internet Access Setup (Ethernet) .....	243
Table 103 New Fields in Menu 4 (PPPoE) .....	244
Table 104 Menu 11.1 Remote Node Profile for Ethernet Encapsulation .....	247
Table 105 Fields in Menu 11.1 (PPPoE Encapsulation Specific) .....	250
Table 106 Remote Node Network Layer Options .....	251
Table 107 Menu 11.6: Traffic Redirect Setup .....	254
Table 108 Menu 12.1 Edit IP Static Route .....	257
Table 109 Applying NAT in Menus 4 & 11.3 .....	259
Table 110 SUA Address Mapping Rules .....	261
Table 111 Menu 15.1.1 First Set .....	262
Table 112 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set .....	263
Table 113 Menu 15.3 Trigger Port Setup .....	272
Table 114 Abbreviations Used in the Filter Rules Summary Menu .....	280
Table 115 Rule Abbreviations Used .....	281
Table 116 Menu 21.1.x.x: TCP/IP Filter Rule .....	282
Table 117 Menu 21.1.x.x: Generic Filter Rule .....	285
Table 118 Menu 22 SNMP Configuration .....	290
Table 119 System Maintenance: Status Menu Fields .....	293
Table 120 Menu 24.2.1 System Maintenance: Information .....	295
Table 121 Menu 24.3.2 System Maintenance: Syslog Logging .....	297
Table 122 System Maintenance Menu Diagnostic .....	301
Table 123 Filename Conventions .....	305
Table 124 General Commands for GUI-based FTP Clients .....	307

Table 125 General Commands for GUI-based TFTP Clients .....	308
Table 126 Menu 24.9.1 - Budget Management .....	316
Table 127 Call History Fields .....	317
Table 128 Time and Date Setting Fields .....	319
Table 129 Menu 24.11 – Remote Management Control .....	321
Table 130 Menu 26.1 Schedule Set Setup .....	323
Table 131 Troubleshooting the Start-Up of Your Prestige .....	326
Table 132 Troubleshooting the LAN Interface .....	326
Table 133 Troubleshooting the WAN Interface .....	327
Table 134 Troubleshooting Internet Access .....	327
Table 135 Troubleshooting the Password .....	327
Table 136 Troubleshooting the Web Configurator .....	328
Table 137 Troubleshooting Telephone .....	328
Table 138 Troubleshooting Voice Service .....	329
Table 139 Device Specifications .....	338
Table 140 Feature Specifications .....	339
Table 141 Prestige Power Adaptor Specifications .....	340
Table 142 Classes of IP Addresses .....	356
Table 143 Allowed IP Address Range By Class .....	357
Table 144 “Natural” Masks .....	357
Table 145 Alternative Subnet Mask Notation .....	358
Table 146 Two Subnets Example .....	358
Table 147 Subnet 1 .....	359
Table 148 Subnet 2 .....	359
Table 149 Subnet 1 .....	360
Table 150 Subnet 2 .....	360
Table 151 Subnet 3 .....	360
Table 152 Subnet 4 .....	361
Table 153 Eight Subnets .....	361
Table 154 Class C Subnet Planning .....	361
Table 155 Class B Subnet Planning .....	362

# Preface

Congratulations on your purchase of the Prestige 2302R VoIP station gateway. Your Prestige is easy to install and configure.

## About This User's Guide

This User's Guide is designed to guide you through the configuration of your Prestige using the web configurator or the SMT. The web configurator parts of this guide contain background information on features configurable by web configurator. The SMT parts of this guide contain background information solely on features not configurable by web configurator.

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

## Related Documentation

- Supporting Disk  
Refer to the included CD for support documents.
- Quick Start Guide  
The Quick Start Guide is designed to help you get up and running right away. It contains a detailed easy-to-follow connection diagram, and information on setting up your network and configuring for Internet access.
- 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.

## Syntax Conventions

- “Enter” means for you to type one or more characters. “Select” or “Choose” means for you to use one of the predefined choices.
- Mouse action sequences are denoted by right angle brackets (>). For example, “**Start** > **Settings** > **Control Panel** > **System**” means click the **Start** button, move the mouse over **Settings**, move the mouse over or click on **Control Panel**, and then click on **System**.

- “e.g.,” is a shorthand for “for instance”, and “i.e.,” means “that is” or “in other words”.
- The Prestige 2302R may be referred to as the Prestige, the router or the device in this user’s guide.

### Graphics Icons Key

Prestige 	Computer 	Notebook Computer 
Server 	Switch 	Router 
Telephone 	Modem 	Trunking Gateway 

# CHAPTER 1

## Introducing the Prestige

This chapter introduces the main features and applications of the Prestige.

### 1.1 Prestige 2302R VoIP Station Gateway Series Overview

The Prestige 2302R VoIP (Voice over IP) station gateway lets you use traditional analog telephones to make telephone calls over the Internet. The Prestige uses SIP (Session Initiation Protocol), an internationally recognized standard for implementing VoIP.

You can call any landline or mobile telephone as well as IP telephones. You don't need to know if the recipient's connection type is an IP, cellular or landline based service. Calls received from IP telephones work exactly as you would expect from the traditional telephone service.

The NAT and DHCP server features allow you to use an Ethernet hub or switch to set up a private network and allow multiple computers to share a single Internet connection. The Prestige also provides content filtering and a firewall for security.

The Prestige's web configurator allows easy management and configuration.

### 1.2 Prestige 2302RL VoIP Analog Telephone Adaptor with Lifeline

The Prestige 2302RL has all of the features of the Prestige 2302R and adds the PSTN (Public Switched Telephone Network) lifeline feature. PSTN lifeline lets you have VoIP phone service and PSTN phone service at the same time.

### 1.3 Features

Your Prestige is packed with a number of features that make it flexible and easy to use.<sup>1</sup>

---

1. Some features documented in this user's guide were not available in the Prestige 2302RL at the time of writing.

## **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**

The Prestige can also block access to web sites containing keywords that you specify. You can define time periods and days during which content filtering is enabled and include or exclude a range of users on the LAN from content filtering.

## **Custom Ring Tones**

You can Interactive Voice Response (IVR) on a telephone to record custom ring tones on the Prestige, and then you can tell the Prestige which tone to use when you get incoming calls and which tone to use when you put someone on hold.

## **Bandwidth Management**

Bandwidth management allows you to allocate network resources according to defined policies. This policy-based bandwidth allocation helps your network to better handle real-time applications such as Voice-over-IP (VoIP).

## **SIP ALG**

The Prestige is a SIP Application Layer Gateway (ALG). It allows VoIP calls to pass through NAT for devices behind the Prestige (such as a SIP-based VoIP software application on a computer).

## **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.

## **10/100Mbps Auto-negotiating Fast Ethernet Interfaces**

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

## **Auto-crossover 10/100 Mbps Ethernet Interfaces**

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



## Reset Button

The Prestige reset button is built into the rear panel. Use this button to restore the factory default password to 1234; IP address to 192.168.1.1, subnet mask to 255.255.255.0 and DHCP server enabled with a pool of 32 IP addresses starting at 192.168.1.33.

## Multiple Telephones

You can connect more than one telephone to a Prestige telephone port. The Ringer Equivalence Number (REN) is used to determine the number of devices that may be connected to the telephone line. See the [Table 139 on page 338](#) for the Prestige's REN.

## PSTN Lifeline

The Prestige 2302RL allows you to connect a PSTN line. You can receive incoming PSTN phone calls even while someone else connected to the Prestige is making VoIP phone calls. You can dial a (prefix) number to make an outgoing PSTN call. You can still make PSTN phone calls if the Prestige 2302RL loses power.

## Dynamic Jitter Buffer

The Prestige has a built-in adaptive, buffer that helps to smooth out the variations in delay (jitter) for voice traffic. This helps ensure good voice quality for your conversations.

## Multiple SIP Accounts

The Prestige allows you to simultaneously use multiple voice (SIP) accounts and assign them to one or both telephone ports.

## STUN

Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators (STUN) allows SIP to pass through NAT routers.

## Outbound Proxy

Some VoIP service providers use a SIP outbound server to handle voice calls. This allows the Prestige to work from behind any type of NAT router and eliminates the need for STUN or a SIP ALG (Application Layer Gateway).

## Multiple Voice Channels

The Prestige can simultaneously handle multiple voice channels (telephone calls). Additionally you can answer an incoming phone call on a VoIP account, even while someone else is using the account for a phone call.

## **Voice Coding**

The Prestige can use the following voice codecs (coder/decoders).

- G.711
- G.729

## **Voice Activity Detection/Silence Suppression**

Voice Activity Detection (VAD) reduces the bandwidth that a call uses by not transmitting when you are not speaking.

## **Comfort Noise Generation**

The Prestige generates background noise to fill moments of silence when the other device in a call stops transmitting because the other party is not speaking (as total silence could easily be mistaken for a lost connection).

## **Echo Cancellation**

The Prestige supports G.168, an ITU-T standard for eliminating the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.

## **QoS (Quality of Service)**

Quality of Service (QoS) mechanisms help to provide better service on a per-flow basis. The Prestige supports Type of Service (ToS) and Differentiated Services (DiffServ). This allows the Prestige to tag voice frames so they can be prioritized over the network.

## **Fax Tone Detection and Pass-through**

The Prestige automatically detects fax messages and sends them over PCM G.711 or T.38.

## **Auto-provisioning**

Your voice service provider can automatically update your Prestige's configuration via an auto-provisioning server.

## **Auto Firmware Upgrade**

The Prestige gives you the option to upgrade to a newer firmware version if it finds one during auto-provisioning. Your voice service provider must have an auto-provisioning server and a server set up with firmware in order for this feature to work.

## **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).

## **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.

## **DHCP (Dynamic Host Configuration Protocol)**

DHCP (Dynamic Host Configuration Protocol) allows the individual client 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, which means it can assign IP addresses, an IP default gateway and DNS servers to all systems that support the DHCP client. The Prestige can also act as a surrogate DHCP server where it relays IP address assignment from the actual real DHCP server to the clients.

## **Port Forwarding**

Use this feature to forward incoming service requests to a server on your local network. 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.

## **Dynamic DNS Support**

With Dynamic DNS (Domain Name System) 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.

## **IP Multicast**

Deliver IP packets to a specific group of hosts using IP multicast. IGMP (Internet Group Management Protocol) is the protocol used to support multicast groups. The latest version is version 2 (see RFC 2236); the Prestige supports both versions 1 and 2.

## **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 LAN interface with the Prestige itself as the gateway for each network.

## **PPPoE**

PPPoE (Point-to-Point Protocol over Ethernet) facilitates the interaction of a host with an Internet modem to achieve access to high-speed data networks via a familiar "dial-up networking" user interface.

## **RoadRunner Support**

In addition to standard cable modem services, the Prestige supports Time Warner's RoadRunner Service.

## **Firmware Upgrades**

Use the web configurator to upload updated firmware to your Prestige.

## **Embedded FTP and TFTP Servers**

The Prestige's embedded FTP and TFTP servers enable fast firmware upgrades as well as configuration file backups and restoration.

## **SNMP**

SNMP (Simple Network Management Protocol) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your Prestige supports SNMP agent functionality, which allows a manager station to manage and monitor the Prestige through the network. The Prestige supports SNMP version one (SNMPv1) and version two (SNMPv2).

## **Logging and Tracing**

- Built-in message logging and packet tracing.
- Syslog facility support.

## **Ease of Installation**

Your Prestige is designed for quick, intuitive and easy installation. Physically, its compact size and lightness make it easy to position anywhere in your busy office. The Prestige is also wall-mountable.

## **1.4 LEDs**

The following graphic displays the labels of the LEDs.

**Figure 1** LEDs**Table 1** LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
PWR/VoIP	Green	On	The Prestige is receiving power.
		Blinking	The Prestige is self-testing.
	Orange	On	The VoIP SIP registration was successful.
		Off	The Prestige is not receiving power.
WAN	Green	On	The Prestige has an Ethernet connection with the cable/DSL modem.
		Blinking	The Prestige is sending/receiving data to /from the cable/DSL modem.
		Off	The Prestige doesn't have an Ethernet connection with the cable/DSL modem.
LAN	Green	On	The Prestige has an Ethernet connection with a computer.
		Blinking	The Prestige is sending/receiving data to /from the computer.
		Off	The Prestige does not have an Ethernet connection with a computer.
Phone 1-2	Green	On	The telephone(s) connected to this port is (are) in use.
		Blinking	The telephone(s) connected to this port is (are) ringing.
		Off	The telephone(s) connected to this port is (are) not in use.

## 1.5 Applications

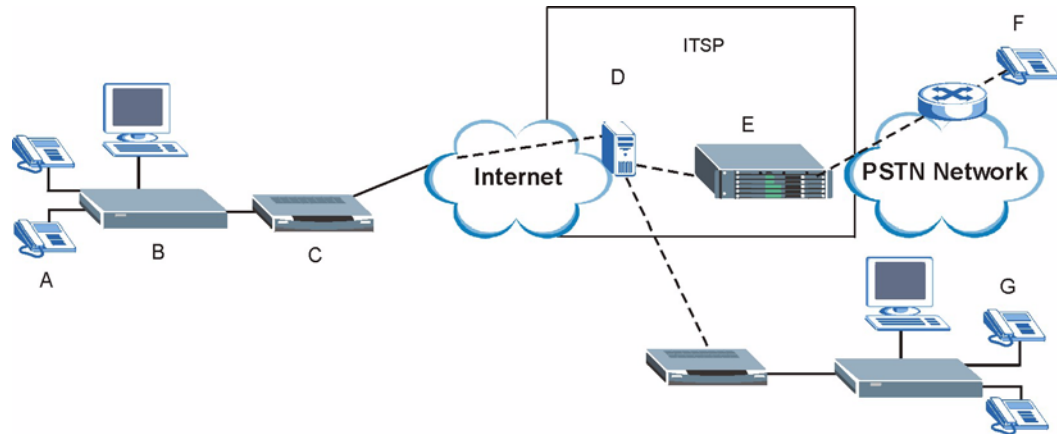
Here are some examples of how you can use your Prestige.

### 1.5.1 Make Calls via Internet Telephony Service Provider

In a home or small office environment, you can use the Prestige to make and receive VoIP telephone calls through an Internet Telephony Service Provider (ITSP).

The following figure shows a basic example of how you would make a VoIP call through an ITSP. You use your analog phone (A in the figure) and the Prestige (B) changes the call into VoIP. The Prestige then sends your call through your modem or router (C) to the Internet and the ITSP's SIP server (D). The VoIP call server forwards calls to PSTN phones (F) through a trunking gateway (E) to the PSTN network. The VoIP call server forwards calls to IP phones (G) through the Internet.

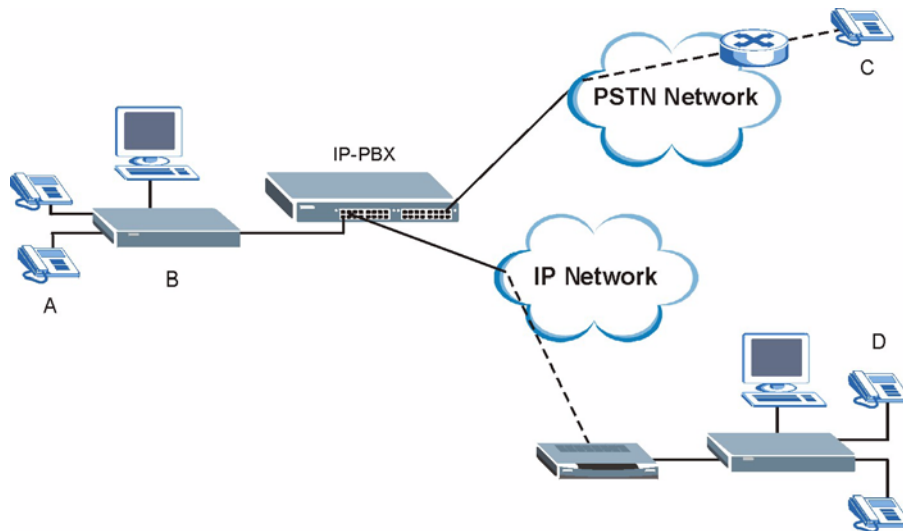
**Figure 2** Internet Telephony Service Provider Application



## 1.5.2 Make Calls via IP-PBX

If your company has an IP-PBX (Internet Protocol Private Branch Exchange), you can use the Prestige to make and receive VoIP telephone calls through it.

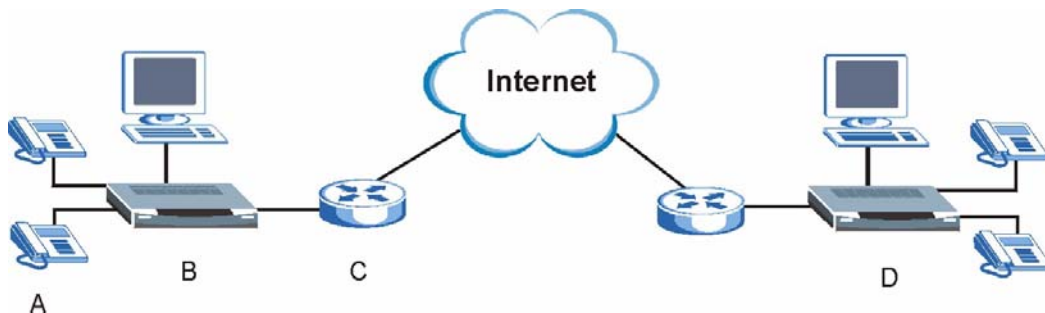
In this example, you use your analog phone (A in the figure) and the Prestige (B) changes the call into VoIP and sends it to the IP-PBX. The IP-PBX forwards calls to PSTN phones (C) to the PSTN network. The IP-PBX forwards calls to IP phones (D) through an IP network (this could include the Internet).

**Figure 3** IP-PBX Application

### 1.5.3 Make Peer-to-peer Calls

Use the Prestige to make a call to the recipient's IP address without using a SIP proxy server. Peer-to-peer calls are also called "Point to Point" or "IP-to-IP" calls. You must know the peer's IP address in order to do this.

The following figure shows a basic example of how you would make a peer-to-peer VoIP call. You use your analog phone (A in the figure) and the Prestige (B) changes the call into VoIP. The Prestige then sends your call through your modem or router (C) and the Internet to the peer VoIP device (D).

**Figure 4** Peer-to-peer Calling





# CHAPTER 2

## Introducing the Web Configurator

This chapter describes how to access the Prestige web configurator and provides an overview of its screens.

### 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 troubleshooting chapter if you want to make sure these functions are allowed in Internet Explorer or Netscape Navigator.

### 2.2 Accessing the Prestige Web Configurator

- 1 Make sure your Prestige hardware is properly connected and prepare your computer/ computer network to connect to the Prestige (refer to [Appendix C on page 344](#)).
- 2 Launch your web browser.
- 3 Type "192.168.1.1" (the Prestige's default LAN IP address) as the URL.

**Figure 5** Web Site Address



- 4 Type "1234" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.

**Figure 6** Enter Password

- 5** You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) and click **Apply** or click **Ignore**.

**Figure 7** Change Password

- 6** You should now see the web configurator **MAIN MENU** screen ([Figure 8 on page 47](#)).

**Note:** The Prestige automatically logs you out if the management session is idle for five minutes. Simply log back in if this happens to you.

## 2.3 Resetting the Prestige

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

### 2.3.1 Procedure To Use The Reset Button

Make sure the **PWR/VoIP** LED is on (not blinking) before you begin this procedure.

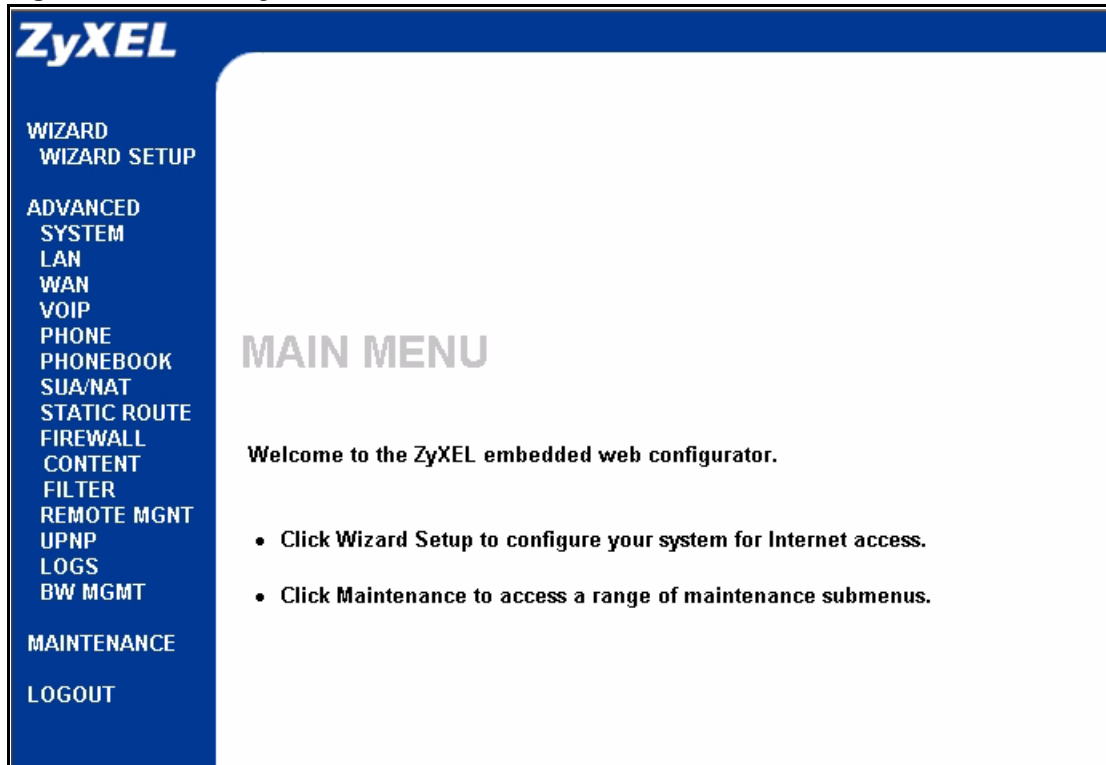
- 1** Press the **RESET** button for five to ten seconds (release it when the **PWR/VoIP** LED begins to blink). When the **PWR/VoIP** LED starts blinking, the defaults have been restored and the Prestige restarts. Otherwise, go to step 2.
- 2** Disconnect and reconnect the Prestige's power.
- 3** Wait for the **PWR/VoIP** LED to stop blinking and stay on steady.
- 4** Press the **RESET** button for five to ten seconds (release it when the **PWR/VoIP** LED begins to blink). When the **PWR/VoIP** LED starts blinking, the defaults have been restored and the Prestige restarts. Otherwise, go to step 2.

## 2.4 Navigating the Prestige Web Configurator

The following summarizes how to navigate the web configurator from the **MAIN MENU** screen.

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

- Click **WIZARD** for initial configuration.
- Click a link under **ADVANCED** to configure Prestige features.
- Click **MAINTENANCE** to view information about your Prestige or upgrade configuration/firmware files. Maintenance includes the **Status**, **DHCP Table**, **F/W** (firmware) **Upload**, **Configuration** (Backup, Restore, Defaults) and **Restart** screens.
- Click **LOGOUT** at any time to exit the web configurator.

**Figure 8** Web Configurator

The following table describes the sub-menus.

**Table 2** Web Configurator Screens Summary

LINK	TAB	FUNCTION
WIZARD SETUP		Use these screens for initial configuration including general setup, ISP parameters for Internet Access, WAN IP/DNS Server/MAC address assignment and VoIP.
SYSTEM	General	Use this screen to configure general system settings.
	DDNS	Use this screen to set up dynamic DNS.
	Password	Use this screen to change your password.
	Time Setting	Use this screen to change your Prestige's time and date.
LAN	IP	Use this screen to configure LAN DHCP and TCP/IP settings.
	IP Alias	Use this screen to partition your LAN interface into subnets.
WAN	Route	This screen allows you to configure route priority.
	WAN ISP	Use this screen to change your Prestige's WAN ISP settings.
	WAN IP	Use this screen to change your Prestige's WAN IP settings.
	WAN MAC	Use this screen to change your Prestige's WAN MAC settings.
	Traffic Redirect	Use this screen to configure your traffic redirect properties and parameters.

**Table 2** Web Configurator Screens Summary (continued)

LINK	TAB	FUNCTION
VOIP	VoIP	Use this screen to configure your Prestige's Voice over IP settings.
	QoS	Use this screen to configure your Prestige's Quality of Service settings.
PHONE	Phone Port	Use this screen to configure your Prestige's phone settings.
	Common	Use this screen to configure general phone port settings.
PHONE BOOK	Speed Dial	Use this screen to configure speed dial for SIP phone numbers that you call often.
	Lifeline	Use this screen to configure your Prestige's settings for PSTN calls (Prestige 2302RL only).
SUA/NAT	SUA Server	Use this screen to configure servers behind the Prestige.
	Address Mapping	Use this screen to configure network address translation mapping rules.
	Trigger Port	Use this screen to change your Prestige's trigger port settings.
STATIC ROUTE	IP Static Route	Use this screen to configure IP static routes.
FIREWALL	Settings	Use this screen to activate/deactivate the firewall and log packets related to firewall rules.
	Services	Use this screen to enable service blocking (LAN to WAN firewall rules).
CONTENT FILTER	Filter	This screen allows you to block sites containing certain keywords in the URL and set the days and times for the Prestige to perform content filtering.
REMOTE MGMT	TELNET	Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the Prestige.
	FTP	Use this screen to configure through which interface(s) and from which IP address(es) users can use FTP to access the Prestige.
	WWW	Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTP to manage the Prestige.
	SNMP	Use this screen to configure your Prestige's settings for Simple Network Management Protocol management.
	DNS	Use this screen to configure through which interface(s) and from which IP address(es) users can send DNS queries to the Prestige.
	Security	Use this screen to change your anti-probing settings.
UPnP	UPnP	Use this screen to enable UPnP on the Prestige.
LOGS	View Log	Use this screen to view the logs for the categories that you selected.
	Log Settings	Use this screen to change your Prestige's log settings.
BW MGMT	Summary	Use this screen to enable bandwidth management on an interface and set the maximum allowed bandwidth and scheduler for the interface.
	Class Setup	Use this screen to define bandwidth classes.
	Monitor	Use this screen to view bandwidth class statistics.

**Table 2** Web Configurator Screens Summary (continued)

LINK	TAB	FUNCTION
MAINTENANCE	Status	This screen contains administrative and system-related information.
	DHCP Table	This screen shows which network clients are using the DHCP server.
	Any IP	This screen lists the devices that are using the Any IP feature to communicate with the Prestige.
	F/W Upload	Use this screen to upload firmware to your Prestige
	Configuration	Use this screen to backup and restore the configuration or reset the factory defaults to your Prestige.
	Restart	This screen allows you to reboot the Prestige without turning the power off.
LOGOUT		Click this label to exit the web configurator.

## 2.5 Common Screen Command Buttons

The following table shows common command buttons found on many web configurator screens.

**Table 3** Common Screen Command Buttons

Apply	Click <b>Apply</b> to save your changes back to the Prestige.
Reset/Cancel	Click <b>Reset</b> or <b>Cancel</b> to begin configuring this screen afresh.

# CHAPTER 3

## Wizard Setup

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

### 3.1 Wizard Setup Overview

The web configurator's setup wizard helps you configure your device to access the Internet and make phone calls over the Internet. Leave a field blank if you don't have information for it.

**Note:** You should have a SIP account already set up.

### 3.2 Wizard 1: General Setup

**Note:** This screen is optional. You can just click **Next** if you do not want to configure it.

**General Setup** contains administrative and system-related information. **System Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name". See [Section 4.3 on page 62](#) for how to find your computer's computer name.

#### 3.2.1 Domain Name

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (System Name) on each individual computer, the domain name can be assigned from the Prestige via DHCP.

Click **Next** to configure the Prestige for Internet access.

**Figure 9** Wizard 1: General Setup

**WIZARD SETUP**

---

**General Setup:**  
This information is optional, but may be helpful in accessing services of your Internet Service Provider, such as mail and news servers and customer support web pages.

Enter a descriptive name for identification purposes. We recommend using your computer's name.

**System Name:**

The ISP's domain name is often sent automatically by the ISP to the router. If you are having difficulty accessing ISP services, you may need to enter the Domain Name manually in the field below.

**Domain Name:**

---

Next

## 3.3 Wizard 2: ISP Parameters for Internet Access

This screen varies depending on what encapsulation type you use. The Prestige offers **Ethernet** and **PPP over Ethernet** encapsulation.

### 3.3.1 Ethernet

Choose **Ethernet** when the WAN port is used as a regular Ethernet.

For ISPs (such as Telstra) that send UDP heartbeat packets to verify that the customer is still online, please create a **WAN to LAN** firewall rule for those packets. Contact your ISP to find the correct port number.



**Figure 10** Wizard 2: Ethernet Encapsulation

The following table describes the labels in this screen.

**Table 4** Wizard 2: Ethernet Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	You must choose the <b>Ethernet</b> option when the WAN port is used as a regular Ethernet. Otherwise, choose <b>PPP over Ethernet</b> for a dial-up connection.
Service Type	Choose from <b>Standard</b> , <b>RR-Toshiba</b> (Roadrunner Toshiba authentication method), <b>RR-Manager</b> (Roadrunner Manager authentication method) or <b>RR-Telstra</b> (RoadRunner Telstra authentication method). The following fields are not applicable ( <b>N/A</b> ) for the <b>Standard</b> service type.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Login Server IP Address	Type the authentication server IP address here if your ISP gave you one.
Back	Click <b>Back</b> to return to the previous screen.
Next	Click <b>Next</b> to continue.

### 3.3.2 PPPoE Encapsulation

Point-to-Point Protocol over Ethernet (PPPoE) functions as a dial-up connection. PPPoE is an IETF (Internet Engineering Task Force) standard specifying how a host personal computer interacts with a broadband modem (for example DSL, cable, wireless, etc.) to achieve access to high-speed data networks.

**Figure 11** Wizard 2: PPPoE Encapsulation

The following table describes the labels in this screen.

**Table 5** Wizard 2: PPPoE Encapsulation

LABEL	DESCRIPTION
ISP Parameter for Internet Access	
Encapsulation	Choose <b>PPP over Ethernet</b> from the pull-down list box. PPPoE forms a dial-up connection.
Service Name	Type the name of your service provider.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Nailed-Up Connection	Select <b>Nailed-Up Connection</b> if you do not want the connection to time out.
Idle Timeout	Type the time in seconds that elapses before the router automatically disconnects from the PPPoE server. The default time is <b>100</b> seconds.
Back	Click <b>Back</b> to return to the previous screen.
Next	Click <b>Next</b> to continue.

## 3.4 Wizard 3: WAN Setup

This wizard screen allows you to configure WAN IP address assignment, DNS server address assignment and the WAN MAC address. See [Chapter 6 on page 82](#) for background information on these fields.

This wizard screen varies according to the type of encapsulation that you selected in the previous wizard screen.

**Figure 12** Wizard 3: WAN Setup

The following table describes the labels in this screen.

**Table 6** Wizard 3: WAN Setup

LABEL	DESCRIPTION
WAN IP Address Assignment	This section is available if you use Ethernet encapsulation with the Standard service type or PPPoE encapsulation (in the previous screen). This section is not available if you use Ethernet encapsulation with one of the RoadRunner (RR-) service types.
Get automatically from ISP (Default)	Select this option if your ISP did not assign you a fixed IP address. This is the default selection.
Use fixed IP address	Select this option if the ISP assigned a fixed IP address.

**Table 6** Wizard 3: WAN Setup

LABEL	DESCRIPTION
My WAN IP Address	Enter your WAN IP address in this field if you selected <b>Use Fixed IP Address</b> .
My WAN IP Subnet Mask (Ethernet only)	Enter the IP subnet mask (if your ISP gave you one) in this field if you selected <b>Use Fixed IP Address</b> .
Gateway IP Address (Ethernet only)	Enter the gateway IP address of the neighboring device, if you know it. If you do not, leave the field set to 0.0.0.0.
My WAN IP Subnet Mask	This field is available if you selected <b>Ethernet</b> encapsulation. Enter the IP subnet mask (if your ISP gave you one) in this field if you selected <b>Use Fixed IP Address</b> .
Gateway IP Address	This field is available if you selected <b>Ethernet</b> encapsulation. Enter the gateway IP address (if your ISP gave you one) in this field if you selected <b>Use Fixed IP Address</b> .
Remote IP Address	This field is available if you selected <b>PPPoE</b> encapsulation. Enter the remote IP Address (if your ISP gave you one) in this field.
Remote IP Subnet Mask	This field is available if you selected <b>PPPoE</b> encapsulation. Enter the remote IP Address (if your ISP gave you one) in this field.
DNS Server Address Assignment (if applicable) 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 computer before you can access it. The Prestige uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.	
First DNS Server	Select <b>From ISP</b> if your ISP dynamically assigns DNS server information (and the Prestige's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.
Second DNS Server	Select <b>User-Defined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right.
Third DNS Server	Select <b>None</b> if you do not want to configure DNS servers. If you do not configure a system DNS server, you must use IP addresses when configuring VPN, DDNS and the time server.
WAN MAC Address	The MAC address field allows you to configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN.
Factory Default	Select this option to use the factory assigned default MAC Address.
Spoof this Computer's MAC address - IP Address	Select this option and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different rom file. It is advisable to clone the MAC address from a computer on your LAN even if your ISP does not presently require MAC address authentication.
Back	Click <b>Back</b> to return to the previous screen.
Next	Click <b>Next</b> to continue.

## 3.5 Wizard 4: SIP 1 Setup

This wizard screen allows you to configure your voice settings for SIP account 1. Fill in the fields with information from your voice service provider. Leave the default settings in fields for which no information was provided (except if otherwise specified). See [Chapter 7 on page 90](#) for background information on these fields.

**Note:** This screen configures SIP account 1. Use the VoIP screens to configure SIP account 2.

**Figure 13** Wizard 4: SIP 1 Setup

**WIZARD SETUP**

**SIP1 Settings**

SIP Number: changeme

SIP Local Port: 5060 (1025-65535)

SIP Server Address: 127.0.0.1

SIP Server Port: 5060 (1-65535)

REGISTER Server Address: 127.0.0.1

REGISTER Server Port: 5060 (1-65535)

SIP Service Domain: 127.0.0.1

**Authentication**

Authentication User-ID: changeme

Authentication Password: \*.\*.\*.\*.\*.\*.\*.\*

**Voice Compression Type**: G.711 > G.729

**NAT Passthrough Type**: NONE

Server Address: 0.0.0.0

Server Port: 0 (1024-65535)

**DTMF Mode**: RFC 2833

**Country Code**: USA

Back Finish

The following table describes the labels in this screen

**Table 7** Wizard 4: SIP 1 Setup

LABEL	DESCRIPTION
SIP Number	Enter your SIP number in this field (use the number or text that comes before the @ symbol in a SIP account like <a href="mailto:1234@VoIP-provider.com">1234@VoIP-provider.com</a> ). You can use up to 127 ASCII characters.
SIP Local Port	Use this field to configure the Prestige's listening port for SIP. Leave this field set to the default if you were not given a local port number for SIP.
SIP Server Address	Type the IP address or domain name of the SIP server in this field. It doesn't matter whether the SIP server is a proxy, redirect or register server. You can use up to 95 ASCII characters.
SIP Server Port	Enter the SIP server's listening port for SIP in this field. Leave this field set to the default if your VoIP service provider did not give you a server port number for SIP.

**Table 7** Wizard 4: SIP 1 Setup

LABEL	DESCRIPTION
REGISTER Server Address	<p>Enter the SIP register server's IP address or domain name in this field. You can use up to 95 ASCII characters.</p> <p><b>Note:</b> If you were not given a register server address, then enter the address from the <b>SIP Server Address</b> field again here.</p>
REGISTER Server Port	<p>Enter the SIP register server's listening port for SIP in this field.</p> <p><b>Note:</b> If you were not given a register server port, then enter the port from the <b>SIP Server Port</b> field again here.</p>
SIP Service Domain	<p>Enter the SIP service domain name in this field (the domain name that comes after the @ symbol in a SIP account like <a href="#">1234@VoIP-provider.com</a>). You can use up to 127 ASCII Extended set characters.</p>
Authentication User ID	<p>This is the user name for registering this SIP account with the SIP register server. Type the user name exactly as it was given to you. You can use up to 95 ASCII characters.</p>
Authentication Password	<p>Type the password associated with the user name above. You can use up to 95 ASCII Extended set characters.</p>
Voice Compression Type	<p>Use this field to select the type of voice coder/decoder (codec) that you want the Prestige to use. G.711 provides higher voice quality than G.729 but requires 64kbps of bandwidth while G.729 only requires 8kbps.</p> <p>Select <b>G.711&gt;G.729</b> if you want the Prestige to first attempt to use the G.711 codec and then the G.729 codec if the peer is not set up to use G.711.</p> <p>Select <b>G.711 only</b> if you want the Prestige to only use the G.711 codec when making VoIP calls. You will not be able to connect to a peer that is not set up to use G.711.</p> <p>Select <b>G.729&gt;G.711</b> if you want the Prestige to first attempt to use the G.729 codec and then the G.711 codec if the peer is not set up to use G.729.</p> <p>Select <b>G.729 only</b> if you want the Prestige to only use the G.729 codec when making VoIP calls. You will not be able to connect to a peer that is not set up to use G.729.</p>
NAT Passthrough Type	<p>Use <b>STUN</b> if there is a NAT router between the Prestige and the voice service provider's SIP server. You do not need to use STUN if the NAT router is also a SIP ALG.</p> <p>Use <b>Outbound Proxy</b> if your VoIP service provider has a SIP outbound server to handle voice calls. This allows the Prestige to work with any type of NAT router and eliminates the need for STUN or a SIP ALG. Turn off a SIP ALG on a NAT router in front of the Prestige to keep it from retranslating the IP address (since this is already handled by the outbound proxy server).</p> <p>Use <b>NONE</b> if you were not given STUN or outbound proxy server information.</p>
Server Address	<p>Type the IP address or domain name of the STUN or outbound proxy server in this field. You can use up to 127 ASCII characters.</p> <p>Ignore the <b>Server Address/Port</b> fields if you selected <b>NONE</b> for the <b>NAT Passthrough Type</b>.</p>

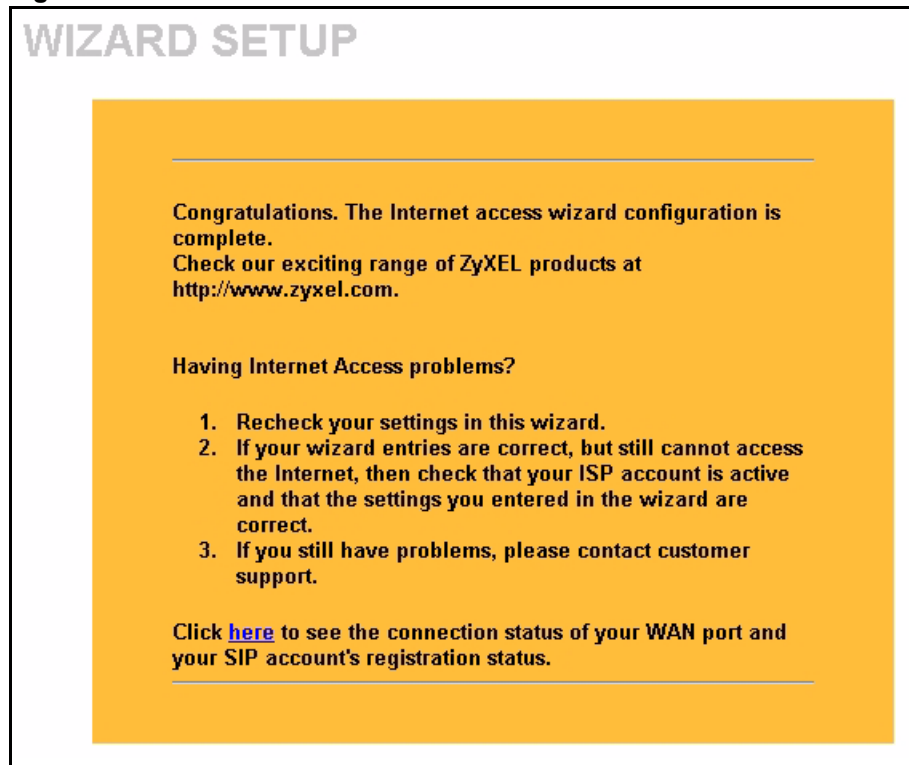
**Table 7** Wizard 4: SIP 1 Setup

LABEL	DESCRIPTION
Server Port	Enter the STUN or outbound proxy server's listening port for STUN or outbound proxy requests in this field. Leave this field set to the default if your VoIP service provider did not give you a server port number for STUN or outbound proxy.
DTMF Mode	The Dual-Tone Multi-Frequency (DTMF) mode sets how the Prestige handles the tones that your telephone makes when you push its buttons. It is recommended that you use the same mode that your VoIP service provider uses. Select <b>RFC 2833</b> to send the DTMF tones in RTP packets. Select <b>PCM</b> (Pulse Code Modulation) to include the DTMF tones in the voice data stream. This method works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.729) could distort the tones. Select <b>SIP INFO</b> to send the DTMF tones in SIP messages.
Country Code	Use the drop-down list box to select the country where your Prestige is located. Do not use <b>Default</b> .
Back	Click <b>Back</b> to return to the previous screen.
Finish	Click <b>Finish</b> to complete the wizard setup and save your configuration.

## 3.6 Wizard Setup Complete

After you click **Finish**, the Prestige attempts to connect to the Internet and register your SIP account. The **PWR/VoIP** LED turns orange after the SIP account registration is successful. You can also click the hyper link in this screen to view the status of the Prestige's WAN port connection and SIP account registration.



**Figure 14** Wizard Finish

Well done! You have set up your Prestige to access the Internet and make VoIP calls.



# CHAPTER 4

## System Screens

This chapter provides information on the **SYSTEM** screens.

### 4.1 System Overview

This chapter describes how to configure the Prestige's general, DDNS, password and time settings.

### 4.2 DNS Overview

You can configure DNS (Domain Name System) setup in the following places.

- 1 Use the **SYSTEM General** screen to configure the Prestige to use a DNS server to resolve domain names for Prestige system features like DDNS and the time server.
- 2 Use the **LAN IP** screen to configure the DNS server information that the Prestige sends to the DHCP client devices on the LAN.
- 3 Use the **Remote Management DNS** screen to configure the Prestige to accept or discard DNS queries.

### 4.3 General Screen

The **General** screen contains administrative and system-related information. **System Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

- In Windows 95/98 click **Start, Settings, Control Panel, Network**. Click the **Identification** tab, note the entry for the **Computer Name** field and enter it as the **System Name**.
- In Windows 2000, click **Start, Settings** and **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**.
- In Windows XP, click **Start, My Computer, View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the Prestige **System Name**.

### 4.3.1 Domain Name

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. While you must enter the host name (System Name) on each individual computer, the domain name can be assigned from the Prestige via DHCP.

### 4.3.2 DNS Server Address Assignment

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of [www.zyxel.com](http://www.zyxel.com) is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

The Prestige can get the DNS server addresses in the following ways.

- 1 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 **SYSTEM General** screen.
- 2 If the ISP did not give you DNS server information, leave the **DNS Server** fields in the **SYSTEM General** screen set to 0.0.0.0 for the ISP to dynamically assign the DNS server IP addresses.

## 4.4 System General Configuration

Click **SYSTEM** in the navigation panel and then **General** to display the following screen.

Figure 15 System General

The following table describes the labels in this screen.

Table 8 System General

LABEL	DESCRIPTION
System Name	This is for identification purposes. Enter your computer's "Computer Name". This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	The Domain Name entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by DHCP from the ISP is used. Use up to 38 alphanumeric characters. Spaces are not allowed, but dashes "-" and periods "." are accepted.
Administrator Inactivity Timer	Type how many minutes a management session can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
System DNS Servers	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa, e.g., the IP address of www.zyxel.com is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.
First DNS Server Second DNS Server Third DNS Server	Select <b>From ISP</b> if your ISP dynamically assigns DNS server information (and the Prestige's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select <b>User-Defined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. Select <b>None</b> if you do not want to configure DNS servers. If you do not configure a system DNS server, you must use IP addresses when configuring DDNS and the time server.

**Table 8** System General (continued)

LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your changes back to the Prestige.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 4.5 Dynamic DNS

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

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

### 4.5.1 DynDNS Wildcard

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

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

## 4.6 Configuring Dynamic DNS

To change your Prestige's DDNS, click **SYSTEM**, then the **DDNS** tab. The screen appears as shown.

Figure 16 DDNS

The following table describes the labels in this screen.

Table 9 DDNS

LABEL	DESCRIPTION
Enable DDNS	Select this check box to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
DDNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider.
Host Names 1~3	Enter the host names in the three fields provided. You can specify up to two host names in each field separated by a comma (",").
User Name	Enter your user name.
Password	Enter the password assigned to you.
Enable Wildcard Option	Select the check box to enable DynDNS Wildcard.
Enable off line option (Only applies to custom DNS)	This option is available when <b>CustomDNS</b> is selected in the <b>DDNS Type</b> field. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
IP Address Update Policy:	
Use WAN IP Address	Select this option to have the Prestige update the domain name with the WAN port's IP address.

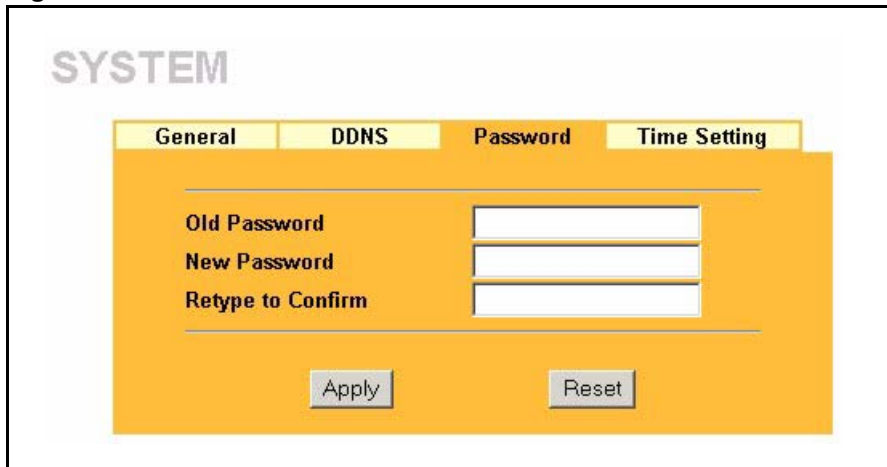
**Table 9** DDNS

LABEL	DESCRIPTION
DDNS server auto detect IP Address	Select this option to update the IP address of the host name(s) automatically by the DDNS server. It is recommended that you select this option. Select this option only when there are one or more NAT routers between the Prestige and the DDNS server. This feature has the DDNS server automatically detect and use the IP address of the NAT router that has a public IP address.  <b>Note:</b> The DDNS server may not be able to detect the proper IP address if there is an HTTP proxy server between the Prestige and the DDNS server.
Use specified IP Address	Select this option to update the IP address of the host name(s) to the IP address specified below. Use this option if you have a static IP address.
IP Addr:	Enter the IP address if you select the <b>User Specify</b> option.
Apply	Click <b>Apply</b> to save your changes back to the Prestige.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 4.7 Configuring Password

To change your Prestige's password (recommended), click **SYSTEM** in the navigation panel, and then the **Password** tab. The screen appears as shown.

**Figure 17** Password



The following table describes the labels in this screen.

**Table 10** 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 (up to 30 characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type.



**Table 10** Password (continued)

LABEL	DESCRIPTION
Retype to Confirm	Type the new password again in this field.
Apply	Click <b>Apply</b> to save your changes back to the Prestige.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 4.8 Pre-defined NTP Time Servers List

The Prestige uses the following pre-defined list of NTP time servers if you do not specify a time server or it cannot synchronize with the time server you specified.

**Note:** The Prestige can use this pre-defined list of time servers regardless of the Time Protocol you select.

When the Prestige uses the pre-defined list of NTP time servers, it randomly selects one server and tries to synchronize with it. If the synchronization fails, then the Prestige goes through the rest of the list in order from the first one tried until either it is successful or all the pre-defined NTP time servers have been tried.

**Table 11** Pre-defined NTP Time Servers

ntp1.cs.wisc.edu
ntp1.gbg.netnod.se
ntp2.cs.wisc.edu
tock.usno.navy.mil
ntp3.cs.wisc.edu
ntp.cs.strath.ac.uk
ntp1.sp.se
time1.stupi.se
tick.stdtime.gov.tw
tock.stdtime.gov.tw
time.stdtime.gov.tw

## 4.9 Configuring Time Setting

To change your Prestige's time and date, click **SYSTEM** in the navigation panel, then the **Time Setting** tab. The screen appears as shown. Use this screen to configure the Prestige's time based on your local time zone.

**Figure 18** Time Setting

**SYSTEM**

General DDNS Password **Time Setting**

Time Protocol: None

Time Server Address:

Current Time (hh-mm-ss): 0 : 12 : 1

New Time (hh-mm-ss): 0 : 11 : 55

Current Date (yyyy-mm-dd): 2000 / 1 / 1

New Date (yyyy-mm-dd): 2000 / 1 / 1

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

Daylight Savings

Start Date (mm-dd): 0 month 0 day

End Date (mm-dd): 0 month 0 day

Apply Reset

The following table describes the labels in this screen.

**Table 12** Time Setting

LABEL	DESCRIPTION
Time Protocol	Select the time service protocol that your time server uses. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main difference between them is the format. <b>Daytime (RFC 867)</b> format is day/month/year/time zone of the server. <b>Time (RFC 868)</b> format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. The default, <b>NTP (RFC 1305)</b> , is similar to Time (RFC 868). Select <b>None</b> to enter the time and date manually.
Time Server Address	Enter the IP address or URL of your time server. Check with your ISP or network administrator if you are unsure of this information.
Current Time	This field displays the Prestige's present time.
New Time	This field displays the last updated time from the time server. When you select <b>None</b> in the <b>Time Protocol</b> field, enter the new time in this field and then click <b>Apply</b> .
Current Date	This field displays the Prestige's present date.

**Table 12** Time Setting (continued)

LABEL	DESCRIPTION
New Date	This field displays the last updated date from the time server. When you select <b>None</b> in the <b>Time Protocol</b> field, enter the new date in this field and then click <b>Apply</b> .
Time Zone	Choose the Time Zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Select this option if you use daylight savings time. Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
Start Date	Enter the month and day that your daylight-savings time starts on if you selected <b>Daylight Savings</b> .
End Date	Enter the month and day that your daylight-savings time ends on if you selected <b>Daylight Savings</b> .
Apply	Click <b>Apply</b> to save your changes back to the Prestige.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

### 4.9.1 Resetting the Time

The Prestige resets the time in the following instances:

- On saving your changes.
- When the Prestige starts up.
- 24-hour intervals after starting.



# CHAPTER 5

## LAN Setup

This chapter describes how to configure LAN settings.

### 5.1 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, manage IP addresses, and partition your physical network into logical networks.

### 5.2 IP Address and Subnet Mask

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

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

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

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

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

## 5.3 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 DHCP service is disabled, you must have another DHCP server on your LAN, or else the computer must be manually configured.

### 5.3.1 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.

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

## 5.4 LAN TCP/IP

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

### 5.4.1 Factory LAN Defaults

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

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

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

## 5.5 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 ISPs 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.

## 5.6 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.

## 5.7 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.

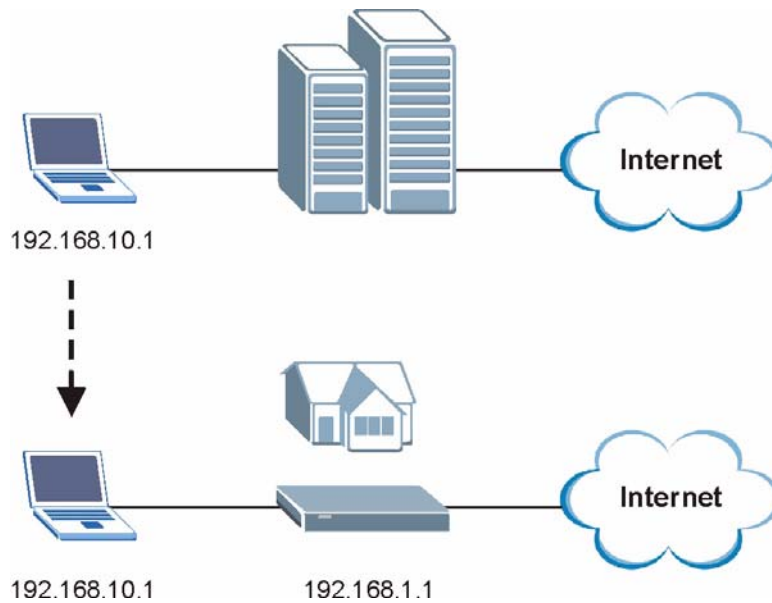
## 5.8 Any IP

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 19** 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.

### 5.8.0.1 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.

## 5.9 Configuring LAN

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

**Figure 20** LAN IP

**LAN**

**IP**    **IP Alias**

---

**DHCP Setup**

**DHCP Server**

**IP Pool Starting Address**     **Pool Size**

**DNS Servers Assigned by DHCP Server**

**First DNS Server**

**Second DNS Server**

**Third DNS Server**

---

**LAN TCP/IP**

**IP Address**     **RIP Direction**

**IP Subnet Mask**     **RIP Version**

**Multicast**

---

**Any IP Setup**

**Active**

---

**Windows Networking (NetBIOS over TCP/IP)**

**Allow between LAN and WAN**

The following table describes the fields in this screen.

**Table 13** LAN IP

LABEL	DESCRIPTION
DHCP	
DHCP Server	<p>Enable the DHCP server to have the Prestige 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>When DHCP is used, the following items need to be set:</p>
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Pool Size	This field specifies the size or count of the IP address pool.
DNS Servers Assigned by DHCP Server	
<p>The Prestige passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. The Prestige only passes this information to the LAN DHCP clients when you select the <b>DHCP Server</b> check box. When you clear the <b>DHCP Server</b> check box, DHCP service is disabled and you must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured.</p>	
First DNS Server Second DNS Server Third DNS Server	<p>Select <b>From ISP</b> if your ISP dynamically assigns DNS server information (and the Prestige's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.</p> <p>Select <b>User-Defined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose <b>User-Defined</b>, but leave the IP address set to 0.0.0.0, <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b>. If you set a second choice to <b>User-Defined</b>, and enter the same IP address, the second <b>User-Defined</b> changes to <b>None</b> after you click <b>Apply</b>.</p> <p>Select <b>DNS Relay</b> to have the Prestige act as a DNS proxy. The Prestige's LAN IP address displays in the field to the right (read-only). The Prestige tells the DHCP clients on the LAN that the Prestige itself is the DNS server. When a computer on the LAN sends a DNS query to the Prestige, the Prestige forwards the query to the Prestige's system DNS server (configured in the <b>SYSTEM General</b> screen) and relays the response back to the computer. You can only select <b>DNS Relay</b> for one of the three servers; if you select DNS Relay for a second or third DNS server, that choice changes to <b>None</b> after you click <b>Apply</b>.</p> <p>Select <b>None</b> if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.</p>
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	The subnet mask specifies the network number portion of an IP address. Your Prestige automatically calculates the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Prestige.
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.
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.

**Table 13** LAN IP (continued)

LABEL	DESCRIPTION
Any IP Setup	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.  When you disable the Any IP feature, only computers with dynamic IP addresses or static IP addresses in the same subnet as the Prestige's LAN IP address can connect to the Prestige or access the Internet through the Prestige.
Apply	Click <b>Apply</b> to save your changes back to the Prestige.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 5.10 Configuring IP Alias

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

**Note:** Make sure that the subnets of the logical networks do not overlap.

The following figure shows a LAN divided into subnets A, B, and C.

**Figure 21** Physical Network & Partitioned Logical Networks

To change your Prestige's IP alias settings, click **LAN**, then the **IP Alias** tab. The screen appears as shown.

Figure 22 LAN IP Alias

The following table describes the labels in this screen.

Table 14 LAN IP Alias

LABEL	DESCRIPTION
IP Alias 1, 2	Select the check box to configure another LAN network for the Prestige.
IP Address	Enter the IP address of your Prestige <sup>®</sup> in dotted decimal notation. Alternatively, click the right mouse button to copy and/or paste the IP address.
IP Subnet Mask	Your Prestige will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Prestige.
RIP Direction	RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The <b>RIP Direction</b> field controls the sending and receiving of RIP packets. Select the RIP direction from <b>Both/In Only/Out Only/None</b> . When set to <b>Both</b> or <b>Out Only</b> , the Prestige will broadcast its routing table periodically. When set to <b>Both</b> or <b>In Only</b> , it will incorporate the RIP information that it receives; when set to <b>None</b> , it will not send any RIP packets and will ignore any RIP packets received.
RIP Version	The <b>RIP Version</b> field controls the format and the broadcasting method of the RIP packets that the Prestige sends (it recognizes both formats when receiving). <b>RIP-1</b> 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 <b>RIP-2B</b> and <b>RIP-2M</b> sends the routing data in RIP-2 format; the difference being that <b>RIP-2B</b> uses subnet broadcasting while <b>RIP-2M</b> uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to <b>Both</b> and the Version set to <b>RIP-1</b> .

**Table 14** LAN IP Alias

LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your changes back to the Prestige.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

# CHAPTER 6

## WAN Screens

This chapter describes how to configure WAN settings.

### 6.1 WAN Overview

Use this chapter to configure the settings for your WAN connection.

### 6.2 Configuring ISP

To change your Prestige's WAN ISP settings, click **WAN**, then the **ISP** tab. The screen differs by the encapsulation.

#### 6.2.1 Ethernet Encapsulation

The screen shown next is for **Ethernet** encapsulation.

**Figure 23** Ethernet Encapsulation

The following table describes the labels in this screen.

**Table 15** Ethernet Encapsulation

LABEL	DESCRIPTION
Encapsulation	You must choose the <b>Ethernet</b> option when the WAN port is used as a regular Ethernet.
Service Type	Choose from <b>Standard</b> , <b>RR-Toshiba</b> (Roadrunner Toshiba authentication method), <b>RR-Manager</b> (Roadrunner Manager authentication method) or <b>RR-Telstra</b> (RoadRunner Telstra authentication method).
User Name	This field is not available if you select the <b>Standard</b> service type. Type the user name given to you by your ISP.
Password	This field is not available if you select the <b>Standard</b> service type. Type the password associated with the user name above.
Retype to Confirm	This field is not available if you select the <b>Standard</b> service type. Type the password again to make sure that you have entered it correctly.
Login Server IP Address	This field is not available if you select the <b>Standard</b> service type. Type the authentication server IP address here if your ISP gave you one.
Apply	Click <b>Apply</b> to save your changes back to the Prestige.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 6.2.2 PPPoE Encapsulation

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

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.

The screen shown next is for **PPPoE** encapsulation.

**Figure 24** PPPoE Encapsulation

The following table describes the labels in this screen.

**Table 16** PPPoE Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	The <b>PPP over Ethernet</b> choice is for a dial-up connection using PPPoE. The Prestige supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (for example DSL, cable, wireless, etc.) connection. Operationally, PPPoE saves significant effort for both the end user and ISP/carrier, as it requires no specific configuration of the broadband modem at the customer site. By implementing PPPoE directly on the router rather than individual computers, the computers on the LAN do not need PPPoE software installed, since the router does that part of the task. Further, with NAT, all of the LAN's computers will have access.

**Table 16** PPPoE Encapsulation

LABEL	DESCRIPTION
Service Name	Type the PPPoE service name provided to you. PPPoE uses a service name to identify and reach the PPPoE server.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Nailed-Up Connection	Select <b>Nailed-Up Connection</b> if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the router automatically disconnects from the PPPoE server.
Apply	Click <b>Apply</b> to save your changes back to the Prestige.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 6.3 WAN IP Address Assignment

Every computer on the Internet must have a unique IP address. If your networks are isolated from the Internet, for instance, 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.

**Table 17** Private IP Address Ranges

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 have it assigned by 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.

## 6.4 Configuring WAN IP

To change your Prestige's WAN IP settings, click **WAN**, then the **WAN IP** tab. This screen varies according to the type of encapsulation you select.

If your ISP did *not* assign you a fixed IP address, click **Get automatically from ISP (Default)**; otherwise click **Use fixed IP Address** and enter the IP address in the field provided.

**Figure 25** WAN: IP

The following table describes the labels in this screen.

**Table 18** WAN: IP

LABEL	DESCRIPTION
WAN IP Address Assignment	This section is available if you use Ethernet encapsulation with the Standard service type or PPPoE encapsulation. This section is not available if you use Ethernet encapsulation with one of the RoadRunner (RR-) service types.
Get automatically from ISP (Default)	Select this option if your ISP did not assign you a fixed IP address. This is the default selection.
Use fixed IP address	Select this option if the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected <b>Use Fixed IP Address</b> .
My WAN IP Subnet Mask	This field is available if you selected <b>Ethernet</b> encapsulation. Enter the IP subnet mask (if your ISP gave you one) in this field if you selected <b>Use Fixed IP Address</b> .
Gateway IP Address	This field is available if you selected <b>Ethernet</b> encapsulation. Enter the gateway IP address (if your ISP gave you one) in this field if you selected <b>Use Fixed IP Address</b> .

**Table 18** WAN: IP

LABEL	DESCRIPTION
Remote IP Address	This field is available if you selected <b>PPPoE</b> encapsulation. Enter the remote IP Address (if your ISP gave you one) in this field.
Remote IP Subnet Mask	This field is available if you selected <b>PPPoE</b> encapsulation. Enter the remote IP Address (if your ISP gave you one) in this field.
Network Address Translation	<p>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).</p> <p>Choose <b>None</b> to disable NAT.</p> <p>Choose <b>SUA Only</b> if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: <b>Many-to-One</b> and <b>Server</b>.</p> <p>Choose <b>Full Feature</b> if you have multiple public IP addresses. <b>Full Feature</b> mapping types include: <b>One-to-One</b>, <b>Many-to-One</b> (SUA/PAT), <b>Many-to-Many Overload</b>, <b>Many- One-to-One</b> and <b>Server</b>. When you select <b>Full Feature</b> you must configure at least one address mapping set!</p> <p>For more information about NAT refer to <a href="#">Chapter 12 on page 128</a>.</p>
Metric	<p>This field is available if you selected <b>PPPoE</b> encapsulation. It sets this route's priority among the routes the Prestige uses.</p> <p>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".</p>
Private	This field is available if you selected <b>PPPoE</b> encapsulation. It determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to Yes, this route is kept private and not included in RIP broadcast. If No, the route to this remote node will be propagated to other hosts through RIP broadcasts.
RIP Direction	<p>RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The <b>RIP Direction</b> field controls the sending and receiving of RIP packets.</p> <p>Choose <b>Both</b>, <b>None</b>, <b>In Only</b> or <b>Out Only</b>.</p> <p>When set to <b>Both</b> or <b>Out Only</b>, the Prestige will broadcast its routing table periodically.</p> <p>When set to <b>Both</b> or <b>In Only</b>, the Prestige will incorporate RIP information that it receives.</p> <p>When set to <b>None</b>, the Prestige will not send any RIP packets and will ignore any RIP packets received.</p> <p>By default, <b>RIP Direction</b> is set to <b>Both</b>.</p>

**Table 18** WAN: IP

LABEL	DESCRIPTION
RIP Version	<p>The <b>RIP Version</b> field controls the format and the broadcasting method of the RIP packets that the Prestige sends (it recognizes both formats when receiving).</p> <p>Choose <b>RIP-1</b>, <b>RIP-2B</b> or <b>RIP-2M</b>.</p> <p><b>RIP-1</b> is universally supported; but <b>RIP-2</b> carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both <b>RIP-2B</b> and <b>RIP-2M</b> sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, the <b>RIP Version</b> field is set to <b>RIP-1</b>.</p>
Multicast	<p>Choose <b>None</b> (default), <b>IGMP-V1</b> or <b>IGMP-V2</b>. 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.</p>
<p>Windows Networking (NetBIOS over TCP/IP):</p> <p>NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN.</p>	
Allow between LAN and WAN	<p>Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN.</p> <p>Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.</p> <p>You also need to configure a firewall rule that allows NetBIOS traffic to pass from the WAN to the LAN.</p>
Allow Trigger Dial	<p>Select this option to allow NetBIOS packets to initiate calls.</p>
Apply	<p>Click <b>Apply</b> to save your changes back to the Prestige.</p>
Reset	<p>Click <b>Reset</b> to begin configuring this screen afresh.</p>

## 6.5 Configuring WAN MAC

To change your Prestige's WAN MAC settings, click **WAN**, then the **MAC** tab. The screen appears as shown.

**Figure 26** MAC Setup

The screenshot shows a web interface for WAN configuration. At the top left, the word "WAN" is displayed. Below it are three tabs: "ISP", "IP", and "MAC". The "MAC" tab is currently selected. Underneath the tabs, there is a section titled "WAN MAC Address". This section contains two radio button options: "Factory default" (which is selected) and "Spoof this computer's MAC Address - IP Address". To the right of the second option is a text input field containing the IP address "192.168.1.20". At the bottom of the form are two buttons: "Apply" and "Reset".

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.

The MAC address screen allows users to configure the WAN port's MAC address by either using the factory default or cloning your computer's MAC address. Choose **Factory Default** to select the factory assigned default MAC Address.

Otherwise, click **Spoof this computer's MAC address - IP Address** and enter the IP address of your computer. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different ROM file. It is recommended that you clone the MAC address prior to hooking up the **WAN** Port.

# CHAPTER 7

## Introduction to VoIP

This chapter provides background information on VoIP and SIP.

### 7.1 VoIP Introduction

VoIP (Voice over IP) is the sending of voice signals over the Internet Protocol. This allows you to make phone calls and send faxes over the Internet at a fraction of the cost of using the traditional circuit-switched telephone network. You can also use servers to run telephone service applications like PBX services and voice mail. Internet Telephony Service Provider (ITSP) companies provide VoIP service. A company could alternatively set up an IP-PBX and provide its own VoIP service.

Circuit-switched telephone networks require 64 kilobits per second (kbps) in each direction to handle a telephone call. VoIP can use advanced voice coding techniques with compression to reduce the required bandwidth.

### 7.2 Introduction to SIP

The Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet.

SIP signaling is separate from the media for which it handles sessions. The media that is exchanged during the session can use a different path from that of the signaling. SIP handles telephone calls and can interface with traditional circuit-switched telephone networks.

#### 7.2.1 SIP Identities

A SIP account uses an identity (sometimes referred to as a SIP address). A complete SIP identity is called a SIP URI (Uniform Resource Identifier). A SIP account's URI identifies the SIP account in a way similar to the way an e-mail address identifies an e-mail account. The format of a SIP identity is SIP-Number@SIP-Service-Domain.

##### 7.2.1.1 SIP Number

The SIP number is the part of the SIP URI that comes before the “@” symbol. A SIP number can use letters like in an e-mail address (johndoe@your-ITSP.com for example) or numbers like a telephone number (1122334455@VoIP-provider.com for example).

### 7.2.1.2 SIP Service Domain

The SIP service domain of the VoIP service provider is the domain name in a SIP URI. For example, if the SIP address is [1122334455@VoIP-provider.com](mailto:1122334455@VoIP-provider.com), then “VoIP-provider.com” is the SIP service domain.

## 7.2.2 SIP Call Progression

The following figure displays the basic steps in the setup and tear down of a SIP call. A calls B.

**Table 19** SIP Call Progression

A		B
1. INVITE		
		2. Ringing
		3. OK
4. ACK		
	5. Dialogue (voice traffic)	
6. BYE		
		7. OK

- 1** A sends a SIP INVITE request to B. This message is an invitation for B to participate in a SIP telephone call.
- 2** B sends a response indicating that the telephone is ringing.
- 3** B sends an OK response after the call is answered.
- 4** A then sends an ACK message to acknowledge that B has answered the call.
- 5** Now A and B exchange voice media (talk).
- 6** After talking, A hangs up and sends a BYE request.
- 7** B replies with an OK response confirming receipt of the BYE request and the call is terminated.

### 7.2.3 SIP Client Server

SIP is a client-server protocol. A SIP client is an application program or device that sends SIP requests. A SIP server responds to the SIP requests.

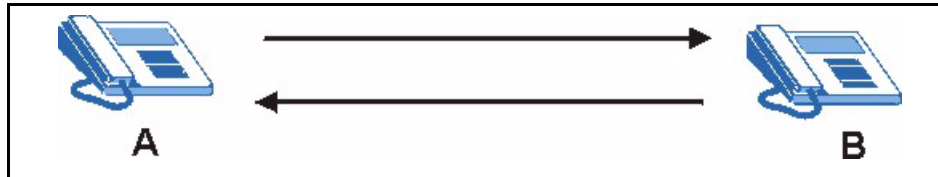
When you use SIP to make a VoIP call, it originates at a client and terminates at a server. A SIP client could be a computer or a SIP phone. One device can act as both a SIP client and a SIP server.



### 7.2.3.1 SIP User Agent

A SIP user agent can make and receive VoIP telephone calls. This means that SIP can be used for peer-to-peer communications even though it is a client-server protocol. In the following figure, either A or B can act as a SIP user agent client to initiate a call. A and B can also both act as a SIP user agent to receive the call.

**Figure 27** SIP User Agent



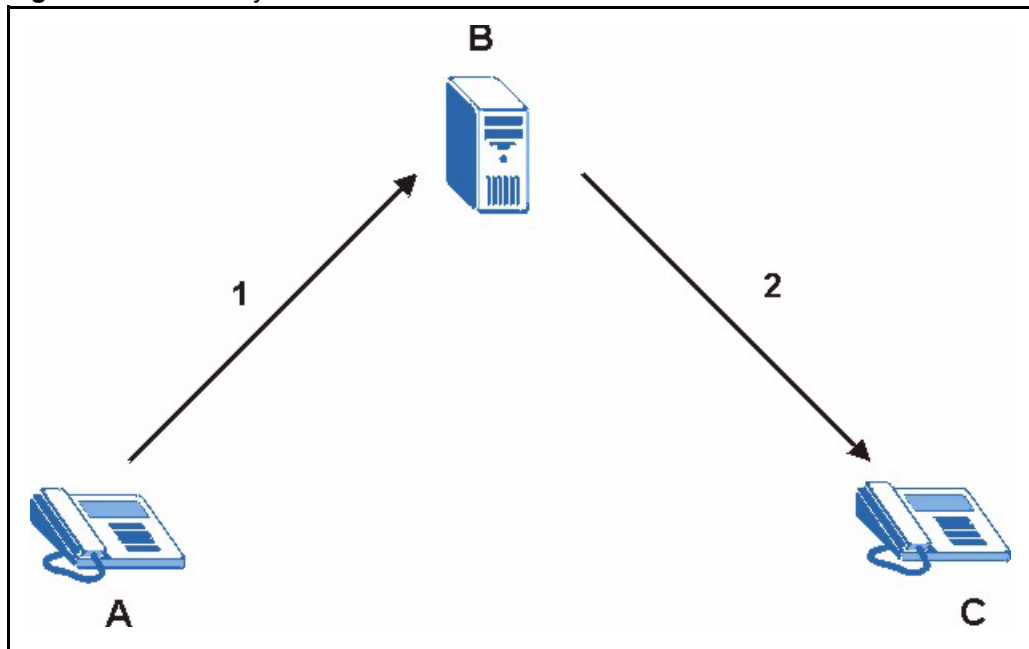
### 7.2.3.2 SIP Proxy Server

A SIP proxy server receives requests from clients and forwards them to another server.

In the following example, you want to use client device A to call someone who is using client device C.

- 1 The client device (A in the figure) sends a call invitation to the SIP proxy server (B).
- 2 The SIP proxy server forwards the call invitation to C.

**Figure 28** SIP Proxy Server



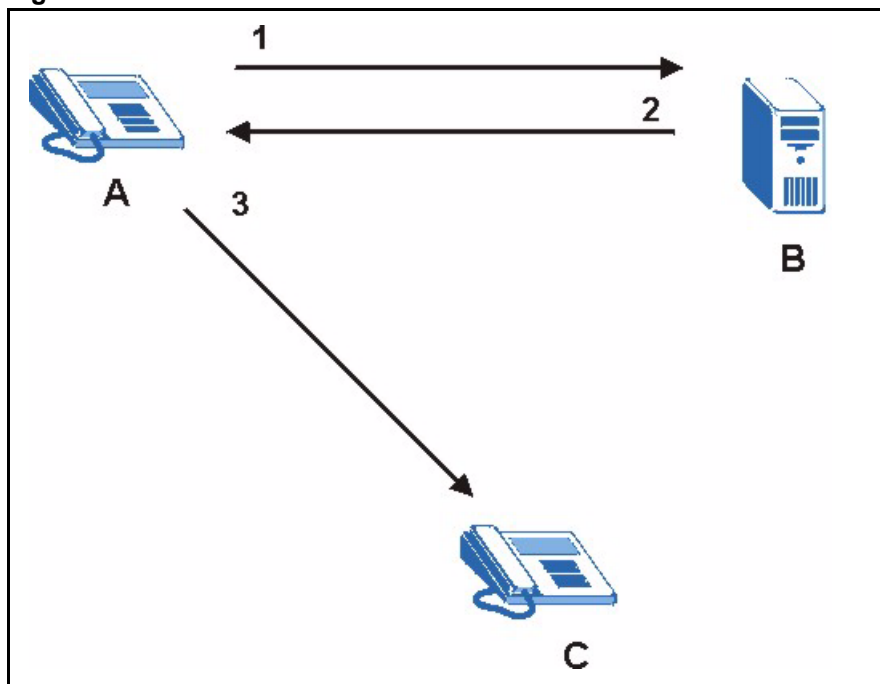
### 7.2.3.3 SIP Redirect Server

A SIP redirect server accepts SIP requests, translates the destination address to an IP address and sends the translated IP address back to the device that sent the request. Then the client device that originally sent the request can send requests to the IP address that it received back from the redirect server. Redirect servers do not initiate SIP requests.

In the following example, you want to use client device A to call someone who is using client device C.

- 1 Client device A sends a call invitation for C to the SIP redirect server (B).
- 2 The SIP redirect server sends the invitation back to A with C's IP address (or domain name).
- 3 Client device A then sends the call invitation to client device C.

**Figure 29** SIP Redirect Server



### 7.2.3.4 SIP Register Server

A SIP register server maintains a database of SIP identity-to-IP address (or domain name) mapping. The register server checks your user name and password when you register.

## 7.2.4 RTP

When you make a VoIP call using SIP, the RTP (Real time Transport Protocol) is used to handle voice data transfer. See RFC 1889 for details on RTP.

## 7.3 NAT

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

In the simplest form, NAT changes the source IP address of a packet received from a device to another IP address before forwarding the packet towards the destination. When the response comes back, NAT translates the destination address back to the device's IP address and forwards it to the device.

NAT routers are commonly used to translate private (or internal) IP addresses in packet headers to public (or external) IP addresses and vice versa. A NAT router maps a private IP address and port pair to a public IP address and port, and whenever the NAT router receives a packet with that public IP address and port, it knows how to reroute the packet back to the private IP address and port.

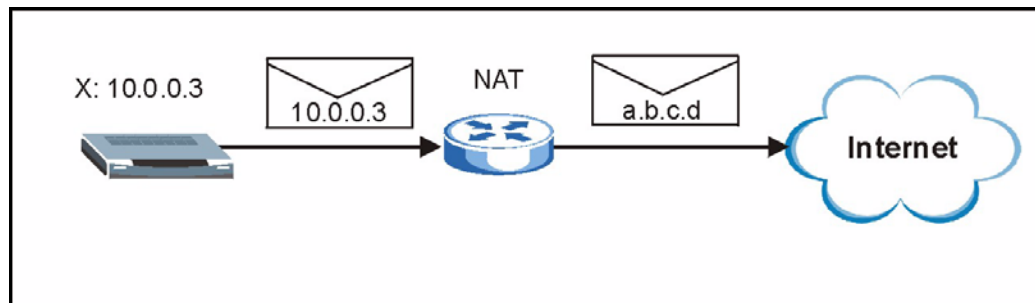
NAT may be implemented on a device that is between your Prestige and the Internet.

### 7.3.1 NAT Example

See the following figure. The Prestige (X) sends packets to the Internet. The Prestige's IP address is 10.0.0.3. This is a private or internal IP address. The NAT router maps the private source IP address to a public source IP address (a.b.c.d). The public source IP address is also known as the external IP address.

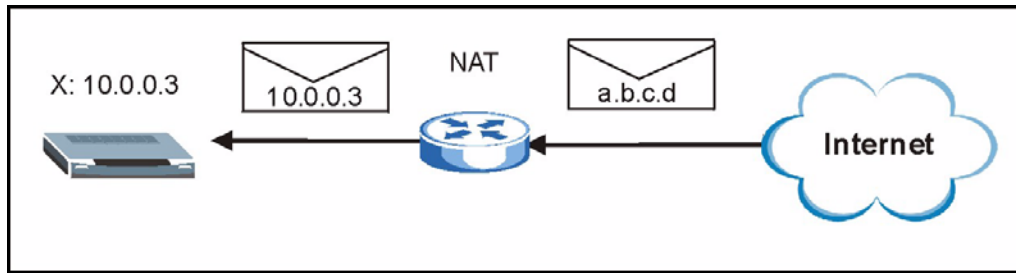
**Note:** The NAT figures in this chapter use lower-case letters (like a.b.c.d for example) to represent public IP addresses.

**Figure 30** NAT: Outgoing



When the NAT router receives packets with destination address IP address a.b.c.d, the NAT router changes a.b.c.d back to the private IP address 10.0.0.3 and sends it to the Prestige.

**Figure 31** NAT: Incoming



### 7.3.2 NAT Types

This section discusses the following NAT types that may be implemented on a router in front of the Prestige.

- Full Cone
- Restricted Cone
- Port Restricted Cone
- Symmetric

The following table summarizes how these NAT types handle outgoing and incoming packets. Read the following sections for more details and examples.

**Table 20** NAT Types

	FULL CONE	RESTRICTED CONE	PORT RESTRICTED CONE	SYMMETRIC
Incoming Packets	Any external host can send packets to the mapped external IP address and port.	Only external hosts with an IP address to which the internal host has already sent a packet can send packets to the mapped external IP address and port.	Only external hosts with an IP address and port to which the internal host has already sent a packet can send packets to the mapped external IP address and port.	A host on the external network can only send packets to the specific mapped external IP address and port that the NAT router used in sending a packet to the external host's IP address and port.
Outgoing Packets	The NAT router maps the internal IP address and port of all outgoing packets to a single IP address and port on the external network.			The NAT router maps the internal IP address and port of each outgoing packet to a different external IP address and port for each different destination IP address and port.

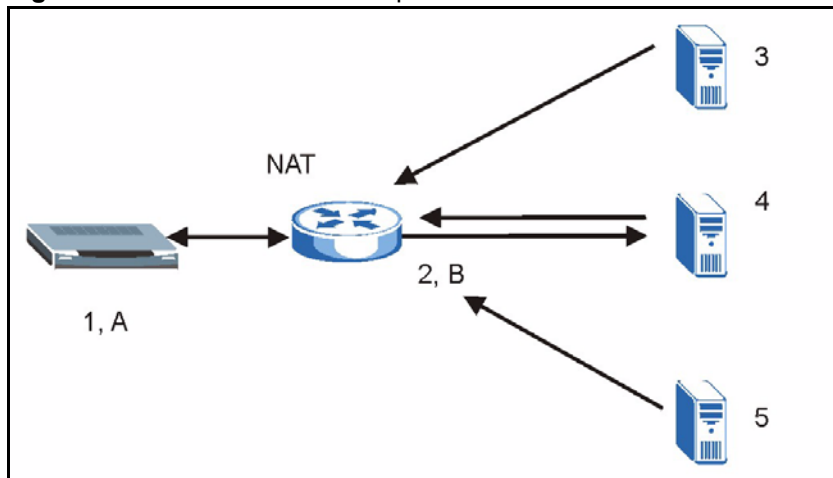
The examples in these NAT type sections describe NAT translation between internal (private) and external (public) IP addresses.

### 7.3.2.1 Full Cone NAT

In full cone NAT, the NAT router maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. The NAT router also maps packets coming to that external IP address and port to the internal IP address and port.

In the following example, the NAT router maps the source address of all packets sent from the Prestige's internal IP address **1** and port **A** to IP address **2** and port **B** on the external network. The NAT router also performs NAT on all incoming packets sent to IP address **2** and port **B** and sends them to IP address **1**, port **A**.

**Figure 32** Full Cone NAT Example



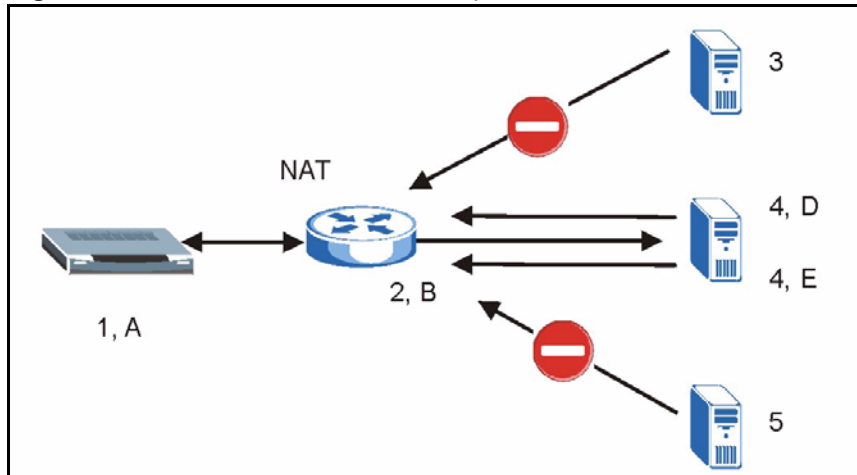
### 7.3.2.2 Restricted Cone NAT

As in full cone NAT, a restricted cone NAT router maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. In the following example, the NAT router maps the source address of all packets sent from internal IP address **1** and port **A** to IP address **2** and port **B** on the external network.

The difference from full cone NAT is in how the restricted cone NAT router handles packets coming in from the external network. A host on the external network (IP address **3** or IP address **4** for example) can only send packets to the internal host if the internal host has already sent a packet to the external host's IP address.

A Prestige with IP address **1** and port **A** sends packets to IP address **3** and IP address **4**. The NAT router changes the Prestige's IP address to **2** and port to **B**.

Both **4, D** and **4, E** can send packets to **2, B** since **1, A** has already sent packets to **4**. The NAT router will perform NAT on the packets from **4, D** and **4, E** and send them to the Prestige at IP address **1**, port **A**. Packets have not been sent from **1, A** to **3** or **5**, so **3** and **5** cannot send packets to **1, A**.

**Figure 33** Restricted Cone NAT Example

### 7.3.2.3 Port Restricted Cone NAT

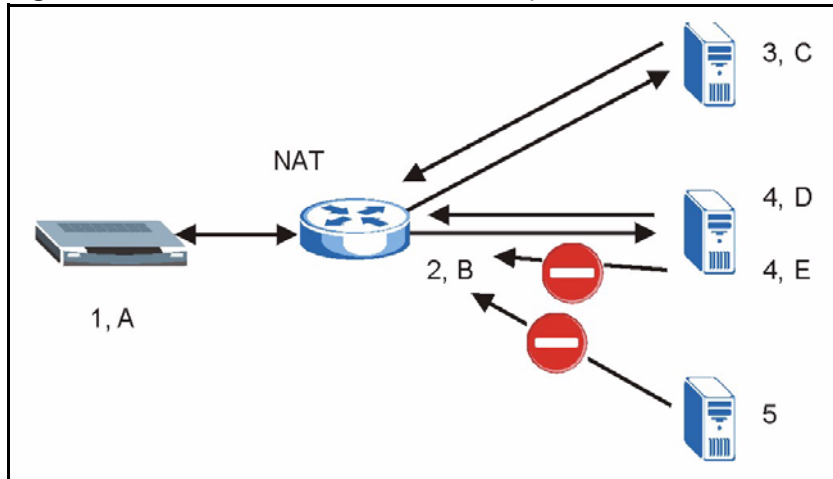
As in full cone NAT, a port restricted cone NAT router maps all outgoing packets from an internal IP address and port to a single IP address and port on the external network. In the following example, the NAT router maps the source address of all packets sent from internal IP address **1** and port **A** to IP address **2** and port **B** on the external network.

The difference from full cone and restricted cone NAT is in how the port restricted cone NAT router handles packets coming in from the external network. A host on the external network (IP address **3** and Port **C** for example) can only send packets to the internal host if the internal host has already sent a packet to the external host's IP address and port.

A Prestige with IP address **1** and port **A** sends packets to IP address **3**, port **C** and IP address **4**, port **D**. The NAT router changes the Prestige's IP address to **2** and port to **B**.

Since **1, A** has already sent packets to **3, C** and **4, D**, they can send packets back to **2, B** and the NAT router will perform NAT on them and send them to the Prestige at IP address **1**, port **A**.

Packets have not been sent from **1, A** to **4, E** or **5**, so they cannot send packets to **1, A**.

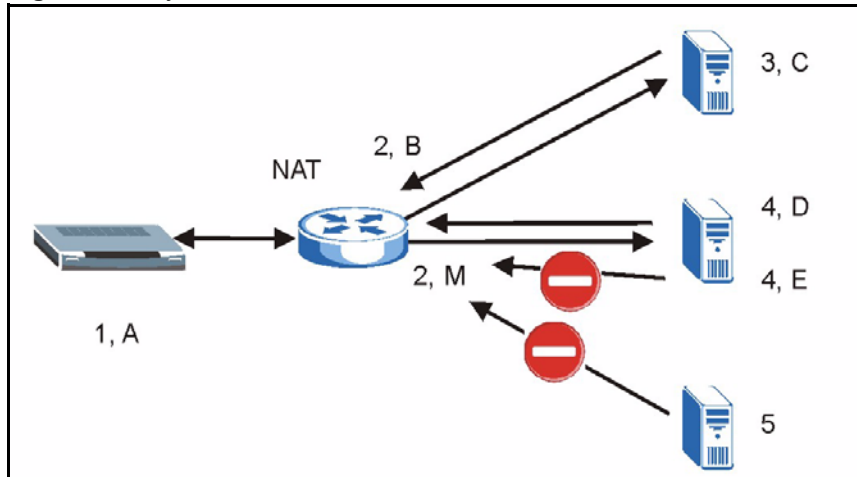
**Figure 34** Port Restricted Cone NAT Example

### 7.3.2.4 Symmetric NAT

The full, restricted and port restricted cone NAT types use the same mapping for an outgoing packet's source address regardless of the destination IP address and port. In symmetric NAT, the mapping of an outgoing packet's source address to a source address in another network is different for each different destination IP address and port.

In the following example, the NAT router maps the Prestige's source address IP address **1** and port **A** to IP address **2** and port **B** on the external network for packets sent to IP address **3** and port **B**. The NAT router uses a different mapping (IP address **2** and port **M**) when the Prestige sends packets to IP address **4** and port **D**.

A host on the external network (IP address **3** and port **C** for example) can only send packets to the internal host via the external IP address and port that the NAT router used in sending a packet to the external host's IP address and port. So in the example, only **3, C** is allowed to send packets to **2, B** and only **4, D** is allowed to send packets to **2, M**.

**Figure 35** Symmetric NAT

## 7.4 NAT and SIP

The Prestige must register its public IP address with a SIP register server. If there is a NAT router between the Prestige and the SIP register server, the Prestige probably has a private IP address. The Prestige lists its IP address in the SIP message that it sends to the SIP register server. NAT does not translate this IP address in the SIP message. The SIP register server gets the Prestige's IP address from inside the SIP message and maps it to your SIP identity. If the Prestige has a private IP address listed in the SIP message, the SIP server cannot map it to your SIP identity.

A SIP ALG (Application Layer Gateway) or the Use NAT, STUN, and outbound proxy features allow the Prestige to list its public IP address in the SIP messages.

## 7.5 SIP ALG

Some NAT routers may include a SIP Application Layer Gateway (ALG). A SIP ALG allows SIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream. When the Prestige registers with the SIP register server, the SIP ALG translates the Prestige's private IP address inside the SIP data stream to a public IP address. You do not need to use STUN or an outbound proxy if your Prestige is behind a SIP ALG.

## 7.6 Use NAT

If you know the NAT router's public IP address and SIP port number, you can use the Use NAT feature to manually configure the Prestige to use a them in the SIP messages. This eliminates the need for STUN or a SIP ALG.

You must also configure the NAT router to forward traffic with this port number to the Prestige.



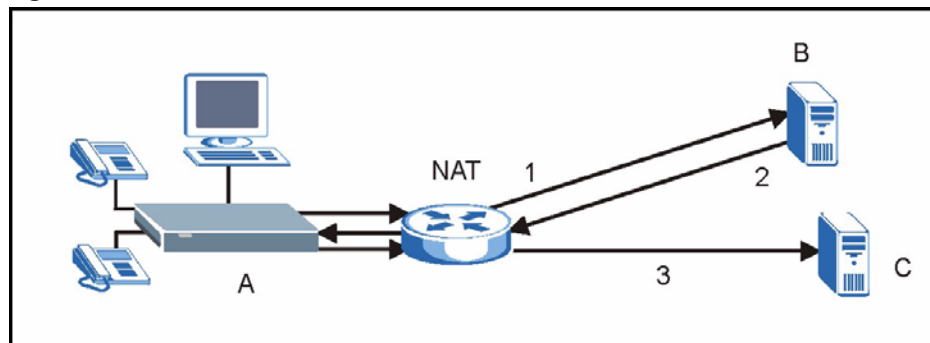
## 7.7 STUN

STUN (Simple Traversal of User Datagram Protocol (UDP) through Network Address Translators) allows the Prestige to find the presence and types of NAT routers and/or firewalls between it and the public Internet. STUN also allows the Prestige to find the public IP address that NAT assigned, so the Prestige can embed it in the SIP data stream. STUN does not work with symmetric NAT routers (see [Section 7.3.2.4 on page 98](#)) or firewalls. See RFC 3489 for details on STUN.

The following figure shows how STUN works.

- 1 The Prestige (A) sends SIP packets to the STUN server (B).
- 2 The STUN server (B) finds the public IP address and port number that the NAT router used on the Prestige's SIP packets and sends them to the Prestige.
- 3 The Prestige uses the public IP address and port number in the SIP packets that it sends to the SIP server (C).

**Figure 36** STUN



## 7.8 Outbound Proxy

Your VoIP service provider may host a SIP outbound proxy server to handle all of the Prestige's VoIP traffic. This allows the Prestige to work with any type of NAT router and eliminates the need for STUN or a SIP ALG. Turn off a SIP ALG on a NAT router in front of the Prestige to keep it from retranslating the IP address (since this is already handled by the outbound proxy server).

## 7.9 Voice Coding

A codec (coder/decoder) codes analog voice signals into digital signals and decodes the digital signals back into voice signals. The Prestige supports the following codecs.

## 7.9.1 Pulse Code Modulation

Pulse Code Modulation (PCM) measures analog signal amplitudes at regular time intervals and converts them into bits.

## 7.9.2 G.711

G.711 is a Pulse Code Modulation (PCM) waveform codec. G.711 provides very good sound quality but requires 64kbps of bandwidth.

## 7.9.3 G.729

G.729 is an Analysis-by-Synthesis (AbS) hybrid waveform codec that uses a filter based on information about how the human vocal tract produces sounds. G.729 provides good sound quality and reduces the required bandwidth to 8kbps.

## 7.10 PSTN Call Setup Signaling

PSTNs (Public Switched Telephone Network)s use DTMF or pulse dialing to set up telephone calls.

Dual-Tone Multi-Frequency (DTMF) signaling uses pairs of frequencies (one lower frequency and one higher frequency) to set up calls. It is also known as Touch Tone®. Each of the keys on a DTMF telephone corresponds to a different pair of frequencies.

Pulse dialing sends a series of clicks to the local phone office in order to dial numbers.<sup>1</sup>

## 7.11 MWI (Message Waiting Indication)

Enable Message Waiting Indication (MWI) enables your phone to give you a message–waiting (beeping) dial tone when you have a voice message(s). Your voice service provider must have a messaging system that sends message waiting status SIP packets as defined in RFC 3842.

---

1. The Prestige supports DTMF at the time of writing.

# CHAPTER 8

## VoIP Screens

This chapter describes how to configure VoIP and QoS settings.

### 8.1 VoIP Introduction

VoIP is the sending of voice signals over the Internet Protocol. This chapter covers the configuration of the **VoIP** screens.

### 8.2 VoIP Configuration

Click **VoIP** in the navigation panel to display the following screen. Use this screen to configure the Prestige's VoIP settings. You should have a voice account already set up and have VoIP information from your VoIP service provider.

**Figure 37** VoIP

The following table describes the labels in this screen.

**Table 21** VoIP

LABEL	DESCRIPTION
SIP Account	You can configure the Prestige to use multiple SIP accounts. Select one to configure its settings on the Prestige.
Active	Select this check box to have the Prestige use this SIP account. Clear the check box to have the Prestige not use this SIP account.
SIP Number	Enter your SIP number in this field (use the number or text that comes before the @ symbol in a full SIP URI). You can use up to 127 ASCII characters.
SIP Local Port	Use this field to configure the Prestige's listening port for SIP. Leave this field set to the default if you were not given a local port number for SIP.
SIP Server Address	Type the IP address or domain name of the SIP server in this field. It doesn't matter whether the SIP server is a proxy, redirect or register server. You can use up to 95 ASCII characters.

**Table 21** VoIP (continued)

LABEL	DESCRIPTION
SIP Server Port	Enter the SIP server's listening port for SIP in this field. Leave this field set to the default if your VoIP service provider did not give you a server port number for SIP.
REGISTER Server Address	Enter the SIP register server's IP address or domain name in this field. You can use up to 95 ASCII characters.  <b>Note:</b> If you were not given a register server address, then enter the address from the <b>SIP Server Address</b> field again here.
REGISTER Server Port	Enter the SIP register server's listening port for SIP in this field.  <b>Note:</b> If you were not given a register server port, then enter the port from the <b>SIP Server Port</b> field again here.
SIP Service Domain	Enter the SIP service domain name in this field (the domain name that comes after the @ symbol in a full SIP URI). You can use up to 127 ASCII Extended set characters.
Authentication User ID	This is the user name for registering this SIP account with the SIP register server. Type the user name exactly as it was given to you. You can use up to 95 ASCII characters.
Authentication Password	Type the password associated with the user name above. You can use up to 95 ASCII Extended set characters.
Sending Caller ID	Select this check box to show identification information when you make VoIP phone calls. Clear the check box to not show identification information when you make VoIP phone calls.
Incoming Call apply to	Phone <b>1</b> and <b>Phone 2</b> correspond to the Prestige's physical <b>PHONE 1</b> and <b>2</b> ports, respectively. Select whether you want to receive calls for this SIP account on <b>Phone 1</b> , <b>Phone 2</b> or both. If you select both, you will not know which SIP account a call is coming in on.
Advanced Settings	Click <b>Settings</b> to open a screen where you can configure the Prestige's advanced VoIP settings like SIP server settings, the RTP port range and the coding type.
Apply	Click <b>Apply</b> to save your changes back to the Prestige.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 8.3 Custom Tones (IVR)

IVR (Interactive Voice Response) is a feature that allows you to use your telephone to interact with the Prestige device. The Prestige allows you to record custom tones for the **Caller Ringing Tone** and **On Hold Tone** functions. The same recordings apply to both the caller ringing and on hold tones.

**Table 22** Custom Tones Details

LABEL	DESCRIPTION
Total Time for All Tones	120 seconds for all custom tones combined

**Table 22** Custom Tones Details

LABEL	DESCRIPTION
Time per Individual Tone	20 seconds
Total Number of Tones Recordable	Ten You can record up to ten different custom tones but the total time must be 120 seconds or less. For example you could record up to ten 12-second tones or up to six 20-second tones.

### 8.3.0.1 Recording Custom Tones

Use the following steps if you would like to create new tones or change your tones:

- 1 Pick up the phone and press “\*\*\*\*” on your phone’s keypad and wait for the message that says you are in the configuration menu.
- 2 Press a number from 1101~1108 on your phone followed by the “#” key.
- 3 Play your desired music or voice recording into the receiver’s mouthpiece. Press the “#” key.
- 4 You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

### 8.3.0.2 Listening to Custom Tones

Do the following to listen to a custom tone:

- 1 Pick up the phone and press “\*\*\*\*” on your phone’s keypad and wait for the message that says you are in the configuration menu.
- 2 Press a number from 1201~1208 followed by the “#” key to listen to the tone.
- 3 You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

### 8.3.0.3 Deleting Custom Tones

Do the following to delete a custom tone:

- 1 Pick up the phone and press “\*\*\*\*” on your phone’s keypad and wait for the message that says you are in the configuration menu.
- 2 Press a number from 1301~1308 followed by the “#” key to delete the tone of your choice. Press 14 followed by the “#” key if you wish to clear all your custom tones.
- 3 You can continue to add, listen to, or delete tones, or you can hang up the receiver when you are done.

## 8.4 Advanced VoIP Settings Configuration

Click **VoIP** in the navigation panel, select a SIP account and then click **Settings** to display the following screen.

Figure 38 VoIP Advanced

VoIP QoS

**Advanced VoIP Settings :SIP1**

---

**SIP Server Settings**

URL Type

Expiration Duration  (20-65535)

Register Re-send timer  (1-65535)

Session Expires  (30-3600)

Min-SE  (20-1800)

---

**RTP Port Range**

From  (1026-65535)

To  (1026-65535)

---

**Voice Compression**

Preferred Compression Type

---

**STUN**

Active

Server Address

Server Port  (1024-65535)

---

**Use NAT**

Active

Server Address

Server Port  (1024-65535)

---

**Outbound Proxy**

Active

Server Address

Server Port  (1024-65535)

---

**NAT Keep Alive**

Enable NAT Keep Alive

Keep Alive Interval  (30-65535)

---

**Dual-Tone-Multi-Frequency (DTMF)**

DTMF Mode

---

**MWI (Message Waiting Indication)**

Enable

Expiration Time  (1-65535)

---

**Fax Option**

Fax Pass-through  T.38

---

**Call Forward**

Call Forward Table

---

**Caller Ringing**

Enable

Caller Ringing Tone

---

**On Hold**

Enable

On Hold Tone

(Note: Currently works with calls that are using G.729 Codec)

The following table describes the labels in this screen.

**Table 23** VoIP Advanced

LABEL	DESCRIPTION
Advanced VoIP Settings	This read-only field displays the number of the SIP account that you are configuring. The changes that you save in this page affect the Prestige's settings with the SIP account displayed here.
SIP Server Settings	
URL Type	Select <b>SIP</b> to have the Prestige include the domain name with the SIP number in the SIP messages that it sends. Select <b>TEL</b> to have the Prestige use the SIP number without a domain name in the SIP messages that it sends.
Expiration Duration	This field sets how long an entry remains registered with the SIP register server. After this time period expires, the SIP register server deletes the Prestige's entry from the database of registered SIP numbers. The register server can use a different time period. The Prestige sends another registration request after half of this configured time period has expired.
Register Re-send timer	Use this field to set how long the Prestige waits before sending a repeat registration request if a registration attempt fails or there is no response from the registration server.
Session Expires	Use this field to set the longest time that the Prestige will allow a SIP session to remain idle (without traffic) before dropping it.
Min-SE	When two SIP devices negotiate a SIP session, they must negotiate a common expiration time for idle SIP sessions. This field sets the shortest expiration time that the Prestige will accept. The Prestige checks the session expiration values of incoming SIP INVITE requests against the minimum session expiration value that you configure here. If the session expiration of an incoming INVITE request is less than the value you configure here, the Prestige negotiates with the other SIP device to increase the session expiration value to match the Prestige's minimum session expiration value.
RTP Port Range	Real time Transport Protocol is used to handle voice data transfer. Use these fields to configure the Prestige's listening port range for RTP traffic. Leave these fields set to the defaults if you were not given a range of RTP ports to use.
From	Type the beginning of the listening port range.
To	Type the end of the listening port range.
Voice Compression	
Preferred Compression Type	<p>Use this field to select the type of voice coder/decoder (codec) that you want the Prestige to use. G.711 provides higher voice quality than G.729 but requires 64kbps of bandwidth while G.729 only requires 8kbps.</p> <p>Select <b>G.711&gt;G.729</b> if you want the Prestige to first attempt to use the G.711 codec and then the G.729 codec if the peer is not set up to use G.711.</p> <p>Select <b>G.711 only</b> if you want the Prestige to only use the G.711 codec when making VoIP calls. You will not be able to connect to a peer that is not set up to use G.711.</p> <p>Select <b>G.729&gt;G.711</b> if you want the Prestige to first attempt to use the G.729 codec and then the G.711 codec if the peer is not set up to use G.729.</p> <p>Select <b>G.729 only</b> if you want the Prestige to only use the G.729 codec when making VoIP calls. You will not be able to connect to a peer that is not set up to use G.729.</p>
STUN	
Active	Check this box if there is a NAT router between the Prestige and the voice service provider's SIP server AND if the NAT router is not a SIP ALG.



**Table 23** VoIP Advanced (continued)

LABEL	DESCRIPTION
Server Address	Your VoIP service provider must host a STUN server in order for you to use STUN. Type the IP address or domain name (up to 127 ASCII characters) of the STUN server in this field.
Server Port	Enter the STUN server's listening port for STUN requests in this field. Leave this field set to the default if your VoIP service provider did not give you a server port number for STUN.
Use NAT	
Active	Check this box to use a NAT router's public IP address and SIP port number in the Prestige's SIP messages. This eliminates the need for STUN or a SIP ALG. You must also configure the NAT router to forward traffic with this port number to the Prestige.
Server Address	Enter the NAT router's public IP address or domain name (up to 127 ASCII characters) in this field.
Server Port	Enter the port number that your SIP sessions use with the public IP address of the NAT router.
Outbound Proxy	
Active	Check this box if your VoIP service provider has a SIP outbound server to handle voice calls. This allows the Prestige to work with any type of NAT router and eliminates the need for STUN or a SIP ALG. Turn off any SIP ALG on a NAT router in front of the Prestige to keep it from retranslating the IP address (since this is already handled by the outbound proxy server).
Server Address	Enter the IP address or domain name (up to 127 ASCII characters) of the SIP outbound proxy server in this field.
Server Port	Enter the SIP outbound proxy server's listening port for SIP outbound proxy requests in this field. Leave this field set to the default if your VoIP service provider did not give you a server port number for the SIP outbound proxy server.
NAT Keep Alive	
Enable NAT Keep Alive	You must have outbound proxy enabled to use NAT keep alive. Enable NAT keep alive to have the Prestige send SIP notify messages to the SIP server. Use this to keep a NAT router located between the Prestige and the SIP server from timing out and dropping your Prestige's SIP NAT sessions.
Keep Alive Interval	Set how often (in seconds) the Prestige should send SIP notify messages to the SIP server.
Dual-Tone-Multi-Frequency (DTMF)	
DTMF Mode	The Dual-Tone Multi-Frequency (DTMF) mode sets how the Prestige handles the tones that your telephone makes when you push its buttons. It is recommended that you use the same mode that your VoIP service provider uses. Select <b>RFC 2833</b> to send the DTMF tones in RTP packets. Select <b>PCM</b> (Pulse Code Modulation) to include the DTMF tones in the voice data stream. This method works best when you are using a codec that does not use compression (like G.711). Codecs that use compression (like G.729) could distort the tones. Select <b>SIP INFO</b> to send the DTMF tones in SIP messages.
MWI (Message Waiting Indication)	

**Table 23** VoIP Advanced (continued)

LABEL	DESCRIPTION
Enable	Check this box to have your phone give you a message–waiting (beeping) dial tone when you have a voice message(s). Your voice service provider must have a messaging system that supports this feature.
Expiration Time	Use this field to set how long the SIP server should continue providing the message waiting service after receiving a SIP SUBSCRIBE message from the Prestige. The SIP server stops providing the message waiting service if it has not received another SIP SUBSCRIBE message from the Prestige before this time period expires.
Fax Option	This field controls how the Prestige handles fax messages.
Fax Pass-through	Select this radio button to have the Prestige send fax messages over G.711. The peer devices must also use G.711.
T.38	Select this radio button to have the Prestige send fax messages over the IP network as UDP or TCP/IP packets. It provides better transmission quality than fax pass-through but may have inter-operability problems. The peer devices must also use T.38.
Call Forward	
Call Forward Table	Select which call forwarding table you want the Prestige to use to block or redirect calls. You can use a different call forwarding table for each SIP account or use the same call forwarding table for both.
Caller Ringing	
Enable	Check this box if you want to specify what tone people hear when they call you. The Prestige provides a default tone, but you can add additional tones using IVR. See <a href="#">Section 8.3 on page 104</a> for more information.
Caller Ringing Tone	Select the tone you want people to hear when they call you. You should setup Tones 1 - 8 using IVR first. See <a href="#">Section 8.3 on page 104</a> for more information.
On Hold	
Enable	Check this box if you want to specify what tone people hear when you put them on hold. The Prestige provides a default tone, but you can add additional tones using IVR. See <a href="#">Section 8.3 on page 104</a> for more information.
On Hold Tone	Select the tone you want people to hear when you put them on hold. You should setup Tones 1 - 8 using IVR first. See <a href="#">Section 8.3 on page 104</a> for more information.
Back	Click <b>Back</b> to return to the VoIP screen without saving configuration changes.
Apply	Click <b>Apply</b> to save your changes back to the Prestige.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 8.5 Quality of Service (QoS)

Quality of Service (QoS) refers to both a network's ability to deliver data with minimum delay, and the networking methods used to provide bandwidth for real-time multimedia applications.

## 8.5.1 Type Of Service (ToS)

Network traffic can be classified by setting the ToS (Type Of Service) values at the data source (for example, at the Prestige) so a server can decide the best method of delivery, that is the least cost, fastest route and so on.

## 8.5.2 DiffServ

DiffServ is a class of service (CoS) model that marks packets so that they receive specific per-hop treatment at DiffServ-compliant network devices along the route based on the application types and traffic flow. Packets are marked with DiffServ Code Points (DSCPs) indicating the level of service desired. This allows the intermediary DiffServ-compliant network devices to handle the packets differently depending on the code points without the need to negotiate paths or remember state information for every flow. In addition, applications do not have to request a particular service or give advanced notice of where the traffic is going.<sup>1</sup>

### 8.5.2.1 DSCP and Per-Hop Behavior

DiffServ defines a new DS (Differentiated Services) field to replace the Type of Service (TOS) field in the IP header. The DS field contains a 2-bit unused field and a 6-bit DSCP field which can define up to 64 service levels. The following figure illustrates the DS field.

DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

**Figure 39** DiffServ: Differentiated Service Field

DSCP (6-bit)	Unused (2-bit)
-----------------	-------------------

The DSCP value determines the forwarding behavior, the PHB (Per-Hop Behavior), that each packet gets across the DiffServ network. Based on the marking rule, different kinds of traffic can be marked for different priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

## 8.5.3 VLAN

Virtual Local Area Network (VLAN) allows a physical network to be partitioned into multiple logical networks. Only stations within the same group can communicate with each other.

Your Prestige can add IEEE 802.1Q VLAN ID tags to voice frames that it sends to the network. This allows the Prestige to communicate with a SIP server that is a member of the same VLAN group. Some ISPs use the VLAN tag to identify voice traffic and give it priority over other traffic.

1. The Prestige does not support DiffServ at the time of writing.

## 8.6 QoS Configuration

Click **VoIP** in the navigation panel and then **QoS** to display the following screen.

**Figure 40** QoS

The following table describes the labels in this screen.

**Table 24** QoS

LABEL	DESCRIPTION
SIP TOS Priority	Type a priority for voice transmissions. The Prestige applies Type of Service priority tags with this priority to voice traffic that it transmits.
RTP TOS Priority	Type a priority for voice transmissions. The Prestige applies Type of Service priority tags with this priority to RTP traffic that it transmits.
Enable VLAN Tag	Enable VLAN tagging if the Prestige needs to be a member of a VLAN group in order to communicate with the SIP server. Your LAN and gateway must also be set up to use VLAN tags. Some switches also give priority to voice traffic based on its VLAN tag. Disable VLAN tagging if the Prestige does not need to be a member of a VLAN group to communicate with the SIP server.
Voice VLAN ID	Type the VLAN ID (VID) from 0 to 4095 for the Prestige to add to voice Ethernet frames that it sends out to the network.
Apply	Click <b>Apply</b> to save your changes back to the Prestige.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

# CHAPTER 9

## Phone

This chapter covers how to adjust the Prestige's phone settings.

### 9.1 Phone Introduction

You can configure the volume, echo cancellation and VAD settings for each individual phone port on the Prestige. You can also select which SIP account to use for making outgoing calls.

#### 9.1.1 Voice Activity Detection/Silence Suppression

Voice Activity Detection (VAD) detects whether or not speech is present. This lets the Prestige reduce the bandwidth that a call uses by not transmitting "silent packets" when you are not speaking.

#### 9.1.2 Comfort Noise Generation

When using VAD, the Prestige generates comfort noise when the other party is not speaking. The comfort noise lets you know that the line is still connected as total silence could easily be mistaken for a lost connection.

#### 9.1.3 Echo Cancellation

G.168 is an ITU-T standard for eliminating the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.

### 9.2 Phone Port Configuration

Click **PHONE** in the navigation panel to display the following screen. Use this screen to configure phone port settings that are specific to an individual phone port.

**Figure 41** Phone Port

**Phone**

Phone Port **Common**

Phone Port Settings: Phone1

**Voice Volume Control**

Speaking Volume Level: -1

Listening Volume Level: -1

**Outgoing Call use**

SIP1  SIP2

**Echo Cancellation**

G.168 Active

**Voice Active Detector (VAD)**

VAD Support

Dialing Interval 3

Apply Reset

The following table describes the labels in this screen.

**Table 25** Phone Port

LABEL	DESCRIPTION
Phone Port Settings	Use this field to select the phone port that you want to configure.
Speaking Volume	Use this field to set the loudness that the Prestige uses for the speech signal that it sends to the peer device. -1 is the quietest and 1 is the loudest.
Listening Volume	Use this field to set the loudness that the Prestige uses for the speech signal that it receives from the peer device and sends to your phone. -1 is the quietest and 1 is the loudest.
Outgoing Call use	<b>SIP 1</b> and <b>SIP 2</b> correspond to the Prestige's SIP accounts. Select whether you want the phone(s) attached to this phone port to use SIP account 1, 2 or both when you make a call. If you select both SIP accounts, the Prestige will first try to use SIP account 2 and then SIP account 1 when you make a call.
G.168 Active	Select this check box to cancel the echo caused by the sound of your voice reverberating in the telephone receiver while you talk.
VAD Support	Select this check box to use Voice Activity Detection (VAD). VAD reduces the bandwidth that a call uses by not transmitting when you are not speaking.

**Table 25** Phone Port (continued)

LABEL	DESCRIPTION
Dialing Interval	When you are dialing a telephone number the Prestige waits this long after you stop pressing the buttons before initiating the call. Select how many seconds you want the Prestige to wait after the last input on the telephone's keypad before dialing (making) a call.
Apply	Click <b>Apply</b> to save your changes back to the Prestige.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 9.3 Supplementary Phone Services Overview

Supplementary services such as call hold, call waiting, call transfer, ... are generally available from your voice service provider. The Prestige supports the following services:

- Call Hold
- Call Waiting
- Making a Second Call
- Call Transfer
- Call Forwarding (see [Section 10.3 on page 122](#))
- Three-Way Conference
- Internal Calls (see [Section 11.3 on page 126](#))

**Note:** To take full advantage of the supplementary phone services available through the Prestige's phone ports, you may need to subscribe to the services from your voice service provider.

### 9.3.1 The Flash Key

Flashing means to press the hook for a short period of time (a few hundred milliseconds) before releasing it. On newer telephones, there should be a "flash" key (button) that generates the signal electronically. If the flash key is not available, you can tap (press and immediately release) the hook by hand to achieve the same effect. However, using the flash key is preferred since the timing is much more precise. The Prestige may interpret manual tapping as hanging up if the duration is too long.

You can invoke all the supplementary services by using the flash key.

### 9.3.2 Europe Type Supplementary Phone Services

This section describes how to use supplementary phone services with the **Europe Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-command before the default sub-command timeout (2 seconds) expires or issue an invalid sub-command, the current operation will be aborted.

**Table 26** European Type Flash Key Commands

COMMAND	SUB-COMMAND	DESCRIPTION
Flash		Put a current call on hold to place a second call. Switch back to the call (if there is no second call).
Flash	0	Drop the call presently on hold or reject an incoming call which is waiting for answer.
Flash	1	Disconnect the current phone connection and answer the incoming call or resume with caller presently on hold.
Flash	2	1. Switch back and forth between two calls. 2. Put a current call on hold to answer an incoming call. 3. Separate the current three-way conference call into two individual calls (one is on-line, the other is on hold).
Flash	3	Create three-way conference connection.
Flash	*98#	Transfer the call to another phone.

### 9.3.2.1 European Call Hold

Call hold allows you to put a call (**A**) on hold by pressing the flash key.

If you have another call, press the flash key and then “2” to switch back and forth between caller **A** and **B** by putting either one on hold.

Press the flash key and then “0” to disconnect the call presently on hold and keep the current call on line.

Press the flash key and then “1” to disconnect the current call and resume the call on hold.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

### 9.3.2.2 European Call Waiting

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to a telephone number, you will hear a call waiting tone. Take one of the following actions.

- Reject the second call.

Press the flash key and then press “0”.

- Disconnect the first call and answer the second call.

Either press the flash key and press “1”, or just hang up the phone and then answer the phone after it rings.



- Put the first call on hold and answer the second call.  
Press the flash key and then “2”.

### 9.3.2.3 European Call Transfer

Do the following to transfer an incoming call (that you have answered) to another phone.

- 1 Press the flash key to put the caller on hold.
- 2 When you hear the dial tone, dial “\*98#” followed by the number to which you want to transfer the call. to operate the Intercom.
- 3 After you hear the ring signal or the second party answers it, hang up the phone.

### 9.3.2.4 European Three-Way Conference

Use the following steps to make three-way conference calls.

- 1 When you are on the phone talking to someone, place the flash key to put the caller on hold and get a dial tone.
- 2 Dial a phone number directly to make another call.
- 3 When the second call is answered, press the flash key and press “3” to create a three-way conversation.
- 4 Hang up the phone to drop the connection.
- 5 If you want to separate the activated three-way conference into two individual connections (one is on-line, the other is on hold), press the flash key and press “2”.

## 9.3.3 USA Type Supplementary Services

This section describes how to use supplementary phone services with the **USA Type Call Service Mode**. Commands for supplementary services are listed in the table below.

After pressing the flash key, if you do not issue the sub-command before the default sub-command timeout (2 seconds) expires or issue an invalid sub-command, the current operation will be aborted.

**Table 27** USA Type Flash Key Commands

COMMAND	SUB-COMMAND	DESCRIPTION
Flash		Put a current call on hold to place a second call. After the second call is successful, press the flash key again to have a three-way conference call. Put a current call on hold to answer an incoming call.
Flash	*98#	Transfer the call to another phone.

### 9.3.3.1 USA Call Hold

Call hold allows you to put a call (**A**) on hold by pressing the flash key.

If you have another call, press the flash key to switch back and forth between caller **A** and **B** by putting either one on hold.

If you hang up the phone but a caller is still on hold, there will be a remind ring.

### 9.3.3.2 USA Call Waiting

This allows you to place a call on hold while you answer another incoming call on the same telephone (directory) number.

If there is a second call to your telephone number, you will hear a call waiting tone.

Press the flash key to put the first call on hold and answer the second call.

### 9.3.3.3 USA Call Transfer

Do the following to transfer an incoming call (that you have answered) to another phone.

- 1 Press the flash key to put the caller on hold.
- 2 When you hear the dial tone, dial “\*98#” followed by the number to which you want to transfer the call. to operate the Intercom.
- 3 After you hear the ring signal or the second party answers it, hang up the phone.

### 9.3.3.4 USA Three-Way Conference

Use the following steps to make three-way conference calls.

- 1 When you are on the phone talking to someone, place the flash key to put the caller on hold and get a dial tone.
- 2 Dial a phone number directly to make another call.
- 3 When the second call is answered, press the flash key, wait for the sub-command tone and press “3” to create a three-way conversation.
- 4 Hang up the phone to drop the connection.
- 5 If you want to separate the activated three-way conference into two individual connections (one is on-line, the other is on hold), press the flash key, wait for the sub-command tone and press “2”.

## 9.4 Common Phone Configuration

Click **PHONE** in the navigation panel and then **Common** to display the following screen. Use this screen to configure general phone port settings.

**Figure 42** Phone Port Common

The screenshot shows a configuration interface for 'Phone Port Common'. It features a title 'Phone' and a sub-header 'Phone Port Common'. The interface includes several fields: 'Country Code' with a dropdown menu set to 'USA'; 'Immediate Dial' with an 'Enable' checkbox; 'Incoming Lifeline Call mapping to:' with checkboxes for 'Phone 1' and 'Phone 2'; and 'Call Service Mode' with a dropdown menu set to 'Europe Type'. At the bottom are 'Apply' and 'Reset' buttons.

The following table describes the labels in this screen.

**Table 28** Phone Common

LABEL	DESCRIPTION
Country Code	Use the drop-down list box to select the country where your Prestige is located. Do not use <b>Default</b> .
Immediate Dial	Use immediate dial to have the Prestige make calls right away instead of waiting for the dialing interval (the time period it waits to make sure you are done pressing the keys). In order to use immediate dial, enable it here. Then press the pound (#) key on your telephone's keypad after dialing a phone number (this has the Prestige make the call right away).
Incoming Lifeline Call mapping to (Lifeline models only)	<b>Phone 1</b> and <b>Phone 2</b> correspond to the Prestige's physical <b>PHONE 1</b> and <b>2</b> ports, respectively. Select whether you want to receive regular (PSTN) phone calls on <b>Phone 1</b> , <b>Phone 2</b> or both. If you select both, all of the phones connected to the Prestige's <b>PHONE</b> ports will ring when a call comes in on the PSTN line.
Call Service Mode	Use this field to set how the Prestige handles supplementary phone services (call hold, call waiting, call transfer and three-way conference calls). Select the mode that your voice service provider supports. Select <b>Europe Type</b> to use the supplementary phone services in European mode. Select <b>USA Type</b> to use the supplementary phone services American mode.  <b>Note:</b> To take full advantage of the supplementary phone services available through the Prestige's phone ports, you may need to subscribe to the services from your voice service provider.
Apply	Click <b>Apply</b> to save your changes back to the Prestige.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.



# CHAPTER 10

## Phone Book

This chapter covers how to configure the Prestige's phone book.

### 10.1 Phone Book Introduction

You can use the phone book feature to configure speed dial entries, call forwarding tables and the lifeline settings.

#### 10.1.1 Speed Dial

Speed dial provides shortcuts for dialing frequently used (VoIP) phone numbers.

##### 10.1.1.1 Peer-to-Peer Calls

You can call another VoIP device directly without going through a SIP server. You must set up a speed dial entry in the phone book in order to do this. Select **Non-Proxy (Use IP or URL)** in the **Type** column and enter the callee's IP address or domain name. The Prestige sends SIP INVITE requests to the peer VoIP device when you use the speed dial entry.

You do not need to configure a SIP account in order to make a peer-to-peer VoIP call.

#### 10.1.2 Lifeline (Prestige 2302RL)

With lifeline you can make and receive regular phone calls. Use a prefix number to make a regular call. When the Prestige 2302RL does not have power, you can make regular calls without dialing a prefix number.

You can also specify phone numbers that should always use the regular phone service (without having to dial a prefix number). Do this for emergency numbers (like those for contacting police, fire or emergency medical services).

### 10.2 Speed Dial Configuration

Click **PHONEBOOK** in the navigation panel and then **Speed Dial** to display the following screen.

**Figure 43** Speed Dial

**PHONE BOOK**

Speed Dial **Call Forward**

Add New Entry

Speed Dial	SIP Number	Name:	Type
#02	4567	friend2	<input type="radio"/> Use Proxy <input checked="" type="radio"/> Non-Proxy (Use IP or URL) friend2.com

Add

Speed Dial Phone Book

Speed Dial	SIP Number	Name:	Destination	
#01	1234	friend1	friend1.com	Delete Edit
#02				Delete Edit
#10				Delete Edit

Push Button to Clear Phone Book

Clear

The following table describes the labels in this screen.

**Table 29** Speed Dial

LABEL	DESCRIPTION
Add New Entry	Use this section of the screen to edit and save new or existing speed dial phone book entries.
Speed Dial	Select a speed dial key combination from the drop-down list box. After configuring the speed dial entry and adding it to the phone book, dial this speed dial key combination to use the speed dial entry to make a call.
SIP Number	Enter the SIP number of the party that you will call (use the number or text that comes before the @ symbol in a full SIP URI). You can use up to 127 ASCII characters.
Name	Enter a descriptive name to identify the party that you will use this entry to call. You can use up to 127 ASCII characters.
Type	Select <b>Use Proxy</b> if calls to this party use your SIP account configured in the <b>VoIP</b> screen. Select <b>Non-Proxy (Use IP or URL)</b> if calls to this party use a different SIP server or go directly to the callee's VoIP phone (peer-to-peer). Enter the SIP server's or the party's IP address or domain name (up to 127 ASCII Extended set characters).
Add	Click this button to save the entry in the speed dial phone book. The speed dial entry displays in the <b>Speed Dial Phone Book</b> section of the screen.
Speed Dial Phone Book	This section of the screen displays the currently saved speed dial entries. You can configure up to 10 entries and use them to make calls.

**Table 29** Speed Dial (continued)

LABEL	DESCRIPTION
Speed Dial	This is the entry's speed dial key combination. Press this key combination on a telephone attached to the Prestige in order to call the party named in this entry.
Name	This is the descriptive name of the party that you will use this speed dial entry to call.
SIP Number	This is the SIP number of the party that you will call.
Type	This field displays <b>Use Proxy</b> if calls to this party use one of your SIP accounts. This field displays the SIP server's or the party's IP address or domain name if calls to this party do not use one of your SIP accounts.
Delete	Click this button to remove an entry from the speed dial phone book.
Edit	Click this button to change the speed dial entry. The speed dial entry displays in the <b>Add New Entry</b> section of the screen where you can edit it.
Clear	Click this button to remove all of the entries from the speed dial phone book.

## 10.3 Call Forward

Click **PHONEBOOK** in the navigation panel and then **Call Forward** to display the following screen.

Use this screen to configure the Prestige to block or redirect calls. You can configure a different call forwarding table for each SIP account or use the same call forwarding table for both.

**Figure 44** Call Forward

## PHONE BOOK

Speed Dial
Call Forward

Table Number: Table 1

---

### Forward to Number Setup

Unconditional Forward to Number

Busy Forward to Number

No Answer Forward to Number

No Answer Waiting Time

0

(Second)

---

### Advanced Setup

Activate	Incoming Call Number	Forward to Number	Condition
1	<input type="checkbox"/>		Unconditional ▾
2	<input type="checkbox"/>		Unconditional ▾
3	<input type="checkbox"/>		Unconditional ▾
4	<input type="checkbox"/>		Unconditional ▾
5	<input type="checkbox"/>		Unconditional ▾
6	<input type="checkbox"/>		Unconditional ▾
7	<input type="checkbox"/>		Unconditional ▾
8	<input type="checkbox"/>		Unconditional ▾
9	<input type="checkbox"/>		Unconditional ▾
10	<input type="checkbox"/>		Unconditional ▾

Apply
Reset

The following table describes the labels in this screen.



**Table 30** Call Forward

LABEL	DESCRIPTION
Table Number	Select which call forwarding table you want to configure. You can configure a different call forwarding table for each SIP account or use the same call forwarding table for both.
	The following applies to the number fields in this screen. Enter a SIP number, use the number or text that comes before the @ symbol in a full SIP URI. You can use up to 127 ASCII characters.
Forward to Number Setup	These are the global call forwarding settings that define the default action to take on incoming calls that do not match any of the <b>Advanced Setup</b> call forwarding entries.
Unconditional Forward to Number	Enable this feature to have the Prestige forward all incoming calls to the number that you configure regardless of whether or not the phone(s) connected to the phone port(s) is busy.
Busy Forward to Number	Enable this feature to have the Prestige forward incoming calls to the number that you configure when the phone(s) connected to the phone port(s) is busy. With call waiting a second call is only forwarded after being rejected.
No Answer Forward to Number	Enable this feature to have the Prestige forward incoming calls to the number that you configure whenever you do not answer the call after a specific time period.
No Answer Waiting Time	Set how long the Prestige should let a call ring before considering the call unanswered.
Advanced Setup	Configure <b>Advanced Setup</b> call forwarding entries to have the Prestige perform specific actions on calls from specific numbers. If a caller's number does not match the <b>Incoming Call Number</b> of any of these entries, the Prestige performs the default action configured in the <b>Forward to Number Setup</b> section.
Activate	Select this check box to turn on an call forwarding entry.
Incoming Call Number	You can set the Prestige to take a particular action on incoming calls from a number that you specify here.
Forward to Number	You can set the Prestige to forward incoming calls to a number that you specify here.
Condition	<p>Select under what circumstances you want the Prestige to use this call forwarding entry.</p> <p>Select <b>Unconditional</b> to have the Prestige immediately forward any calls from the number specified in the <b>Incoming Call Number</b> field to the number in the <b>Forward to Number</b> field.</p> <p>Select <b>Busy</b> to have the Prestige forward any calls from the number specified in the <b>Incoming Call Number</b> field to the number in the <b>Forward to Number</b> field when your SIP account has a call connected.</p> <p>Select <b>No Answer</b> to have the Prestige forward any calls from the number specified in the <b>Incoming Call Number</b> field to the number in the <b>Forward to Number</b> field when the <b>No Answer Waiting Time</b> period expires (whether or not the no answer feature is enabled in the <b>Forward to Number Setup</b> section).</p> <p>Select <b>Block</b> to have the Prestige reject calls from the number specified in the call forwarding entry.</p> <p>Select <b>Accept</b> to have the Prestige allow calls from the number specified in the <b>Incoming Call Number</b> field.</p>
Apply	Click <b>Apply</b> to save your changes back to the Prestige.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 10.4 Lifeline Configuration (Prestige 2302RL)

Click **PHONEBOOK** in the navigation panel and then **Lifeline** to display the following screen.

**Figure 45** Lifeline

The following table describes the labels in this screen.

**Table 31** Lifeline

LABEL	DESCRIPTION
PSTN Pre-fix Number	Specify the prefix number for dialing regular calls.
Relay to PSTN	Use these fields to specify phone numbers to which the Prestige will always send calls through the regular phone service without the need of dialing a prefix number. These numbers must be for phones on the PSTN (not VoIP phones).
Apply	Click <b>Apply</b> to save your changes back to the Prestige.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

# CHAPTER 11

## Phone Usage

This chapter describes how to use a phone connected to your Prestige for basic tasks.

### 11.1 Dialing a Telephone Number

The **VoIP/PWR** LED turns orange when your SIP account is registered. Dial a SIP number like “12345” on your phone’s keypad.

Use speed dial entries (see [Section 10.2 on page 120](#)) for peer-to-peer calls or SIP numbers that use letters. Dial the speed dial entry on your telephone’s keypad.

Use your voice service provider’s dialing plan to call regular telephone numbers.

### 11.2 Using Speed Dial to Dial a Telephone Number

After configuring the speed dial entry and adding it to the phone book, press the speed dial entry’s key combination on your phone’s keypad.

### 11.3 Internal Calls

Press “#####” on your phone’s keypad to call the Prestige’s other phone port.

### 11.4 Checking the Prestige’s IP Address

Do the following to listen to the Prestige’s IP current address.

- 1 Pick up your phone’s receiver.
- 2 Press “\*\*\*\*” on your phone’s keypad and wait for the message that says you are in the configuration menu.
- 3 Press “5” followed by the # key.
- 4 Listen to the IP address and make a note of it.
- 5 Hang up the receiver.

## 11.5 Auto Firmware Upgrade

During auto-provisioning, the Prestige checks to see if there is a newer firmware version. If newer firmware is available, the Prestige plays a recording when you pick up your phone's handset.

Press “\*99#” to upgrade the Prestige's firmware.

Press “#99#” to not upgrade the Prestige's firmware.

# CHAPTER 12

## Network Address Translation (NAT) Screens

This chapter discusses how to configure NAT on the Prestige.

### 12.1 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 is changed to a different IP address known within another network.

#### 12.1.1 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 32** NAT Definitions

TERM	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.

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

## 12.1.2 What NAT Does

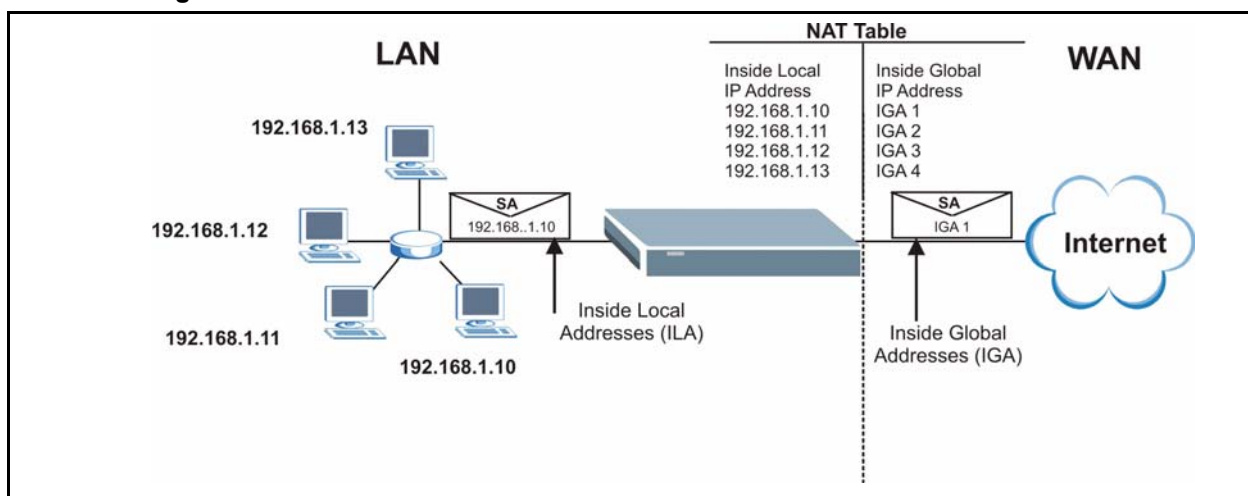
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address)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

## 12.1.3 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.

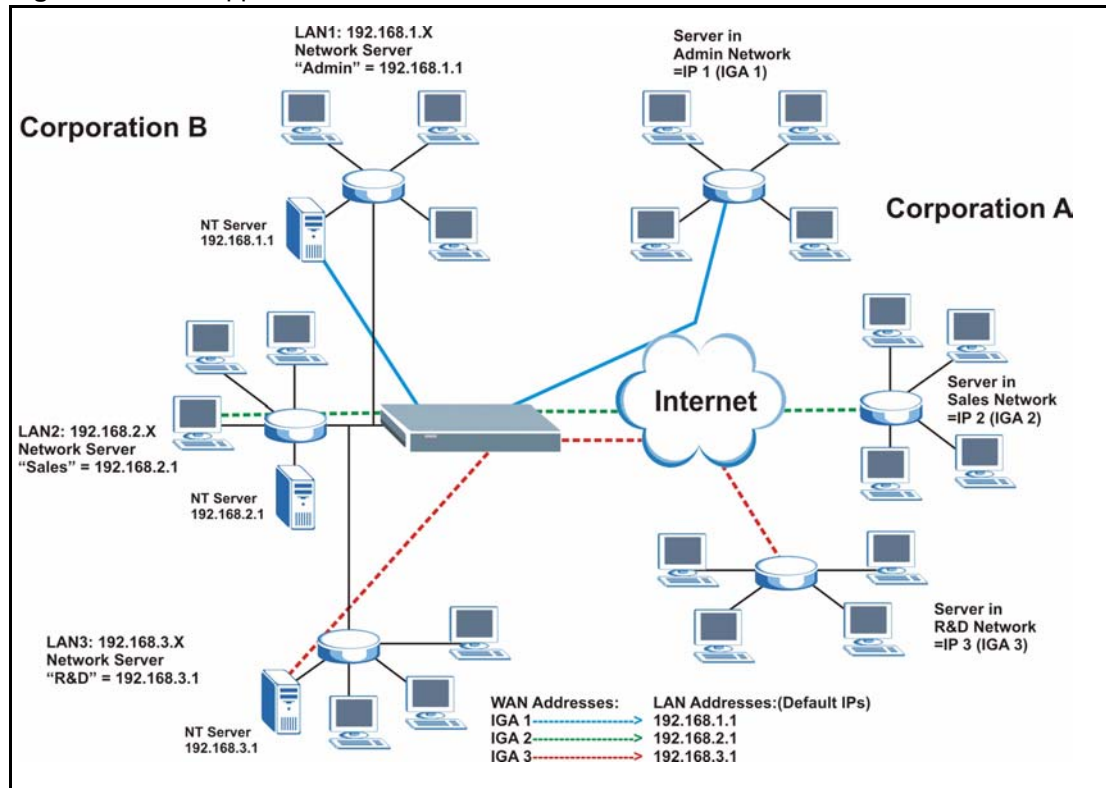
**Figure 46** How NAT Works



## 12.1.4 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 47** NAT Application With IP Alias



## 12.1.5 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 (i.e., PAT, port address translation), ZyXEL's Single User Account feature (the SUA Only option).
- **Many-to-Many Overload:** In Many-to-Many Overload mode, the Prestige maps the multiple local IP addresses to shared global IP addresses.
- **Many One-to-One:** In Many-One-to-One 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.

**Note:** Port numbers do not change for One-to-One and Many One-to-One NAT mapping types.

The following table summarizes these types.

**Table 33** NAT Mapping Types

TYPE	IP MAPPING	ABBREVIATION
One-to-One	ILA1 $\leftrightarrow$ IGA1	1-1
Many-to-One (SUA/PAT)	ILA1 $\leftrightarrow$ IGA1 ILA2 $\leftrightarrow$ IGA1 ...	M-1
Many-to-Many Overload	ILA1 $\leftrightarrow$ IGA1 ILA2 $\leftrightarrow$ IGA2 ILA3 $\leftrightarrow$ IGA1 ILA4 $\leftrightarrow$ IGA2 ...	M-M Ov
Many One-to-One	ILA1 $\leftrightarrow$ IGA1 ILA2 $\leftrightarrow$ IGA2 ILA3 $\leftrightarrow$ IGA3 ...	M-1-1
Server	Server 1 IP $\leftrightarrow$ IGA1 Server 2 IP $\leftrightarrow$ IGA1 Server 3 IP $\leftrightarrow$ IGA1	Server

## 12.2 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. Select either **SUA Only** or **Full Feature** in the **WAN IP** screen.

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

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

## 12.3 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.

**Note:** 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.

### 12.3.1 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

**Note:** If you do not assign a default server IP address, the Prestige discards all packets received for ports that are not specified in this screen or remote management.

### 12.3.2 Port Forwarding: Services and Port Numbers

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

Use the **SUA Server** page to forward incoming service requests to the server(s) on your local network. 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.

In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

The most often used port numbers are shown in the following table. Please refer to RFC 1700 for further information about port numbers. Please also refer to the Supporting CD for more examples and details on SUA/NAT.

**Table 34** Services and Port Numbers

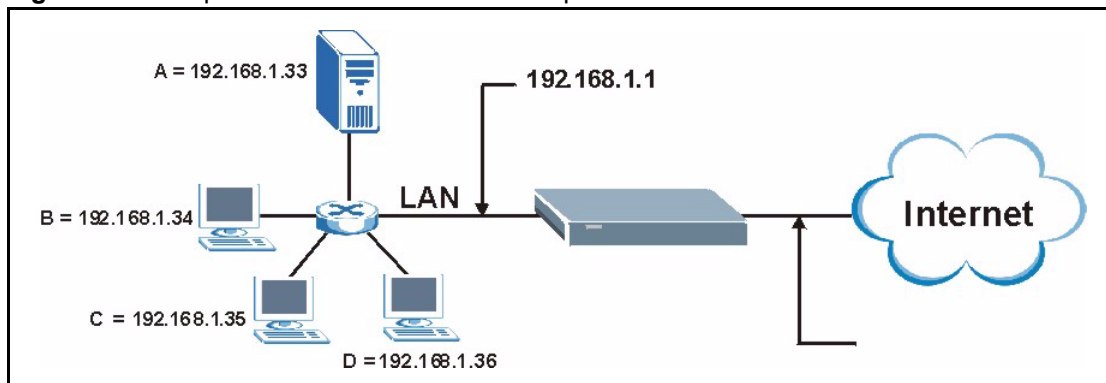
SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25

**Table 34** Services and Port Numbers

SERVICES	PORT NUMBER
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

### 12.3.3 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

**Figure 48** Multiple Servers Behind NAT Example

## 12.4 Configuring SUA Server

**Note:** If you do not assign a default server IP address, the Prestige discards all packets received for ports that are not specified in this screen or remote management.

Click **SUA/NAT** to open the **SUA Server** screen.

Refer to [Table 34 on page 132](#) for port numbers commonly used for particular services.

Figure 49 SUA/NAT Setup

**SUA/NAT**

SUA Server    Addr Mapping    Trigger Port

Default Server: 0.0.0.0

#	Active	Name	Start Port	End Port	Server IP Address
1	<input type="checkbox"/>		0	0	0.0.0.0
2	<input type="checkbox"/>		0	0	0.0.0.0
3	<input type="checkbox"/>		0	0	0.0.0.0
4	<input type="checkbox"/>		0	0	0.0.0.0
5	<input type="checkbox"/>		0	0	0.0.0.0
6	<input type="checkbox"/>		0	0	0.0.0.0
7	<input type="checkbox"/>		0	0	0.0.0.0
8	<input type="checkbox"/>		0	0	0.0.0.0
9	<input type="checkbox"/>		0	0	0.0.0.0
10	<input type="checkbox"/>		0	0	0.0.0.0

Apply    Reset

The following table describes the labels in this screen.

Table 35 SUA/NAT Setup

LABEL	DESCRIPTION
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a <b>Default Server</b> IP Address, the Prestige discards all packets received for ports that are not specified in this screen or remote management.
#	Number of an individual SUA server entry.
Active	Select this check box to enable the SUA server entry. Clear this check box to disallow forwarding of these ports to an inside server without having to delete the entry.
Name	Enter a name to identify this port-forwarding rule.
Start Port	Type a port number in this field. To forward only one port, type the port number again in the <b>End Port</b> field. To forward a series of ports, type the start port number here and the end port number in the <b>End Port</b> field.

**Table 35** SUA/NAT Setup

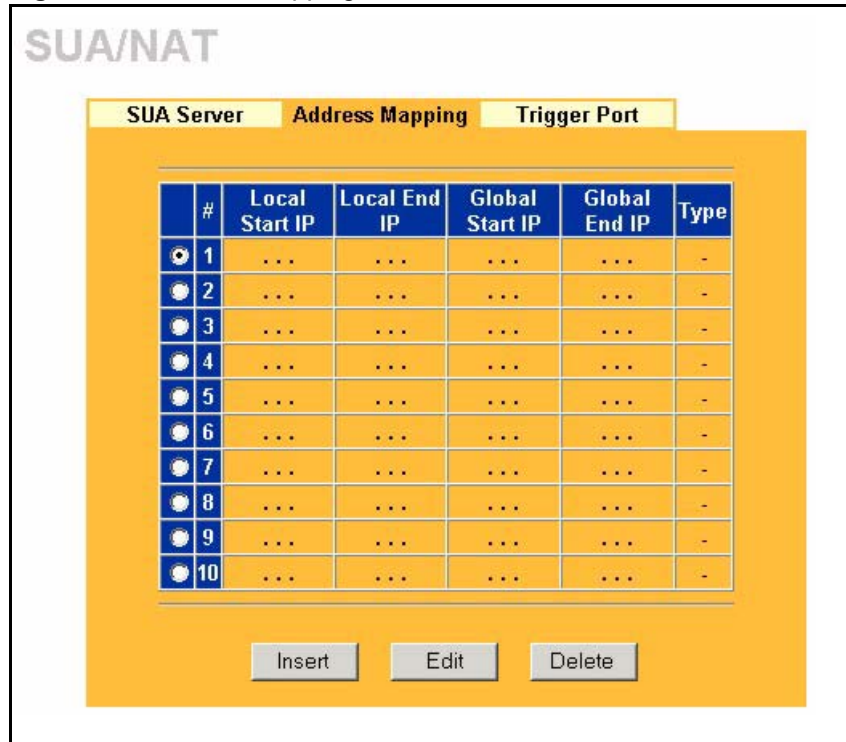
LABEL	DESCRIPTION
End Port	Type a port number in this field. To forward only one port, type the port number in the <b>Start Port</b> field above and then type it again in this field. To forward a series of ports, type the last port number in a series that begins with the port number in the <b>Start Port</b> field above.
Server IP Address	Enter the inside IP address of the server here.
Apply	Click <b>Apply</b> to save your changes back to the Prestige.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 12.5 Configuring Address Mapping

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

To change your Prestige's address mapping settings, click **SUA/NAT**, then the **Address Mapping** tab. The screen appears as shown.

Figure 50 Address Mapping



The following table describes the labels in this screen.

Table 36 Address Mapping

LABEL	DESCRIPTION
Local Start IP	This refers to the Inside Local Address (ILA), which is the starting local IP address. 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. Local IP addresses are <b>N/A</b> for <b>Server</b> port mapping.
Local End IP	This is the end Inside Local Address (ILA). If the rule is for all local IP addresses, then this field displays 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 refers to the Inside Global IP Address (IGA). 0.0.0.0 is for a dynamic IP address from your ISP with <b>Many-to-One</b> and <b>Server</b> mapping types.
Global End IP	This is the end Inside Global 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.
Type	<ol style="list-style-type: none"> <li>1. <b>1-1</b> (One-to-One) mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-One NAT mapping type.</li> <li>2. <b>M-1</b> (Many-to-One) mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only.</li> <li>3. <b>M-M-Ov</b> (Many-to-Many Overload) mode maps multiple local IP addresses to shared global IP addresses.</li> <li>4. <b>M-1-1</b> (Many One-to-One) mode maps each local IP address to unique global IP addresses.</li> <li>5. <b>Server</b> allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.</li> </ol>
Insert	Click <b>Insert</b> to insert a new mapping rule before an existing one.

**Table 36** Address Mapping

LABEL	DESCRIPTION
Edit	Click <b>Edit</b> to go to the <b>Address Mapping Rule</b> screen.
Delete	Click <b>Delete</b> to delete an address mapping rule.

## 12.5.1 Configuring Address Mapping

To edit an address mapping rule, select the radio button of a rule and click the **Edit** button to display the screen shown next.

**Figure 51** Address Mapping Edit

The screenshot shows a configuration window titled 'SUA/NAT' with a sub-header 'Address Mapping Rule'. The form contains the following elements:

- Type:** A dropdown menu set to 'One-to-One'.
- Local Start IP:** A text input field containing '0.0.0.0'.
- Local End IP:** A text input field containing 'N/A'.
- Global Start IP:** A text input field containing '0.0.0.0'.
- Global End IP:** A text input field containing 'N/A'.

At the bottom of the form are two buttons: 'Apply' and 'Cancel'.

The following table describes the labels in this screen.

**Table 37** Address Mapping Edit

LABEL	DESCRIPTION
Type	<p>Choose the port mapping type from one of the following.</p> <p><b>One-to-One:</b> One-to-One mode maps one local IP address to one global IP address.</p> <p><b>Many to One:</b> Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature (the SUA Only option).</p> <p><b>Many-to-Many Overload:</b> Many-to-Many Overload mode maps the multiple local IP addresses to shared global IP addresses.</p> <p><b>Many One-to-One:</b> Many-One-to-One mode maps each local IP address to a unique global IP address.</p> <p><b>Server:</b> This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.</p>
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.

**Table 37** Address Mapping Edit

LABEL	DESCRIPTION
Local End IP	This is the end Inside Local IP Address (ILA). If your rule is for all local IP addresses, then enter 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.
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.
Apply	Click <b>Apply</b> to save your changes back to the Prestige.
Cancel	Click <b>Cancel</b> to return to the previous screen and not save your changes.

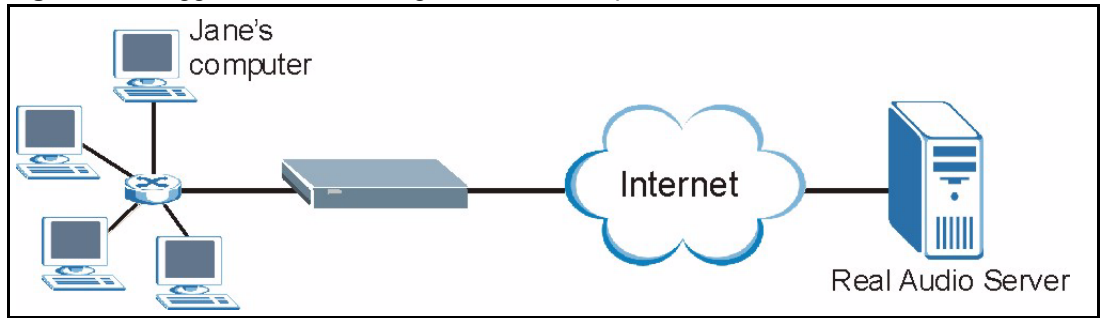
## 12.6 Trigger Port Forwarding

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address,

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The Prestige records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a "trigger" port). When the Prestige's WAN port receives a response with a specific port number and protocol ("incoming" port), the Prestige forwards the traffic to the LAN IP address of the computer that sent the request. After that computer's connection for that service closes, another computer on the LAN can use the service in the same manner. This way you do not need to configure a new IP address each time you want a different LAN computer to use the application.

### 12.6.1 Trigger Port Forwarding Example

The following is an example of trigger port forwarding.

**Figure 52** Trigger Port Forwarding Process: Example

- 1 Jane requests a file from the Real Audio server (port 7070).
- 2 Port 7070 is a “trigger” port and causes the Prestige to record Jane’s computer IP address. The Prestige associates Jane's computer IP address with the "incoming" port range of 6970-7170.
- 3 The Real Audio server responds using a port number ranging between 6970-7170.
- 4 The Prestige forwards the traffic to Jane’s computer IP address.
- 5 Only Jane can connect to the Real Audio server until the connection is closed or times out. The Prestige times out in three minutes with UDP (User Datagram Protocol), or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

## 12.6.2 Two Points To Remember About Trigger Ports

- 1 Trigger events only happen on data that is going coming from inside the Prestige and going to the outside.
- 2 If an application needs a continuous data stream, that port (range) will be tied up so that another computer on the LAN can't trigger it.

## 12.7 Configuring Trigger Port Forwarding

To change your Prestige’s trigger port settings, click **SUA/NAT** and the **Trigger Port** tab. The screen appears as shown.

**Note:** Only one LAN computer can use a trigger port (range) at a time



Figure 53 Trigger Port

SUA/NAT

SUA Server    Addr Mapping    **Trigger Port**

#	Name	Incoming		Trigger	
		Start Port	End Port	Start Port	End Port
1		0	0	0	0
2		0	0	0	0
3		0	0	0	0
4		0	0	0	0
5		0	0	0	0
6		0	0	0	0
7		0	0	0	0
8		0	0	0	0
9		0	0	0	0
10		0	0	0	0
11		0	0	0	0
12		0	0	0	0

Apply    Reset

The following table describes the labels in this screen.

Table 38 Trigger Port

LABEL	DESCRIPTION
#	This is the rule index number (read-only).
Name	Type a unique name (up to 15 characters) for identification purposes. All characters are permitted - including spaces.
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The Prestige forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the Prestige to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Apply	Click <b>Apply</b> to save your changes back to the Prestige.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.



# CHAPTER 13

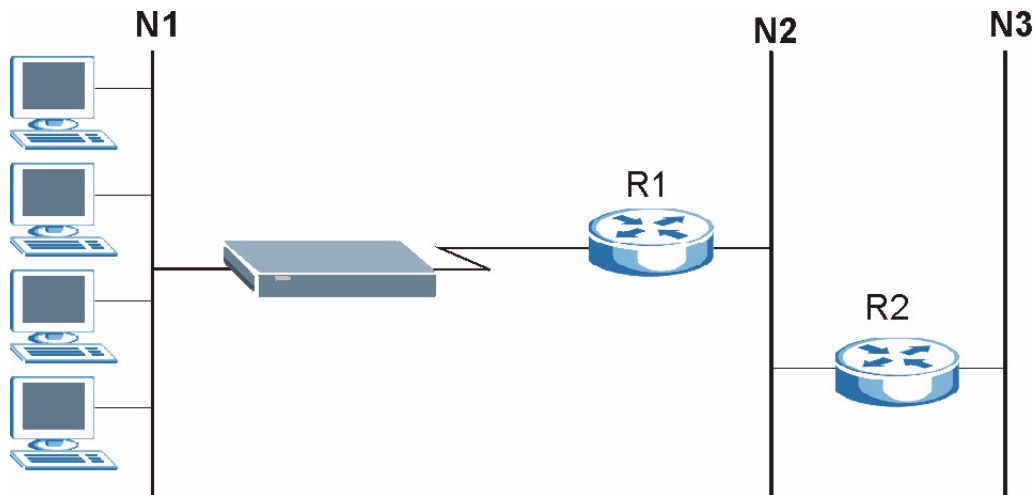
## Static Route

This chapter shows you how to configure static routes for your Prestige.

### 13.1 Static Route Overview

Each remote node specifies only the network to which the gateway is directly connected, and the Prestige has no knowledge of the networks beyond. For instance, the Prestige knows about network N2 in the following figure through remote node Router 1. However, the Prestige is unable to route a packet to network N3 because it doesn't know that there is a route through the same remote node Router 1 (via gateway Router 2). The static routes are for you to tell the Prestige about the networks beyond the remote nodes.

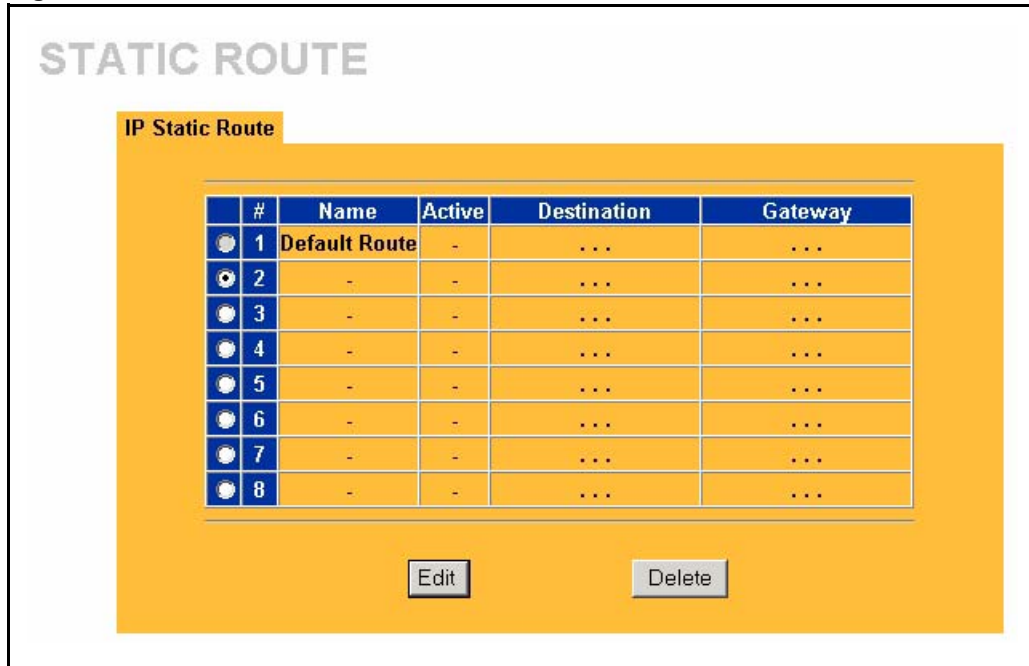
**Figure 54** Example of Static Routing Topology



### 13.2 Configuring IP Static Route

Click **STATIC ROUTE** to open the **IP Static Route** screen shown next.

**Note:** The first static route entry is the Prestige's default route and cannot be modified or deleted.

**Figure 55** IP Static Route

The following table describes the labels in this screen.

**Table 39** IP Static Route

LABEL	DESCRIPTION
#	This is the number of an individual static route.
Name	This is the name that describes or identifies this route.
Active	This field shows whether this static route is active ( <b>Yes</b> ) or not ( <b>No</b> ).
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Edit	Select the radio button next to a static route index number and then click <b>Edit</b> to set up a static route on the Prestige.
Delete	Select the radio button next to a static route index number and then click <b>Delete</b> to remove a static route on the Prestige.

### 13.2.1 Configuring a Static Route Entry

Select a static route index number and click **Edit**. The screen shown next appears. Fill in the required information for each static route.

**Figure 56** Edit IP Static Route

**STATIC ROUTE**

Route Name

Active

Destination IP Address

IP Subnet Mask

Gateway IP Address

Metric

Private

The following table describes the labels in this screen.

**Table 40** Edit IP Static Route

LABEL	DESCRIPTION
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	Enter the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Metric	Metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Private	This parameter determines if the Prestige will include this route to a remote node in its RIP broadcasts. Select this check box to keep this route private and not included in RIP broadcasts. Clear this check box to propagate this route to other hosts through RIP broadcasts.
Apply	Click <b>Apply</b> to save your changes back to the Prestige.
Cancel	Click <b>Cancel</b> to exit this screen without saving.



# CHAPTER 14

## Firewall

This chapter gives some background information on firewalls and explains how to get started with the Prestige firewall.

### 14.1 Firewall Introduction

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

#### 14.1.1 Stateful Inspection Firewall.

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also "inspect" the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency; however, they may lack the granular application level access control or caching that some proxies support. Firewalls, of one type or another, have become an integral part of standard security solutions for enterprises.

#### 14.1.2 About the Prestige Firewall

The Prestige firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated (click **FIREWALL** and then click the **Enable Firewall** check box). The Prestige's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The Prestige can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network.

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

The Prestige has one Ethernet WAN port and four Ethernet LAN ports, which are used to physically separate the network into two areas. The WAN (Wide Area Network) port attaches to the broadband (cable or DSL) modem to the Internet.

The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers will have access to Internet services such as e-mail, FTP and the World Wide Web. However, "inbound access" is not allowed (by default) unless the remote host is authorized to use a specific service.

### 14.1.3 Guidelines For Enhancing Security With Your Firewall

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

## 14.2 Firewall Settings Screen

In the navigation panel, click **FIREWALL** to open the **Settings** screen.



Figure 57 Firewall: Settings

**FIREWALL**

**Settings**   **Services**

**Enable Firewall**

**Bypass Triangle Route**

Make sure this check box is selected to have the firewall protect your LAN from Denial of Service (DoS) attacks.

1. LAN to WAN  
All traffic originating from the LAN is forwarded unless you block certain services in the Services screen. All blocked LAN-to-WAN packets are considered alerts. Packets to Log

2. WAN to LAN  
All traffic originating from the WAN is blocked unless you configure port forwarding rules, One-to-One mapping rules, Many-One-to-One mapping rules and/or allow remote management. Forwarded WAN-to-LAN packets are not considered alerts. Packets to Log

A trusted computer has full access to all blocked resources. 0.0.0.0 means there is no trusted computer.

**Trusted Computer IP Address:**

The following table describes the labels in this screen.

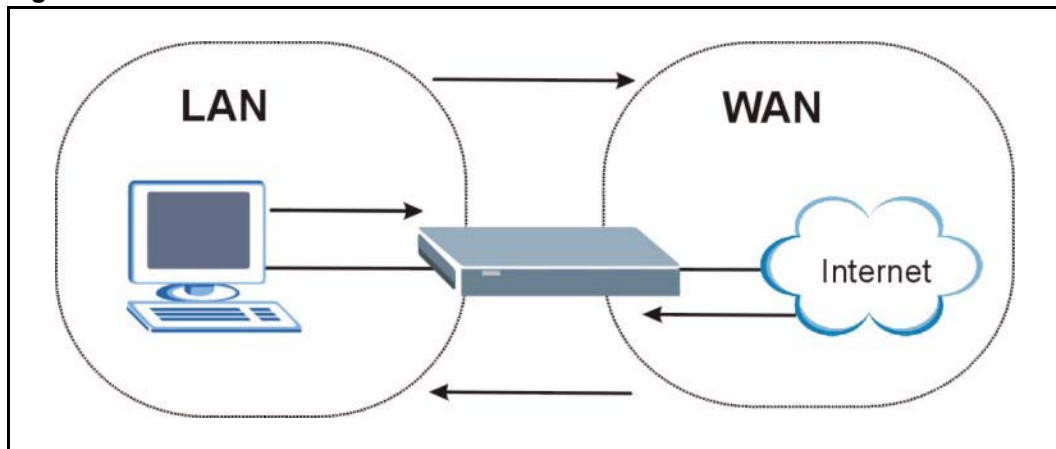
Table 41 Firewall: Settings

LABEL	DESCRIPTION
Enable Firewall	Select this check box to activate the firewall. The Prestige performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Bypass Triangle Route	Select this check box to have the Prestige firewall permit the use of triangle route topology on the network.  <b>Note:</b> Allowing triangle routes may let traffic from the WAN go directly to a LAN computer without passing through the Prestige. See the appendices for more on triangle route topology and how to deal with this problem.
LAN to WAN	To log packets related to firewall rules, make sure that <b>Access Control</b> under <b>Log</b> is selected in the <b>Logs, Log Settings</b> screen.
Packets to Log	Choose what <b>LAN to WAN</b> packets to log. Choose from: <b>No Log</b> <b>Log Blocked</b> (blocked LAN to WAN services appear in the <b>Blocked Services</b> text box in the <b>Services</b> screen (with <b>Enable Services Blocking</b> selected)) <b>Log All</b> (log all <b>LAN to WAN</b> packets)

**Table 41** Firewall: Settings

LABEL	DESCRIPTION
WAN to LAN	To log packets related to firewall rules, make sure that <b>Access Control</b> under <b>Log</b> is selected in the <b>Logs, Log Settings</b> screen.
Packets to Log	Choose what <b>WAN to LAN</b> and WAN to WAN/Prestige packets to log. Choose from: <b>No Log</b> <b>Log Forwarded</b> (see how to forward WAN to LAN traffic in the next section) <b>Log All</b> (log all <b>WAN to LAN</b> packets).
Trusted Computer IP Address	You can allow a specific computer to access all Internet resources without restriction. Enter the IP address of the trusted computer in this field.
Apply	Click <b>Apply</b> to save the settings.
Reset	Click <b>Reset</b> to start configuring this screen again.

## 14.3 The Firewall, NAT and Remote Management

**Figure 58** Firewall Rule Directions

### 14.3.1 LAN-to-WAN rules

**LAN-to-WAN** rules are local network to Internet firewall rules. The default is to forward all traffic from your local network to the Internet.

How can you block certain LAN to WAN traffic?

You may choose to block certain **LAN-to-WAN** traffic in the **Services** screen (click the **Services** tab). All services displayed in the **Blocked Services** list box are **LAN-to-WAN** firewall rules that block those services originating from the LAN.

Blocked **LAN-to-WAN** packets are considered alerts. Alerts are “higher priority logs” that include system errors, attacks and attempted access to blocked web sites. Alerts appear in red in the **View Log** screen. You may choose to have alerts e-mailed immediately in the **Log Settings** screen.

LAN-to-LAN/Prestige means the LAN to the Prestige LAN interface. This is always allowed, as this is how you manage the Prestige from your local computer.

### 14.3.2 WAN-to-LAN rules

**WAN-to-LAN** rules are Internet to your local network firewall rules. The default is to block all traffic from the Internet to your local network.

How can you forward certain WAN to LAN traffic? You may allow traffic originating from the WAN to be forwarded to the LAN by:

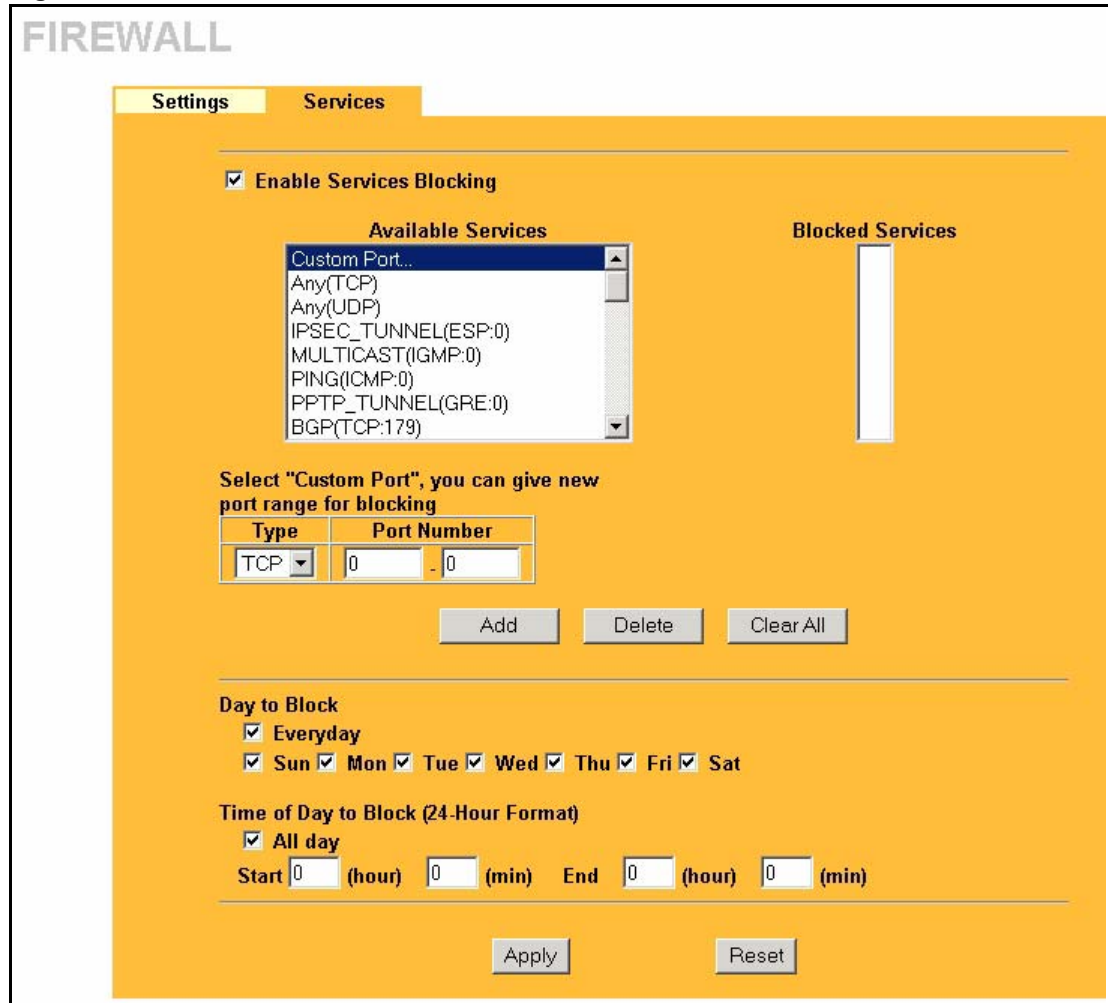
- Configuring NAT port forwarding rules in the web configurator **SUA Server** screen or SMT NAT menus.
- Configuring **One-to-One** and **Many-One-to-One** NAT mapping rules in the web configurator **Address Mapping** screen or SMT NAT menus.
- Configuring **WAN** or **LAN & WAN** access for services in the **Remote Management** screens or SMT menus. When you allow remote management from the WAN, you are actually configuring WAN-to-WAN/Prestige firewall rules. WAN-to-WAN/Prestige firewall rules are Internet to the Prestige WAN interface firewall rules. The default is to block all such traffic. When you decide what WAN-to-LAN packets to log, you are in fact deciding what **WAN-to-LAN** and WAN-to-WAN/Prestige packets to log.

Forwarded **WAN-to-LAN** packets are not considered alerts.

## 14.4 Services

Click on the **Services** tab. The screen appears as shown next. Use this screen to enable service blocking, enter/delete/modify the services you want to block and the date/time you want to block them.

**Figure 59** Firewall: Service



The following table describes the labels in this screen.

**Table 42** Firewall: Service

LABEL	DESCRIPTION
Enable Services Blocking	Select this check box to enable this feature.
Available Service	This is a list of pre-defined services (ports) you may prohibit your LAN computers from using. Select the port you want to block using the drop-down list and click <b>Add</b> to add the port to the <b>Blocked Service</b> field.
Blocked Service	This is a list of services (ports) that will be inaccessible to computers on your LAN once you enable service blocking. Choose the IP port ( <b>TCP</b> , <b>UDP</b> or <b>TCP/UDP</b> ) that defines your customized port from the drop down list box.
“Custom Port”	A custom port is a service that is not available in the pre-defined <b>Available Services</b> list and you must define using the next two fields.
Type	Services are either <b>TCP</b> and/or <b>UDP</b> . Select from either <b>TCP</b> or <b>UDP</b> .
Port Number	Enter the port number range that defines the service. For example, suppose you want to define the Gnutella service. Select TCP type and enter a port range from 6345-6349.

**Table 42** Firewall: Service

LABEL	DESCRIPTION
Add	Select a service from the <b>Available Services</b> drop-down list and then click <b>Add</b> to add a service to the Blocked Service.
Delete	Select a service from the <b>Blocked Services List</b> and then click <b>Delete</b> to remove this service from the list.
Clear All	Click <b>Clear All</b> to empty the <b>Blocked Service</b> .
Day to Block:	Select a check box to configure which days of the week (or everyday) you want the content filtering to be active.
Time of Day to Block (24-Hour Format)	Select the time of day you want service blocking to take effect. Configure blocking to take effect all day by selecting the <b>All Day</b> check box. You can also configure specific times that by entering the start time in the <b>Start (hr)</b> and <b>Start (min)</b> fields and the end time in the <b>End (hr)</b> and <b>End (min)</b> fields. Enter times in 24-hour format, for example, "3:00pm" should be entered as "15:00".
Apply	Click <b>Apply</b> to save the settings.
Reset	Click <b>Reset</b> to start configuring this screen again.



# CHAPTER 15

## Content Filtering

This chapter covers how to configure content filtering.

### 15.1 Introduction to Content Filtering

Internet content filtering allows you to create and enforce Internet access policies tailored to their needs. Content filtering is the ability to block certain web features or specific URL keywords and should not be confused with packet filtering via SMT menu 21.1. To access these functions, click **Content Filter** in the navigation panel.

### 15.2 Restrict Web Features

The Prestige can block web features such as ActiveX controls, Java applets, cookies and disable web proxies.

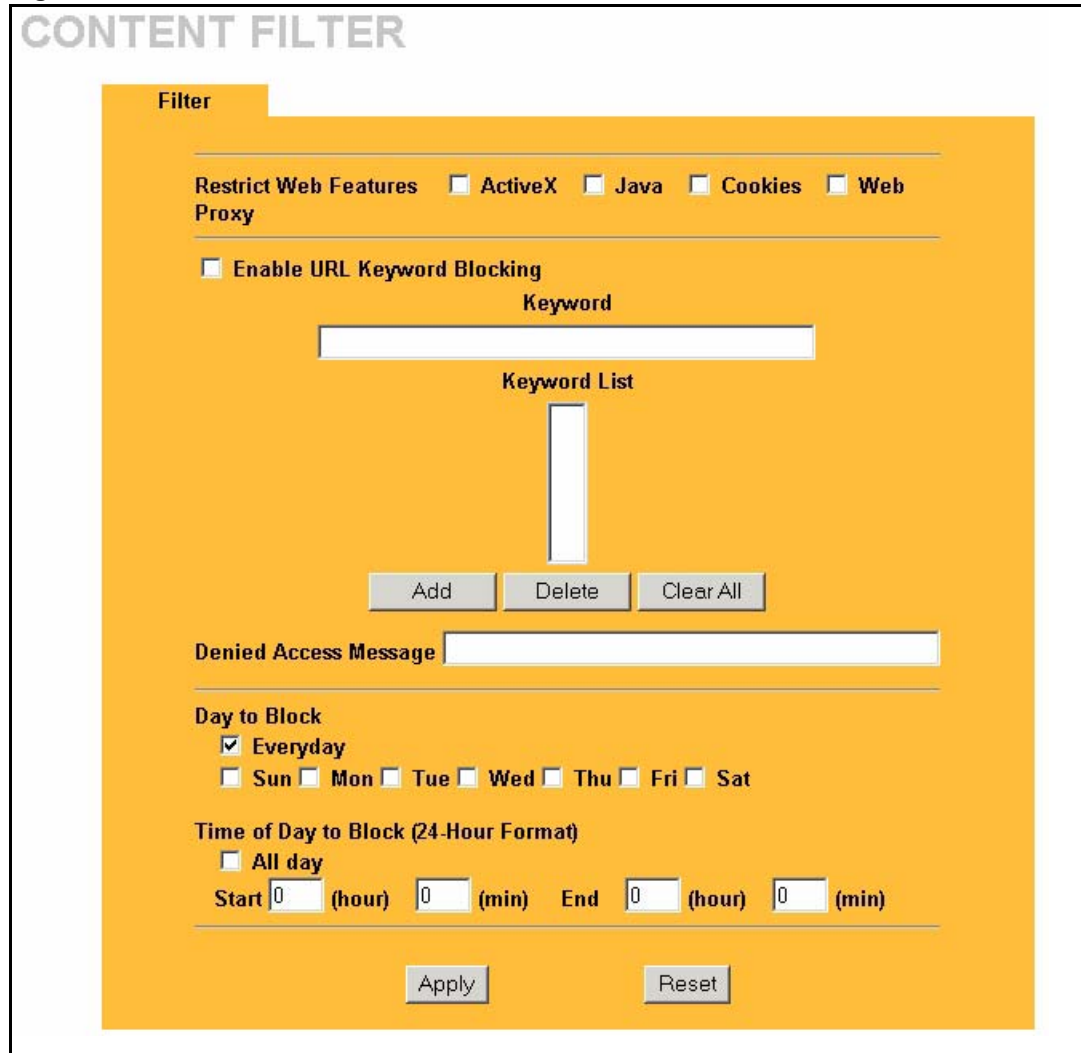
### 15.3 Days and Times

The Prestige also allows you to define time periods and days during which the Prestige performs content filtering.

### 15.4 Configure Content Filtering

Click **Content Filter** on the navigation panel, to open the following screen.

**Figure 60** Content Filter



The following table describes the labels in this screen.

**Table 43** Content Filter

LABEL	DESCRIPTION
Restrict Web Features	Select the box(es) to restrict a feature. When you download a page containing a restricted feature, that part of the web page will appear blank or grayed out.
ActiveX	A tool for building dynamic and active Web pages and distributed object applications. When you visit an ActiveX Web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again.
Java	A programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds.
Cookies	Used by Web servers to track usage and provide service based on ID.
Web Proxy	A server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server.



**Table 43** Content Filter

LABEL	DESCRIPTION
Enable URL Keyword Blocking	The Prestige can block Web sites with URLs that contain certain keywords in the domain name or IP address. For example, if the keyword "bad" was enabled, all sites containing this keyword in the domain name or IP address will be blocked, e.g., URL http://www.website.com/bad.html would be blocked. Select this check box to enable this feature.
Keyword	Type a keyword in this field. You may use any character (up to 64 characters). Wildcards are not allowed. You can also enter a numerical IP address.
Keyword List	This list displays the keywords already added.
Add	Click <b>Add</b> after you have typed a keyword. Repeat this procedure to add other keywords. Up to 64 keywords are allowed. When you try to access a web page containing a keyword, you will get a message telling you that the content filter is blocking this request.
Delete	Highlight a keyword in the lower box and click <b>Delete</b> to remove it. The keyword disappears from the text box after you click <b>Apply</b> .
Clear All	Click this button to remove all of the listed keywords.
Denied Access Message	Enter a message to be displayed when the Prestige's content filter feature blocks a user's access to a web site.
Day to Block	Select check boxes for the days that you want the Prestige to perform content filtering. Select the <b>Everyday</b> check box to have content filtering turned on all days of the week.
Time of Day to Block	Time of Day to Block allows the administrator to define during which time periods content filtering is enabled. Time of Day to Block restrictions only apply to the keywords (see above). Restrict web server data, such as ActiveX, Java, Cookies and Web Proxy are not affected. Enter the time period, in 24-hour format, during which content filtering will be enforced. Select the <b>All Day</b> check box to have content filtering always active on the days selected in <b>Day to Block</b> with time of day limitations not enforced.
Apply	Click <b>Apply</b> to save your changes.
Reset	Click <b>Reset</b> to begin configuring this screen afresh



# CHAPTER 16

## Remote Management Screens

This chapter provides information on the **Remote Management** screens.

### 16.1 Remote Management Overview

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

You may manage your Prestige from a remote location via:

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

To disable remote management of a service, select **Disable** in the corresponding **Server Access** field.

You may only have one remote management session running at a time. The Prestige automatically disconnects a remote management session of lower priority when another remote management session of higher priority starts. The priorities for the different types of remote management sessions are as follows.

- 1 Telnet
- 2 HTTP

#### 16.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

- 1 A filter in SMT menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
- 2 You have disabled that service in one of the remote management screens.
- 3 The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the Prestige will disconnect the session immediately.
- 4 There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.

## 16.1.2 Remote Management and NAT

When NAT is enabled:

- Use the Prestige's WAN IP address when configuring from the WAN.
- Use the Prestige's LAN IP address when configuring from the LAN.

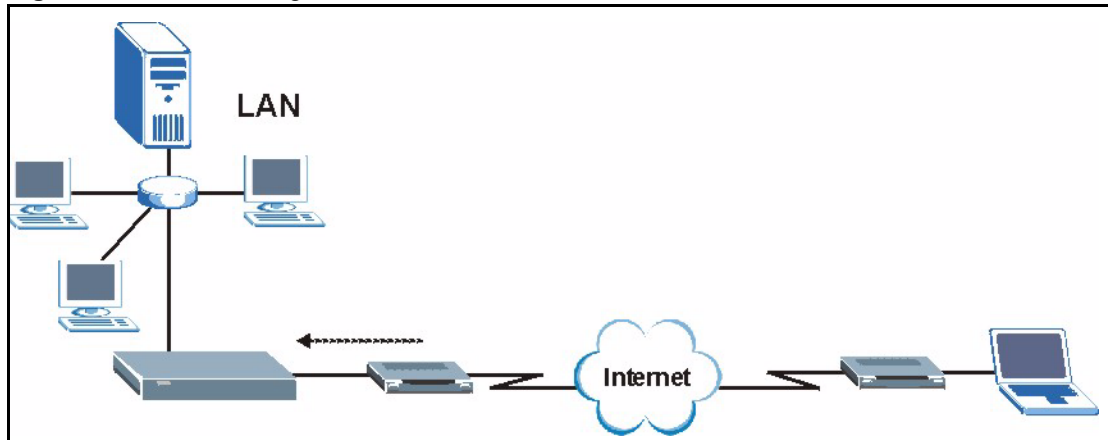
## 16.1.3 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The Prestige automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling. You can change the timeout period in the **SYSTEM General** screen.

## 16.2 Configuring Telnet

You can configure your Prestige for remote Telnet access as shown next. The administrator uses Telnet from a computer on a remote network to access the Prestige.

**Figure 61** Telnet Configuration on a TCP/IP Network



## 16.3 Configuring TELNET

Click **REMOTE MGMT** and the **TELNET** tab to display the screen as shown.

**Figure 62** Remote Management: Telnet

The following table describes the labels in this screen.

**Table 44** Remote Management: Telnet

LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the Prestige using this service.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the Prestige using this service. Select <b>All</b> to allow any computer to access the Prestige using this service. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the Prestige using this service.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 16.4 Configuring FTP

You can upload and download the Prestige’s firmware and configuration files using FTP, please see the chapter on firmware and configuration file maintenance for details. To use this feature, your computer must have an FTP client.

To change your Prestige’s FTP settings, click **REMOTE MGMT**, then the **FTP** tab. The screen appears as shown.

**Figure 63** Remote Management: FTP

The following table describes the labels in this screen.

**Table 45** Remote Management: FTP

LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the Prestige using this service.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the Prestige using this service. Select <b>All</b> to allow any computer to access the Prestige using this service. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the Prestige using this service.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 16.5 Configuring WWW

To change your Prestige’s remote HTTP access settings, click **REMOTE MGMT** to display the **WWW** screen.

**Figure 64** Remote Management: WWW

The following table describes the labels in this screen.

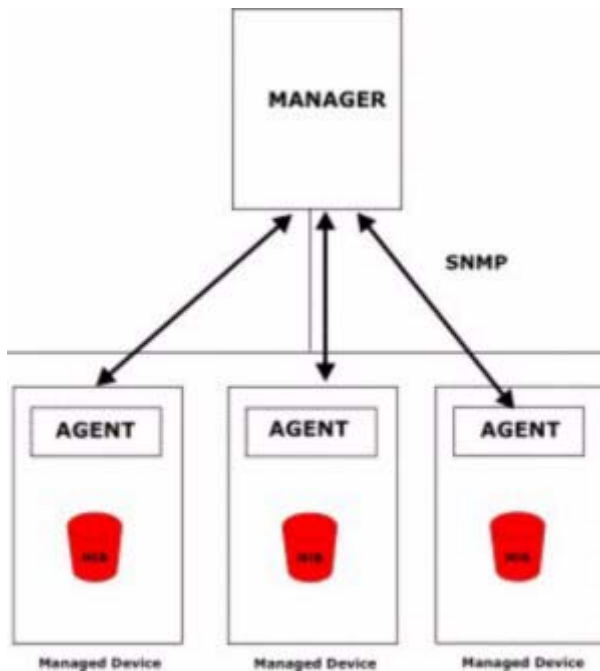
**Table 46** Remote Management: WWW

LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the Prestige using this service.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the Prestige using this service. Select <b>All</b> to allow any computer to access the Prestige using this service. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the Prestige using this service.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 16.6 SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your Prestige supports SNMP agent functionality, which allows a manager station to manage and monitor the Prestige through the network. The Prestige supports SNMP version one (SNMPv1) and version two (SNMPv2). The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

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

**Figure 65** SNMP Management Model

An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the Prestige). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

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

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.



## 16.6.1 Supported MIBs

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

## 16.6.2 SNMP Traps

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

**Table 47** SNMPv1 Traps

TRAP #	TRAP NAME	DESCRIPTION
0	coldStart (defined in <i>RFC-1215</i> )	A trap is sent after booting (power on).
1	warmStart (defined in <i>RFC-1215</i> )	A trap is sent after booting (software reboot).
4	authenticationFailure (defined in <i>RFC-1215</i> )	A trap is sent to the manager when receiving any SNMP get or set requirements with the wrong community (password).
6	whyReboot (defined in ZYXEL-MIB)	A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start).
6a	For intentional reboot :	A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (for example, download new files, CLI command "sys reboot", etc.).
6b	For fatal error :	A trap is sent with the message of the fatal code if the system reboots because of fatal errors.

**Table 48** SNMPv2 Traps

TRAP NAME	OBJECT IDENTIFIER # (OID)	DESCRIPTION
Generic Traps		
coldStart	1.3.6.1.6.3.1.1.5.1	This trap is sent after booting (power on). This trap is defined in RFC-1215.
warmStart	1.3.6.1.6.3.1.1.5.2	This trap is sent after booting (software reboot). This trap is defined in RFC-1215.
linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
authenticationFailure (defined in <i>RFC-1215</i> )	1.3.6.1.6.3.1.1.5.5	The device sends this trap when it receives any SNMP get or set requirements with the wrong community (password). Note: snmpEnableAuthenTraps, OID 1.3.6.1.2.1.11.30 (defined in RFC 1214 and RFC 1907) must be enabled on in order for the device to send authenticationFailure traps. Use a MIB browser to enable or disable snmpEnableAuthenTraps.

**Table 48** SNMPv2 Traps

TRAP NAME	OBJECT IDENTIFIER # (OID)	DESCRIPTION
Traps defined in the ZyXEL Private MIB.		
whyReboot	1.3.6.1.4.1.890.1.5.13.0.1	This trap is sent with the reason for restarting before the system reboots (warm start). "System reboot by user!" is added for an intentional reboot (for example, download new files, CLI command "sys reboot"). If the system reboots because of fatal errors, a code for the error is listed.

Some traps include an SNMP interface index. The following table maps the SNMP interface indexes to the G-1000's physical ports.

**Table 49** SNMP Interface Index to Physical Port Mapping

INTERFACE TYPE	PHYSICAL PORT
enet0	WLAN
enet1	Ethernet port

### 16.6.3 Configuring SNMP

To change your Prestige's SNMP settings, click **REMOTE MGMT**, then the **SNMP** tab. The screen appears as shown.

**Figure 66** Remote Management: SNMP

The following table describes the labels in this screen.

**Table 50** Remote Management: SNMP

LABEL	DESCRIPTION
SNMP Configuration	
Get Community	Enter the <b>Get Community</b> , which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the <b>Set community</b> , which is the password for incoming Set requests from the management station. The default is public and allows all requests.
Trap	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Destination	Type the IP address of the station to send your SNMP traps to.
SNMP	
Service Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Service Access	Select the interface(s) through which a computer may access the Prestige using this service.

**Table 50** Remote Management: SNMP

LABEL	DESCRIPTION
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the Prestige using this service. Select <b>All</b> to allow any computer to access the Prestige using this service. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to access the Prestige using this service.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 16.7 Configuring DNS

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa. See [Section 4.3.2 on page 63](#) for background information.

To change your Prestige’s DNS settings, click **REMOTE MGMT**, then the **DNS** tab. The screen appears as shown.

**Figure 67** Remote Management: DNS

The following table describes the labels in this screen.

**Table 51** Remote Management: DNS

LABEL	DESCRIPTION
Server Port	The DNS service port number is 53 and cannot be changed here.
Server Access	Select the interface(s) through which a computer may send DNS queries to the Prestige.

**Table 51** Remote Management: DNS

LABEL	DESCRIPTION
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to send DNS queries to the Prestige. Select <b>All</b> to allow any computer to send DNS queries to the Prestige. Choose <b>Selected</b> to just allow the computer with the IP address that you specify to send DNS queries to the Prestige.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 16.8 Configuring Security

To change your Prestige’s security settings, click **REMOTE MGMT**, then the **Security** tab. The screen appears as shown.

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

**Figure 68** Security

The screenshot shows the 'REMOTE MANAGEMENT' interface with the 'Security' tab selected. The 'ICMP' section is visible, containing a 'Respond to Ping on' dropdown menu set to 'LAN & WAN' and an unchecked checkbox for 'Do not respond to requests for unauthorized services'. 'Apply' and 'Reset' buttons are located at the bottom of the configuration area.

The following table describes the labels in this screen.

**Table 52** Security

LABEL	DESCRIPTION
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.
Respond to Ping on	The Prestige will not respond to any incoming Ping requests when <b>Disable</b> is selected. Select <b>LAN</b> to reply to incoming LAN Ping requests. Select <b>WAN</b> to reply to incoming WAN Ping requests. Otherwise select <b>LAN &amp; WAN</b> to reply to both incoming LAN and WAN Ping requests.
Do not respond to requests for unauthorized services	Select this option to prevent hackers from finding the Prestige by probing for unused ports. If you select this option, the Prestige will not respond to port request(s) for unused ports, thus leaving the unused ports and the Prestige unseen. By default this option is not selected and the Prestige will reply with an ICMP Port Unreachable packet for a port probe on its unused UDP ports, and a TCP Reset packet for a port probe on its unused TCP ports.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

# CHAPTER 17

## Universal Plug-and-Play (UPnP)

This chapter introduces the UPnP feature in the web configurator.

### 17.1 Introducing Universal Plug and Play

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

#### 17.1.1 How do I know if I'm using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network will appear as a separate icon. Selecting the icon of a UPnP device will allow you to access the information and properties of that device.

#### 17.1.2 NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices and enable exchange of simple product and service descriptions. NAT traversal allows the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

See [Chapter 12 on page 128](#) chapter for further information about NAT.

#### 17.1.3 Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports may present network security issues. Network information and configuration may also be obtained and modified by users in some network environments.

All UPnP-enabled devices may communicate freely with each other without additional configuration. Disable UPnP if this is not your intention.

## 17.2 UPnP and ZyXEL

ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum Creates UPnP™ Implementors Corp. (UIC). ZyXEL's UPnP implementation supports IGD 1.0 (Internet Gateway Device). At the time of writing ZyXEL's UPnP implementation supports Windows Messenger 4.6 and 4.7 while Windows Messenger 5.0 and Xbox are still being tested.

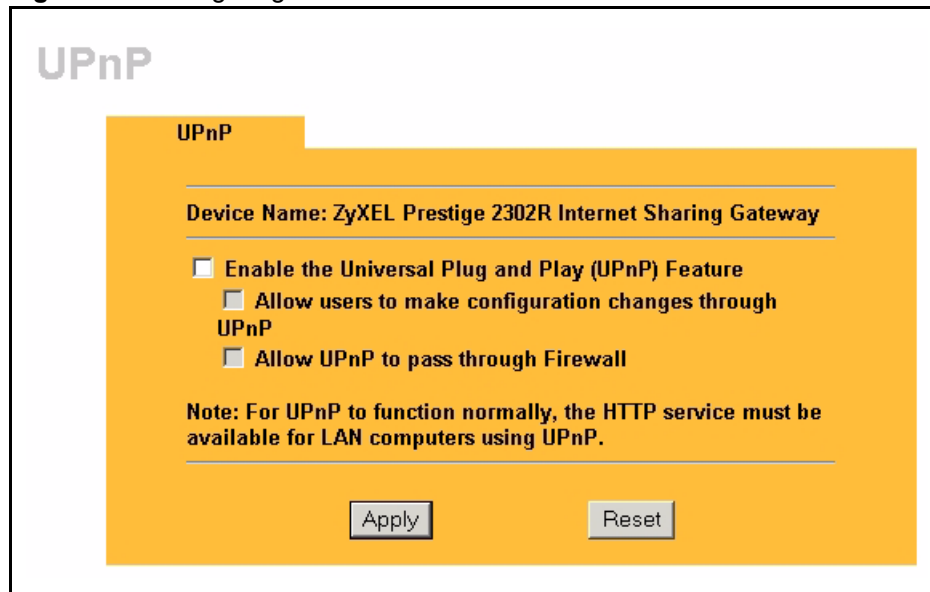
The Prestige only sends UPnP multicasts to the LAN.

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

### 17.2.1 Configuring UPnP

Click **UPnP** in the navigation panel to display the screen shown next.

**Figure 69** Configuring UPnP



The following table describes the fields in this screen.



**Table 53** Configuring UPnP

LABEL	DESCRIPTION
Device Name	This identifies your device in UPnP applications.
Enable the Universal Plug and Play (UPnP) Service	Select this checkbox to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the Prestige's IP address (although you must still enter the password to access the web configurator).
Allow users to make configuration changes through UPnP	Select this check box to allow UPnP-enabled applications to automatically configure the Prestige so that they can communicate through the Prestige, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.
Allow UPnP to pass through Firewall	Select this check box to allow traffic from UPnP-enabled applications to bypass the firewall. Clear this check box to have the firewall block all UPnP application packets (for example, MSN packets).
Apply	Click <b>Apply</b> to save the setting to the Prestige.
Cancel	Click <b>Cancel</b> to return to the previously saved settings.

## 17.3 Installing UPnP in Windows Example

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

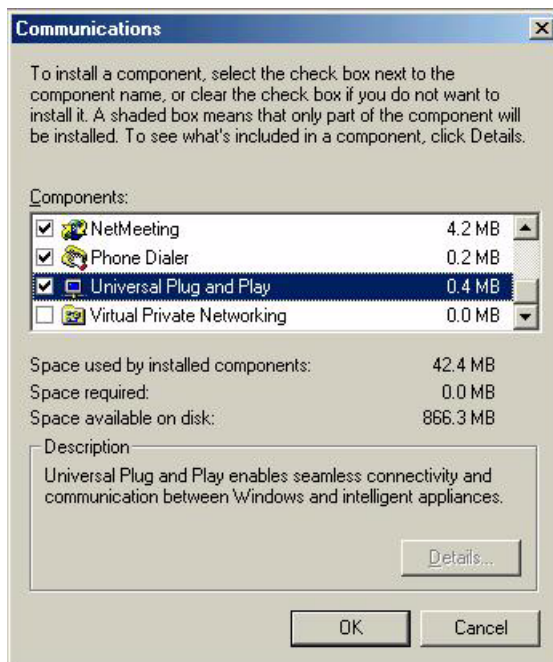
### 17.3.1 Installing UPnP in Windows Me

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

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

**Figure 70** Add/Remove Programs: Windows Setup: Communication

- 3 In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.

**Figure 71** Add/Remove Programs: Windows Setup: Communication: Components

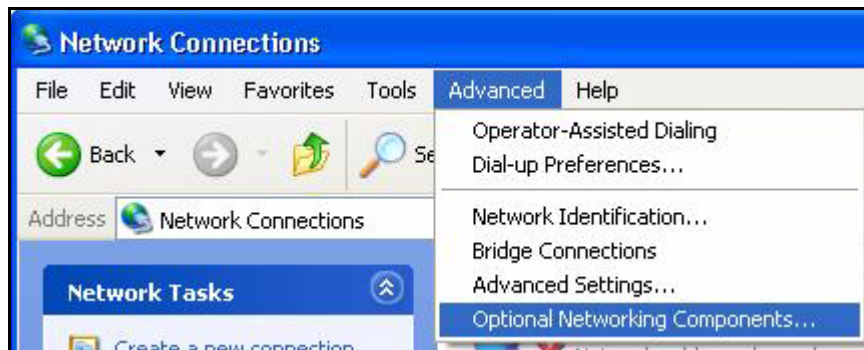
- 4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.
- 5 Restart the computer when prompted.

## 17.3.2 Installing UPnP in Windows XP

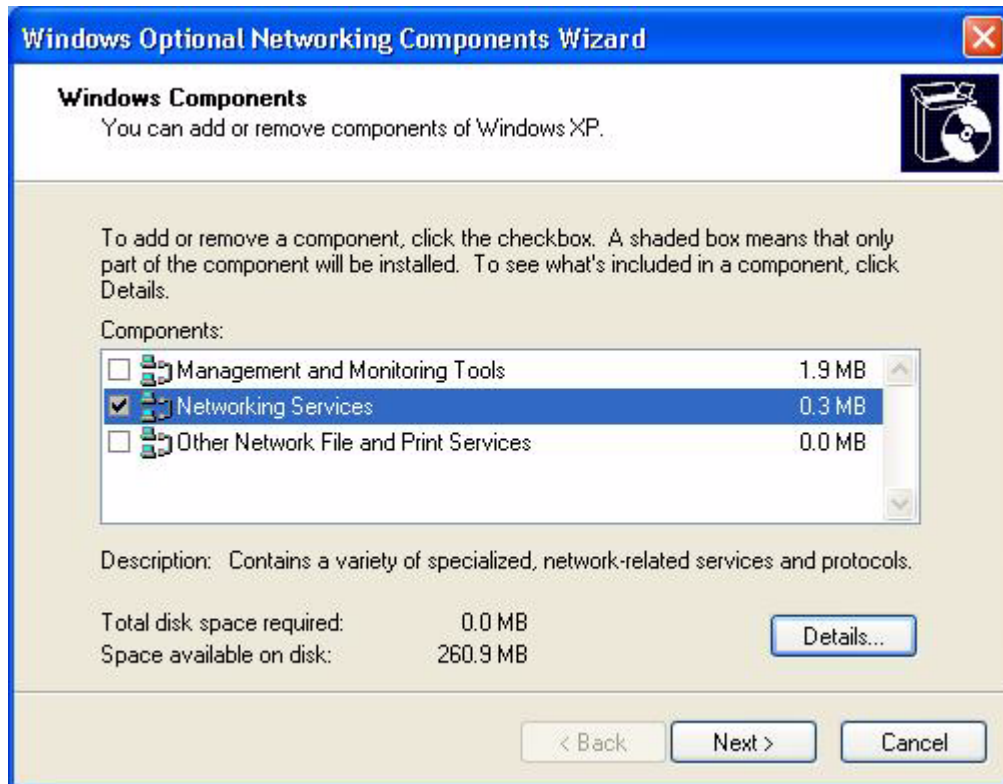
Follow the steps below to install the UPnP in Windows XP.

- 1 Click **Start** and **Control Panel**.
- 2 Double-click **Network Connections**.
- 3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ....**

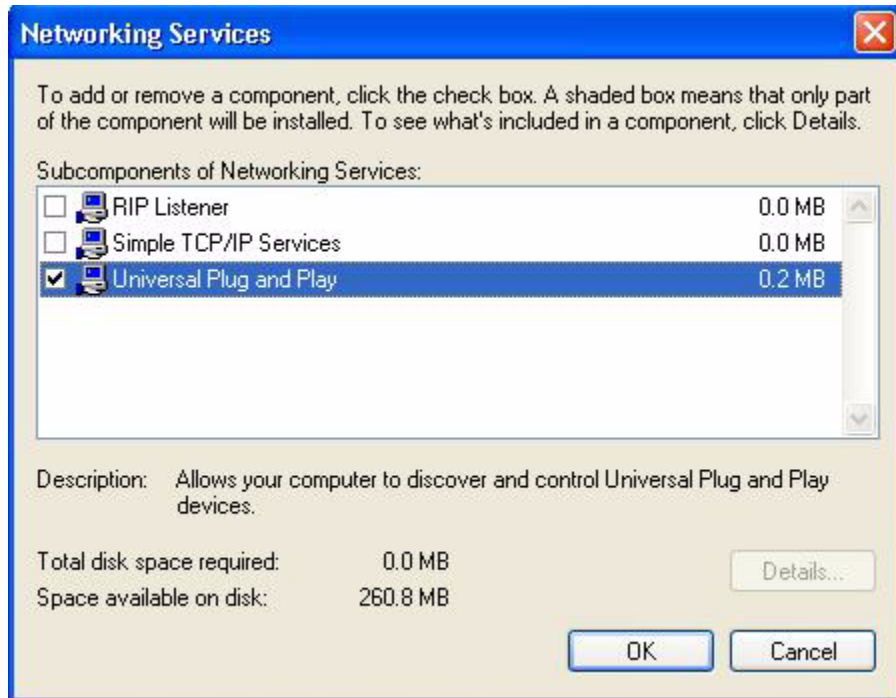
**Figure 72** Network Connections



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

**Figure 73** Windows Optional Networking Components Wizard

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

**Figure 74** Networking Services

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

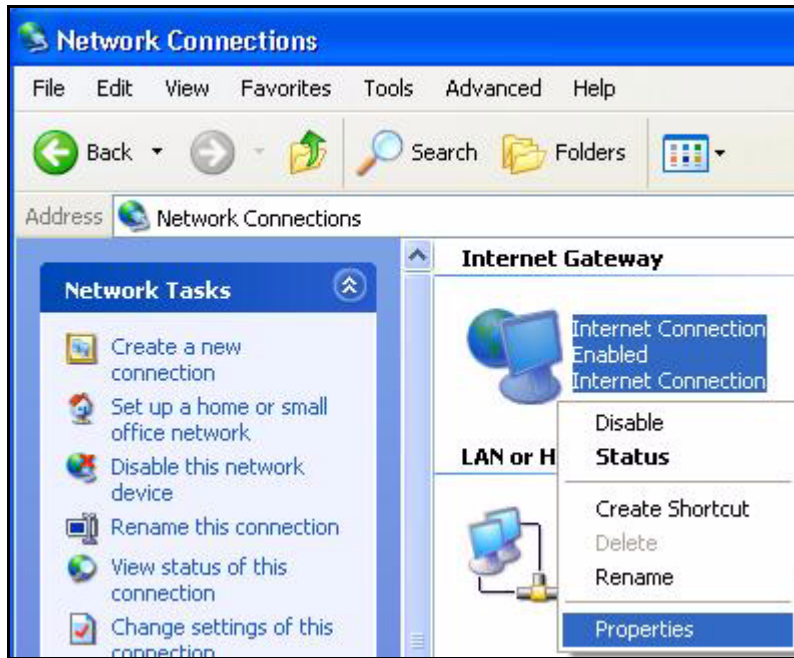
## 17.4 Using UPnP in Windows XP Example

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

Make sure the computer is connected to a LAN port of the Prestige. Turn on your computer and the Prestige.

### 17.4.1 Auto-discover Your UPnP-enabled Network Device

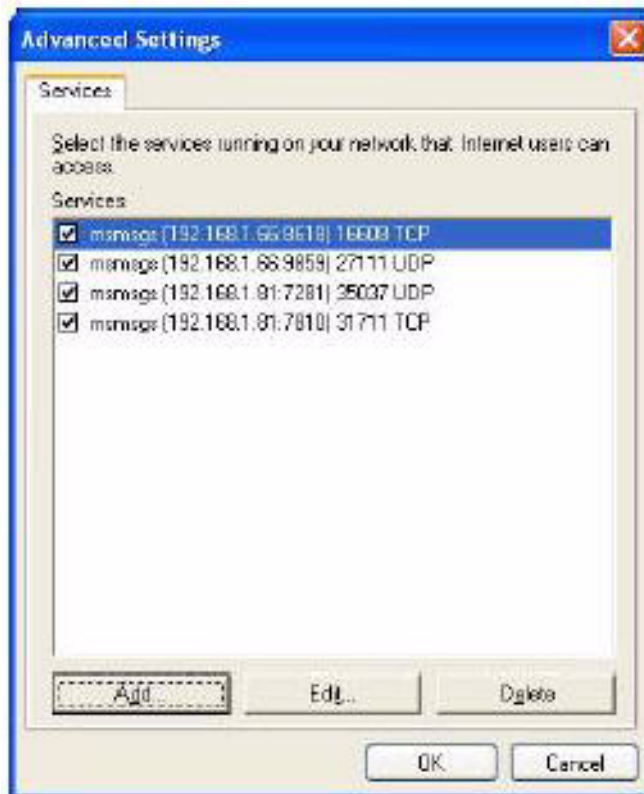
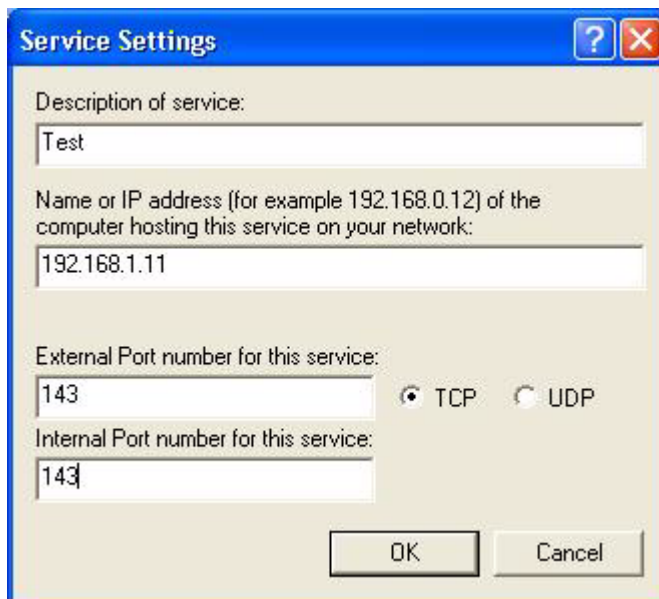
- 1** Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.
- 2** Right-click the icon and select **Properties**.

**Figure 75** Network Connections

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

**Figure 76** Internet Connection Properties

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

**Figure 77** Internet Connection Properties: Advanced Settings**Figure 78** Internet Connection Properties: Advanced Settings: Add

- 5** When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.
- 6** Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.



**Figure 79** System Tray Icon

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

**Figure 80** Internet Connection Status

## 17.4.2 Web Configurator Easy Access

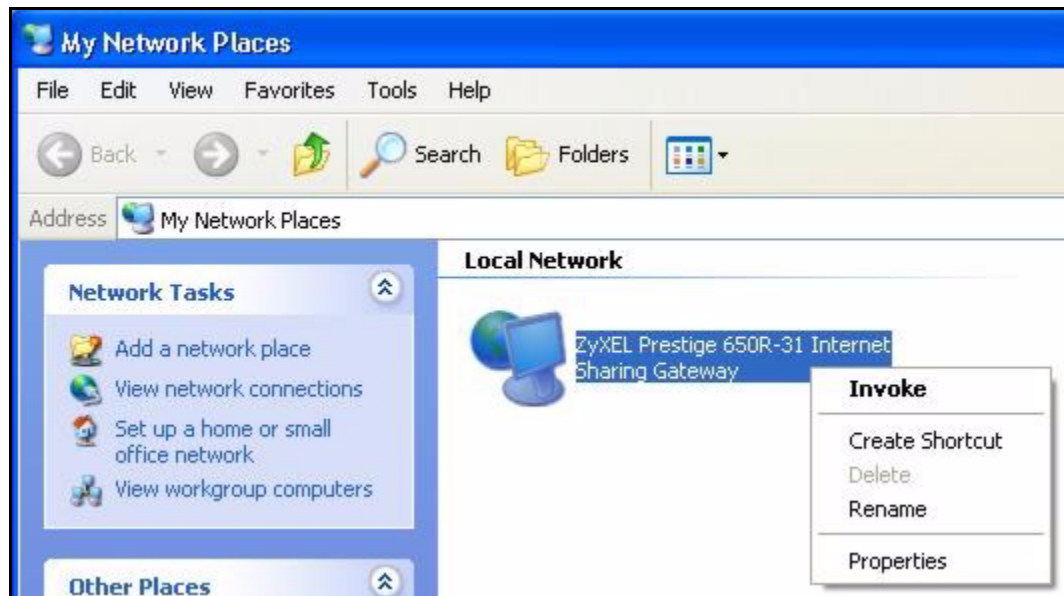
With UPnP, you can access the web-based configurator on the Prestige without finding out the IP address of the Prestige first. This comes helpful if you do not know the IP address of the Prestige.

Follow the steps below to access the web configurator.

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

**Figure 81** Network Connections

- 4 An icon with the description for each UPnP-enabled device displays under **Local Network**.
- 5 Right-click on the icon for your Prestige and select **Invoke**. The web configurator login screen displays.

**Figure 82** Network Connections: My Network Places

- 6 Right-click on the icon for your Prestige and select **Properties**. A properties window displays with basic information about the Prestige.

**Figure 83** Network Connections: My Network Places: Properties: Example



# CHAPTER 18

## Logs

This chapter contains information about configuring general log settings and viewing the logs.

### 18.1 Configuring View Log

The web configurator allows you to look at all of the logs in one location.

Click **LOGS** to open the **View Log** screen. The **View Log** screen displays logs for the categories that you selected in the **Log Settings** screen (see [Figure 85 on page 196](#)).

You can view logs and alert messages in this screen. Log entries in red indicate alerts. Once the log table is full, old logs are deleted as new logs are created.

Click a column heading to sort the entries. A triangle indicates the direction of the sort order.

**Figure 84** View Log

The screenshot shows the 'View Log' screen with a yellow header and a table of log entries. The table has the following data:

#	Time ▲	Message	Source	Destination	Notes
1	01/01/2000 00:30:19	Packet Trigger: Protocol=1, Data=Packet Trigger: Protocol=1, Dat			PACKET TRIGGER
2	01/01/2000 00:30:19	board 0 line 0 channel 0, call 50, C01 Outgoing Call dev=6 ch=0			CALL DETAIL RECORD
3	01/01/2000 00:29:49	Packet Trigger: Protocol=1, Data=Packet Trigger: Protocol=1, Dat			PACKET TRIGGER
4	01/01/2000 00:29:49	board 0 line 0 channel 0, call 49, C01 Outgoing Call dev=6 ch=0			CALL DETAIL RECORD
5	01/01/2000 00:29:18	board 0 line 0 channel 0, call 48, C01 Outgoing Call dev=6 ch=0			CALL DETAIL RECORD
6	01/01/2000 00:28:48	Packet Trigger: Protocol=1, Data=Packet Trigger: Protocol=1, Dat			PACKET TRIGGER

The following table describes the labels in this screen.

**Table 54** View Log

LABEL	DESCRIPTION
Display	Select a log category from the drop down list box to display logs within the selected category. To view all logs, select <b>All Logs</b> . The number of categories shown in the drop down list box depends on the selection in the <b>Log Settings</b> page.
Email Log Now	Click <b>Email Log Now</b> to send the log screen to the e-mail address specified in the <b>Log Settings</b> page.
Refresh	Click <b>Refresh</b> to renew the log screen.
Clear Log	Click <b>Clear Log</b> to clear all the logs.
Time	This field displays the time the log was recorded.
Message	This field states the reason for the log.
Source	This field lists the source IP address and the port number of the incoming packet.
Destination	This field lists the destination IP address and the port number of the incoming packet.
Notes	This field displays additional information about the log entry.

### 18.1.1 Log Message Descriptions

The following tables provide descriptions of example log messages.

**Table 55** System Error Logs

LOG MESSAGE	DESCRIPTION
WAN connection is down.	The WAN connection is down. You cannot access the network through this interface.
%s exceeds the max. number of session per host!	This attempt to create a NAT session exceeds the maximum number of NAT session table entries allowed to be created per host.

**Table 56** System Maintenance Logs

LOG MESSAGE	DESCRIPTION
Time calibration is successful	The device has adjusted its time based on information from the time server.
Time calibration failed	The device failed to get information from the time server.
WAN interface gets IP: %s	The WAN interface got a new IP address from the DHCP or PPPoE server.
DHCP client gets %s	A DHCP client got a new IP address from the DHCP server.
DHCP client IP expired	A DHCP client's IP address has expired.
DHCP server assigns %s	The DHCP server assigned an IP address to a client.

**Table 56** System Maintenance Logs (continued)

LOG MESSAGE	DESCRIPTION
Successful WEB login	Someone has logged on to the device's web configurator interface.
WEB login failed	Someone has failed to log on to the device's web configurator interface.
TELNET Login Successfully	Someone has logged on to the router via telnet.
TELNET Login Fail	Someone has failed to log on to the router via telnet.
Successful FTP login	Someone has logged on to the device via ftp.
FTP login failed	Someone has failed to log on to the device via ftp.
NAT Session Table is Full!	The maximum number of NAT session table entries has been exceeded and the table is full.
Time initialized by Daytime Server	The device got the time and date from the Daytime server.
Time initialized by Time server	The device got the time and date from the time server.
Time initialized by NTP server	The device got the time and date from the NTP server.
Connect to Daytime server fail	The device was not able to connect to the Daytime server.
Connect to Time server fail	The device was not able to connect to the Time server.
Connect to NTP server fail	The device was not able to connect to the NTP server.
Too large ICMP packet has been dropped	The device dropped an ICMP packet that was too large.
Configuration Change: PC = 0x%x, Task ID = 0x%x	The device is saving configuration changes.

**Table 57** Access Control Logs

LOG MESSAGE	DESCRIPTION
Firewall default policy: [ TCP   UDP   IGMP   ESP   GRE   OSPF ] <Packet Direction>	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched the default policy and was blocked or forwarded according to the default policy's setting.
Firewall rule [NOT] match:[ TCP   UDP   IGMP   ESP   GRE   OSPF ] <Packet Direction>, <rule:%d>	Attempted TCP/UDP/IGMP/ESP/GRE/OSPF access matched (or did not match) a configured firewall rule (denoted by its number) and was blocked or forwarded according to the rule.
Triangle route packet forwarded: [ TCP   UDP   IGMP   ESP   GRE   OSPF ]	The firewall allowed a triangle route session to pass through.
Packet without a NAT table entry blocked: [ TCP   UDP   IGMP   ESP   GRE   OSPF ]	The router blocked a packet that didn't have a corresponding NAT table entry.
Router sent blocked web site message: TCP	The router sent a message to notify a user that the router blocked access to a web site that the user requested.

**Table 57** Access Control Logs (continued)

LOG MESSAGE	DESCRIPTION
Exceed maximum sessions per host (%d).	The device blocked a session because the host's connections exceeded the maximum sessions per host.
Firewall allowed a packet that matched a NAT session: [ TCP   UDP ]	A packet from the WAN (TCP or UDP) matched a cone NAT session and the device forwarded it to the LAN.

**Table 58** TCP Reset Logs

LOG MESSAGE	DESCRIPTION
Under SYN flood attack, sent TCP RST	The router sent a TCP reset packet when a host was under a SYN flood attack (the TCP incomplete count is per destination host.)
Exceed TCP MAX incomplete, sent TCP RST	The router sent a TCP reset packet when the number of TCP incomplete connections exceeded the user configured threshold. (the TCP incomplete count is per destination host.)
Peer TCP state out of order, sent TCP RST	The router sent a TCP reset packet when a TCP connection state was out of order. Note: The firewall refers to RFC793 Figure 6 to check the TCP state.
Firewall session time out, sent TCP RST	The router sent a TCP reset packet when a dynamic firewall session timed out. The default timeout values are as follows: ICMP idle timeout: 3 minutes UDP idle timeout: 3 minutes TCP connection (three way handshaking) timeout: 270 seconds TCP FIN-wait timeout: 2 MSL (Maximum Segment Lifetime set in the TCP header). TCP idle (established) timeout (s): 150 minutes TCP reset timeout: 10 seconds
Exceed MAX incomplete, sent TCP RST	The router sent a TCP reset packet when the number of incomplete connections (TCP and UDP) exceeded the user-configured threshold. (Incomplete count is for all TCP and UDP connections through the firewall.) Note: When the number of incomplete connections (TCP + UDP) > "Maximum Incomplete High", the router sends TCP RST packets for TCP connections and destroys TOS (firewall dynamic sessions) until incomplete connections < "Maximum Incomplete Low".
Access block, sent TCP RST	The router sends a TCP RST packet and generates this log if you turn on the firewall TCP reset mechanism (via CLI command: <code>sys firewall tcprst</code> ).

**Table 59** Packet Filter Logs

LOG MESSAGE	DESCRIPTION
[ TCP   UDP   ICMP   IGMP   Generic ] packet filter matched (set: %d, rule: %d)	Attempted access matched a configured filter rule (denoted by its set and rule number) and was blocked or forwarded according to the rule.



For type and code details, see [Table 67 on page 191](#).

**Table 60** ICMP Logs

LOG MESSAGE	DESCRIPTION
Firewall default policy: ICMP <Packet Direction>, <type:%d>, <code:%d>	ICMP access matched the default policy and was blocked or forwarded according to the user's setting.
Firewall rule [NOT] match: ICMP <Packet Direction>, <rule:%d>, <type:%d>, <code:%d>	ICMP access matched (or didn't match) a firewall rule (denoted by its number) and was blocked or forwarded according to the rule.
Triangle route packet forwarded: ICMP	The firewall allowed a triangle route session to pass through.
Packet without a NAT table entry blocked: ICMP	The router blocked a packet that didn't have a corresponding NAT table entry.
Unsupported/out-of-order ICMP: ICMP	The firewall does not support this kind of ICMP packets or the ICMP packets are out of order.
Router reply ICMP packet: ICMP	The router sent an ICMP reply packet to the sender.

**Table 61** CDR Logs

LOG MESSAGE	DESCRIPTION
board %d line %d channel %d, call %d, %s C01 Outgoing Call dev=%x ch=%x %s	The router received the setup requirements for a call. "call" is the reference (count) number of the call. "dev" is the device type (3 is for dial-up, 6 is for PPPoE). "channel" or "ch" is the call channel ID. For example, "board 0 line 0 channel 0, call 3, C01 Outgoing Call dev=6 ch=0" Means the router has dialed to the PPPoE server 3 times.
board %d line %d channel %d, call %d, %s C02 OutCall Connected %d %s	The PPPoE or dial-up call is connected.
board %d line %d channel %d, call %d, %s C02 Call Terminated	The PPPoE or dial-up call was disconnected.

**Table 62** PPP Logs

LOG MESSAGE	DESCRIPTION
ppp:LCP Starting	The PPP connection's Link Control Protocol stage has started.
ppp:LCP Opening	The PPP connection's Link Control Protocol stage is opening.
ppp:CHAP Opening	The PPP connection's Challenge Handshake Authentication Protocol stage is opening.
ppp:IPCP Starting	The PPP connection's Internet Protocol Control Protocol stage is starting.
ppp:IPCP Opening	The PPP connection's Internet Protocol Control Protocol stage is opening.

**Table 62** PPP Logs (continued)

LOG MESSAGE	DESCRIPTION
ppp:LCP Closing	The PPP connection's Link Control Protocol stage is closing.
ppp:IPCP Closing	The PPP connection's Internet Protocol Control Protocol stage is closing.

**Table 63** UPnP Logs

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

**Table 64** Content Filtering Logs

LOG MESSAGE	DESCRIPTION
%s: Keyword blocking	The content of a requested web page matched a user defined keyword.
%s: Not in trusted web list	The web site is not in a trusted domain, and the router blocks all traffic except trusted domain sites.
%s: Forbidden Web site	The web site is in the forbidden web site list.
%s: Contains ActiveX	The web site contains ActiveX.
%s: Contains Java applet	The web site contains a Java applet.
%s: Contains cookie	The web site contains a cookie.
%s: Proxy mode detected	The router detected proxy mode in the packet.
%s: Trusted Web site	The web site is in a trusted domain.
%s	When the content filter is not on according to the time schedule.
Waiting content filter server timeout	The external content filtering server did not respond within the timeout period.
DNS resolving failed	The Prestige cannot get the IP address of the external content filtering via DNS query.
Creating socket failed	The Prestige cannot issue a query because TCP/IP socket creation failed, port:port number.
Connecting to content filter server fail	The connection to the external content filtering server failed.
License key is invalid	The external content filtering license key is invalid.

For type and code details, see [Table 67 on page 191](#).

**Table 65** Attack Logs

LOG MESSAGE	DESCRIPTION
attack [ TCP   UDP   IGMP   ESP   GRE   OSPF ]	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF attack.
attack ICMP (type:%d, code:%d)	The firewall detected an ICMP attack.
land [ TCP   UDP   IGMP   ESP   GRE   OSPF ]	The firewall detected a TCP/UDP/IGMP/ESP/GRE/OSPF land attack.
land ICMP (type:%d, code:%d)	The firewall detected an ICMP land attack.
ip spoofing - WAN [ TCP   UDP   IGMP   ESP   GRE   OSPF ]	The firewall detected an IP spoofing attack on the WAN port.
ip spoofing - WAN ICMP (type:%d, code:%d)	The firewall detected an ICMP IP spoofing attack on the WAN port.
icmp echo : ICMP (type:%d, code:%d)	The firewall detected an ICMP echo attack.
syn flood TCP	The firewall detected a TCP syn flood attack.
ports scan TCP	The firewall detected a TCP port scan attack.
teardrop TCP	The firewall detected a TCP teardrop attack.
teardrop UDP	The firewall detected an UDP teardrop attack.
teardrop ICMP (type:%d, code:%d)	The firewall detected an ICMP teardrop attack.
illegal command TCP	The firewall detected a TCP illegal command attack.
NetBIOS TCP	The firewall detected a TCP NetBIOS attack.
ip spoofing - no routing entry [ TCP   UDP   IGMP   ESP   GRE   OSPF ]	The firewall classified a packet with no source routing entry as an IP spoofing attack.
ip spoofing - no routing entry ICMP (type:%d, code:%d)	The firewall classified an ICMP packet with no source routing entry as an IP spoofing attack.
vulnerability ICMP (type:%d, code:%d)	The firewall detected an ICMP vulnerability attack.
traceroute ICMP (type:%d, code:%d)	The firewall detected an ICMP traceroute attack.
ports scan UDP	The firewall detected a UDP port scan attack.
Firewall sent TCP packet in response to DoS attack TCP	The firewall sent TCP packet in response to a DoS attack
ICMP Source Quench ICMP	The firewall detected an ICMP Source Quench attack.
ICMP Time Exceed ICMP	The firewall detected an ICMP Time Exceed attack.
ICMP Destination Unreachable ICMP	The firewall detected an ICMP Destination Unreachable attack.

**Table 65** Attack Logs (continued)

LOG MESSAGE	DESCRIPTION
ping of death. ICMP	The firewall detected an ICMP ping of death attack.
smurf ICMP	The firewall detected an ICMP smurf attack.

**Table 66** Remote Management Logs

LOG MESSAGE	DESCRIPTION
Remote Management: FTP denied	Attempted use of FTP service was blocked according to remote management settings.
Remote Management: TELNET denied	Attempted use of TELNET service was blocked according to remote management settings.
Remote Management: HTTP or UPnP denied	Attempted use of HTTP or UPnP service was blocked according to remote management settings.
Remote Management: WWW denied	Attempted use of WWW service was blocked according to remote management settings.
Remote Management: HTTPS denied	Attempted use of HTTPS service was blocked according to remote management settings.
Remote Management: SSH denied	Attempted use of SSH service was blocked according to remote management settings.
Remote Management: ICMP Ping response denied	Attempted use of ICMP service was blocked according to remote management settings.
Remote Management: SNMP denied	Attempted use of SNMP service was blocked according to remote management settings.
Remote Management: DNS denied	Attempted use of DNS service was blocked according to remote management settings.

**Table 67** ICMP Notes

TYPE	CODE	DESCRIPTION
0		Echo Reply
	0	Echo reply message
3		Destination Unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)
	5	Source route failed
4		Source Quench

**Table 67** ICMP Notes (continued)

TYPE	CODE	DESCRIPTION
	0	A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host
8		Echo
	0	Echo message
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp Reply
	0	Timestamp reply message
15		Information Request
	0	Information request message
16		Information Reply
	0	Information reply message

**Table 68** SIP Logs

LOG MESSAGE	DESCRIPTION
SIP Registration Success by SIP:SIP Phone Number	The listed SIP account was successfully registered with a SIP register server.
SIP Registration Fail by SIP:SIP Phone Number	An attempt to register the listed SIP account with a SIP register server was not successful.
SIP UnRegistration Success by SIP:SIP Phone Number	The listed SIP account's registration was deleted from the SIP register server.
SIP UnRegistration Fail by SIP:SIP Phone Number	An attempt to delete the listed SIP account's registration from the SIP register server failed.

**Table 69** RTP Logs

LOG MESSAGE	DESCRIPTION
Error, RTP init fail	The initialization of an RTP session failed.
Error, Call fail: RTP connect fail	A VoIP phone call failed because the RTP session could not be established.
Error, RTP connection cannot close	The termination of an RTP session failed.

**Table 70** FSM Logs: Caller Side

LOG MESSAGE	DESCRIPTION
VoIP Call Start Ph[Phone Port Number] <- Outgoing Call Number	Someone used a phone connected to the listed phone port to initiate a VoIP call to the listed destination.
VoIP Call Established Ph[Phone Port] -> Outgoing Call Number	Someone used a phone connected to the listed phone port to make a VoIP call to the listed destination.
VoIP Call End Phone[Phone Port]	A VoIP phone call made from a phone connected to the listed phone port has terminated.

**Table 71** FSM Logs: Callee Side

LOG MESSAGE	DESCRIPTION
VoIP Call Start from SIP[SIP Port Number]	A VoIP phone call came to the Prestige from the listed SIP number.
VoIP Call Established Ph[Phone Port] <- Outgoing Call Number	A VoIP phone call was set up from the listed SIP number to the Prestige.
VoIP Call End Phone[Phone Port]	A VoIP phone call that came into the Prestige has terminated.

**Table 72** Lifeline Logs

LOG MESSAGE	DESCRIPTION
PSTN Call Start	A PSTN call has been initiated.
PSTN Call End	A PSTN call has terminated.
PSTN Call Established	A PSTN call has been set up.

## 18.1.2 Syslog Logs

There are two types of syslog: event logs and traffic logs. The device generates an event log when a system event occurs, for example, when a user logs in or the device is under attack. The device generates a traffic log when a "session" is terminated. A traffic log summarizes the session's type, when it started and stopped the amount of traffic that was sent and received and so on. An external log analyzer can reconstruct and analyze the traffic flowing through the device after collecting the traffic logs.

**Table 73** Syslog Logs

LOG MESSAGE	DESCRIPTION
Event Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>" devID="<mac address>" cat="<category>"	This message is sent by the system ("RAS" displays as the system name if you haven't configured one) when the router generates a syslog. The facility is defined in the <b>Log Settings</b> screen. The severity is the log's syslog class. The definition of messages and notes are defined in the various log charts throughout this appendix. The "devID" is the MAC address of the router's LAN port. The "cat" is the same as the category in the router's logs.
Traffic Log: <Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="Traffic Log" note="Traffic Log" devID="<mac address>" cat="Traffic Log" duration=seconds sent=sentBytes rcvd=receiveBytes dir="<from:to>" protoID=IPProtocolID proto="serviceName" trans="IPSec/ Normal"	This message is sent by the device when the connection (session) is closed. The facility is defined in the Log Settings screen. The severity is the traffic log type. The message and note always display "Traffic Log". The "proto" field lists the service name. The "dir" field lists the incoming and outgoing interfaces ("LAN:LAN", "LAN:WAN", "LAN:DEV" for example).

The following table shows RFC-2408 ISAKMP payload types that the log displays. Please refer to the RFC for detailed information on each type.

**Table 74** RFC-2408 ISAKMP Payload Types

LOG DISPLAY	PAYLOAD TYPE
SA	Security Association
PROP	Proposal
TRANS	Transform
KE	Key Exchange
ID	Identification
CER	Certificate
CER_REQ	Certificate Request
HASH	Hash
SIG	Signature
NONCE	Nonce
NOTFY	Notification

**Table 74** RFC-2408 ISAKMP Payload Types (continued)

LOG DISPLAY	PAYLOAD TYPE
DEL	Delete
VID	Vendor ID

## 18.2 Configuring Log Settings

To change your log settings, click **LOGS** and then **Log Settings**. The **Log Settings** screen opens.

Use the **Log Settings** screen to configure to where the Prestige is to send the logs; the schedule for when the Prestige is to send the logs and which logs and/or immediate alerts the Prestige is to send.

An alert is a type of log that warrants more serious attention. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts are displayed in red and logs are displayed in black.



Figure 85 Log Settings

View Log
Log Settings

**Address Info:**

---

**Mail Server:**  (Outgoing SMTP Server NAME or IP Address)  
**Mail Subject:**   
**Send log to:**  (E-Mail Address)  
**Send alerts to:**  (E-Mail Address)

---

**Syslog Logging:**

Active  
**Syslog IP Address:**  (Server NAME or IP Address)  
**Log Facility:**

---

**Send Log:**

**Log Schedule:**   
**Day for Sending Log:**   
**Time for Sending Log:**  (hour)  (minute)  
 Clear log after sending mail

---

Log	Send immediate alert
<input checked="" type="checkbox"/> System Maintenance	<input type="checkbox"/> System Errors
<input checked="" type="checkbox"/> System Errors	<input type="checkbox"/> Access Control
<input checked="" type="checkbox"/> Access Control	<input type="checkbox"/> Blocked Web Sites
<input checked="" type="checkbox"/> TCP Reset	<input type="checkbox"/> Blocked Java etc.
<input checked="" type="checkbox"/> Packet Filter	<input type="checkbox"/> Attacks
<input checked="" type="checkbox"/> ICMP	
<input checked="" type="checkbox"/> Remote Management	
<input checked="" type="checkbox"/> CDR	
<input checked="" type="checkbox"/> PPP	
<input checked="" type="checkbox"/> UPnP	
<input checked="" type="checkbox"/> Forward Web Sites	
<input checked="" type="checkbox"/> Blocked Web Sites	
<input checked="" type="checkbox"/> Blocked Java etc.	
<input checked="" type="checkbox"/> Attacks	
<input checked="" type="checkbox"/> Any IP	
<input checked="" type="checkbox"/> SIP	

---

The following table describes the labels in this screen.

**Table 75** Log Settings

LABEL	DESCRIPTION
Address Info	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via e-mail.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the Prestige sends.
Send Log to	Logs are sent to the e-mail address specified in this field. If this field is left blank, logs will not be sent via e-mail.
Send Alerts to	Enter the e-mail address where the alert messages will be sent. If this field is left blank, alert messages will not be sent via e-mail.
Syslog Logging	Syslog logging sends a log to an external syslog server used to store logs.
Active	Click <b>Active</b> to enable syslog logging.
Syslog IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Send Log	
Log Schedule	<p>This drop-down menu is used to configure the frequency of log messages being sent as E-mail:</p> <ul style="list-style-type: none"> <li>• Daily</li> <li>• Weekly</li> <li>• Hourly</li> <li>• When Log is Full</li> <li>• None.</li> </ul> <p>If the <b>Weekly</b> or the <b>Daily</b> option is selected, specify a time of day when the E-mail should be sent. If the <b>Weekly</b> option is selected, then also specify which day of the week the E-mail should be sent. If the <b>When Log is Full</b> option is selected, an alert is sent when the log fills up. If you select <b>None</b>, no log messages are sent.</p>
Day for Sending Log	This field is only available when you select <b>Weekly</b> in the <b>Log Schedule</b> field. Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Clear log after sending mail	Select the check box to clear all logs after logs and alert messages are sent via e-mail.
Log	Select the categories of logs that you want to record.
Send Immediate Alert	Select the categories of alerts for which you want the Prestige to immediately send e-mail alerts.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Reset	Click <b>Reset</b> to reconfigure all the fields in this screen.

# CHAPTER 19

## Bandwidth Management

This chapter describes the functions and configuration of bandwidth management.

### 19.1 Bandwidth Management Overview

Bandwidth management allows you to allocate an interface's outgoing capacity to specific types of traffic. It can also help you make sure that the Prestige forwards certain types of traffic (especially real-time applications) with minimum delay. With the use of real-time applications such as Voice-over-IP (VoIP) increasing, the requirement for bandwidth allocation is also increasing.

Bandwidth management addresses questions such as:

- Who gets how much access to specific applications?
- What priority level should you give to each type of traffic?
- Which traffic must have guaranteed delivery?
- How much bandwidth should be allotted to guarantee delivery?

Bandwidth management also allows you to configure the allowed output for an interface to match what the network can handle. This helps reduce delays and dropped packets at the next routing device. For example, you can set the WAN interface speed to 1024 kbps (or less) if the broadband device connected to the WAN port has an upstream speed of 1024 kbps.

### 19.2 Bandwidth Classes and Filters

Use bandwidth classes and sub-classes to allocate specific amounts of bandwidth capacity (bandwidth budgets). Configure a bandwidth filter to define a bandwidth class (or sub-class) based on a specific application and/or subnet. Use the **Class Setup** screen (see [Section 19.11.1 on page 206](#)) to set up a bandwidth class's name, bandwidth allotment, and bandwidth filter. You can configure up to one bandwidth filter per bandwidth class. You can also configure bandwidth classes without bandwidth filters. However, it is recommended that you configure sub-classes with filters for any classes that you configure without filters. The Prestige leaves the bandwidth budget allocated and unused for a class that does not have a filter or sub-classes with filters. View your configured bandwidth classes and sub-classes in the **Class Setup** screen (see [Section 19.11 on page 205](#) for details).

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

## 19.3 Proportional Bandwidth Allocation

Bandwidth management allows you to define how much bandwidth each class gets; however, the actual bandwidth allotted to each class decreases or increases in proportion to actual available bandwidth.

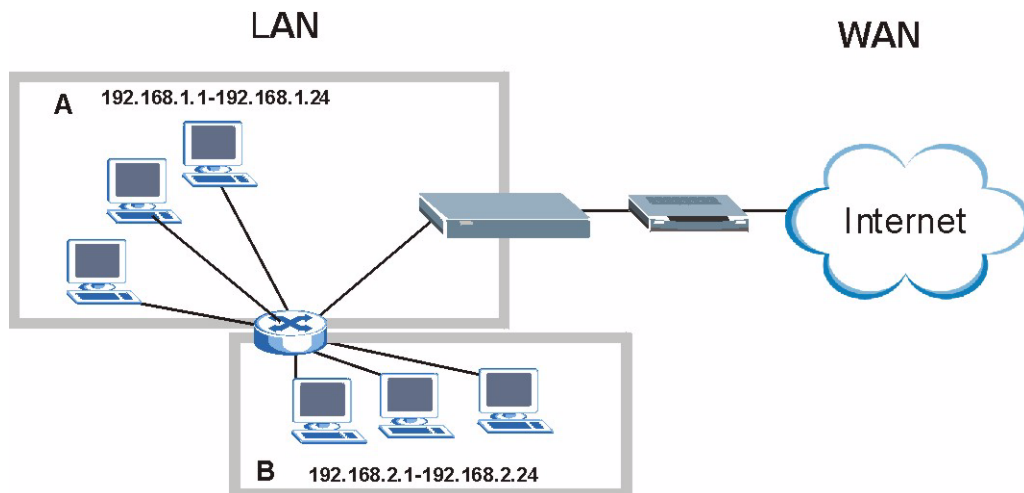
## 19.4 Application-based Bandwidth Management

You can create bandwidth classes based on individual applications (like VoIP, Web, FTP, E-mail and Video for example).

## 19.5 Subnet-based Bandwidth Management

You can create bandwidth classes based on subnets. The following figure shows LAN subnets. You could configure one bandwidth class for subnet A and another for subnet B.

**Figure 86** Subnet-based Bandwidth Management Example



## 19.6 Application and Subnet-based Bandwidth Management

You could also create bandwidth classes based on a combination of a subnet and an application. The following example table shows bandwidth allocations for application specific traffic from separate LAN subnets.

**Table 76** Application and Subnet-based Bandwidth Management Example

TRAFFIC TYPE	FROM SUBNET A	FROM SUBNET B
VoIP	64 Kbps	64 Kbps
Web	64 Kbps	64 Kbps

**Table 76** Application and Subnet-based Bandwidth Management Example (continued)

TRAFFIC TYPE	FROM SUBNET A	FROM SUBNET B
FTP	64 Kbps	64 Kbps
E-mail	64 Kbps	64 Kbps
Video	64 Kbps	64 Kbps

## 19.7 Scheduler

The scheduler divides up an interface's bandwidth among the bandwidth classes. The Prestige has two types of scheduler: fairness-based and priority-based.

### 19.7.1 Priority-based Scheduler

With the priority-based scheduler, the Prestige forwards traffic from bandwidth classes according to the priorities that you assign to the bandwidth classes. The larger a bandwidth class's priority number is, the higher the priority. Assign real-time applications (like those using audio or video) a higher priority number to provide smoother operation.

### 19.7.2 Fairness-based Scheduler

The Prestige divides bandwidth equally among bandwidth classes when using the fairness-based scheduler; thus preventing one bandwidth class from using all of the interface's bandwidth.

## 19.8 Maximize Bandwidth Usage

The maximize bandwidth usage option ([Figure 87 on page 204](#)) allows the Prestige to divide up any available bandwidth on the interface (including unallocated bandwidth and any allocated bandwidth that a class is not using) among the bandwidth classes that require more bandwidth.

When you enable maximize bandwidth usage, the Prestige first makes sure that each bandwidth class gets up to its bandwidth allotment. Next, the Prestige divides up an interface's available bandwidth (bandwidth that is unbudgeted or unused by the classes) depending on how many bandwidth classes require more bandwidth and on their priority levels. When only one class requires more bandwidth, the Prestige gives extra bandwidth to that class.

When multiple classes require more bandwidth, the Prestige gives the highest priority classes the available bandwidth first (as much as they require, if there is enough available bandwidth), and then to lower priority classes if there is still bandwidth available. The Prestige distributes the available bandwidth equally among classes with the same priority level.

## 19.8.1 Reserving Bandwidth for Non-Bandwidth Class Traffic

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

- 1 Leave some of the interface's bandwidth unbudgeted.
- 2 Do not enable the interface's **Maximize Bandwidth Usage** option.
- 3 Do not enable bandwidth borrowing on the sub-classes (see [Section 19.9 on page 202](#)).

## 19.8.2 Maximize Bandwidth Usage Example

Here is an example of a Prestige that has maximize bandwidth usage enabled on an interface. The following table shows each bandwidth class's bandwidth budget. The classes are set up based on subnets. The interface is set to 10240 kbps. Each subnet is allocated 2048 kbps. The unbudgeted 2048 kbps allows traffic not defined in any of the bandwidth filters to go out when you do not select the maximize bandwidth option.

**Table 77** Maximize Bandwidth Usage Example

BANDWIDTH CLASSES AND ALLOTMENTS	
Root Class: 10240 kbps	Administration: 2048 kbps
	Sales: 2048 kbps
	Marketing: 2048 kbps
	Research: 2048 kbps

The Prestige divides up the unbudgeted 2048 kbps among the classes that require more bandwidth. If the administration department only uses 1024 kbps of the budgeted 2048 kbps, the Prestige also divides the remaining 1024 kbps among the classes that require more bandwidth. Therefore, the Prestige divides a total of 3072 kbps of unbudgeted and unused bandwidth among the classes that require more bandwidth.

### 19.8.2.1 Priority-based Allotment of Unused and Unbudgeted Bandwidth

The following table shows the priorities of the bandwidth classes and the amount of bandwidth that each class gets.

**Table 78** Priority-based Allotment of Unused and Unbudgeted Bandwidth Example

BANDWIDTH CLASSES, PRIORITIES AND ALLOTMENTS	
Root Class: 10240 kbps	Administration: Priority 4, 1024 kbps
	Sales: Priority 6, 3584 kbps
	Marketing: Priority 6, 3584 kbps
	Research: Priority 5, 2048 kbps

Suppose that all of the classes except for the administration class need more bandwidth.

- Each class gets up to its budgeted bandwidth. The administration class only uses 1024 kbps of its budgeted 2048 kbps.
- The sales and marketing are first to get extra bandwidth because they have the highest priority (6). If they each require 1536 kbps or more of extra bandwidth, the Prestige divides the total 3072 kbps total of unbudgeted and unused bandwidth equally between the sales and marketing departments (1536 kbps extra to each for a total of 3584 kbps for each) because they both have the highest priority level.
- Research requires more bandwidth but only gets its budgeted 2048 kbps because all of the unbudgeted and unused bandwidth goes to the higher priority sales and marketing classes.

### 19.8.2.2 Fairness-based Allotment of Unused and Unbudgeted Bandwidth

The following table shows the amount of bandwidth that each class gets.

**Table 79** Fairness-based Allotment of Unused and Unbudgeted Bandwidth Example

BANDWIDTH CLASSES AND ALLOTMENTS	
Root Class: 10240 kbps	Administration: 1024 kbps
	Sales: 3072 kbps
	Marketing: 3072 kbps
	Research: 3072 kbps

Suppose that all of the classes except for the administration class need more bandwidth.

- Each class gets up to its budgeted bandwidth. The administration class only uses 1024 kbps of its budgeted 2048 kbps.
- The Prestige divides the total 3072 kbps total of unbudgeted and unused bandwidth equally among the other classes. 1024 kbps extra goes to each so the other classes each get a total of 3072 kbps

## 19.9 Bandwidth Borrowing

Bandwidth borrowing allows a sub-class to borrow unused bandwidth from its parent class, whereas maximize bandwidth usage allows any bandwidth class to borrow any unused or unbudgeted bandwidth on the whole interface.

Enable bandwidth borrowing on a sub-class to allow the sub-class to use the parent class's unused bandwidth. The parent class's unused bandwidth is given to the highest priority sub-class first (see [Section 19.9.1 on page 203](#)).

The total of the bandwidth allotments for sub-classes cannot exceed the bandwidth allotment of the parent class. The Prestige uses the scheduler to divide the parent class's unused bandwidth among the sub-classes that have bandwidth borrowing enabled.

## 19.9.1 Bandwidth Borrowing Example

Here is an example of bandwidth management with classes configured for bandwidth borrowing. The classes are set up based on departments and individuals within certain departments.

**Table 80** Bandwidth Borrowing Example

BANDWIDTH CLASSES AND BANDWIDTH BORROWING SETTINGS	
Root Class:	Administration: Borrowing Enabled
	Sales: Borrowing Disabled
	Marketing: Borrowing Enabled
	Research: Borrowing Enabled

- The Sales class cannot borrow unused bandwidth from the Root class because the Sales class has bandwidth borrowing disabled.

## 19.9.2 Maximize Bandwidth Usage With Bandwidth Borrowing

If you configure both maximize bandwidth usage (on the interface) and bandwidth borrowing (on individual sub-classes), the Prestige functions as follows.

- 1 The Prestige sends traffic according to each bandwidth class's bandwidth budget.
- 2 The Prestige assigns a parent class's unused bandwidth to its sub-classes that have more traffic than their budgets and have bandwidth borrowing enabled. The Prestige gives priority to sub-classes of higher priority and treats classes of the same priority equally.
- 3 The Prestige assigns any remaining unused or unbudgeted bandwidth on the interface to any class that requires it. The Prestige gives priority to classes of higher priority and treats classes of the same level equally.
- 4 If the bandwidth requirements of all of the traffic classes are met and there is still some unbudgeted bandwidth, the Prestige assigns it to traffic that does not match any of the classes.

## 19.10 Configuring Summary

Click **BW MGMT** to open the **Summary** screen.

Use this screen to enable bandwidth management on an interface and set the maximum allowed bandwidth and scheduler for the interface. You can also enable or disable maximize bandwidth usage.



**Figure 87** Bandwidth Manager: Summary

**BW MANAGER**

Summary    Class Setup    Monitor

BW Manager manages the bandwidth of traffic flowing out of router on the specific interface. BW Manager can be switched on/off independently for each interface.

LAN

Speed: 30000 (kbps)

Scheduler: Priority-Based

Maximize bandwidth usage

WAN

Speed: 10000 (kbps)

Scheduler: Priority-Based

Maximize bandwidth usage

Apply    Reset

The following table describes the labels in this screen.

**Table 81** Bandwidth Manager: Summary

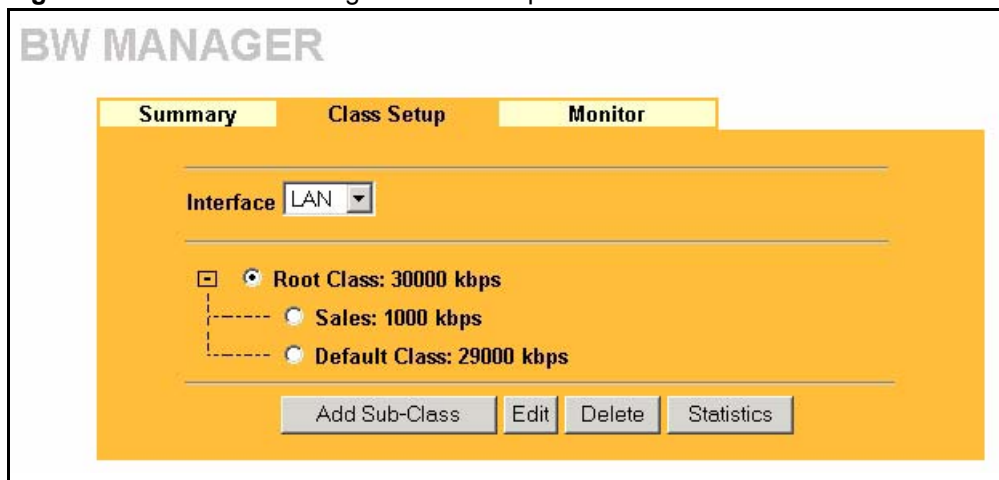
LABEL	DESCRIPTION
LAN WAN	These read-only labels represent the physical interfaces. Select an interface's check box to enable bandwidth management on that interface. Bandwidth management applies to all traffic flowing out of the router through the interface, regardless of the traffic's source.  Traffic redirect or IP alias may cause LAN-to-LAN traffic to pass through the Prestige and be managed by bandwidth management.
Speed (kbps)	Enter the amount of bandwidth for this interface that you want to allocate using bandwidth management.  This appears as the bandwidth budget of the interface's root class (see <a href="#">Section 19.11 on page 205</a> ). The recommendation is to set this speed to match what the device connected to the port can handle. For example, set the WAN interface speed to 1000 kbps if the broadband device connected to the WAN port has an upstream speed of 1000 kbps.
Scheduler	Select either <b>Priority-Based</b> or <b>Fairness-Based</b> from the drop-down menu to control the traffic flow. Select <b>Priority-Based</b> to give preference to bandwidth classes with higher priorities. Select <b>Fairness-Based</b> to treat all bandwidth classes equally. See <a href="#">Section 19.7 on page 200</a> .
Maximize Bandwidth Usage	Select this check box to have the Prestige divide up all of the interface's unallocated and/or unused bandwidth among the bandwidth classes that require bandwidth. Do not select this if you want to reserve bandwidth for traffic that does not match a bandwidth class (see <a href="#">Section 19.8.1 on page 201</a> ) or you want to limit the speed of this interface (see the <b>Speed</b> field description).
Apply	Click <b>Apply</b> to save your changes back to the Prestige.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 19.11 Configuring Class Setup

The class setup screen displays the configured bandwidth classes by individual interface. Select an interface and click the buttons to perform the actions described next. Click “+” to expand the class tree or click “-” to collapse the class tree. Each interface has a permanent root class. The bandwidth budget of the root class is equal to the speed you configured on the interface (see [Section 19.10 on page 203](#) to configure the speed of the interface). Configure sub-classes for the root class. A default class automatically displays for all the bandwidth in the Root Class that is not allocated to bandwidth classes.

To add or delete child classes on an interface, click **BW MGMT**, then the **Class Setup** tab. The screen appears as shown (with example classes).

**Figure 88** Bandwidth Manager: Class Setup



The following table describes the labels in this screen.

**Table 82** Bandwidth Manager: Class Setup

LABEL	DESCRIPTION
Class Setup	
Interface	Select an interface from the drop-down list box for which you wish to set up classes. Bandwidth management controls outgoing traffic on an interface, not incoming. In order to limit the download bandwidth of the LAN users, set the bandwidth management class on the LAN. In order to limit the upload bandwidth, set the bandwidth management class on the corresponding WAN interface.
Add Sub-Class	Click <b>Add Sub-class</b> to add a sub-class.
Edit	Click <b>Edit</b> to configure the selected class. You cannot edit the root class.
Delete	Click <b>Delete</b> to delete the class and all its sub-classes. You cannot delete the root class.
Statistics	Click <b>Statistics</b> to display the status of the selected class.

## 19.11.1 Bandwidth Manager Class Configuration

Configure a bandwidth management class in the **Class Setup** screen. You must use the **Summary** screen to enable bandwidth management on an interface before you can configure classes for that interface.

To add a child class, click **BW MGMT**, then the **Class Setup** tab. Click the **Add Sub-Class** button to open the following screen.

**Figure 89** Bandwidth Manager: Edit Class

**BW MANAGER - EDIT CLASS**

Class Name: LAN-2

Bandwidth Budget: 0 (kbps)

Priority: 3 (0-7)

Borrow bandwidth from parent class

Enable Bandwidth Filter

Application: None

Destination IP Address: [ ]

Destination Subnet Mask: [ ]

Destination Port: 0

Source IP Address: [ ]

Source Subnet Mask: [ ]

Source Port: 0

Protocol ID: 0

Apply Cancel

The following table describes the labels in this screen.

**Table 83** Bandwidth Manager: Edit Class

LABEL	DESCRIPTION
Class Configuration	
Class Name	Use the auto-generated name or enter a descriptive name of up to 20 alphanumeric characters, including spaces.
Bandwidth Budget (kbps)	Specify the maximum bandwidth allowed for the class in kbps. The recommendation is a setting between 20 kbps and 20000 kbps for an individual class.
Priority	Enter a number between 0 and 7 to set the priority of this class. The higher the number, the higher the priority. The default setting is 3.

**Table 83** Bandwidth Manager: Edit Class (continued)

LABEL	DESCRIPTION
Borrow bandwidth from parent class	<p>Select this option to allow a sub-class to borrow bandwidth from its parent class if the parent class is not using up its bandwidth budget.</p> <p>Bandwidth borrowing is governed by the priority of the sub-classes. That is, a sub-class with the highest priority (7) is the first to borrow bandwidth from its parent class.</p> <p>Do not select this for the classes directly below the root class if you want to leave bandwidth available for other traffic types (see <a href="#">Section 19.8.1 on page 201</a>) or you want to set the interface's speed to match what the next device in network can handle (see the <b>Speed</b> field description in <a href="#">Table 81 on page 204</a>).</p>
Filter Configuration	
Enable Bandwidth Filter	<p>Select <b>Enable Bandwidth Filter</b> to have the Prestige use this bandwidth filter when it performs bandwidth management.</p> <p>You must enter a value in at least one of the following fields (other than the <b>Subnet Mask</b> fields which are only available when you enter the destination or source IP address).</p>
Application	<p>This field simplifies bandwidth class configuration by allowing you to select a predefined application. When you select a predefined application, you do not configure the rest of the bandwidth filter fields (other than enabling or disabling the filter).</p> <p><b>FTP</b> (File Transfer Program) is a program to enable fast transfer of files, including large files that may not be possible by e-mail. Select FTP from the drop-down list box to configure the bandwidth filter for FTP traffic.</p> <p><b>SIP</b> (Session Initiation Protocol) is a signaling protocol used in Internet telephony, instant messaging, events notification and conferencing. The Prestige supports SIP traffic pass-through. Select SIP from the drop-down list box to configure this bandwidth filter for SIP traffic. This option makes it easier to manage bandwidth for SIP traffic and is useful for example when there is a VoIP (Voice over Internet Protocol) device on your LAN.</p> <p>Select <b>None</b> from the drop-down list box if you do not want to use a predefined application for the bandwidth class. When you select <b>None</b>, you need to configure at least one of the following fields (other than the <b>Subnet Mask</b> fields which you only enter if you also enter a corresponding destination or source IP address).</p>
Destination IP Address	Enter the destination IP address in dotted decimal notation.
Destination Subnet Mask	Enter the destination subnet mask. This field is N/A if you do not specify a <b>Destination IP Address</b> . Refer to <a href="#">Appendix D on page 356</a> for more information on IP subnetting.
Destination Port	Enter the port number of the destination. See <a href="#">Table 84 on page 208</a> for a table of services and port numbers.
Source IP Address	Enter the source IP address.
Source Subnet Mask	Enter the source subnet mask. This field is N/A if you do not specify a <b>Source IP Address</b> . Refer to <a href="#">Appendix D on page 356</a> for more information on IP subnetting.
Source Port	Enter the port number of the source. See the following table for some common services and port numbers.
Protocol ID	Enter the protocol ID (service type) number, for example: 1 for ICMP, 6 for TCP or 17 for UDP.

**Table 83** Bandwidth Manager: Edit Class (continued)

LABEL	DESCRIPTION
Apply	Click <b>Apply</b> to save your changes back to the Prestige.
Cancel	Click <b>Cancel</b> to exit this screen without saving.

**Table 84** Services and Port Numbers

SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

## 19.11.2 Bandwidth Management Statistics

Use the **Bandwidth Management Statistics** screen to view network performance information. Click the **Statistics** button in the **Class Setup** screen to open the **Statistics** screen.

**Figure 90** Bandwidth Management Statistics

Tx Packets		Tx Bytes		Dropped Packets		Dropped Bytes	
527		207624		0		0	

Bandwidth Statistics for the Past 8 Seconds							
t-8	t-7	t-6	t-5	t-4	t-3	t-2	t-1
0	0	0	0	0	0	30	66

Update Period	<input type="text" value="5"/>	(Seconds)	<input type="button" value="Set Interval"/>	<input type="button" value="Stop Update"/>	<input type="button" value="Clear Counter"/>
---------------	--------------------------------	-----------	---	--	--

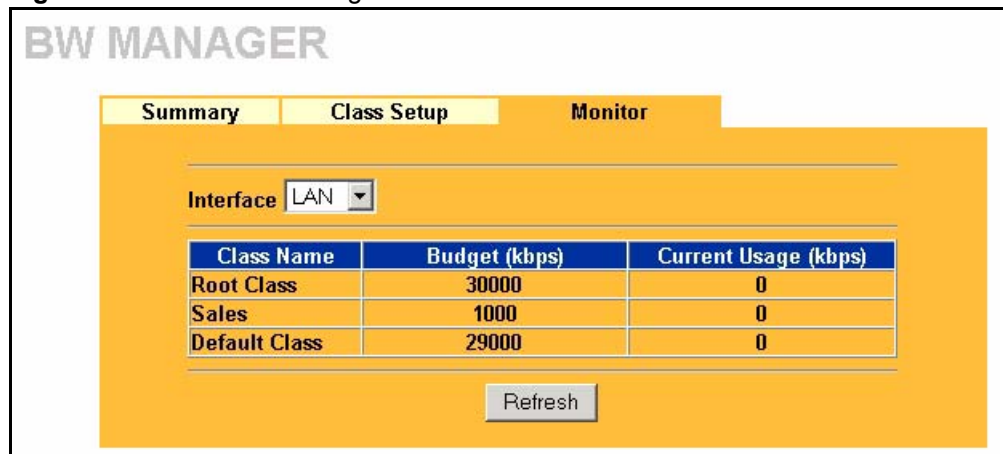
The following table describes the labels in this screen.

**Table 85** Bandwidth Management Statistics

LABEL	DESCRIPTION
Class Name	This field displays the name of the class the statistics page is showing.
Budget (kbps)	This field displays the amount of bandwidth allocated to the class.
Tx Packets	This field displays the total number of packets transmitted.
Tx Bytes	This field displays the total number of bytes transmitted.
Dropped Packets	This field displays the total number of packets dropped.
Dropped Bytes	This field displays the total number of bytes dropped.
Bandwidth Statistics for the Past 8 Seconds (t-8 to t-1)	
This field displays the bandwidth statistics (in bps) for the past one to eight seconds. For example, t-1 means one second ago.	
Update Period (Seconds)	Enter the time interval in seconds to define how often the information should be refreshed.
Set Interval	Click <b>Set Interval</b> to apply the new update period you entered in the <b>Update Period</b> field above.
Stop Update	Click <b>Stop Update</b> to stop the browser from refreshing bandwidth management statistics.
Clear Counter	Click <b>Clear Counter</b> to clear all of the bandwidth management statistics.

## 19.12 Configuring Monitor

To view the device's bandwidth usage and allotments, click **BW MGMT**, then the **Monitor** tab. The screen appears as shown.

**Figure 91** Bandwidth Manager Monitor

The following table describes the labels in this screen.

**Table 86** Bandwidth Manager Monitor

LABEL	DESCRIPTION
Interface	Select an interface from the drop-down list box to view the bandwidth usage of its bandwidth classes.
Class Name	This field displays the name of the bandwidth class. A <b>Default Class</b> automatically displays for all the bandwidth in the <b>Root Class</b> that is not allocated to bandwidth classes. If you do not enable maximize bandwidth usage on an interface, the Prestige uses the bandwidth in this default class to send traffic that does not match any of the bandwidth classes. <sup>a</sup>
Budget (kbps)	This field displays the amount of bandwidth allocated to the bandwidth class.
Current Usage (kbps)	This field displays the amount of bandwidth that each bandwidth class is using.
Refresh	Click <b>Refresh</b> to update the page.

a. If you allocate all the root class's bandwidth to the bandwidth classes, the default class still displays a budget of 2 kbps (the minimum amount of bandwidth that can be assigned to a bandwidth class).





# CHAPTER 20

## Maintenance

This chapter explains how to use the maintenance screens.

### 20.1 Maintenance Overview

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

### 20.2 Status Screen

Click **MAINTENANCE** in the navigation panel to open the **Status** screen, where you can monitor your Prestige. Note that these fields are READ-ONLY and are meant to be used for diagnostic purposes.

**Figure 92** System Status

The following table describes the labels in this screen.

**Table 87** System Status

LABEL	DESCRIPTION
System Name	This is the <b>System Name</b> . It is for identification purposes. You can configure it in the <b>SYSTEM General</b> screen.
Model Name	The model name identifies your device type. The model name should also be on a sticker on your device. If you are uploading firmware, be sure to upload firmware for this exact model name.
ZyNOS Firmware Version:	This is the ZyNOS firmware version and the date the firmware was created. ZyNOS is ZyXEL's proprietary Network Operating System.
Routing Protocols	This shows the routing protocol that the Prestige handles - <b>IP</b> . This is not configurable.
WAN Port	
IP Address	This is the WAN port IP address.
IP Subnet Mask	This is the WAN port subnet mask.
DHCP	This is the WAN port DHCP role - <b>Client</b> or <b>None</b> .
LAN Port	
IP Address	This is the LAN port IP address.

**Table 87** System Status (continued)

LABEL	DESCRIPTION
IP Subnet Mask	This is the LAN port subnet mask.
DHCP	This is the LAN port DHCP role - <b>Server, Relay</b> or <b>None</b> .
VoIP status	
SIP1/SIP 2	This is the SIP account configured on the Prestige
SIP Registration Status	This is the SIP registration status of the SIP account. This field displays <b>Registered</b> when the Prestige has successfully registered the SIP account with the SIP register server. This field displays <b>Not Register</b> when the Prestige has not successfully registered the SIP account with the SIP register server.
Used Port	This field displays the Prestige's listening port for SIP traffic on this SIP account.
Register/ Unregister	Click <b>Register</b> to have the Prestige attempt to register the SIP account with the SIP register server. Click <b>Unregister</b> to delete the SIP account's registration on the SIP register server. This removes the SIP registration server's SIP identity-to-IP address (or domain name) mapping for this SIP account, it does not cancel your SIP account.
IVR Status	
Remaining Time	This field displays the amount of time left for recording custom tones. IVR (Interactive Voice Response) is a feature that allows you to use your telephone to interact with the Prestige. You can use your phone to record custom tones for the caller ringing and on hold tone functions.
Show Statistics	Click <b>Show Statistics</b> to display the real-time system statistics.

## 20.2.1 System Statistics

Read-only information here includes port status and packet specific statistics. Also provided are "system up time" and "poll interval(s)". The **Poll Interval(s)** field is configurable.

**Figure 93** Maintenance System Statistics

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	Down	0	0	0	0	0	00:00:00
LAN	100M/Full	2072	1677	0	64	130	4:59:05

System Up Time : 4:59:17

Poll Interval(s) :  sec

The following table describes the labels in this screen.

**Table 88** Maintenance System Statistics

LABEL	DESCRIPTION
Port	This is the WAN or LAN port.
Status	This displays the port speed and duplex setting if you're using Ethernet encapsulation and <b>down</b> (line is down), <b>idle</b> (line (ppp) idle), <b>dial</b> (starting to trigger a call) and <b>drop</b> (dropping a call) if you're using PPPoE encapsulation.
TxPkts	This is the number of transmitted packets on this port.
RxPkts	This is the number of received packets on this port.
Collisions	This is the number of collisions on this port.
Tx B/s	This displays the transmission speed in bytes per second on this port.
Rx B/s	This displays the reception speed in bytes per second on this port.
Up Time	This is the total amount of time the line has been up.
System Up Time	This is the total time the Prestige has been on.
Poll Interval(s)	Enter the time interval for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the <b>Poll Interval(s)</b> field.
Stop	Click <b>Stop</b> to stop refreshing statistics, click <b>Stop</b> .

## 20.3 DHCP Table Screen

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the Prestige as a DHCP server or disable it. When configured as a DHCP server, the Prestige provides the TCP/IP configuration for the clients. If the Prestige is not configured as a DHCP server, you must have another DHCP server on your LAN, or else the computer must be manually configured.

Click **MAINTENANCE**, and then the **DHCP Table** tab. Read-only information here relates to your DHCP status. The DHCP table shows current DHCP client information (including **IP Address**, **Host Name** and **MAC Address**) of all network clients using the DHCP server.

**Figure 94** Maintenance DHCP Table

The screenshot shows a web interface titled "DHCP TABLE". At the top, there are navigation tabs: "Status", "DHCP Table", "Any IP", "F/W Upload", "Configuration", and "Restart". The "DHCP Table" tab is selected. Below the tabs is a table with the following data:

#	IP Address	Host Name	MAC Address
1	192.168.1.33	TW11746	00:05:1c:15:10:7f

Below the table is a "Refresh" button.

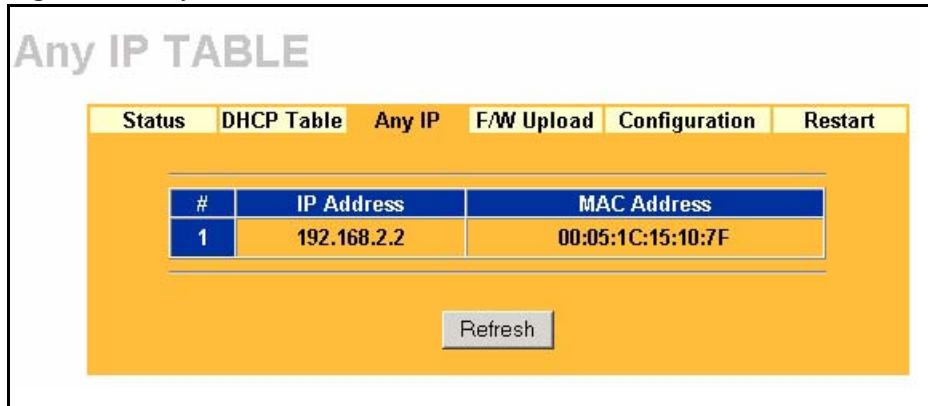
The following table describes the labels in this screen.

**Table 89** Maintenance DHCP Table

LABEL	DESCRIPTION
#	This is the index number of the host computer.
IP Address	This field displays the IP address relative to the # field listed above.
Host Name	This field displays the computer host name.
MAC Address	This field shows the MAC address of the computer with the name in the <b>Host Name</b> field. 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.
Refresh	Click <b>Refresh</b> to renew the screen.

## 20.4 Any IP Table Screen

Click **Maintenance, Any IP**. The Any IP table shows current read-only information (including the IP address and the MAC address) of all network devices that use the Any IP feature to communicate with the Prestige. Refer to [Section 5.8 on page 75](#) for more information.

**Figure 95** Any IP Table

The following table describes the labels in this screen.

**Table 90** Any IP Table

LABEL	DESCRIPTION
#	This field displays the index number.
IP Address	This field displays the IP address of the network device.
MAC Address	This field displays the MAC (Media Access Control) address of the computer with the displayed IP address. Every Ethernet device has a unique MAC address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
Refresh	Click <b>Refresh</b> to update this screen.

## 20.5 F/W Upload Screen

Find firmware at [www.zyxel.com](http://www.zyxel.com) in a file that (usually) uses the system model name with a ".bin" extension, e.g., "Prestige.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Click **MAINTENANCE** in the navigation panel and then the **F/W UPLOAD** tab. Follow the instructions in this screen to upload firmware to your Prestige.

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

**Figure 96** Firmware Upload

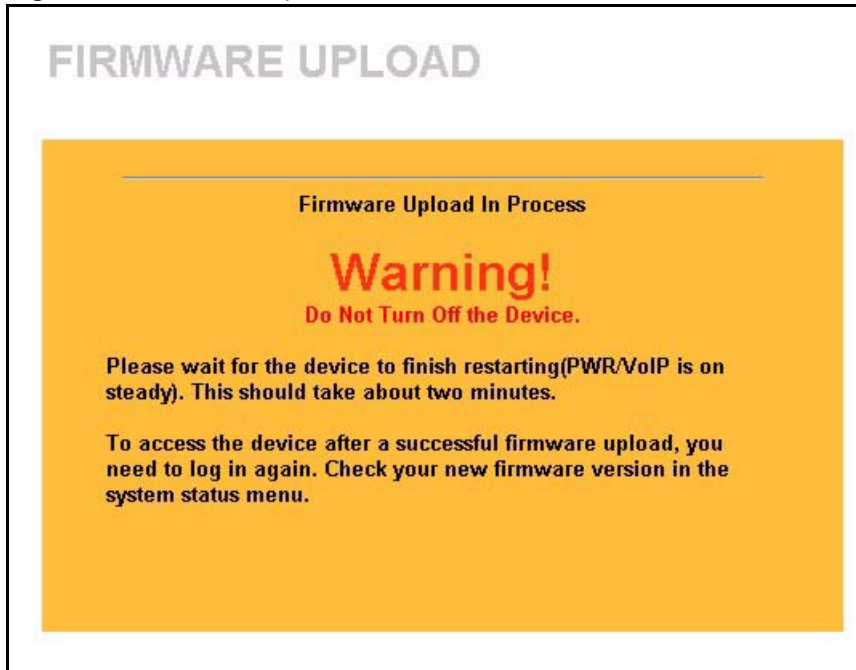
The following table describes the labels in this screen.

**Table 91** Firmware Upload

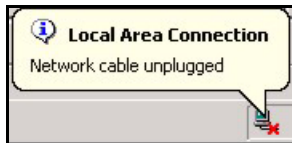
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Browse...</b> to find it.
Browse...	Click <b>Browse...</b> to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click <b>Upload</b> to begin the upload process. This process may take up to two minutes.

**Note:** Do not turn off the device while firmware upload is in progress!

After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the device again.

**Figure 97** Firmware Upload In Process

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

**Figure 98** Network Temporarily Disconnected

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

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **F/W Upload** screen.

**Figure 99** Firmware Upload Error



## 20.6 Configuration Screen

Click **MAINTENANCE** in the navigation panel and then the **Configuration** tab. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

**Figure 100** Configuration

The screenshot shows a web interface titled "MAINTENANCE" with a navigation bar containing tabs: Status, DHCP Table, Any IP, F/W Upload, Configuration, and Restart. The "Configuration" tab is active. The main content area is yellow and contains three sections:

- Backup Configuration:** A section with a heading "Backup Configuration" and a description: "Click Backup to save the current configuration of your system to your computer." Below this is a "Backup" button.
- Restore Configuration:** A section with a heading "Restore Configuration" and a description: "To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload." Below this is a "File Path:" label, a text input field, a "Browse..." button, and an "Upload" button.
- Back to Factory Defaults:** A section with a heading "Back to Factory Defaults" and a description: "Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the" followed by a list:
  - Password will be 1234
  - LAN IP address will be 192.168.1.1
  - DHCP will be reset to server
 Below this is a "Reset" button.

### 20.6.1 Backup Configuration

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

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

## 20.6.2 Restore Configuration

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

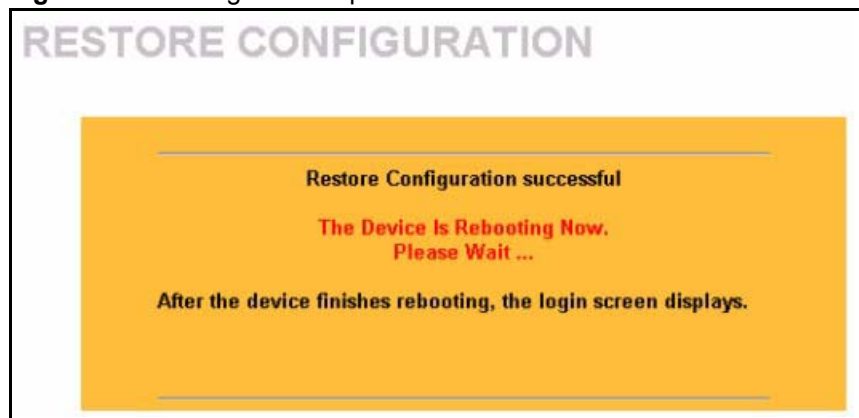
**Table 92** Restore Configuration

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Browse...</b> to find it.
Browse...	Click <b>Browse...</b> to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click <b>Upload</b> to begin the upload process.

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

After you see a “configuration upload successful” screen, you must then wait one minute before logging into the device again.

**Figure 101** Configuration Upload Successful



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

**Figure 102** Network Temporarily Disconnected



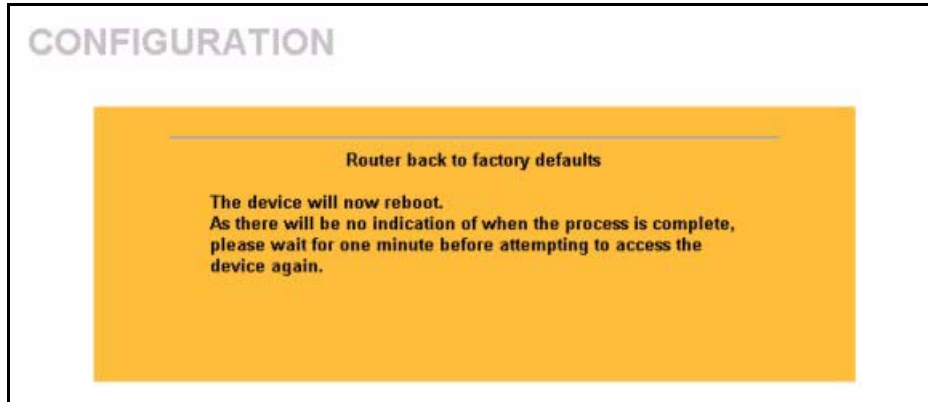
If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default management IP address (192.168.5.1). See your Quick Start Guide or the appendices for details on how to set up your computer's IP address.

If the upload was not successful, a **Configuration Upload Error** screen will appear. Click **Return** to go back to the **Configuration** screen.

### 20.6.3 Back to Factory Defaults

Clicking the **Reset** button in this section clears all user-entered configuration information and returns the Prestige to its factory defaults as shown on the screen. The following warning screen will appear.

**Figure 103** Reset Warning Message

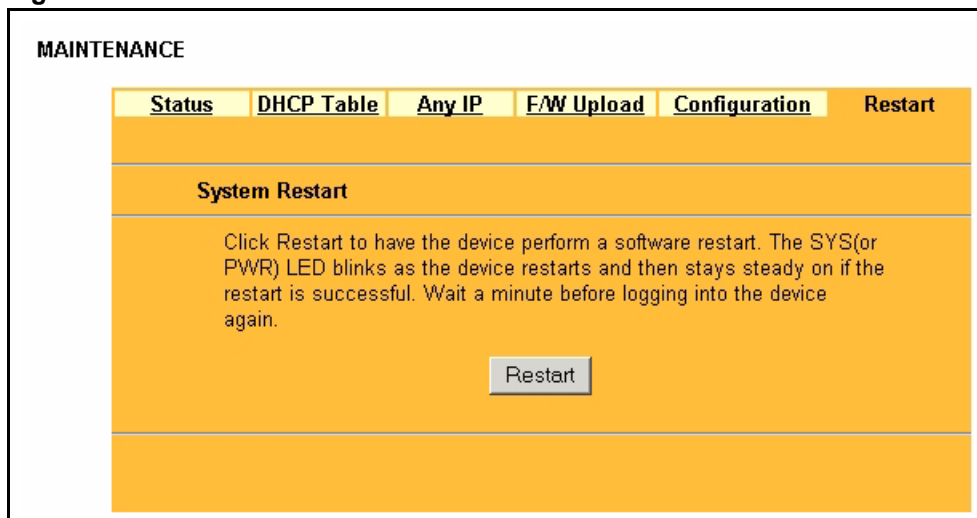


You can also press the **RESET** button on the rear panel to reset the factory defaults of your Prestige. For more information on the **RESET** button, see [Section 2.3 on page 45](#).

## 20.7 Restart Screen

System restart allows you to reboot the Prestige without turning the power off.

Click **MAINTENANCE** in the navigation panel and then **Restart**. Click **Restart** to have the Prestige reboot. This does not affect the Prestige's configuration.

**Figure 104** Restart Screen

# CHAPTER 21

## Introducing the SMT

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

### 21.1 SMT Introduction

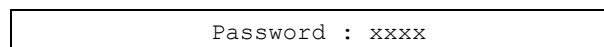
The Prestige's SMT (System Management Terminal) is a menu-driven interface that you can access through a telnet connection. This chapter shows you how to access the SMT (System Management Terminal) menus, how to navigate the SMT and how to configure SMT menus.

### 21.2 Accessing the SMT via Telnet

The following procedure details how to telnet into your Prestige.

- 1 In Windows, click **Start** (usually in the bottom left corner), **Run** and then type "telnet 192.168.1.1" (the default IP address) and click **OK**.
- 2 For your first login, enter the default password "1234". As you type the password, the screen displays an asterisk "\*" for each character you type.

**Figure 105** Login Screen



```
Password : xxxx
```

- 3 After entering the password you will see the main menu.

Please note that if there is no activity for longer than five minutes (default timeout period) after you log in, your Prestige will automatically log you out. You will then have to telnet into the Prestige again. You can use the web configurator or the CI commands to change the inactivity time out period.

### 21.3 Navigating the SMT Interface

The SMT (System Management Terminal) is the interface that you use to configure your Prestige.

Several operations that you should be familiar with before you attempt to modify the configuration are listed in the table below.

**Table 93** Main Menu Commands

OPERATION	KEYSTROKE	DESCRIPTION
Move down to another menu	[ENTER]	To move forward to a submenu, type in the number of the desired submenu and press [ENTER].
Move up to a previous menu	[ESC]	Press [ESC] to move back to the previous menu.
Move to a "hidden" menu	Press [SPACE BAR] to change <b>No</b> to <b>Yes</b> then press [ENTER].	Fields beginning with "Edit" lead to hidden menus and have a default setting of <b>No</b> . Press [SPACE BAR] once to change <b>No</b> to <b>Yes</b> , and then press [ENTER] to go to the "hidden" menu.
Move the cursor	[ENTER] or [UP]/[DOWN] arrow keys.	Within a menu, press [ENTER] to move to the next field. You can also use the [UP]/[DOWN] arrow keys to move to the previous and the next field, respectively.  When you are at the top of a menu, press the [UP] arrow key to move to the bottom of a menu.
Entering information	Type in or press [SPACE BAR], then press [ENTER].	You need to fill in two types of fields. The first requires you to type in the appropriate information. The second allows you to cycle through the available choices by pressing [SPACE BAR].
Required fields	<? > or <b>ChangeMe</b>	All fields with the symbol <?> must be filled in order to be able to save the new configuration.  All fields with <b>ChangeMe</b> must not be left blank in order to be able to save the new configuration.
N/A fields	<N/A>	Some of the fields in the SMT will show a <N/A>. This symbol refers to an option that is Not Applicable.
Save your configuration	[ENTER]	Save your configuration by pressing [ENTER] at the message "Press ENTER to confirm or ESC to cancel". Saving the data on the screen will take you, in most cases to the previous menu.  Make sure you save your settings in each screen that you configure.
Exit the SMT	Type 99, then press [ENTER].	Type 99 at the main menu prompt and press [ENTER] to exit the SMT interface.

After you enter the password, the SMT displays the main menu, as shown next.

**Figure 106** SMT Main Menu

```

Copyright (c) 1994 - 2005 ZyXEL Communications Corp.
Prestige 2302R Main Menu

Getting Started
  1. General Setup
  2. WAN Setup
  3. LAN Setup
  4. Internet Access Setup

Advanced Applications
  11. Remote Node Setup
  12. Static Routing Setup
  15. NAT Setup

Advanced Management
  21. Filter and Firewall Setup
  22. SNMP Configuration
  23. System Password
  24. System Maintenance
  26. Schedule Setup

99. Exit

Enter Menu Selection Number:

```

### 21.3.1 System Management Terminal Interface Summary

The following table describes the fields in the previous screen.

**Table 94** Main Menu Summary

#	MENU TITLE	DESCRIPTION
1	General Setup	Use this menu to set up your general information.
2	WAN Setup	Use this menu to clone a MAC address from a computer on your LAN.
3	LAN Setup	Use this menu to set up your LAN connection.
4	Internet Access Setup	Configure your Internet Access setup (Internet address, gateway, login, etc.) with this menu.
11	Remote Node Setup	Use this menu to configure detailed remote node settings (your ISP is also a remote node) as well as apply WAN filters.
12	Static Routing Setup	Use this menu to set up static routes.
15	NAT Setup	Use this menu to specify inside servers when NAT is enabled.
21	Filter and Firewall Setup	Configure filters and activate/deactivate the firewall.
22	SNMP Configuration	Use this menu to set up SNMP related parameters.
23	System Password	Use this menu to change your password.
24	System Maintenance	This menu provides system status, diagnostics, software upload, etc.
26	Schedule Setup	Use this menu to schedule outgoing calls.
99	Exit	Use this to exit from SMT and return to a blank screen.

## 21.3.2 Prestige SMT Menus Overview

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

**Table 95** SMT Menu Overview

MENUS	SUB MENUS		
1 General Setup	1.1 Configure Dynamic DNS		
2 WAN Setup			
3 LAN Setup	3.1 LAN Port Filter Setup		
	3.2 TCP/IP and DHCP Setup	3.2.1 IP Alias Setup	
4 Internet Access Setup			
11 Remote Node Setup	11.1 Remote Node Profile		
	11.3 Remote Node Network Layer Options		
	11.5 Remote Node Filter		
	11.6 Traffic Redirect Setup		
12 Static Routing Setup	12.1 Edit Static Route Setup		
15 NAT Setup	15.1 Address Mapping Sets	15.1.1 Address Mapping Rules	15.1.1.x Address Mapping Rule
	15.2 Port Forwarding Setup		
	15.3 Trigger Port Setup		
21 Filter and Firewall Setup	21.1 Filter Set Configuration	21.1.x Filter Rules Summary	21.1.x.x Generic Filter Rule
			21.1.x.x TCP/IP Filter Rule
	21.2 Firewall Setup		
23 Password			



**Table 95** SMT Menus Overview (continued)

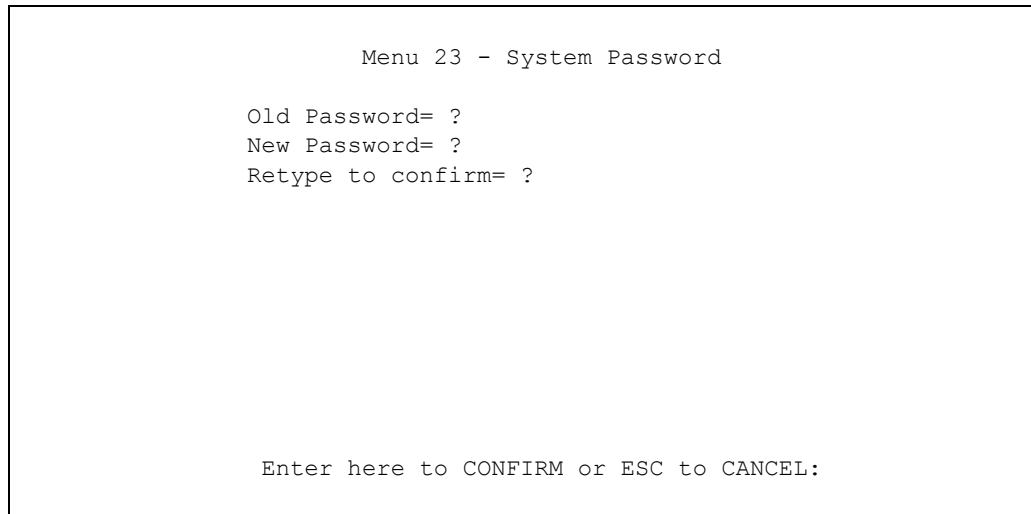
MENUS	SUB MENUS		
24 System Maintenance	24.1 System Status		
	24.2 System Information and Console Port Speed	24.2.1 System Information	
		24.2.2 Console Port Speed	
	24.3 Log and Trace	24.3.2 Syslog Logging	
		24.3.4 Call-Triggering Packet	
	24.4 Diagnostic		
	24.5 Backup Configuration		
	24.6 Restore Configuration		
	24.7 Upload Firmware	24.7.1 Upload System Firmware	
		24.7.2 Upload System Configuration File	
	24.8 Command Interpreter Mode		
	24.9 Call Control	24.9.1 Budget Management	
		24.9.2 Call History	
24.10 Time and Date Setting			
24.11 Remote Management Setup			

## 21.4 Changing the System Password

Change the Prestige default password by following the steps shown next.

- 1** Enter 23 in the main menu to display **Menu 23 System Password**.
- 2** Type your existing system password in the **Old Password** field, for example “1234”, and press [ENTER]

**Figure 107** Menu 23 System Password



```
Menu 23 - System Password

Old Password= ?
New Password= ?
Retype to confirm= ?

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

- 3** Type your new system password in the **New Password** field (up to 30 characters), and press [ENTER].
- 4** Re-type your new system password in the **Retype to confirm** field for confirmation and press [ENTER].

**Note:** When you type in a password, the screen displays an "\*" for each character typed

# CHAPTER 22

## General Setup

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

### 22.1 General Setup Introduction

See [Chapter 4 on page 62](#) for background information on general setup.

### 22.2 General Setup Configuration

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

**Figure 108** Menu 1 General Setup.

```

Menu 1 - General Setup

System Name=
Domain Name= zyxel.com.tw
First System DNS Server= From ISP
IP Address= N/A
Second System DNS Server= From ISP
IP Address= N/A
Third System DNS Server= From ISP
IP Address= N/A
Edit Dynamic DNS= No
Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the fields in this menu.

**Table 96** Menu 1 General Setup

FIELD	DESCRIPTION
System Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. You can go to menu 24.8 and type "sys domain name" to see the current domain name used by your router. Use up to 38 alphanumeric characters. Spaces are not allowed, but dashes "-" and periods "." are accepted.  The domain name entered by you is given priority over the ISP assigned domain name. If you want to clear this field just press [SPACE BAR] and then [ENTER].

**Table 96** Menu 1 General Setup (continued)

FIELD	DESCRIPTION
First System DNS Server Second System DNS Server Third System DNS Server	<p>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 Prestige uses a system DNS server (in the order you specify here) to resolve domain names for DDNS and the time server.</p> <p>Press [SPACE BAR] and then [ENTER] to select an option. Select <b>From ISP</b> if your ISP dynamically assigns DNS server information (and the Prestige's WAN IP address). The <b>IP Address</b> field below displays the (read-only) DNS server IP address that the ISP assigns.</p> <p>Select <b>User-Defined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the <b>IP Address</b> field. If you select <b>User-Defined</b>, but leave the IP address set to 0.0.0.0, <b>User-Defined</b> changes to <b>None</b> after you save your changes. If you set a second choice to <b>User-Defined</b>, and enter the same IP address, the second <b>User-Defined</b> changes to <b>None</b> after you save your changes.</p> <p>Select <b>None</b> if you do not want to configure DNS servers. If you do not configure a system DNS server, you must use IP addresses when configuring DDNS and the time server.</p>
Edit Dynamic DNS	Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> or <b>No</b> (default). Select <b>Yes</b> to configure <b>Menu 1.1: Configure Dynamic DNS</b> discussed next.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

## 22.2.1 Procedure to Configure Dynamic DNS

**Note:** If you have a private WAN IP address, then you cannot use Dynamic DNS

To configure Dynamic DNS, go to **Menu 1 — General Setup** and select **Yes** in the **Edit Dynamic DNS** field. Press [ENTER] to display **Menu 1.1— Configure Dynamic DNS** as shown next.

**Figure 109** Menu 1.1 Configure Dynamic DNS

```

Menu 1.1 - Configure Dynamic DNS

Service Provider= WWW.DynDNS.ORG
Active= No
DDNS Type= DynamicDNS
Host Name 1=
Host Name 2=
Host Name 3=
Username=
Password= *****
Enable Wildcard Option= No
Enable Off Line Option= N/A
IP Address Update Policy:
  DDNS Server Auto Detect IP Address= No
  Use Specified IP Address= No
  Use IP Address= N/A

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

```

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

**Table 97** Menu 1.1 Configure Dynamic DNS

FIELD	DESCRIPTION
Service Provider	This is the name of your Dynamic DNS service provider.
Active	Press [SPACE BAR] to select <b>Yes</b> and then press [ENTER] to make dynamic DNS active.
DDNSType	Press [SPACE BAR] and then [ENTER] to select <b>DynamicDNS</b> if you have a dynamic IP address(es). Select <b>StaticDNS</b> if you have a static IP address(es). Select <b>CustomDNS</b> to have dyns.org provide DNS service for a domain name that you already have from a source other than dyndns.org.
Host 1- 3	Enter your host name(s) in the fields provided. You can specify up to two host names separated by a comma in each field.
USER	Enter your user name.
Password	Enter the password assigned to you.
Enable Wildcard Option	Your Prestige supports DYNDNS Wildcard. Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> or <b>No</b> . This field is <b>N/A</b> when you choose DDNS client as your service provider.
Enable Offline Option	This field is only available when <b>CustomDNS</b> is selected in the <b>DDNS Type</b> field. Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> . When <b>Yes</b> is selected, <a href="http://www.dyndns.org/">http://www.dyndns.org/</a> traffic is redirected to a URL that you have previously specified (see <a href="http://www.dyndns.org/">www.dyndns.org</a> for details).

**Table 97** Menu 1.1 Configure Dynamic DNS (continued)

FIELD	DESCRIPTION
	<p>IP Address Update Policy:</p> <p>You can select <b>Yes</b> in either the <b>DDNS Server Auto Detect IP Address field</b> (recommended) or the <b>Use Specified IP Address field</b>, but not both.</p> <p>With the <b>DDNS Server Auto Detect IP Address field</b> and <b>Use Specified IP Address fields</b> both set to <b>No</b>, the DDNS server automatically updates the IP address of the host name(s) with the Prestige's WAN IP address.</p> <p>DDNS does not work with a private IP address. When both fields are set to <b>No</b>, the Prestige must have a public WAN IP address in order for DDNS to work.</p>
DDNS Server Auto Detect IP Address	<p>Press [SPACE BAR] to select <b>Yes</b> and then press [ENTER] to have the DDNS server automatically update the IP address of the host name(s) with the public IP address that the Prestige uses or is behind.</p> <p>You can set this field to <b>Yes</b> whether the IP address is public or private, static or dynamic.</p>
Use Specified IP Address	<p>Press [SPACE BAR] to select <b>Yes</b> and then press [ENTER] to update the IP address of the host name(s) to the IP address specified below.</p> <p>Only select <b>Yes</b> if the Prestige uses or is behind a static public IP address.</p>
IP Address	<p>Enter the static public IP address if you select <b>Yes</b> in the <b>User Specified IP Address field</b>.</p>
<p>When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.</p>	

**Note:** The IP address updates when you reconfigure menu 1 or perform DHCP client renewal

# CHAPTER 23

## WAN Setup

This chapter describes how to configure the WAN using menu 2.

### 23.1 Introduction to WAN

This chapter explains how to configure settings for your WAN port. Refer to [Chapter 6 on page 82](#) for background information.

### 23.2 WAN Setup

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

**Figure 110** Menu 2 WAN Setup

```

Menu 2 - WAN Setup

MAC Address:
Assigned By= Factory default
IP Address= N/A

Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the fields in this menu.

**Table 98** Menu 2 WAN Setup

FIELD	DESCRIPTION
MAC Address	
Assigned By	Press [SPACE BAR] and then [ENTER] to choose one of two methods to assign a MAC Address. Choose <b>Factory Default</b> to select the factory assigned default MAC Address. Choose <b>IP address attached on LAN</b> to use the MAC Address of that computer whose IP you give in the following field.
IP Address	This field is applicable only if you choose the <b>IP address attached on LAN</b> method in the <b>Assigned By</b> field. Enter the IP address of the computer on the LAN whose MAC you are cloning.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	





# CHAPTER 24

## LAN Setup

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

### 24.1 LAN Setup

This chapter describes how to configure the Ethernet using **Menu 3 — LAN Setup**. From the main menu, enter 3 to display menu 3. See [Chapter 5 on page 72](#) for background information.

**Figure 111** Menu 3 LAN Setup

```
Menu 3 - LAN Setup

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

Enter Menu Selection Number:
```

#### 24.1.1 General Ethernet Setup

This menu allows you to specify filter set(s) that you wish to apply to the Ethernet traffic. You seldom need to filter Ethernet traffic; however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches

**Figure 112** Menu 3.1 LAN Port Filter Setup.

```
Menu 3.1 - LAN Port Filter Setup

Input Filter Sets:
  protocol filters=
  device filters=
Output Filter Sets:
  protocol filters=
  device filters=

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

If you need to define filters, please read [Chapter 30 on page 276](#) first, then return to this menu to define the filter sets.

## 24.2 TCP/IP Ethernet Setup and DHCP

Use menu 3.2 to configure your Prestige for TCP/IP.

To edit menu 3.2, enter 3 from the main menu to display **Menu 3 — LAN Setup**. When menu 3 appears, press 2 and press [ENTER] to display **Menu 3.2 — TCP/IP and DHCP Ethernet Setup**, as shown next:

**Figure 113** Menu 3.2 TCP/IP and DHCP Ethernet Setup

```

Menu 3.2 - TCP/IP and DHCP Ethernet Setup

DHCP= Server                      TCP/IP Setup:
Client IP Pool:                   IP Address= 192.168.1.1
  Starting Address= 192.168.1.33  IP Subnet Mask= 255.255.255.0
  Size of Client IP Pool= 32      RIP Direction= Both
First DNS Server= From ISP        Version= RIP-1
  IP Address= N/A                Multicast= None
Second DNS Server= From ISP       Edit IP Alias= No
  IP Address= N/A
Third DNS Server= From ISP
  IP Address= N/A
DHCP Server Address= N/A

Press ENTER to Confirm or ESC to Cancel:

```

Follow the instructions in the next table on how to configure the DHCP fields.

**Table 99** DHCP Ethernet Setup Fields

FIELD	DESCRIPTION
DHCP	This field enables/disables the DHCP server. If set to <b>Server</b> , your Prestige will act as a DHCP server. If set to <b>None</b> , the DHCP server will be disabled. If set to <b>Relay</b> the Prestige acts as a surrogate DHCP server and relays requests and responses between the remote server and the clients. When set to <b>Server</b> , the following items need to be set:
Client IP Pools	
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.

**Table 99** DHCP Ethernet Setup Fields (continued)

FIELD	DESCRIPTION
First DNS Server Second DNS Server Third DNS Server	<p>The Prestige passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients.</p> <p>Select <b>From ISP</b> if your ISP dynamically assigns DNS server information (and the Prestige's WAN IP address). The <b>IP Address</b> field below displays the (read-only) DNS server IP address that the ISP assigns.</p> <p>Select <b>User-Defined</b> if you have the IP address of a DNS server. Enter the DNS server's IP address in the <b>IP Address</b> field below. If you chose <b>User-Defined</b>, but leave the IP address set to 0.0.0.0, <b>User-Defined</b> changes to <b>None</b> after you save your changes. If you set a second choice to <b>User-Defined</b>, and enter the same IP address, the second <b>User-Defined</b> changes to <b>None</b> after you save your changes.</p> <p>Select <b>DNS Relay</b> to have the Prestige act as a DNS proxy. The Prestige's LAN IP address displays in the <b>IP Address</b> field below (read-only). The Prestige tells the DHCP clients on the LAN that the Prestige itself is the DNS server. When a computer on the LAN sends a DNS query to the Prestige, the Prestige forwards the query to the Prestige's system DNS server (configured in menu 1) and relays the response back to the computer. You can only select <b>DNS Relay</b> for one of the three servers; if you select DNS Relay for a second or third DNS server, that choice changes to <b>None</b> after you save your changes.</p> <p>Select <b>None</b> if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.</p>
DHCP Server Address	If <b>Relay</b> is selected in the <b>DHCP</b> field above, then type the IP address of the actual, remote DHCP server here.

Use the instructions in the following table to configure TCP/IP parameters for the LAN port.

**Table 100** Menu 3.2: LAN TCP/IP Setup Fields

FIELD	DESCRIPTION
TCP/IP Setup:	
IP Address	Enter the IP address of your Prestige in dotted decimal notation
IP Subnet Mask	Your Prestige will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Prestige.
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction. Options are: <b>Both, In Only, Out Only</b> or <b>None</b> .
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are: <b>RIP-1, RIP-2B</b> or <b>RIP-2M</b> .
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The Prestige supports both IGMP version 1 ( <b>IGMP-v1</b> ) and version 2 ( <b>IGMP-v2</b> ). Press [SPACE BAR] and then [ENTER] to enable IP Multicasting or select <b>None</b> (default) to disable it.
Edit IP Alias	The Prestige supports three logical LAN interfaces via its single physical Ethernet interface with the Prestige itself as the gateway for each LAN network. Press [SPACE BAR] to select <b>Yes</b> and then press [ENTER] to display menu 3.2.1
When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm...] to save your configuration, or press [ESC] at any time to cancel.	

## 24.2.1 IP Alias Setup

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

Use menu 3.2 to configure the first network. Move the cursor to the **Edit IP Alias** field, press [SPACE BAR] to choose **Yes** and press [ENTER] to configure the second and third networks.

Press [ENTER] to open **Menu 3.2.1 - IP Alias Setup**, as shown next.

**Figure 114** Menu 3.2.1: IP Alias Setup

```

Menu 3.2.1 - IP Alias Setup

IP Alias 1= Yes
IP Address=
IP Subnet Mask= 0.0.0.0
RIP Direction= None
    Version= RIP-1
Incoming protocol filters=
Outgoing protocol filters=
IP Alias 2= No
IP Address= N/A
IP Subnet Mask= N/A
RIP Direction= N/A
    Version= N/A
Incoming protocol filters= N/A
Outgoing protocol filters= N/A

Enter here to CONFIRM or ESC to CANCEL:

```

Use the instructions in the following table to configure IP alias parameters.

**Table 101** Menu 3.2.1: IP Alias Setup

FIELD	DESCRIPTION
IP Alias 1, 2	Choose <b>Yes</b> to configure the LAN network for the Prestige.
IP Address	Enter the IP address of your Prestige in dotted decimal notation.
IP Subnet Mask	Your Prestige will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Prestige.
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction. Options are <b>Both</b> , <b>In Only</b> , <b>Out Only</b> or <b>None</b> .
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are <b>RIP-1</b> , <b>RIP-2B</b> or <b>RIP-2M</b> .
Incoming protocol filters	Enter the filter set(s) you wish to apply to the incoming traffic between this node and the Prestige.

**Table 101** Menu 3.2.1: IP Alias Setup (continued)

FIELD	DESCRIPTION
Outgoing protocol filters	Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the Prestige.
When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm...] to save your configuration, or press [ESC] at any time to cancel.	



# CHAPTER 25

## Internet Access

This chapter shows you how to configure your Prestige for Internet access.

### 25.1 Introduction to Internet Access Setup

Use information from your ISP along with the instructions in this chapter to set up your Prestige to access the Internet. There are different menu 4 screens depending on whether you chose **Ethernet** or **PPPoE** Encapsulation. Contact your ISP to determine what encapsulation type you should use.

### 25.2 Ethernet Encapsulation

From the main menu, type 4 to display **Menu 4 - Internet Access Setup**.

If you choose **Ethernet** in menu 4 you will see the next menu.

**Figure 115** Menu 4 Internet Access Setup

```
Menu 4 - Internet Access Setup

ISP's Name= MyISP
Encapsulation= Ethernet
Service Type= Standard
  My Login= N/A
    Password= N/A
  Retype to Confirm= N/A
  Login Server= N/A

IP Address Assignment= Dynamic
  IP Address= N/A
  IP Subnet Mask= N/A
  Gateway IP Address= N/A
  Network Address Translation= SUA Only

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

The following table describes the fields in this menu.

**Table 102** Internet Access Setup (Ethernet)

FIELD	DESCRIPTION
ISP's Name	Enter the name of your Internet Service Provider, e.g., myISP. This information is for identification purposes only.
Encapsulation	Press [SPACE BAR] and then press [ENTER] to choose <b>Ethernet</b> . The encapsulation method influences your choices for the <b>IP Address</b> field.
Service Type	Press [SPACE BAR] and then [ENTER] to select <b>Standard</b> , <b>RR-Toshiba</b> (RoadRunner Toshiba authentication method), <b>RR-Manager</b> (RoadRunner Manager authentication method) or <b>RR-Telstra</b> . Choose a RoadRunner flavor if your ISP is Time Warner's RoadRunner; otherwise choose <b>Standard</b> .
Note: DSL users must choose the <b>Standard</b> option only. The <b>My Login</b> , <b>My Password</b> and <b>Login Server</b> fields are not applicable in this case.	
My Login	Enter the login name given to you by your ISP.
My Password	Type your password again for confirmation.
Retype to Confirm	Enter your password again to make sure that you have entered is correctly.
Login Server	The Prestige will find the RoadRunner Server IP if this field is left blank. If it does not, then you must enter the authentication server IP address.
IP Address Assignment	If your ISP did not assign you a fixed IP address, press [SPACE BAR] and then [ENTER] to select <b>Dynamic</b> , otherwise select <b>Static</b> and enter the IP address and subnet mask in the following fields.
IP Address	Enter the (fixed) IP address assigned to you by your ISP (static IP address assignment is selected in the previous field).
IP Subnet Mask	Enter the subnet mask associated with your static IP.
Gateway IP Address	Enter the gateway IP address associated with your static IP.
Network Address Translation	<p>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).</p> <p>Choose <b>None</b> to disable NAT.</p> <p>Choose <b>SUA Only</b> if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: <b>Many-to-One</b> and <b>Server</b>.</p> <p>Choose <b>Full Feature</b> if you have multiple public IP addresses. <b>Full Feature</b> mapping types include: <b>One-to-One</b>, <b>Many-to-One</b> (SUA/PAT), <b>Many-to-Many Overload</b>, <b>Many- One-to-One</b> and <b>Server</b>. When you select <b>Full Feature</b> you must configure at least one address mapping set!</p> <p>Please see <a href="#">Chapter 12 on page 128</a> for a more detailed discussion on the Network Address Translation feature.</p>
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	

## 25.3 Configuring the PPPoE Client

If you enable PPPoE in menu 4, you will see the next screen. For more information on PPPoE, please see the appendix.



**Figure 116** Internet Access Setup (PPPoE)

```

Menu 4 - Internet Access Setup

ISP's Name= MyISP
Encapsulation= PPPoE
Service Type= N/A
My Login=
My Password= *****
Retype to Confirm= *****
Idle Timeout= 100
IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Address= N/A
Network Address Translation= SUA Only

Press ENTER to Confirm or ESC to Cancel:

```

The following table contains instructions about the new fields when you choose **PPPoE** in the **Encapsulation** field in menu 4.

**Table 103** New Fields in Menu 4 (PPPoE)

FIELD	DESCRIPTION
Encapsulation	Press [SPACE BAR] and then press [ENTER] to choose <b>PPPoE</b> . The encapsulation method influences your choices in the <b>IP Address</b> field.
Idle Timeout	This value specifies the time in seconds that elapses before the Prestige automatically disconnects from the PPPoE server.

If you need a PPPoE service name to identify and reach the PPPoE server, please go to menu 11 and enter the PPPoE service name provided to you in the **Service Name** field.

## 25.4 Basic Setup Complete

Well done! You have successfully connected, installed and set up your Prestige to operate on your network as well as access the Internet.



# CHAPTER 26

## Remote Node Configuration

This chapter covers remote node configuration.

### 26.1 Introduction to Remote Node Setup

A remote node is required for placing calls to a remote gateway. A remote node represents both the remote gateway and the network behind it across a WAN connection. Note that when you use menu 4 to set up Internet access, you are actually configuring a remote node. The following describes how to configure **Menu 11.1 Remote Node Profile**, **Menu 11.3 - Remote Node Network Layer Options**, **Menu 11.5 - Remote Node Filter** and **Menu 11.6 - Traffic Redirect Setup**.

### 26.2 Remote Node Profile Setup

From the main menu, select menu option 11 to open **Menu 11 Remote Node Profile** (shown below).

The following explains how to configure the remote node profile menu.

#### 26.2.1 Ethernet Encapsulation

There are two variations of menu 11 depending on whether you choose **Ethernet Encapsulation** or **PPPoE Encapsulation**. You must choose the **Ethernet** option when the WAN port is used as a regular Ethernet. The first menu 11.1 screen you see is for Ethernet encapsulation shown next.

**Figure 117** Menu 11.1 Remote Node Profile for Ethernet Encapsulation

```

Menu 11.1 - Remote Node Profile

Rem Node Name= MyISP                Route= IP
Active= Yes

Encapsulation= Ethernet             Apply Alias= None
Service Type= Standard              Edit IP= No
Service Name= N/A                   Session Options:
Outgoing:                            Edit Filter Sets= No
  My Login= N/A                      Edit Traffic Redirect= No
  My Password= N/A
  Retype to Confirm= N/A
  Server= N/A

Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the fields in this menu.

**Table 104** Menu 11.1 Remote Node Profile for Ethernet Encapsulation

FIELD	DESCRIPTION
Rem Node Name	Enter a descriptive name for the remote node. This field can be up to eight characters.
Active	Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> (activate remote node) or <b>No</b> (deactivate remote node).
Encapsulation	<b>Ethernet</b> is the default encapsulation. Press [SPACE BAR] and then [ENTER] to change to <b>PPPoE</b> encapsulation.
Service Type	Press [SPACE BAR] and then [ENTER] to select from <b>Standard</b> , <b>RR-Toshiba</b> (RoadRunner Toshiba authentication method), <b>RR-Manager</b> (RoadRunner Manager authentication method), or <b>RR-Telstra</b> . Choose one of the RoadRunner methods if your ISP is Time Warner's RoadRunner; otherwise choose <b>Standard</b> .
Outgoing	
My Login	This field is applicable for <b>PPPoE</b> encapsulation only. Enter the login name assigned by your ISP when the Prestige calls this remote node. Some ISPs append this field to the <b>Service Name</b> field above (e.g., jim@poellic) to access the PPPoE server.
My Password	Enter the password assigned by your ISP when the Prestige calls this remote node. Valid for <b>PPPoE</b> encapsulation only.
Retype to Confirm	Type your password again to make sure that you have entered it correctly.
Server	This field is valid only when <b>RoadRunner</b> is selected in the <b>Service Type</b> field. The Prestige will find the RoadRunner Server IP automatically if this field is left blank. If it does not, then you must enter the authentication server IP address here.

**Table 104** Menu 11.1 Remote Node Profile for Ethernet Encapsulation (continued)

FIELD	DESCRIPTION
Route	This field refers to the protocol that will be routed by your Prestige – IP is the only option for the Prestige.
Apply Alias	Press [SPACE BAR] to select an IP alias if you want to use one for this static route. Leave <b>None</b> selected to use the regular LAN IP address.
Edit IP	This field leads to a “hidden” menu. Press [SPACE BAR] to select <b>Yes</b> and press [ENTER] to go to <b>Menu 11.3 - Remote Node Network Layer Options</b> .
Session Options	
Edit Filter Sets	This field leads to another “hidden” menu. Use [SPACE BAR] to select <b>Yes</b> and press [ENTER] to open menu 11.5 to edit the filter sets. See <a href="#">Section 26.4 on page 252</a> for more details.
Edit Traffic Redirect	Press [SPACE BAR] to select <b>Yes</b> or <b>No</b> . Select <b>Yes</b> and press [ENTER] to configure <b>Menu 11.6 Traffic Redirect Setup</b> . Select <b>No</b> (default) if you do not want to configure this feature.
Once you have configured this menu, press [ENTER] at the message “Press ENTER to Confirm...” to save your configuration, or press [ESC] at any time to cancel.	

## 26.2.2 PPPoE Encapsulation

The Prestige supports PPPoE (Point-to-Point Protocol over Ethernet). You can only use PPPoE encapsulation when you're using the Prestige with a DSL modem as the WAN device. If you change the Encapsulation to **PPPoE**, then you will see the next screen. Please see the appendix for more information on PPPoE.

**Figure 118** Menu 11.1 Remote Node Profile for PPPoE Encapsulation

```
Menu 11.1 - Remote Node Profile

Rem Node Name= MyISP           Route= IP
Active= Yes

Encapsulation= PPPoE          Apply Alias= Alias 1
Service Type= Standard        Edit IP= No
Service Name=                 Telco Option:
Outgoing:                     Allocated Budget(min)= 0
  My Login=                   Period(hr)= 0
  My Password= *****       Schedules=
  Retype to Confirm= *****  Nailed-Up Connection= No
  Authen= CHAP/PAP

                               Session Options:
                               Edit Filter Sets= No
                               Idle Timeout(sec)= 0

                               Edit Traffic Redirect= No

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

### 26.2.2.1 Outgoing Authentication Protocol

Generally speaking, you should employ the strongest authentication protocol possible, for obvious reasons. However, some vendor's implementation includes a specific authentication protocol in the user profile. It will disconnect if the negotiated protocol is different from that in the user profile, even when the negotiated protocol is stronger than specified. If you encounter a case where the peer disconnects right after a successful authentication, please make sure that you specify the correct authentication protocol when connecting to such an implementation.

### 26.2.2.2 Nailed-Up Connection

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.

The following table describes the fields not already described in [Table 104 on page 247](#).

**Table 105** Fields in Menu 11.1 (PPPoE Encapsulation Specific)

FIELD	DESCRIPTION
Service Name	If you are using <b>PPPoE</b> encapsulation, then type the name of your PPPoE service here. Only valid with <b>PPPoE</b> encapsulation.
Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are: <ul style="list-style-type: none"> <li>• <b>CHAP/PAP</b> - Your Prestige will accept either <b>CHAP</b> or <b>PAP</b> when requested by this remote node.</li> <li>• <b>CHAP</b>- accept CHAP only.</li> <li>• <b>PAP</b>- accept PAP only.</li> </ul>
Telco Option	
Allocated Budget	The field sets a ceiling for outgoing call time for this remote node. The default for this field is 0 meaning no budget control.
Period(hr)	This field is the time period that the budget should be reset. For example, if we are allowed to call this remote node for a maximum of 10 minutes every hour, then the <b>Allocated Budget</b> is (10 minutes) and the <b>Period(hr)</b> is 1 (hour).
Schedules	You can apply up to four schedule sets here.
Nailed-Up Connection	This field specifies if you want to make the connection to this remote node a nailed-up connection. More details are given earlier in this section.
Session Options	
Idle Timeout	Type the length of idle time (when there is no traffic from the Prestige to the remote node) in seconds that can elapse before the Prestige automatically disconnects the PPPoE connection. This option only applies when the Prestige initiates the call.

## 26.3 Edit IP

Move the cursor to the **Edit IP** field in menu 11.1, then press [SPACE BAR] to select **Yes**. Press [ENTER] to open **Menu 11.3 - Remote Node Network Layer Options**.

**Figure 119** Menu 11.3 Remote Node Network Layer Options for Ethernet Encapsulation

```

Menu 11.3 - Remote Node Network Layer Options

IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Addr= N/A

Network Address Translation= SUA Only
Metric= 1
Private= N/A
RIP Direction= None
    Version= N/A
Multicast= None

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

This menu displays the **My WAN Addr** field for **PPPoE** encapsulation and **Gateway IP Addr** field for **Ethernet** encapsulation. The following table describes the fields in this menu.

**Table 106** Remote Node Network Layer Options

FIELD	DESCRIPTION
IP Address Assignment	If your ISP did not assign you an explicit IP address, press [SPACE BAR] and then [ENTER] to select <b>Dynamic</b> ; otherwise select <b>Static</b> and enter the IP address & subnet mask in the following fields.
(Rem) IP Address	If you have a static IP Assignment, enter the IP address assigned to you by your ISP.
(Rem) IP Subnet Mask	If you have a static IP Assignment, enter the subnet mask assigned to you.
Gateway IP Addr	This field is applicable to <b>Ethernet</b> encapsulation only. Enter the gateway IP address assigned to you if you are using a static IP address.
My WAN Addr	This field is applicable to <b>PPPoE</b> encapsulation only. Some implementations, especially the UNIX derivatives, require the WAN link to have a separate IP network number from the LAN and each end must have a unique address within the WAN network number. If this is the case, enter the IP address assigned to the WAN port of your Prestige. Note that this is the address assigned to your local Prestige, not the remote router.
Network Address Translation	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). Choose <b>None</b> to disable NAT. Choose <b>SUA Only</b> if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: <b>Many-to-One</b> and <b>Server</b> . Choose <b>Full Feature</b> if you have multiple public IP addresses. <b>Full Feature</b> mapping types include: <b>One-to-One</b> , <b>Many-to-One (SUA/PAT)</b> , <b>Many-to-Many Overload</b> , <b>Many- One-to-One</b> and <b>Server</b> . When you select <b>Full Feature</b> you must configure at least one address mapping set! See for a full discussion on this feature.
Metric	Enter a number from 1 to 15 to set this route's priority among the Prestige's routes. The smaller the number, the higher priority the route has.



**Table 106** Remote Node Network Layer Options (continued)

FIELD	DESCRIPTION
Private	This field is valid only for PPPoE encapsulation. This parameter determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to <b>Yes</b> , this route is kept private and not included in RIP broadcast. If <b>No</b> , the route to this remote node will be propagated to other hosts through RIP broadcasts.
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction from <b>Both/ None/ In Only/Out Only</b> . The default for RIP on the WAN side is <b>None</b> . It is recommended that you do not change this setting.
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version from <b>RIP-1/RIP-2B/ RIP-2M</b> or <b>None</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 version 2 ( <b>IGMP-v2</b> ). Press [SPACE BAR] to enable IP Multicasting or select <b>None</b> to disable it. See <a href="#">Section 5.7 on page 75</a> for more information on this feature.
Once you have completed filling in <b>Menu 11.3 Remote Node Network Layer Options</b> , press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration and return to menu 11, or press [ESC] at any time to cancel.	

## 26.4 Remote Node Filter

Move the cursor to the field **Edit Filter Sets** in menu 11.1, and then press [SPACE BAR] to set the value to **Yes**. Press [ENTER] to open **Menu 11.5 - Remote Node Filter**.

Use menu 11.5 to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the Prestige to prevent certain packets from triggering calls. You can specify up to 4 filter sets separated by commas, for example, 1, 5, 9, 12, in each filter field. Note that spaces are accepted in this field. For PPPoE encapsulation, you have the additional option of specifying remote node call filter sets.

**Figure 120** Menu 11.5: Remote Node Filter (Ethernet Encapsulation)

```
Menu 11.5 - Remote Node Filter

Input Filter Sets:
  protocol filters=
  device filters=
Output Filter Sets:
  protocol filters=
  device filters=

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

**Figure 121** Menu 11.5: Remote Node Filter (PPPoE Encapsulation)

```
Menu 11.5 - Remote Node Filter

Input Filter Sets:
  protocol filters=
  device filters=
Output Filter Sets:
  protocol filters=
  device filters=
Call Filter Sets:
  protocol filters=
  device filters=

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

## 26.4.1 Traffic Redirect Setup

Configure parameters that determine when the Prestige will forward traffic to the backup gateway using **Menu 11.6 — Traffic Redirect Setup**.

**Figure 122** Menu 11.6: Traffic Redirect Setup

```

Menu 11.6 - Traffic Redirect Setup

Active= Yes
Configuration:
  Backup Gateway IP Address= 0.0.0.0
  Metric= 14
  Check WAN IP Address= 0.0.0.0
  Fail Tolerance= 2
  Period(sec)= 5
  Timeout(sec)= 3

Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the fields in this screen.

**Table 107** Menu 11.6: Traffic Redirect Setup

FIELD	DESCRIPTION
Active	Press [SPACE BAR] and select <b>Yes</b> (to enable) or <b>No</b> (to disable) traffic redirect setup. The default is <b>No</b> .
Configuration:	
Backup Gateway IP Address	Enter the IP address of your backup gateway in dotted decimal notation. The Prestige automatically forwards traffic to this IP address if the Prestige's Internet connection terminates.
Metric	Enter a number from 1 to 15 to set this route's priority among the Prestige's routes. The smaller the number, the higher priority the route has.
Check WAN IP Address	Enter the IP address of a reliable nearby computer (for example, your ISP's DNS server address) to test your Prestige's WAN accessibility. The Prestige uses the default gateway IP address if you do not enter an IP address here.  If you are using PPPoE Encapsulation, enter "0.0.0.0" to configure the Prestige to check the PVC (Permanent Virtual Circuit).
Fail Tolerance	Enter the number of times your Prestige may attempt and fail to connect to the Internet before traffic is forwarded to the backup gateway. Two to five is usually a good number.
Period (sec)	Enter the time interval (in seconds) between WAN connection checks. Five to 60 is usually a good number.
Timeout (sec)	Enter the number of seconds the Prestige waits for a ping response from the IP Address in the <b>Check WAN IP Address</b> field before it times out. The number in this field should be less than the number in the <b>Period</b> field. Three to 50 is usually a good number.  The WAN connection is considered "down" after the Prestige times out the number of times specified in the <b>Fail Tolerance</b> field.
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen	



# CHAPTER 27

## Static Route Setup

This chapter shows how to setup IP static routes.

### 27.1 Static Route Introduction

See [Chapter 13 on page 142](#) for background information on IP static routes.

### 27.2 IP Static Route Setup

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

**Figure 123** Menu 12 IP Static Route Setup

```
Menu 12 - IP Static Route Setup

1. Default Route
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____

Enter selection number:
```

Now, type the route number of a static route you want to configure.

**Note:** The first static route entry is the Prestige's default route and cannot be modified or deleted.

**Figure 124** Menu12.1 Edit IP Static Route

```

Menu 12.1 - Edit IP Static Route

Route #: 2
Route Name= ?
Active= No
Destination IP Address= ?
IP Subnet Mask= ?
Gateway IP Address= ?
Metric= 2
Private= No

Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the fields for **Menu 12.1 – Edit IP Static Route Setup**.

**Table 108** Menu12.1 Edit IP Static Route

FIELD	DESCRIPTION
Route #	This is the index number of the static route that you chose in menu 12.1.
Route Name	Type a descriptive name for this route. This is for identification purpose only.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Type the subnet mask for this destination. Follow the discussion on <i>IP Subnet Mask</i> in this manual.
Gateway IP Address	Type the IP address of the gateway. The gateway is an immediate neighbor of your Prestige that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your Prestige; over WAN, the gateway must be the IP address of one of the remote nodes.
Metric	Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Type a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Private	This parameter determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to <b>Yes</b> , this route is kept private and is not included in RIP broadcasts. If <b>No</b> , the route to this remote node will be propagated to other hosts through RIP broadcasts.
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

# CHAPTER 28

## Network Address Translation (NAT)

This chapter discusses how to configure NAT on the Prestige.

### 28.1 NAT Introduction

See [Chapter 12 on page 128](#) for background information on NAT.

### 28.2 Applying NAT

You apply NAT via menus 4 or 11.3 as displayed next. The next figure shows you how to apply NAT for Internet access in menu 4. Enter 4 from the main menu to go to **Menu 4 - Internet Access Setup**.

**Figure 125** Menu 4 Applying NAT for Internet Access

```
Menu 4 - Internet Access Setup

ISP's Name= MyISP
Encapsulation= Ethernet
  Service Type= Standard
  My Login= N/A
    Password= N/A
  Retype to Confirm= N/A
  Login Server= N/A

IP Address Assignment= Dynamic
  IP Address= N/A
  IP Subnet Mask= N/A
  Gateway IP Address= N/A
  Network Address Translation= SUA Only

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

The following figure shows how you apply NAT to the remote node in menu 11.1.

- 1 Enter 11 from the main menu.
- 2 When menu 11 appears, as shown in the following figure, type the number of the remote node that you want to configure.

- 3 Move the cursor to the **Edit IP** field, press [SPACE BAR] to select **Yes** and then press [ENTER] to bring up **Menu 11.3 - Remote Node Network Layer Options**.

**Figure 126** Menu 11.3 Applying NAT to the Remote Node

```

Menu 11.3 - Remote Node Network Layer Options

IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Addr= N/A
Network Address Translation= SUA Only
Metric= 1
Private= N/A
RIP Direction= None
  Version= N/A
Multicast= None

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

The following table describes the options for Network Address Translation.

**Table 109** Applying NAT in Menus 4 & 11.3

FIELD	DESCRIPTION
NAT	Press [SPACE BAR] and then [ENTER] to select <b>Full Feature</b> if you have multiple public WAN IP addresses for your Prestige. The SMT uses the address mapping set that you configure and enter in the <b>Address Mapping Set</b> field (menu 15.1 - see <a href="#">Section 28.3.1 on page 260</a> ).
	Select <b>None</b> to disable NAT.
	When you select <b>SUA Only</b> , the SMT uses Address Mapping Set 255 (menu 15.1 - see <a href="#">Section 28.3.1 on page 260</a> ). Choose <b>SUA Only</b> if you have just one public WAN IP address for your Prestige.

## 28.3 NAT Setup

Use the address mapping sets menus and submenus to create the mapping table used to assign global addresses to computers on the LAN. **Set 255** is used for SUA. When you select **Full Feature** in menu 4 or 11.3, the SMT will use **Set 1**. When you select **SUA Only**, the SMT will use the pre-configured **Set 255** (read only).

The server set is a list of LAN servers mapped to external ports. To use this set, a server rule must be set up inside the NAT address mapping set. Please see [Section 12.3.2 on page 132](#) for further information on these menus. To configure NAT, enter 15 from the main menu to bring up the following screen.



**Figure 127** Menu 15 NAT Setup

```

Menu 15 - NAT Setup

1. Address Mapping Sets
2. Port Forwarding Setup
3. Trigger Port Setup

Enter Menu Selection Number:

```

### 28.3.1 Address Mapping Sets

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

**Figure 128** Menu 15.1 Address Mapping Sets

```

Menu 15.1 - Address Mapping Sets

1. NAT_SET
255. SUA (read only)

Enter Menu Selection Number:

```

Enter 255 to display the next screen (see [Section 12.3 on page 131](#) for more on SUA). The fields in this menu cannot be changed.

**Figure 129** Menu 15.1.255 SUA Address Mapping Rules

```

Menu 15.1.255 - Address Mapping Rules

Set Name= SUA
Idx  Local Start IP  Local End IP    Global Start IP  Global End IP    Type
---  -
1.   0.0.0.0          255.255.255.255  0.0.0.0          Server
2.
3.
4.
5.
6.
7.
8.
9.
10.

Press ENTER to Confirm or ESC to Cancel:

```

The following table explains the fields in this menu.

**Table 110** SUA Address Mapping Rules

FIELD	DESCRIPTION
Set Name	This is the name of the set you selected in menu 15.1 or enter the name of a new set you want to create.
Idx	This is the index or rule number.
Local Start IP	<b>Local Start IP</b> is the starting local IP address (ILA).
Local End IP	<b>Local End IP</b> is the ending local IP address (ILA). If the rule is for all local IPs, then the Start IP is 0.0.0.0 and the End IP is 255.255.255.255.
Global Start IP	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the <b>Global Start IP</b> .
Global End IP	This is the ending global IP address (IGA).
Type	These are the mapping types. <b>Server</b> allows us to specify multiple servers of different types behind NAT to this machine. See later for some examples.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

**Note:** Menu 15.1.255 is read-only.

### 28.3.1.1 User-Defined Address Mapping Sets

Now let's look at option 1 in menu 15.1. Enter 1 to bring up this menu. We'll just look at the differences from the previous menu. Note the extra **Action** and **Select Rule** fields mean you can configure rules in this screen. Note also that the [?] in the **Set Name** field means that this is a required field and you must enter a name for the set.

**Figure 130** Menu 15.1.1 First Set

```

Menu 15.1.1 - Address Mapping Rules

Set Name= NAT_SET
Idx  Local Start IP  Local End IP  Global Start IP  Global End IP  Type
-----
1.
2.
3.
4.
5.
6.
7.
8.
9.
10.

Action= Edit      Select Rule=

Press ENTER to Confirm or ESC to Cancel:

```

**Note:** If the Set Name field is left blank, the entire set will be deleted.

**Note:** The Type, Local and Global Start/End IPs are configured in menu 15.1.1.1 (described later) and the values are displayed here

### 28.3.1.2 Ordering Your Rules

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

Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so as old rule 5 becomes rule 4, old rule 6 becomes rule 5 and old rule 7 becomes rule 6.

**Table 111** Menu 15.1.1 First Set

FIELD	DESCRIPTION
Set Name	Enter a name for this set of rules. This is a required field. If this field is left blank, the entire set will be deleted.

**Table 111** Menu 15.1.1 First Set

FIELD	DESCRIPTION
Action	The default is <b>Edit</b> . <b>Edit</b> means you want to edit a selected rule (see following field). <b>Insert Before</b> means to insert a rule before the rule selected. The rules after the selected rule will then be moved down by one rule. <b>Delete</b> means to delete the selected rule and then all the rules after the selected one will be advanced one rule. <b>None</b> disables the <b>Select Rule</b> item.
Select Rule	When you choose <b>Edit</b> , <b>Insert Before</b> or <b>Delete</b> in the previous field the cursor jumps to this field to allow you to select the rule to apply the action in question.

**Note:** You must press [ENTER] at the bottom of the screen to save the whole set. You must do this again if you make any changes to the set – including deleting a rule. No changes to the set take place until this action is taken

Selecting **Edit** in the **Action** field and then selecting a rule brings up the following menu, **Menu 15.1.1.1 - Address Mapping Rule** in which you can edit an individual rule and configure the **Type**, **Local** and **Global Start/End IPs**.

**Note:** An End IP address must be numerically greater than its corresponding IP Start address

**Figure 131** Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set

```

Menu 15.1.1.1 Address Mapping Rule

Type= One-to-One
Local IP:
  Start=
  End = N/A
Global IP:
  Start=
  End = N/A

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

The following table explains the fields in this menu.

**Table 112** Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set

FIELD	DESCRIPTION
Type	Press [SPACE BAR] and then [ENTER] to select from a total of five types. These are the mapping types discussed in the chapter on NAT web configurator screens. <b>Server</b> allows you to specify multiple servers of different types behind NAT to this computer. See <a href="#">Section 28.5 on page 265</a> for examples.
Local IP	Only local IP fields are <b>N/A</b> for server; Global IP fields <b>MUST</b> be set for <b>Server</b> .
Start	This is the starting local IP address (ILA).
End	This is the ending local IP address (ILA). If the rule is for all local IPs, then put the <b>Start IP</b> as 0.0.0.0 and the <b>End IP</b> as 255.255.255.255. This field is <b>N/A</b> for One-to-One and Server types.
Global IP	

**Table 112** Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set

FIELD	DESCRIPTION
Start	This is the starting inside global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the <b>Global IP Start</b> . Note that <b>Global IP Start</b> can be set to 0.0.0.0 only if the types are <b>Many-to-One</b> or <b>Server</b> .
End	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 types</b> .

When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.

## 28.4 Configuring a Server behind NAT

Follow these steps to configure a server behind NAT:

- 1 Enter 15 in the main menu to go to **Menu 15 - NAT Setup**.
- 2 Enter 2 to display **Menu 15.2 - NAT Server Setup** as shown next.

**Figure 132** Menu 15.2 NAT Server Setup

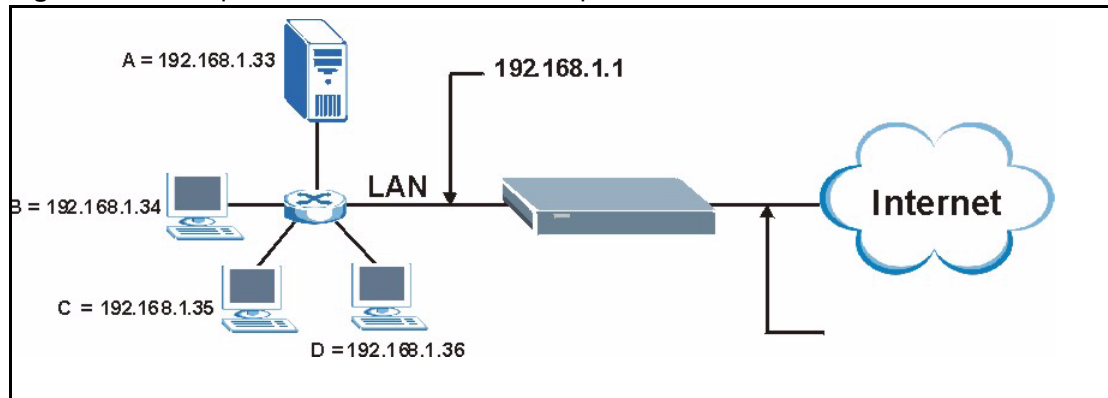
Menu 15.2 - NAT Server Setup			
Rule	Start Port No.	End Port No.	IP Address
1.	Default	Default	0.0.0.0
2.	21	25	192.168.1.33
3.	0	0	0.0.0.0
4.	0	0	0.0.0.0
5.	0	0	0.0.0.0
6.	0	0	0.0.0.0
7.	0	0	0.0.0.0
8.	0	0	0.0.0.0
9.	0	0	0.0.0.0
10.	0	0	0.0.0.0
11.	0	0	0.0.0.0
12.	0	0	0.0.0.0

Press ENTER to Confirm or ESC to Cancel:

- 3 Enter a port number in an unused **Start Port No** field. To forward only one port, enter it again in the **End Port No** field. To specify a range of ports, enter the last port to be forwarded in the **End Port No** field.
- 4 Enter the inside IP address of the server in the **IP Address** field. In the following figure, you have a computer acting as an FTP, Telnet and SMTP server (ports 21, 23 and 25) at 192.168.1.33.
- 5 Press [ENTER] at the "Press ENTER to confirm ..." prompt to save your configuration after you define all the servers or press [ESC] at any time to cancel.

You assign the private network IP addresses. The NAT network appears as a single host on the Internet. A is the FTP/Telnet/SMTP server.

**Figure 133** Multiple Servers Behind NAT Example



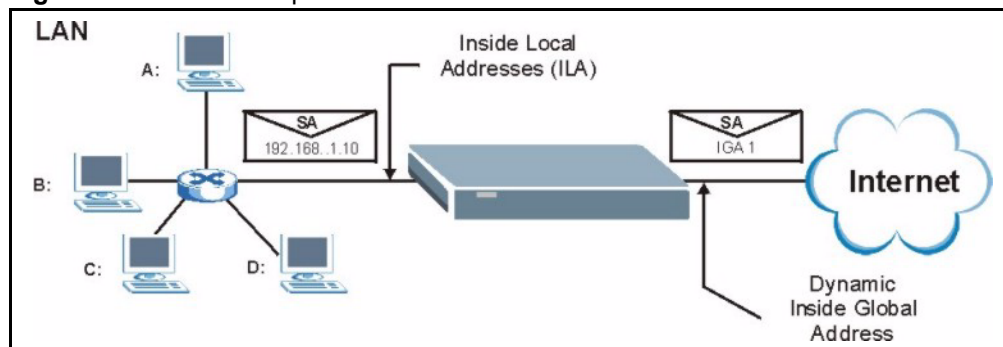
## 28.5 General NAT Examples

The following are some examples of NAT configuration.

### 28.5.1 Example 1: Internet Access Only

In the following Internet access example, you only need one rule where the ILAs (Inside Local Addresses) of computers A through D map to one dynamic IGA (Inside Global Address) assigned by your ISP.

**Figure 134** NAT Example 1



**Figure 135** Menu 4 Internet Access & NAT Example

```

Menu 4 - Internet Access Setup

ISP's Name= MyISP
Encapsulation= Ethernet
Service Type= Standard
My Login= N/A
My Password= N/A
Retype to Confirm= N/A
Login Server= N/A

IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Address= N/A
Network Address Translation = SUA Only

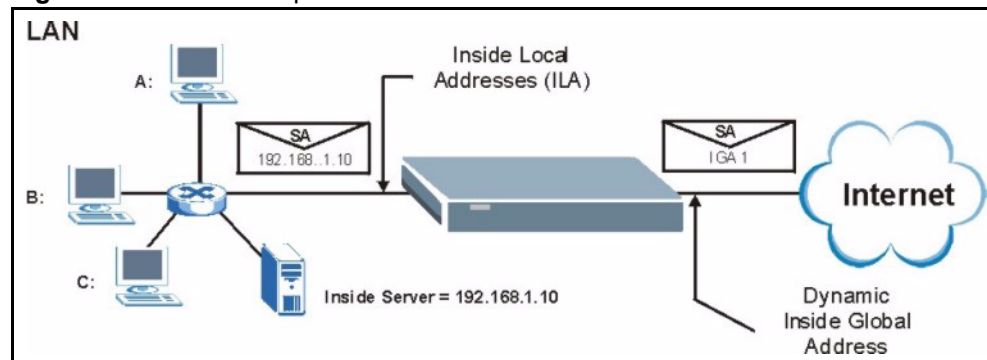
Press ENTER to Confirm or ESC to Cancel:

```

From menu 4, choose the **SUA Only** option from the **Network Address Translation** field. This is the Many-to-One mapping discussed in [Section 28.5 on page 265](#). The **SUA Only** read-only option from the **Network Address Translation** field in menus 4 and 11.3 is specifically pre-configured to handle this case.

## 28.5.2 Example 2: Internet Access with an Inside Server

The dynamic Inside Global Address is assigned by the ISP.

**Figure 136** NAT Example 2

In this case, you do exactly as above (use the convenient pre-configured **SUA Only** set) and also go to menu 15.2 to specify the Inside Server behind the NAT as shown in the next figure.

**Figure 137** Menu 15.2 Specifying an Inside Server

Menu 15.2 - NAT Server Setup			
Rule	Start Port No.	End Port No.	IP Address
1.	<b>Default</b>	<b>Default</b>	<b>192.168.1.10</b>
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.	1026	1026	192.168.1.1

Press ENTER to Confirm or ESC to Cancel:

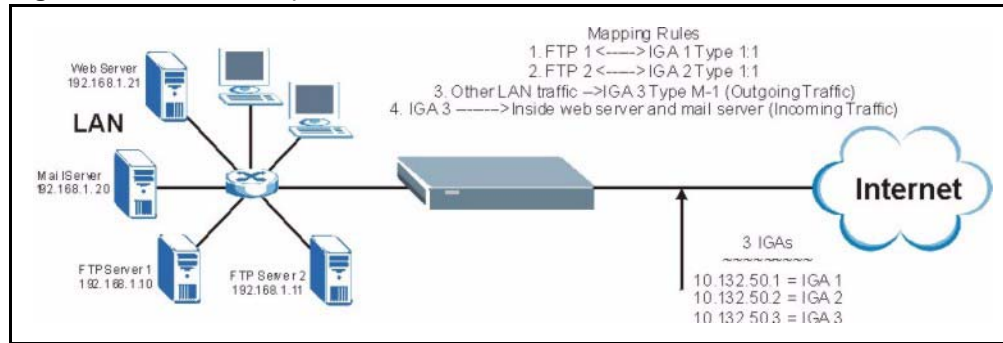
### 28.5.3 Example 3: Multiple Public IP Addresses With Inside Servers

In this example, there are 3 IGAs from our ISP. There are many departments but two have their own FTP server. All departments share the same router. The example will reserve one IGA for each department with an FTP server and all departments use the other IGA. Map the FTP servers to the first two IGAs and the other LAN traffic to the remaining IGA. Map the third IGA to an inside web server and mail server. Four rules need to be configured, two bi-directional and two unidirectional as follows.

- 1** Map the first IGA to the first inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).
- 2** Map the second IGA to our second inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).
- 3** Map the other outgoing LAN traffic to IGA3 (**Many : 1** mapping).
- 4** You also map your third IGA to the web server and mail server on the LAN. Type **Server** allows you to specify multiple servers, of different types, to other computers behind NAT on the LAN.

The example situation looks somewhat like this:



**Figure 138** NAT Example 3

- 1 In this case you need to configure Address Mapping Set 1 from **Menu 15.1 - Address Mapping Sets**. Therefore you must choose the **Full Feature** option from the **Network Address Translation** field (in menu 4 or menu 11.3). See [Figure 119 on page 251](#).
- 2 Then enter 15 from the main menu.
- 3 Enter 1 to configure the Address Mapping Sets.
- 4 Enter 1 to begin configuring this new set. Enter a Set Name, choose the **Edit Action** and then enter 1 for the **Select Rule** field. Press [ENTER] to confirm.
- 5 Select **Type** as **One-to-One** (direct mapping for packets going both ways), and enter the local **Start IP** as 192.168.1.10 (the IP address of FTP Server 1), the global **Start IP** as 10.132.50.1 (our first IGA). See [Figure 140 on page 269](#).
- 6 Repeat the previous step for rules 2 to 4 as outlined above.
- 7 When finished, menu 15.1.1.1 should look like as shown in [Figure 141 on page 269](#).

**Figure 139** NAT Example 3: Menu 11.3

```

Menu 11.3 - Remote Node Network Layer Options

IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Addr= N/A

Network Address Translation = Full Feature
Metric= 1
Private= N/A
RIP Direction= None
  Version= N/A
Multicast= None

Enter here to CONFIRM or ESC to CANCEL:

```

The following figures show how to configure the first rule.

**Figure 140** Example 3: Menu 15.1.1.1

```

Menu 15.1.1.1 Address Mapping Rule

Type= One-to-One
Local IP:
  Start= 192.168.1.10
  End = N/A
Global IP:
  Start= 10.132.50.1
  End = N/A

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

```

**Figure 141** Example 3: Final Menu 15.1.1

```

Menu 15.1.1 - Address Mapping Rules
Set Name= NAT_SET
Idx  Local Start IP  Local End IP  Global Start IP  Global End IP  Type
-----
1.  192.168.1.10
2.  192.168.1.11
3.  0.0.0.0          255.255.255.255  10.132.50.3
4.
5.
6.
7.
8.
9.
10.
Action= None          Select Rule= N/A

Press ENTER to Confirm or ESC to Cancel:

```

Now configure the IGA3 to map to our web server and mail server on the LAN.

**8** Enter 15 from the main menu.

**9** Enter 2 in **Menu 15 - NAT Setup**.

**10** Enter 1 in **Menu 15.2 - NAT Server Setup** to see the following menu. Configure it as shown.

Figure 142 Example 3: Menu 15.2

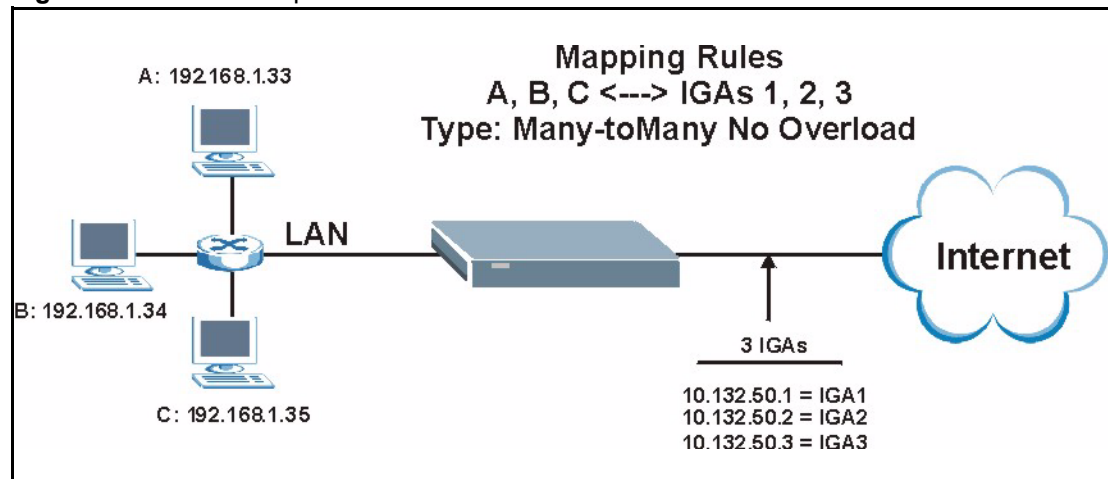
Menu 15.2 - NAT Server Setup			
Rule	Start Port No.	End Port No.	IP Address
1.	Default	Default	0.0.0.0
2.	80	80	192.168.1.21
3.	25	25	192.168.1.20
4.	0	0	0.0.0.0
5.	0	0	0.0.0.0
6.	0	0	0.0.0.0
7.	0	0	0.0.0.0
8.	0	0	0.0.0.0
9.	0	0	0.0.0.0
10.	0	0	0.0.0.0
11.	0	0	0.0.0.0
12.	1026	1026	192.168.1.1

Press ENTER to Confirm or ESC to Cancel:  
 HTTP:80 FTP:21 Telnet:23 SMTP:25 POP3:110 PPTP:1723

## 28.5.4 Example 4: NAT Unfriendly Application Programs

Some applications do not support NAT Mapping using TCP or UDP port address translation. In this case it is better to use **Many-to-Many No Overload** mapping as port numbers do *not* change for **Many-to-Many No Overload** (and **One-to-One**) NAT mapping types. The following figure illustrates this.

Figure 143 NAT Example 4



**Note:** Other applications such as some gaming programs are NAT unfriendly because they embed addressing information in the data stream. These applications won't work through NAT even when using One-to-One and Many-to-Many No Overload mapping types.

Follow the steps outlined in example 3 to configure these two menus as follows

**Figure 144** Example 4: Menu 15.1.1.1 Address Mapping Rule.

```

Menu 15.1.1.1 Address Mapping Rule

Type= Many-One-to-One
Local IP:
  Start= 192.168.1.10
  End  = 192.168.1.12
Global IP:
  Start= 10.132.50.1
  End  = 10.132.50.3

Press ENTER to Confirm or ESC to Cancel:

```

After you've configured your rule, you should be able to check the settings in menu 15.1.1 as shown next.

**Figure 145** Example 4: Menu 15.1.1 Address Mapping Rules

```

Menu 15.1.1 - Address Mapping Rules

Set Name= Example4
Idx  Local Start IP  Local End IP  Global Start IP  Global End IP  Type
---  -
1.   192.168.1.10   192.168.1.12   10.132.50.1     10.132.50.3   M:M NO OV
2.
3.
4.
5.
6.
7.
8.
9.
10.

Action= Edit          Select Rule=
Press ENTER to Confirm or ESC to Cancel:

```

## 28.6 Configuring Trigger Port Forwarding

**Note:** Only one LAN computer can use a trigger port (range) at a time.

Enter 3 in menu 15 to display **Menu 15.3 — Trigger Port Setup**, shown next.

**Figure 146** Menu 15.3 Trigger Port Setup

Menu 15.3 - Trigger Port Setup					
Rule	Name	Incoming		Trigger	
		Start Port	End Port	Start Port	End Port
1.	Real Audio	6970	7170	7070	7070
2.		0	0	0	0
3.		0	0	0	0
4.		0	0	0	0
5.		0	0	0	0
6.		0	0	0	0
7.		0	0	0	0
8.		0	0	0	0
9.		0	0	0	0
10.		0	0	0	0
11.		0	0	0	0
12.		0	0	0	0

Press ENTER to Confirm or ESC to Cancel:

The following table describes the fields in this screen.

**Table 113** Menu 15.3 Trigger Port Setup

FIELD	DESCRIPTION
Rule	This is the rule index number.
Name	Enter a unique name for identification purposes. You may enter up to 15 characters in this field. All characters are permitted - including spaces.
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The Prestige forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Start Port	Enter a port number or the starting port number in a range of port numbers.
End Port	Enter a port number or the ending port number in a range of port numbers.
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the Prestige to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start Port	Enter a port number or the starting port number in a range of port numbers.
End Port	Enter a port number or the ending port number in a range of port numbers.
Press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.	



# CHAPTER 29

## Enabling the Firewall

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

### 29.1 Remote Management and the Firewall

When SMT menu 24.11 is configured to allow management and the firewall is enabled:

- The firewall blocks remote management from the WAN unless you configure a firewall rule to allow it.
- The firewall allows remote management from the LAN.

### 29.2 Access Methods

The web configurator is, by far, the most comprehensive firewall configuration tool your Prestige has to offer. For this reason, it is recommended that you configure your firewall using the web configurator, see the following chapters for instructions. SMT screens allow you to activate the firewall and view firewall logs.

### 29.3 Enabling the Firewall

From the main menu enter 21 to go to **Menu 21 - Filter Set and Firewall Configuration** to display the screen shown next.

**Figure 147** Menu 21: Filter and Firewall Setup

```
Menu 21 - Filter and Firewall Setup

    1. Filter Setup
    2. Firewall Setup

Enter Menu Selection Number:
```

Enter option 2 in this menu to bring up the following screen. Press [SPACE BAR] and then [ENTER] to select **Yes** in the **Active** field to activate the firewall. The firewall must be active to protect against Denial of Service (DoS) attacks. Additional rules may be configured using the web configurator.

**Figure 148** Menu 21.2 Firewall Setup

```
Menu 21.2 - Firewall Setup
The firewall protects against Denial of Service (DOS) attacks when
it is active.

Your network is vulnerable to attacks when the firewall is turned off.

Refer to the User's Guide for details about the firewall default
policies.

You may define additional Policy rules or modify existing ones but
please exercise extreme caution in doing so
Active: Yes

You can use the Web Configurator to configure the firewall.

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

Use the web configurator or the command interpreter to configure the firewall rules

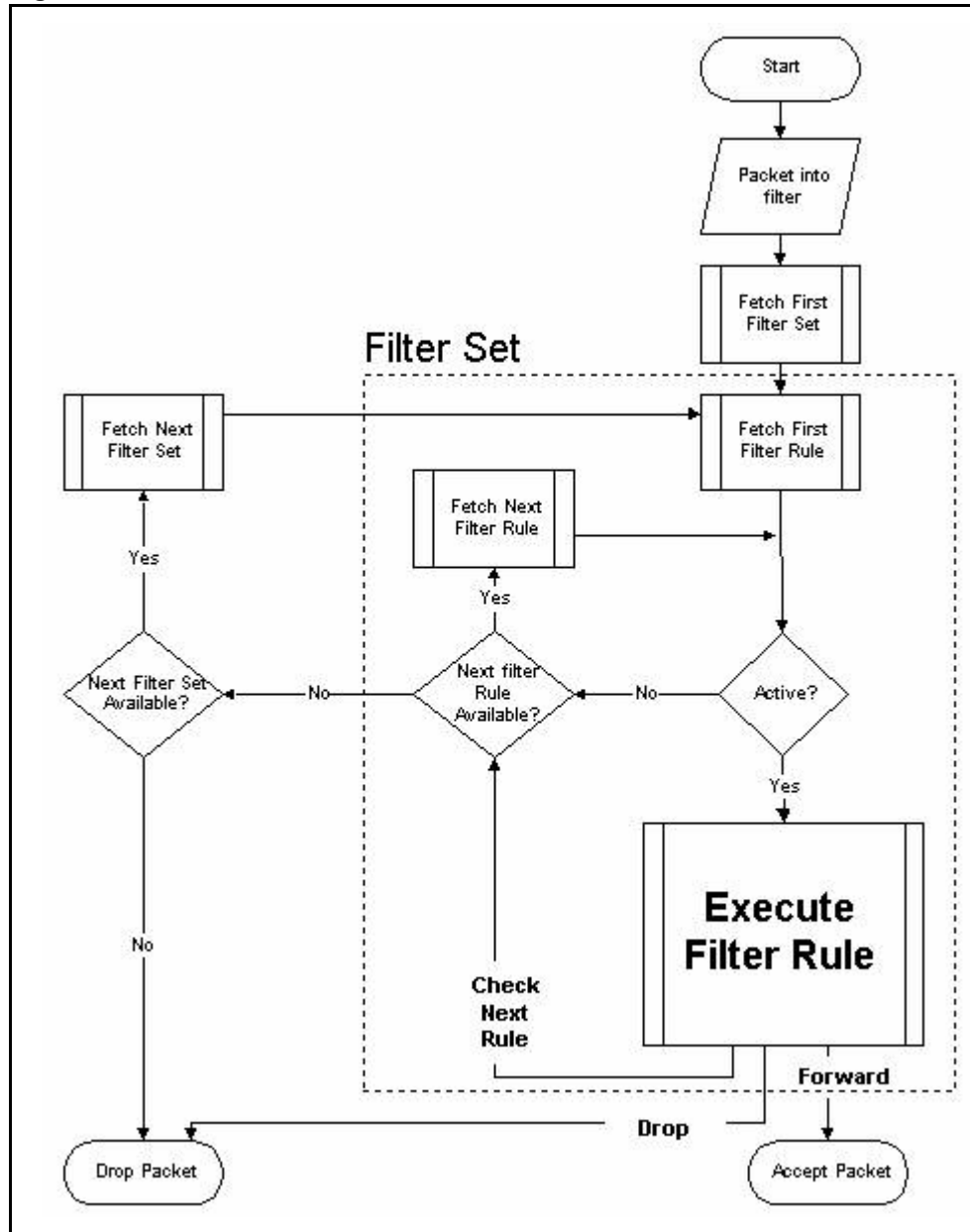




### 30.1.1 The Filter Structure of the Prestige

A filter set consists of one or more filter rules. Usually, you would group related rules, e.g., all the rules for NetBIOS, into a single set and give it a descriptive name. The Prestige allows you to configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system. You cannot mix device filter rules and protocol filter rules within the same set. You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

The following figure illustrates the logic flow when executing a filter rule. See also [Figure 155 on page 284](#) for the logic flow when executing an IP filter.

**Figure 150** Filter Rule Process

You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

## 30.2 Configuring a Filter Set

The Prestige includes filtering for NetBIOS over TCP/IP packets by default. To configure another filter set, follow the procedure below.

- 1 Enter 21 in the main menu to open menu 21.

**Figure 151** Menu 21: Filter and Firewall Setup

```

Menu 21 - Filter and Firewall Setup

      1. Filter Setup
      2. Firewall Setup

Enter Menu Selection Number:
    
```

**2** Enter 1 to bring up the following menu.

**Figure 152** Menu 21.1: Filter Set Configuration

```

Menu 21.1 - Filter Set Configuration

Filter Set #      Comments      Filter Set #      Comments
-----
1                _____      7                _____
2                _____      8                _____
3                _____      9                _____
4                _____     10               _____
5                _____     11               _____
6                _____     12               _____

Enter Filter Set Number to Configure= 0
Edit Comments= N/A
Press ENTER to Confirm or ESC to Cancel:
    
```

- 3** Select the filter set you wish to configure (1-12) and press [ENTER].
- 4** Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].
- 5** Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.x - Filter Rules Summary**.

**Figure 153** Menu 21.1.x: Filter Rules Summary

Menu 21.1.2 - Filter Rules Summary			
#	A	Type	Filter Rules
-----			
1	N		
2	N		
3	N		
4	N		
5	N		
6	N		

Enter Filter Rule Number (1-6) to Configure:

This screen shows the summary of the existing rules in the filter set. The following tables contain a brief description of the abbreviations used in the previous menus.

**Table 114** Abbreviations Used in the Filter Rules Summary Menu

FIELD	DESCRIPTION
#	The filter rule number: 1 to 6.
A	Active: "Y" means the rule is active. "N" means the rule is inactive.
Type	The type of filter rule: "GEN" for Generic, "IP" for TCP/IP.
Filter Rules	These parameters are displayed here.
M	More. "Y" means there are more rules to check which form a rule chain with the present rule. An action cannot be taken until the rule chain is complete. "N" means there are no more rules to check. You can specify an action to be taken i.e., forward the packet, drop the packet or check the next rule. For the latter, the next rule is independent of the rule just checked.
m	Action Matched. "F" means to forward the packet immediately and skip checking the remaining rules. "D" means to drop the packet. "N" means to check the next rule.
n	Action Not Matched "F" means to forward the packet immediately and skip checking the remaining rules. "D" means to drop the packet. "N" means to check the next rule.

The protocol dependent filter rules abbreviation are listed as follows:

**Table 115** Rule Abbreviations Used

ABBREVIATION	DESCRIPTION
IP	
Pr	Protocol
SA	Source Address
SP	Source Port number
DA	Destination Address
DP	Destination Port number
GEN	
Off	Offset
Len	Length

Refer to the next section for information on configuring the filter rules.

### 30.2.1 Configuring a Filter Rule

To configure a filter rule, type its number in **Menu 21.1.x - Filter Rules Summary** and press [ENTER] to open menu 21.1.x.x for the rule.

To speed up filtering, all rules in a filter set must be of the same class, i.e., protocol filters or generic filters. The class of a filter set is determined by the first rule that you create. When applying the filter sets to a port, separate menu fields are provided for protocol and device filter sets. If you include a protocol filter set in a device filter field or vice versa, the Prestige will warn you and will not allow you to save.

### 30.2.2 Configuring a TCP/IP Filter Rule

This section shows you how to configure a TCP/IP filter rule. TCP/IP rules allow you to base the rule on the fields in the IP and the upper layer protocol, for example, UDP and TCP headers.

To configure TCP/IP rules, select **TCP/IP Filter Rule** from the **Filter Type** field and press [ENTER] to open **Menu 21.1.x.x - TCP/IP Filter Rule**, as shown next.

**Figure 154** Menu 21.1.x.x: TCP/IP Filter Rule

```

Menu 21.1.2.3 - TCP/IP Filter Rule

Filter #: 1,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 0      IP Source Route= No
Destination: IP Addr=
                IP Mask=
                Port #=
                Port # Comp= None
Source: IP Addr=
          IP Mask=
          Port #=
          Port # Comp= None
TCP Estab= N/A
More= No          Log= None
Action Matched= Check Next Rule
Action Not Matched= Check Next Rule

Press ENTER to Confirm or ESC to Cancel:

```

The following table describes how to configure your TCP/IP filter rule.

**Table 116** Menu 21.1.x.x: TCP/IP Filter Rule

FIELD	DESCRIPTION
Active	Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> to activate the filter rule or <b>No</b> to deactivate it.
IP Protocol	Protocol refers to the upper layer protocol, e.g., TCP is 6, UDP is 17 and ICMP is 1. Type a value between 0 and 255. A value of 0 matches ANY protocol.
IP Source Route	Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> to apply the rule to packets with an IP source route option. Otherwise the packets must not have a source route option. The majority of IP packets do not have source route.
Destination	
IP Addr	Enter the destination IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.
IP Mask	Enter the IP mask to apply to the <b>Destination: IP Addr</b> .
Port #	Enter the destination port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.
Port # Comp	Press [SPACE BAR] and then [ENTER] to select the comparison to apply to the destination port in the packet against the value given in <b>Destination: Port #</b> . Options are <b>None</b> , <b>Equal</b> , <b>Not Equal</b> , <b>Less</b> and <b>Greater</b> .
Source	
IP Addr	Enter the source IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.
IP Mask	Enter the IP mask to apply to the <b>Source: IP Addr</b> .

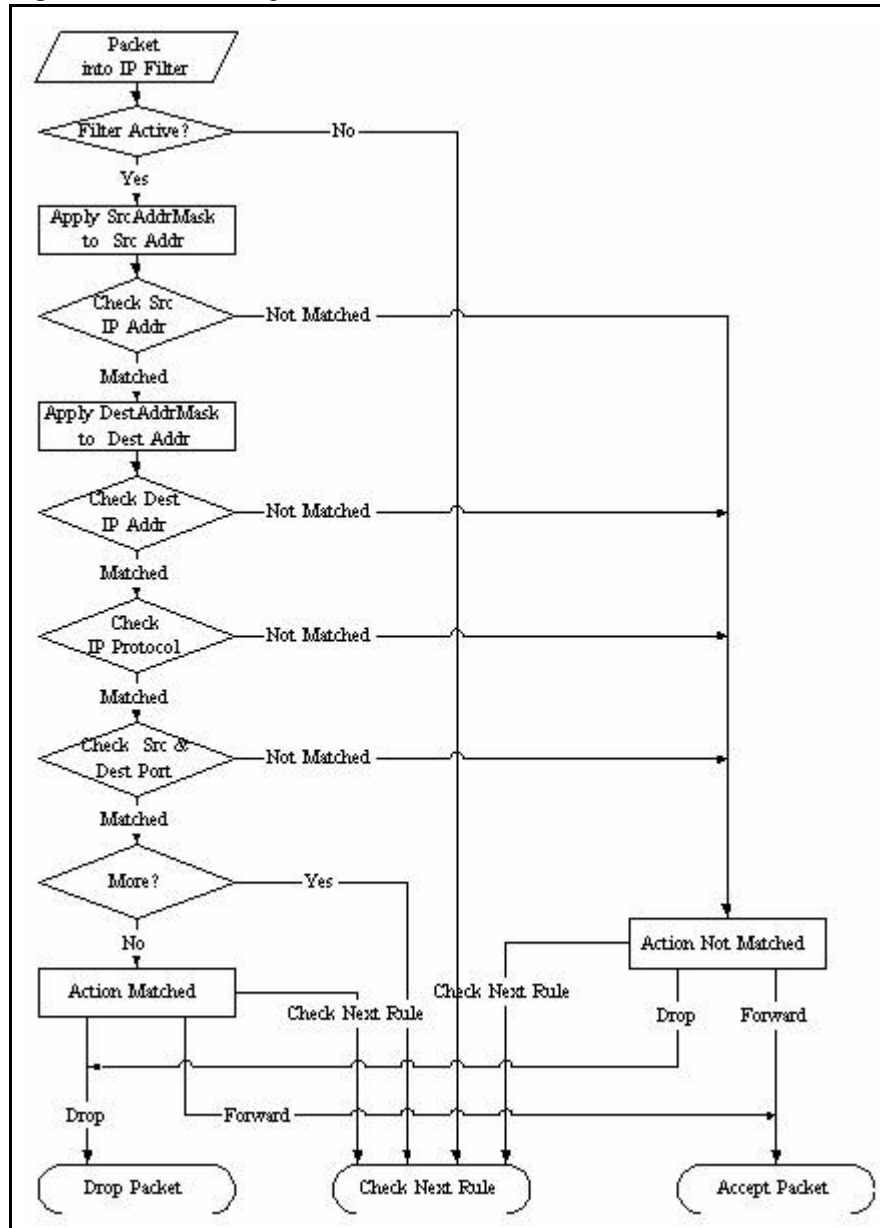
**Table 116** Menu 21.1.x.x: TCP/IP Filter Rule

FIELD	DESCRIPTION
Port #	Enter the source port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.
Port # Comp	Press [SPACE BAR] and then [ENTER] to select the comparison to apply to the source port in the packet against the value given in <b>Source: Port #</b> . Options are <b>None</b> , <b>Equal</b> , <b>Not Equal</b> , <b>Less</b> and <b>Greater</b> .
TCP Estab	This field is applicable only when the IP Protocol field is 6, TCP. Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> , to have the rule match packets that want to establish a TCP connection (SYN=1 and ACK=0); if <b>No</b> , it is ignored.
More	Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> or <b>No</b> . If <b>Yes</b> , a matching packet is passed to the next filter rule before an action is taken; if <b>No</b> , the packet is disposed of according to the action fields. If <b>More</b> is <b>Yes</b> , then <b>Action Matched</b> and <b>Action Not Matched</b> will be <b>N/A</b> .
Log	Press [SPACE BAR] and then [ENTER] to select a logging option from the following: <b>None</b> – No packets will be logged. <b>Action Matched</b> - Only packets that match the rule parameters will be logged. <b>Action Not Matched</b> - Only packets that do not match the rule parameters will be logged. <b>Both</b> – All packets will be logged.
Action Matched	Press [SPACE BAR] and then [ENTER] to select the action for a matching packet. Options are <b>Check Next Rule</b> , <b>Forward</b> and <b>Drop</b> .
Action Not Matched	Press [SPACE BAR] and then [ENTER] to select the action for a packet not matching the rule. Options are <b>Check Next Rule</b> , <b>Forward</b> and <b>Drop</b> .
When you have <b>Menu 21.1.x.x - TCP/IP Filter Rule</b> configured, press [ENTER] at the message "Press ENTER to Confirm" to save your configuration, or press [ESC] to cancel. This data will now be displayed on <b>Menu 21.1.x - Filter Rules Summary</b> .	

The following figure illustrates the logic flow of an IP filter.



Figure 155 Executing an IP Filter



### 30.2.3 Configuring a Generic Filter Rule

This section shows you how to configure a generic filter rule. The purpose of generic rules is to allow you to filter non-IP packets. For IP, it is generally easier to use the IP rules directly.

For generic rules, the Prestige treats a packet as a byte stream as opposed to an IP or IPX packet. You specify the portion of the packet to check with the **Offset** (from 0) and the **Length** fields, both in bytes. The Prestige applies the Mask (bit-wise ANDing) to the data portion before comparing the result against the Value to determine a match. The **Mask** and **Value** are specified in hexadecimal numbers. Note that it takes two hexadecimal digits to represent a byte, so if the length is 4, the value in either field will take 8 digits, for example, FFFFFFFF.

To configure a generic rule, select **Generic Filter Rule** in the **Filter Type** field in menu 21.1.x.x and press [ENTER] to open Generic Filter Rule, as shown below.

**Figure 156** Menu 21.1.x.x: Generic Filter Rule

```

Menu 21.1.2.3 - Generic Filter Rule

Filter #: 1,1
Filter Type= Generic Filter Rule
Active= No
Offset= 0
Length= 0
Mask= N/A
Value= N/A
More= No           Log= None
Action Matched= Check Next Rule
Action Not Matched= Check Next Rule

Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the fields in the **Generic Filter Rule** menu.

**Table 117** Menu 21.1.x.x: Generic Filter Rule

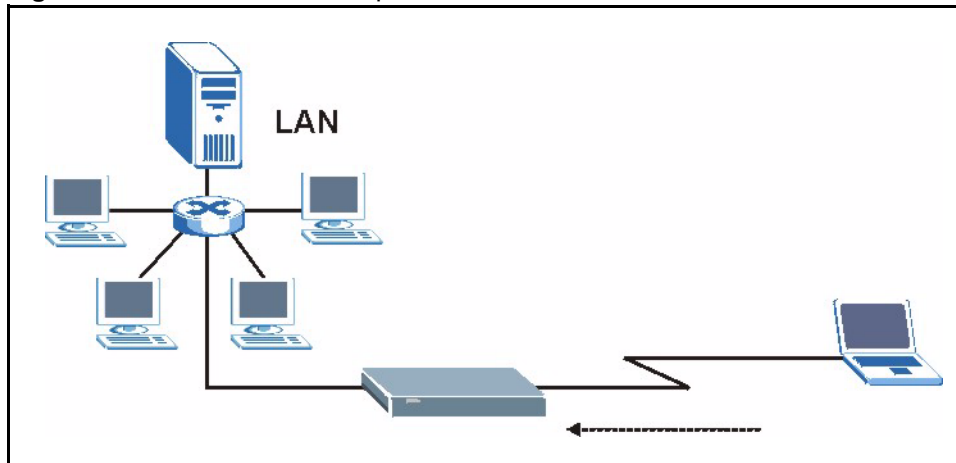
FIELD	DESCRIPTION
Filter #	This is the filter set, filter rule co-ordinates, i.e., 2,3 refers to the second filter set and the third rule of that set.
Filter Type	Use [SPACE BAR] and then [ENTER] to select a rule type. Parameters displayed below each type will be different. TCP/IP filter rules are used to filter IP packets while generic filter rules allow filtering of non-IP packets. Options are <b>Generic Filter Rule</b> and <b>TCP/IP Filter Rule</b> .
Active	Select <b>Yes</b> to turn on the filter rule or <b>No</b> to turn it off.
Offset	Enter the starting byte of the data portion in the packet that you wish to compare. The range for this field is from 0 to 255.
Length	Enter the byte count of the data portion in the packet that you wish to compare. The range for this field is 0 to 8.
Mask	Enter the mask (in Hexadecimal notation) to apply to the data portion before comparison.
Value	Enter the value (in Hexadecimal notation) to compare with the data portion.
More	If <b>Yes</b> , a matching packet is passed to the next filter rule before an action is taken; else the packet is disposed of according to the action fields. If <b>More</b> is <b>Yes</b> , then Action Matched and Action Not Matched will be <b>No</b> .
Log	Select the logging option from the following: <b>None</b> - No packets will be logged. <b>Action Matched</b> - Only packets that match the rule parameters will be logged. <b>Action Not Matched</b> - Only packets that do not match the rule parameters will be logged. <b>Both</b> - All packets will be logged.
Action Matched	Select the action for a packet matching the rule. Options are <b>Check Next Rule</b> , <b>Forward</b> and <b>Drop</b> .

**Table 117** Menu 21.1.x.x: Generic Filter Rule

FIELD	DESCRIPTION
Action Not Matched	Select the action for a packet not matching the rule. Options are <b>Check Next Rule</b> , <b>Forward</b> and <b>Drop</b> .
Once you have completed filling in <b>Menu 21.1.x.x - Generic Filter Rule</b> , press [ENTER] at the message "Press ENTER to Confirm" to save your configuration, or press [ESC] to cancel. This data will now be displayed on <b>Menu 21.1.x - Filter Rules Summary</b> .	

### 30.3 Example Filter

Let's look at an example to block outside users from accessing the Prestige via telnet.

**Figure 157** Telnet Filter Example

- 1 Enter 21 from the main menu to open **Menu 21 - Filter and Firewall Setup**.
- 2 Enter 1 to open **Menu 21.1 - Filter Set Configuration**.
- 3 Enter the index of the filter set you wish to configure (say 3) and press [ENTER].
- 4 Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].
- 5 Press [ENTER] at the message
- 6 [Press ENTER to confirm] to open **Menu 21.1.3 - Filter Rules Summary**.
- 7 Enter 1 to configure the first filter rule (the only filter rule of this set). Make the entries in this menu as shown in the following figure.

**Figure 158** Example Filter: Menu 21.1.3.1

```

Menu 21.1.3.1 - TCP/IP Filter Rule

Filter #: 3,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6      IP Source Route= No
Destination: IP Addr= 0.0.0.0
              IP Mask= 0.0.0.0
              Port # = 23
              Port # Comp= Equal
Source: IP Addr= 0.0.0.0
        IP Mask= 0.0.0.0
        Port # = 0
        Port # Comp= None

TCP Estab= No
More= No          Log= None
Action Matched= Drop
Action Not Matched= Forward

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

```

The port number for the telnet service (TCP protocol) is **23**. See RFC 1060 for port numbers of well-known services.

When you press [ENTER] to confirm, you will see the following screen. Note that there is only one filter rule in this set.

**Figure 159** Example Filter Rules Summary: Menu 21.1.3

```

Menu 21.1.3 - Filter Rules Summary

# A Type          Filter Rules          M m n
- - - - -
1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23      N D F
2 N
3 N
4 N
5 N
6 N

Enter Filter Rule Number (1-6) to Configure: 1

```

This shows you that you have configured and activated (**A = Y**) a TCP/IP filter rule (**Type = IP, Pr = 6**) for destination telnet ports (**DP = 23**).

**M = N** means an action can be taken immediately. The action is to drop the packet (**m = D**) if the action is matched and to forward the packet immediately (**n = F**) if the action is not matched no matter whether there are more rules to be checked (there aren't in this example).

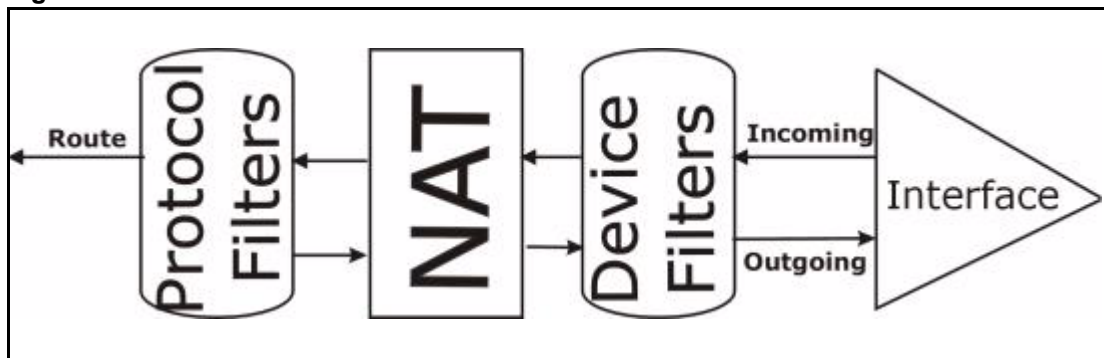
After you've created the filter set, you must apply it.

- 1 Enter 11 from the main menu to go to menu 11.
- 2 Go to the **Edit Filter Sets** field, press [SPACE BAR] to select **Yes** and press [ENTER].
- 3 This brings you to menu 11.5. Apply a filter set (our example filter set 3).
- 4 Press [ENTER] to confirm after you enter the set numbers and to leave menu 11.5.

## 30.4 Filter Types and NAT

There are two classes of filter rules, **Generic Filter** (Device) rules and protocol filter (**TCP/IP**) rules. Generic filter rules act on the raw data from/to LAN and WAN. Protocol filter rules act on the IP packets. Generic and TCP/IP filter rules are discussed in more detail in the next section. When NAT (Network Address Translation) is enabled, the inside IP address and port number are replaced on a connection-by-connection basis, which makes it impossible to know the exact address and port on the wire. Therefore, the Prestige applies the protocol filters to the "native" IP address and port number before NAT for outgoing packets and after NAT for incoming packets. On the other hand, the generic, or device filters are applied to the raw packets that appear on the wire. They are applied at the point when the Prestige is receiving and sending the packets; i.e. the interface. The interface can be an Ethernet port or any other hardware port. The following diagram illustrates this.

**Figure 160** Protocol and Device Filter Sets



## 30.5 Applying a Filter

This section shows you where to apply the filter(s) after you design it (them).

### 30.5.1 Applying LAN Filters

LAN traffic filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 3.1 (shown next) and enter the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by entering their numbers separated by commas, e.g., 3, 4, 6, 11. Input filter sets filter incoming traffic to the Prestige and output filter sets filter outgoing traffic from the Prestige. For PPPoE encapsulation, you have the additional option of specifying remote node call filter sets.

**Figure 161** Filtering LAN Traffic

```
Menu 3.1 - LAN Port Filter Setup

Input Filter Sets:
  protocol filters=
  device filters=
Output Filter Sets:
  protocol filters=
  device filters=

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

### 30.5.2 Applying Remote Node Filters

Go to menu 11.5 (shown below – note that call filter sets are only present for PPPoE encapsulation) and enter the number(s) of the filter set(s) as appropriate. You can cascade up to four filter sets by entering their numbers separated by commas. The Prestige already has filters to prevent NetBIOS traffic from triggering calls.

**Figure 162** Filtering Remote Node Traffic

```
Menu 11.5 - Remote Node Filter

Input Filter Sets:
  protocol filters=
  device filters=
Output Filter Sets:
  protocol filters=
  device filters=

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

# CHAPTER 31

## SNMP Configuration

This chapter explains SNMP Configuration menu 22.

### 31.1 SNMP Introduction

See [Section 16.6 on page 162](#) for background information on SNMP.

### 31.2 SNMP Configuration

To configure SNMP, select option 22 from the main menu to open **Menu 22 — SNMP Configuration** as shown next. The “community” for Get, Set and Trap fields is SNMP terminology for password.

**Figure 163** Menu 22 SNMP Configuration

```

Menu 22 - SNMP Configuration

SNMP:
  Get Community= public
  Set Community= public
  Trusted Host= 0.0.0.0
Trap:
  Community= public
  Destination= 0.0.0.0

Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the SNMP configuration parameters.

**Table 118** Menu 22 SNMP Configuration

FIELD	DESCRIPTION
SNMP:	
Get Community	Type the <b>Get Community</b> , which is the password for the incoming Get- and GetNext requests from the management station.
Set Community	Type the <b>Set</b> community, which is the password for incoming Set requests from the management station.
Trusted Host	If you enter a trusted host, your Prestige will only respond to SNMP messages from this address. A blank (default) field means your Prestige will respond to all SNMP messages it receives, regardless of source.

**Table 118** Menu 22 SNMP Configuration (continued)

FIELD	DESCRIPTION
Trap:	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager.
Destination	Type the IP address of the station to send your SNMP traps to.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	



# CHAPTER 32

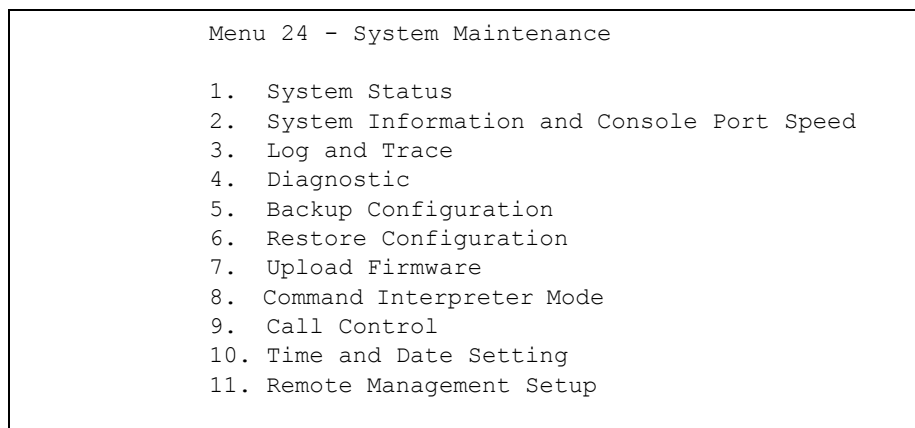
## System Information and Diagnosis

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

These tools include system status, port status and log and trace capabilities. This chapter describes how to use these tools in detail.

Type 24 in the main menu to open **Menu 24 – System Maintenance**, as shown in the following figure.

**Figure 164** Menu 24 System Maintenance



### 32.1 System Status

The first selection, system status gives you information on the status and statistics of the ports, as shown next. system status is a tool that can be used to monitor your Prestige. Specifically, it gives you information on your ADSL telephone line status, number of packets sent and received.

To get to the system status menu, type 24 to go to **Menu 24 — System Maintenance**. From this menu, type 1. **System Status**. There are two commands in **Menu 24.1 — System Maintenance — Status**. Entering 1 resets the counters; [ESC] takes you back to the previous screen.

The following table describes the fields present in **Menu 24.1 — System Maintenance — Status** which are read-only and meant for diagnostic purposes.

**Figure 165** Menu 24.1 System Maintenance: Status

```

Menu 24.1 - System Maintenance - Status                                07:15:35
                                                                    Sat. Jan. 01, 2000

Port  Status      TxPkts    RxPkts    Cols    Tx B/s    Rx B/s    Up Time
WAN   Down          168       199       0        0         0         0:00:00
LAN   100M/Full     3040      2456      0        258       128       7:15:26

Port  Ethernet Address      IP Address      IP Mask      DHCP
WAN   00:13:49:52:78:34     192.168.2.5    255.255.255.0  None
LAN   00:13:49:52:78:33     192.168.1.1    255.255.255.0  Server

System up Time:      7:15:39

Name: P2302R.Zyxel.com
Routing: IP
ZyNOS F/W Version: V3.60(MM.4)b1 | 11/08/2005

Press Command:

COMMANDS: 1-Drop WAN 9-Reset Counters  ESC-Exit

```

The following table describes the fields present in **Menu 24.1 — System Maintenance — Status**. These fields are READ-ONLY and meant for diagnostic purposes. The upper right corner of the screen shows the time and date according to the format you set in menu 24.10.

**Table 119** System Maintenance: Status Menu Fields

FIELD	DESCRIPTION
Port	Identifies a port (WAN, LAN) on the Prestige.
Status	Shows the port speed and duplex setting if you're using <b>Ethernet Encapsulation</b> and <b>Down</b> (line is down), <b>idle</b> (line (ppp) idle), <b>dial</b> (starting to trigger a call) and <b>drop</b> (dropping a call) if you're using <b>PPPoE Encapsulation</b> .
TxPkts	The number of transmitted packets on this port.
RxPkts	The number of received packets on this port.
Cols	The number of collisions on this port.
Tx B/s	Shows the transmission speed in Bytes per second on this port.
Rx B/s	Shows the reception speed in Bytes per second on this port.
Up Time	Total amount of time the line has been up.
Ethernet Address	The Ethernet address of the port listed on the left.
IP Address	The IP address of the port listed on the left.
IP Mask	The IP mask of the port listed on the left.
DHCP	The DHCP setting of the port listed on the left.
System up Time	The total time the Prestige has been on.

**Table 119** System Maintenance: Status Menu Fields (continued)

FIELD	DESCRIPTION
Name	This is the Prestige's system name + domain name assigned in menu 1. For example, System Name= xxx; Domain Name= baboo.mickey.com Name= xxx.baboo.mickey.com
Routing	Refers to the routing protocol used.
ZyNOS F/W Version	The ZyNOS Firm Ware version and the date created.
You may enter 1 to drop the WAN connection, 9 to reset the counters or [ESC] to return to menu 24.	

## 32.2 System Information

To get to the system information menu:

- 1** Enter 24 to display **Menu 24 – System Maintenance**.
- 2** Enter 2 to display **Menu 24.2 — System Information and Console Port Speed**.
- 3** From this menu you have two choices as shown in the next figure:

**Figure 166** Menu 24.2 System Information and Console Port Speed

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

### 32.2.1 System Information

Enter 1 in menu 24.2 to display the screen shown next

**Figure 167** Menu 24.2.1 System Maintenance: Information

```

Menu 24.2.1 - System Maintenance - Information

Name: P2302R.Zyxel.com
Routing: IP
ZyNOS F/W Version: V3.60(MM.4)b1 | 11/08/2005
Country Code: 255

LAN
Ethernet Address: 00:13:49:52:78:33
IP Address: 192.168.1.1
IP Mask: 255.255.255.0
DHCP: Server

Press ESC or RETURN to Exit:
    
```

The following table describes the fields in this menu.

**Table 120** Menu 24.2.1 System Maintenance: Information

FIELD	DESCRIPTION
Name	Displays the system name of your Prestige. This information can be changed in <b>Menu 1 – General Setup</b> .
Routing	Refers to the routing protocol used.
ZyNOS F/W Version	Refers to the ZyNOS (ZyXEL Network Operating System) system firmware version. ZyNOS is a registered trademark of ZyXEL Communications Corporation.
Country Code	This is the country code of the firmware.
LAN	
Ethernet Address	Refers to the Ethernet MAC (Media Access Control) of your Prestige.
IP Address	This is the IP address of the Prestige in dotted decimal notation.
IP Mask	This shows the subnet mask of the Prestige.
DHCP	This field shows the DHCP setting (None, Relay or Server) of the Prestige.

### 32.2.2 Console Port Speed

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

You can set up different port speeds for the console port through **Menu 24.2.2 – System Maintenance – Console Port Speed**. Your Prestige supports 9600 (default), 19200, 38400, 57600 and 115200 bps. Press [SPACE BAR] and then [ENTER] to select the desired speed in menu 24.2.2, as shown in the following figure.

**Figure 168** Menu 24.2.2 System Maintenance: Change Console Port Speed

```
Menu 24.2.2 - System Maintenance - Change Console Port Speed

Console Port Speed: 9600

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

## 32.3 Log and Trace

To get to the log and trace menu:

- 1 Enter 24 to display **Menu 24 – System Maintenance**.
- 2 Enter 3 to display **Menu 24.3 — System Maintenance - Log and Trace**.
- 3 There are two logging facilities in the Prestige as shown in the next figure. The first is the error logs and trace records that are stored locally. The second is the syslog facility for message logging.

**Figure 169** Menu 24.2 System Information and Console Port Speed

```
Menu 24.3 - System Maintenance - Log and Trace

2. Syslog Logging

4. Call-Triggering Packet

Please enter selection:
```

### 32.3.1 Syslog Logging

The Prestige uses the syslog facility to log the CDR (Call Detail Record) and system messages to a syslog server. Syslog and accounting can be configured in **Menu 24.3.2 — System Maintenance - Syslog Logging**, as shown next.

**Figure 170** Menu 24.3.2 System Maintenance: Syslog Logging

```

Menu 24.3.2 - System Maintenance - Syslog Logging

Syslog:
Active= No
Syslog Server IP Address= 0.0.0.0
Log Facility= Local 1

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

You need to configure the syslog parameters described in the following table to activate syslog then choose what you want to log.

**Table 121** Menu 24.3.2 System Maintenance: Syslog Logging

PARAMETER	DESCRIPTION
Syslog:	
Active	Press [SPACE BAR] and then [ENTER] to turn syslog on or off.
Syslog Server IP Address	Enter the IP address of the syslog server that will log the CDR (Call Detail Record) and system messages.
Log Facility	Press [SPACE BAR] and then [ENTER] to select a Local option. The log facility allows you to log the message to different files in the server. Please refer to the documentation of your syslog program for more details.
When finished configuring this screen, press [ENTER] to confirm or [ESC] to cancel.	

Your Prestige sends five types of syslog messages. Some examples (not all Prestige specific) of these syslog messages with their message formats are shown next:

### 32.3.1.1 CDR

```

CDR Message Format
SdcmdSyslogSend ( SYSLOG_CDR, SYSLOG_INFO, String);
String = board xx line xx channel xx, call xx, str
board = the hardware board ID
line = the WAN ID in a board
Channel = channel ID within the WAN
call = the call reference number which starts from 1 and increments by 1 for each new
call
str = C01 Outgoing Call dev xx ch xx (dev:device No. ch:channel No.)
C01 Incoming Call xxxxBps xxxxx (L2TP, xxxxx = Remote Call ID)
C01 Incoming Call xxxx (= connected speed) xxxxx (= Remote Call ID)
L02 Tunnel Connected (L2TP)
C02 OutCall Connected xxxx (= connected speed) xxxxx (= Remote Call ID)
C02 CLID call refused
L02 Call Terminated
C02 Call Terminated
Jul 19 11:19:27 192.168.102.2 ZYXEL: board 0 line 0 channel 0, call 1, C01 Outgoing
Call dev=2 ch=0 40002
Jul 19 11:19:32 192.168.102.2 ZYXEL: board 0 line 0 channel 0, call 1, C02 OutCall
Connected 64000 40002
Jul 19 11:20:06 192.168.102.2 ZYXEL: board 0 line 0 channel 0, call 1, C02 Call
Terminated

```

### 32.3.1.2 Packet triggered

```

Packet triggered Message Format
SdcmdSyslogSend( SYSLOG_PKTTRI, SYSLOG_NOTICE, String );
String = Packet trigger: Protocol=xx Data=xxxxxxxxxxxx...x
Protocol: (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG)
Data: We will send forty-eight Hex characters to the server
Jul 19 11:28:39 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a6b6c
6d6e6f7071727374
Jul 19 11:28:56 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600220008cd40000
020405b4
Jul 19 11:29:06 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=45000028240140001f06ac12c0a86614ca849a7b0427001700195b451d1430135004000077600000

```

### 32.3.1.3 Filter log

```

Filter log Message Format
SdcmdSyslogSend(SYSLOG_FILLOG, SYSLOG_NOTICE, String );
String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx] S04>R01mD
IP[...] is the packet header and S04>R01mD means filter set 4 (S) and rule 1 (R), match
(m) drop (D).
Src: Source Address
Dst: Destination Address
prot: Protocol ("TCP", "UDP", "ICMP")
spo: Source port
dpo: Destination port
Mar 03 10:39:43 202.132.155.97 ZyXEL:
GEN[fffffffffnordff0080] }S05>R01mF
Mar 03 10:41:29 202.132.155.97 ZyXEL:
GEN[00a0c5f502fnord010080] }S05>R01mF
Mar 03 10:41:34 202.132.155.97 ZyXEL:
IP[Src=192.168.2.33 Dst=202.132.155.93 ICMP]}S04>R01mF
Mar 03 11:59:20 202.132.155.97 ZyXEL:
GEN[00a0c5f502fnord010080] }S05>R01mF
Mar 03 12:00:52 202.132.155.97 ZyXEL:
GEN[fffffffffff0080] }S05>R01mF
Mar 03 12:00:57 202.132.155.97 ZyXEL:
GEN[00a0c5f502010080] }S05>R01mF
Mar 03 12:01:06 202.132.155.97 ZyXEL:
IP[Src=192.168.2.33 Dst=202.132.155.93 TCP spo=01170 dpo=00021]}S04>R01mF

```

### 32.3.1.4 PPP log

```

PPP Log Message Format
SdcmdSyslogSend( SYSLOG_PPPLOG, SYSLOG_NOTICE, String );
String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto
Shutdown
Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP /
IPXCP
Jul 19 11:42:44 192.168.102.2 ZyXEL: ppp:LCP Closing
Jul 19 11:42:49 192.168.102.2 ZyXEL: ppp:IPCP Closing
Jul 19 11:42:54 192.168.102.2 ZyXEL: ppp:CCP Closing

```

## 32.3.2 Call-Triggering Packet

Call-triggering packet displays information about the packet that triggered a dial-out call in an easy readable format. Equivalent information is available in menu 24.1 in hex format. An example is shown next.



**Figure 171** Call-Triggering Packet Example

```

IP Frame: ENET0-RECV Size: 44/ 44   Time: 17:02:44.262
Frame Type:

  IP Header:
    IP Version           = 4
    Header Length        = 20
    Type of Service      = 0x00 (0)
    Total Length         = 0x002C (44)
    Identification      = 0x0002 (2)
    Flags                = 0x00
    Fragment Offset      = 0x00
    Time to Live         = 0xFE (254)
    Protocol              = 0x06 (TCP)
    Header Checksum      = 0xFB20 (64288)
    Source IP            = 0xC0A80101 (192.168.1.1)
    Destination IP      = 0x00000000 (0.0.0.0)

  TCP Header:
    Source Port          = 0x0401 (1025)
    Destination Port     = 0x000D (13)
    Sequence Number      = 0x05B8D000 (95997952)
    Ack Number           = 0x00000000 (0)
    Header Length        = 24
    Flags                = 0x02 (...S.)
    Window Size          = 0x2000 (8192)
    Checksum             = 0xE06A (57450)
    Urgent Ptr           = 0x0000 (0)
    Options              =
      0000: 02 04 02 00

  RAW DATA:
    0000: 45 00 00 2C 00 02 00 00-FE 06 FB 20 C0 A8 01 01  E.....
    0010: 00 00 00 00 04 01 00 0D-05 B8 D0 00 00 00 00 00  .....
    0020: 60 02 20 00 E0 6A 00 00-02 04 02 00

Press any key to continue...

```

## 32.4 Diagnostic

The diagnostic facility allows you to test the different aspects of your Prestige to determine if it is working properly. Menu 24.4 allows you to choose among various types of diagnostic tests to evaluate your system, as shown in the following figure.

Follow the procedure next to get to the diagnostic menu:

- 1** From the main menu, type 24 to open **Menu 24 – System Maintenance**.
- 2** From this menu, type 4 to open **Menu 24.4 – System Maintenance – Diagnostic**.

**Figure 172** Menu 24.4 System Maintenance: Diagnostic

```

Menu 24.4 - System Maintenance - Diagnostic

TCP/IP
  1. Ping Host
  2. WAN DHCP Release
  3. WAN DHCP Renewal
  4. Internet Setup Test

System
  11. Reboot System

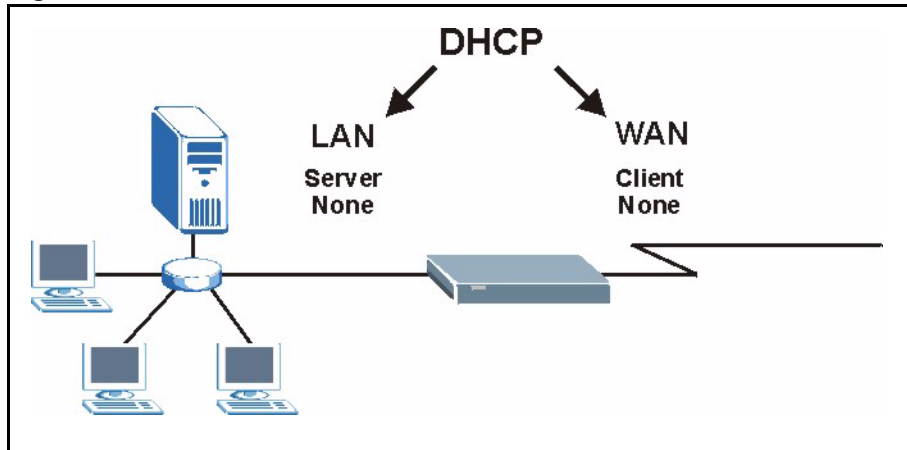
Enter Menu Selection Number:

Host IP Address= N/A

```

### 32.4.1 WAN DHCP

DHCP functionality can be enabled on the LAN or WAN as shown in the following figure. LAN DHCP has already been discussed. The Prestige can act either as a WAN DHCP client (**IP Address Assignment** field in menu 4 or menu 11.3 is **Dynamic** and the **Encapsulation** field in menu 4 or menu 11 is **Ethernet**) or **None**, (when you have a static IP). The **WAN Release** and **Renewal** fields in menu 24.4 conveniently allow you to release and/or renew the assigned WAN IP address, subnet mask and default gateway in a fashion similar to winipcfg.

**Figure 173** LAN & WAN DHCP

The following table describes the diagnostic tests available in menu 24.4 for your Prestige and associated connections.

**Table 122** System Maintenance Menu Diagnostic

FIELD	DESCRIPTION
Ping Host	Enter 1 to ping any machine (with an IP address) on your LAN or WAN. Enter its IP address in the <b>Host IP Address</b> field below.
WAN DHCP Release	Enter 2 to release your WAN DHCP settings.

**Table 122** System Maintenance Menu Diagnostic (continued)

FIELD	DESCRIPTION
WAN DHCP Renewal	Enter 3 to renew your WAN DHCP settings.
Internet Setup Test	Enter 4 to test the Internet setup. You can also test the Internet setup in <b>Menu 4 - Internet Access</b> . Please refer to <a href="#">Chapter 25 on page 242</a> for more details. This feature is only available for dial-up connections using PPPoE encapsulation.
Reboot System	Enter 11 to reboot the Prestige.
Host IP Address=	If you entered 1 in <b>Ping Host</b> , then enter the IP address of the computer you want to ping in this field.
Enter the number of the selection you would like to perform or press [ESC] to cancel.	



# CHAPTER 33

## Firmware and Configuration File Maintenance

This chapter tells you how to backup and restore your configuration file as well as upload new firmware and configuration files.

### 33.1 Filename Conventions

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

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

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

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

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

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

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

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

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

**Table 123** Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	Rom-0	This is the configuration filename on the Prestige. Uploading the rom-0 file replaces the entire ROM file system, including your Prestige configurations, system-related data (including the default password), the error log and the trace log.	*.rom
Firmware	Ras	This is the generic name for the ZyNOS firmware on the Prestige.	*.bin

## 33.2 Backup Configuration

Option 5 from **Menu 24 – System Maintenance** allows you to backup the current Prestige configuration to your computer. Backup is highly recommended once your Prestige is functioning properly. FTP is the preferred methods for backing up your current configuration to your computer since they are faster.

Please note that terms “download” and “upload” are relative to the computer. Download means to transfer from the Prestige to the computer, while upload means from your computer to the Prestige.

### 33.2.1 Backup Configuration

Follow the instructions as shown in the next screen.

**Figure 174** Telnet in Menu 24.5

```

Menu 24.5 - System Maintenance - Backup Configuration
To transfer the configuration file to your workstation, follow the procedure
below:
1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your Prestige. Then type "root" and
   SMT password as requested.
3. Locate the 'rom-0' file.
4. Type 'get rom-0' to back up the current Prestige configuration to
   your workstation.
For details on FTP commands, please consult the documentation of your FTP
client program. For details on backup using TFTP (note that you must remain
in this menu to back up using TFTP), please see your Prestige manual.
Press ENTER to Exit:

```

### 33.2.2 Using the FTP Command from the Command Line

- 1 Launch the FTP client on your computer.
- 2 Enter “open”, followed by a space and the IP address of your Prestige.
- 3 Press [ENTER] when prompted for a username.
- 4 Enter your password as requested (the default is “1234”).
- 5 Enter “bin” to set transfer mode to binary.
- 6 Use “get” to transfer files from the Prestige to the computer, for example, “get rom-0 config.rom” transfers the configuration file on the Prestige to your computer and renames it “config.rom”. See earlier in this chapter for more information on filename conventions.
- 7 Enter “quit” to exit the ftp prompt.

### 33.2.3 Example of FTP Commands from the Command Line

**Figure 175** FTP Session Example

```

331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 16384 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit

```

### 33.2.4 GUI-based FTP Clients

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

**Table 124** General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode. Configuration and firmware files should be transferred in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

### 33.2.5 TFTP and FTP over WAN Management Limitations

TFTP, FTP and Telnet over WAN will not work when:

- You have disabled Telnet service in menu 24.11.
- You have applied a filter in menu 3.1 (LAN) or in menu 11.5 (WAN) to block Telnet service.
- The IP address in the **Secured Client IP** field in menu 24.11 does not match the client IP. If it does not match, the Prestige will disconnect the Telnet session immediately.
- There is an SMT console session running.

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

### 33.2.6 Backup Configuration Using TFTP

The Prestige supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To backup the configuration file, follow the procedure shown next.

- 1 Use telnet from your computer to connect to the Prestige and log in. Because TFTP does not have any security checks, the Prestige records the IP address of the telnet client and accepts TFTP requests only from this address.



- 2 Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
- 3 Enter command “sys stdio 0” to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command “sys stdio 5” to restore the five-minute SMT timeout (default) when the file transfer is complete.
- 4 Launch the TFTP client on your computer and connect to the Prestige. Set the transfer mode to binary before starting data transfer.
- 5 Use the TFTP client (see the example below) to transfer files between the Prestige and the computer. The file name for the configuration file is “rom-0” (rom-zero, not capital o).

Note that the telnet connection must be active and the SMT in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the Prestige to the computer and “binary” to set binary transfer mode.

### 33.2.7 TFTP Command Example

The following is an example TFTP command:

```
tftp [-i] host get rom-0 config.rom
```

where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the Prestige IP address, “get” transfers the file source on the Prestige (rom-0, name of the configuration file on the Prestige) to the file destination on the computer and renames it config.rom.

### 33.2.8 GUI-based TFTP Clients

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

**Table 125** General Commands for GUI-based TFTP Clients

COMMAND	DESCRIPTION
Host	Enter the IP address of the Prestige. 192.168.1.1 is the Prestige's default IP address when shipped.
Send/Fetch	Use “Send” to upload the file to the Prestige and “Fetch” to back up the file on your computer.
Local File	Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer.
Remote File	This is the filename on the Prestige. The filename for the firmware is “ras” and for the configuration file, is “rom-0”.
Binary	Transfer the file in binary mode.
Abort	Stop transfer of the file.

## 33.3 Restore Configuration

This section shows you how to restore a previously saved configuration. Note that this function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

FTP is the preferred method for restoring your current computer configuration to your Prestige since FTP is faster. Please note that you must wait for the system to automatically restart after the file transfer is complete.

**Note:** WARNING! Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR Prestige.

### 33.3.1 Restore Using FTP

For details about backup using (T)FTP please refer to earlier sections on FTP and TFTP file upload in this chapter

**Figure 176** Telnet into Menu 24.6.

```
Menu 24.6 -- System Maintenance - Restore Configuration

To transfer the firmware and configuration file to your workstation, follow
the procedure below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your Prestige. Then type "root" and
SMT password as requested.
3. Type "put backupfilename rom-0" where backupfilename is the name of
your backup configuration file on your workstation and rom-0 is the
remote file name on the Prestige. This restores the configuration to
your Prestige.
4. The system reboots automatically after a successful file transfer

For details on FTP commands, please consult the documentation of your FTP
client program. For details on backup using TFTP (note that you must remain
in this menu to back up using TFTP), please see your Prestige manual.
Press ENTER to Exit:
```

- 1** Launch the FTP client on your computer.
- 2** Enter “open”, followed by a space and the IP address of your Prestige.
- 3** Press [ENTER] when prompted for a username.
- 4** Enter your password as requested (the default is “1234”).
- 5** Enter “bin” to set transfer mode to binary.
- 6** Find the “rom” file (on your computer) that you want to restore to your Prestige.

- 7 Use “put” to transfer files from the Prestige to the computer, for example, “put config.rom rom-0” transfers the configuration file “config.rom” on your computer to the Prestige. See earlier in this chapter for more information on filename conventions.
- 8 Enter “quit” to exit the ftp prompt. The Prestige will automatically restart after a successful restore process.

### 33.3.2 Restore Using FTP Session Example

**Figure 177** Restore Using FTP Session Example

```
ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
ftp>quit
```

## 33.4 Uploading Firmware and Configuration Files

This section shows you how to upload firmware and configuration files. You can upload configuration files by following the procedure in [Section 33.3 on page 309](#) or by following the instructions in **Menu 24.7.2 – System Maintenance – Upload System Configuration File**.

**Note:** WARNING! Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR Prestige.

### 33.4.1 Firmware File Upload

FTP is the preferred method for uploading the firmware and configuration. To use this feature, your computer must have an FTP client.

When you telnet into the Prestige, you will see the following screens for uploading firmware and the configuration file using FTP.

**Figure 178** Telnet Into Menu 24.7.1 Upload System Firmware

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

To upload the system firmware, follow the procedure below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your system. Then type "root" and
   SMT password as requested.
3. Type "put firmware filename ras" where "firmwarefilename" is the name
   of your firmware upgrade file on your workstation and "ras" is the
   remote file name on the system.
4. The system reboots automatically after a successful firmware upload.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP),
please see your manual.
Press ENTER to Exit:
```

### 33.4.2 Configuration File Upload

You see the following screen when you telnet into menu 24.7.2

**Figure 179** Telnet Into Menu 24.7.2 System Maintenance

```
Menu 24.7.2 - System Maintenance - Upload System Configuration File

To upload the system configuration file, follow the procedure below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your system. Then type "root" and
   SMT password as requested.
3. Type "put configuration filename rom-0" where "configurationfilename"
   is the name of your system configuration file on your workstation, which
   will be transferred to the "rom-0" file on the system.
4. The system reboots automatically after the upload system configuration
   file process is complete.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP),
please see your manual.
Press ENTER to Exit:
```

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

### 33.4.3 FTP File Upload Command from the DOS Prompt Example

- 1 Launch the FTP client on your computer.
- 2 Enter "open", followed by a space and the IP address of your Prestige.
- 3 Press [ENTER] when prompted for a username.

- 4 Enter your password as requested (the default is “1234”).
- 5 Enter “bin” to set transfer mode to binary.
- 6 Use “put” to transfer files from the computer to the Prestige, for example, “put firmware.bin ras” transfers the firmware on your computer (firmware.bin) to the Prestige and renames it “ras”. Similarly, “put config.rom rom-0” transfers the configuration file on your computer (config.rom) to the Prestige and renames it “rom-0”. Likewise “get rom-0 config.rom” transfers the configuration file on the Prestige to your computer and renames it “config.rom.” See earlier in this chapter for more information on filename conventions.
- 7 Enter “quit” to exit the ftp prompt.

**Note:** The Prestige automatically restarts after a successful file upload.

### 33.4.4 FTP Session Example of Firmware File Upload

**Figure 180** FTP Session Example of Firmware File Upload

```

331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit

```

More commands (found in GUI-based FTP clients) are listed earlier in this chapter.

### 33.4.5 TFTP File Upload

The Prestige also supports the uploading of firmware files using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To transfer the firmware and the configuration file, follow the procedure shown next.

- 1 Use telnet from your computer to connect to the Prestige and log in. Because TFTP does not have any security checks, the Prestige records the IP address of the telnet client and accepts TFTP requests only from this address.
- 2 Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
- 3 Enter the command “sys stdio 0” to disable the management session idle timeout, so the TFTP transfer will not be interrupted. Enter “command sys stdio 5” to restore the five-minute management session idle timeout (default) when the file transfer is complete.

- 4 Launch the TFTP client on your computer and connect to the Prestige. Set the transfer mode to binary before starting data transfer.
- 5 Use the TFTP client (see the example below) to transfer files between the Prestige and the computer. The file name for the firmware is “ras”.

Note that the telnet connection must be active and the Prestige in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “get” to transfer from the Prestige to the computer, “put” the other way around, and “binary” to set binary transfer mode.

### 33.4.6 TFTP Upload Command Example

The following is an example TFTP command:

```
tftp [-i] host put firmware.bin ras
```

where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the Prestige’s IP address and “put” transfers the file source on the computer (firmware.bin – name of the firmware on the computer) to the file destination on the remote host (ras - name of the firmware on the Prestige).

Commands that you may see in GUI-based TFTP clients are listed earlier in this chapter.

# CHAPTER 34

## System Maintenance

This chapter leads you through SMT menus 24.8 to 24.10.

### 34.1 Command Interpreter Mode

The Command Interpreter (CI) is a part of the main system firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. Enter the CI from the SMT by selecting menu 24.8. See the included disk or the [zyxel.com](http://zyxel.com) web site for more detailed information on CI commands. Enter 8 from **Menu 24 — System Maintenance** to use the command prompt.

**Figure 181** Command Mode in Menu 24

```
Menu 24 - System Maintenance

1. System Status
2. System Information and Console Port Speed
3. Log and Trace
4. Diagnostic
5. Backup Configuration
6. Restore Configuration
7. Firmware Update
8. Command Interpreter Mode
9. Call Control
10. Time and Date Setting
11. Remote Management Setup

Enter Menu Selection Number:
```

#### 34.1.1 Command Syntax

- The command keywords are in `courier new` font.
- Enter the command keywords exactly as shown, do not abbreviate.
- The required fields in a command are enclosed in angle brackets `<>`.
- The optional fields in a command are enclosed in square brackets `[]`.
- The `|` symbol means “or”.
- For example,

```
sys filter netbios config <type> <on|off>
```

- means that you must specify the type of netbios filter and whether to turn it on or off.

## 34.1.2 Command Usage

A list of commands can be found by typing `help` or `?` at the command prompt. Always type the full command. Type `exit` to return to the SMT main menu when finished.

**Figure 182** Valid Commands Example

```
Copyright (c) 1994 - 2005 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys          exit          device          ether
poe          config         ip              ppp
bm           voice           dsp
```

## 34.2 Call Control Support

The Prestige provides two call control functions: budget management and call history. Please note that this menu is only applicable when **Encapsulation** is set to **PPPoE** in menu 4 or menu 11.1.

The budget management function allows you to set a limit on the total outgoing call time of the Prestige within certain times. When the total outgoing call time exceeds the limit, the current call will be dropped and any future outgoing calls will be blocked.

To access the call control menu, select option 9 in menu 24 to go to **Menu 24.9 — System Maintenance — Call Control**, as shown in the next table.

**Figure 183** Menu 24.9 System Maintenance: Call Control

```
Menu 24.9 - System Maintenance - Call Control

1. Budget Management
2. Call History

Enter Menu Selection Number:
```

### 34.2.1 Budget Management

Menu 24.9.1 shows the budget management statistics for outgoing calls. Enter 1 from **Menu 24.9 - System Maintenance - Call Control** to bring up the following menu.



**Figure 184** Menu 24.9.1 Budget Management

Menu 24.9.1 - Budget Management		
Remote Node	Connection Time/Total Budget	Elapsed Time/Total Period
1.MyISP	No Budget	No Budget
Reset Node (0 to update screen):		

The total budget is the time limit on the accumulated time for outgoing calls to a remote node. When this limit is reached, the call will be dropped and further outgoing calls to that remote node will be blocked. After each period, the total budget is reset. The default for the total budget is 0 minutes and the period is 0 hours, meaning no budget control. You can reset the accumulated connection time in this menu by entering the index of a remote node. Enter 0 to update the screen. The budget and the reset period can be configured in menu 11.1 for the remote node.

**Table 126** Menu 24.9.1 - Budget Management

FIELD	DESCRIPTION
Remote Node	Enter the index number of the remote node you want to reset (just one in this case)
Connection Time/Total Budget	This is the total connection time that has gone by (within the allocated budget that you set in menu 11.1).
Elapsed Time/Total Period	The period is the time cycle in hours that the allocation budget is reset (see menu 11.1). The elapsed time is the time used up within this period.
Enter "0" to update the screen or press [ESC] to return to the previous screen.	

## 34.2.2 Call History

This is the second option in **Menu 24.9 - System Maintenance - Call Control**. It displays information about past incoming and outgoing calls. Enter 2 from **Menu 24.9 - System Maintenance - Call Control** to bring up the following menu.

**Figure 185** Menu 24.9.2 - Call History

Menu 24.9.2 - Call History							
	Phone Number	Dir	Rate	#call	Max	Min	Total
1.							
2.							
3.							
4.							
5.							
6.							
7.							
8.							
9.							
10.							
Enter Entry to Delete(0 to exit):							

The following table describes the fields in this menu.

**Table 127** Call History Fields

FIELD	DESCRIPTION
Phone Number	The PPPoE service names are shown here.
Dir	This shows whether the call was incoming or outgoing.
Rate	This is the transfer rate of the call.
#call	This is the number of calls made to or received from that telephone number.
Max	This is the length of time of the longest telephone call.
Min	This is the length of time of the shortest telephone call.
Total	This is the total length of time of all the telephone calls to/from that telephone number.
You may enter an entry number to delete it or "0" to exit.	

### 34.3 Time and Date Setting

The Prestige has a software mechanism to set the time manually or get the current time and date from an external server when you turn on your Prestige. Menu 24.10 allows you to update the time and date settings of your Prestige. The real time is then displayed in the Prestige logs.

Select menu 24 in the main menu to open **Menu 24 - System Maintenance**, as shown next.

**Figure 186** Menu 24: System Maintenance

```

Menu 24 - System Maintenance

1. System Status
2. System Information and Console Port Speed
3. Log and Trace
4. Diagnostic
5. Backup Configuration
6. Restore Configuration
7. Upload Firmware
8. Command Interpreter Mode
9. Call Control
10. Time and Date Setting
11. Remote Management Setup

Enter Menu Selection Number:

```

Enter 10 to go to **Menu 24.10 - System Maintenance - Time and Date Setting** to update the time and date settings of your Prestige as shown in the following screen.

**Figure 187** Menu 24.10 System Maintenance: Time and Date Setting

```

Menu 24.10 - System Maintenance - Time and Date Setting

Time Protocol= Manual
Time Server Address= N/A

Current Time:                00 : 01 : 18
New Time (hh:mm:ss):        00 : 00 : 54

Current Date:                2000 - 01 - 01
New Date (yyyy-mm-dd):      2000 - 01 - 01

Time Zone= GMT

Daylight Saving= No
Start Date (mm-dd):          01 - 01
End Date (mm-dd):            01 - 01

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

```

The following table describes the fields in this screen.

**Table 128** Time and Date Setting Fields

FIELD	DESCRIPTION
Time Protocol	<p>Enter the time service protocol that your timeserver uses. Not all timeservers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main differences between them are the format.</p> <p><b>Daytime (RFC 867)</b> format is day/month/year/time zone of the server.</p> <p><b>Time (RFC-868)</b> format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.</p> <p><b>NTP (RFC-1305)</b> is similar to <b>Time (RFC-868)</b>.</p> <p><b>None</b> enter the time manually.</p>
Time Server Address	Enter the IP address or domain name of your timeserver. Check with your ISP/network administrator if you are unsure of this information. The default is tick.stdtime.gov.tw
Current Time	This field displays the Prestige's present time.
New Time	Enter the new time in hour, minute and second format.
Current Date	This field displays the Prestige's present date.
New Date	Enter the new date in year, month and day format.
Time Zone	Press [SPACE BAR] and then [ENTER] to set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Saving	Daylight Saving Time is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daylight time in the evenings. If you use daylight saving time, then choose <b>Yes</b> .
Start Date	Enter the month and day that your daylight-saving time starts on if you selected <b>Yes</b> in the <b>Daylight Saving</b> field.
End Date	Enter the month and day that your daylight-saving time ends on if you selected <b>Yes</b> in the <b>Daylight Saving</b> field.
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.	

# CHAPTER 35

## Remote Management

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

You may manage your Prestige from a remote location via:

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

To disable remote management of a service, select **Disable** in the corresponding **Server Access** field.

Enter 11 from menu 24 to bring up **Menu 24.11 – Remote Management Control**.

**Figure 188** Menu 24.11 – Remote Management Control

```

Menu 24.11 - Remote Management Control

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

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

Web Server:         Port = 80          Access = ALL
                   Secure Client IP = 0.0.0.0

SNMP Service:       Port = 161         Access = LAN only
                   Secure Client IP = 0.0.0.0

DNS Service:        Port = 53          Access = LAN only
                   Secure Client IP = 0.0.0.0

Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the fields in this screen.

**Table 129** Menu 24.11 – Remote Management Control

FIELD	DESCRIPTION
Telnet Server FTP Server Web Server SNMP Service DNS Service	Each of these read-only labels denotes a service or protocol.
Port	This field shows the port number for the service or protocol. You may change the port number if needed, but you must use the same port number to access the Prestige.
Access	Select the access interface (if any) by pressing [SPACE BAR], then [ENTER] to choose from: <b>LAN only</b> , <b>WAN only</b> , <b>ALL</b> or <b>Disable</b> .
Secure Client IP	The default 0.0.0.0 allows any client to use this service or protocol to access the Prestige. Enter an IP address to restrict access to a client with a matching IP address.
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.	

Remote management over LAN or WAN will not work when:

- 1** A filter in menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
- 2** You have disabled that service in menu 24.11.
- 3** The IP address in the **Secure Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the Prestige will disconnect the session immediately.
- 4** There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.

# CHAPTER 36

## Call Scheduling

Call scheduling (applicable for PPPoE encapsulation only) allows you to dictate when a remote node should be called and for how long.

The call scheduling feature allows the Prestige to manage a remote node and dictate when a remote node should be called and for how long. This feature is similar to the scheduler in a videocassette recorder (you can specify a time period for the VCR to record). You can apply up to 4 schedule sets in **Menu 11.1 — Remote Node Profile**. From the main menu, enter 26 to access **Menu 26 — Schedule Setup** as shown next.

**Figure 189** Menu 26 Schedule Setup

Menu 26 - Schedule Setup			
Schedule Set #	Name	Schedule Set #	Name
1	_____	7	_____
2	_____	8	_____
3	_____	9	_____
4	_____	10	_____
5	_____	11	_____
6	_____	12	_____

Enter Schedule Set Number to Configure= 0

Edit Name= N/A

Press ENTER to Confirm or ESC to Cancel:

Lower numbered sets take precedence over higher numbered sets thereby avoiding scheduling conflicts. For example, if sets 1, 2, 3 and 4 in are applied in the remote node then set 1 will take precedence over set 2, 3 and 4 as the Prestige, by default, applies the lowest numbered set first. Set 2 will take precedence over set 3 and 4, and so on.

You can design up to 12 schedule sets but you can only apply up to four schedule sets for a remote node.

**Note:** To delete a schedule set, enter the set number and press [SPACE BAR] and then [ENTER] (or delete) in the Edit Name field.

To setup a schedule set, select the schedule set you want to setup from menu 26 (1-12) and press [ENTER] to see **Menu 26.1 — Schedule Set Setup** as shown next.

**Figure 190** Menu 26.1 Schedule Set Setup

```

Menu 26.1 - Schedule Set Setup

Active= Yes
Start Date (yyyy/mm/dd) = 2000 - 01 - 01
How Often= Once
Once:
    Date (yyyy/mm/dd) = 2000 - 01 - 01
Weekdays:
    Sunday= N/A
    Monday= N/A
    Tuesday= N/A
    Wednesday= N/A
    Thursday= N/A
    Friday= N/A
    Saturday= N/A
Start Time (hh:mm)= 00 : 00
Duration (hh:mm)= 00 : 00
Action= Forced On

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

If a connection has been already established, your Prestige will not drop it. Once the connection is dropped manually or it times out, then that remote node can't be triggered up until the end of the **Duration**.

**Table 130** Menu 26.1 Schedule Set Setup

FIELD	DESCRIPTION
Active	Press [SPACE BAR] to select <b>Yes</b> or <b>No</b> . Choose <b>Yes</b> and press [ENTER] to activate the schedule set.
Start Date	Enter the start date when you wish the set to take effect in year -month-date format. Valid dates are from the present to 2036-February-5.
How Often	Should this schedule set recur weekly or be used just once only? Press the [SPACE BAR] and then [ENTER] to select <b>Once</b> or <b>Weekly</b> . Both these options are mutually exclusive. If <b>Once</b> is selected, then all weekday settings are <b>N/A</b> . When <b>Once</b> is selected, the schedule rule deletes automatically after the scheduled time elapses.
Once: Date	If you selected <b>Once</b> in the <b>How Often</b> field above, then enter the date the set should activate here in year-month-date format.
Weekday: Day	If you selected <b>Weekly</b> in the <b>How Often</b> field above, then select the day(s) when the set should activate (and recur) by going to that day(s) and pressing [SPACE BAR] to select <b>Yes</b> , then press [ENTER].
Start Time	Enter the start time when you wish the schedule set to take effect in hour-minute format.
Duration	Enter the maximum length of time this connection is allowed in hour-minute format.
Action	<b>Forced On</b> means that the connection is maintained whether or not there is a demand call on the line and will persist for the time period specified in the <b>Duration</b> field. <b>Forced Down</b> means that the connection is blocked whether or not there is a demand call on the line. <b>Enable Dial-On-Demand</b> means that this schedule permits a demand call on the line. <b>Disable Dial-On-Demand</b> means that this schedule prevents a demand call on the line.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	



Once your schedule sets are configured, you must then apply them to the desired remote node(s). Enter 11 from the **Main Menu** and then enter the target remote node index. Using [SPACE BAR], select **PPPoE** or **PPPoA** in the **Encapsulation** field and then press [ENTER] to make the schedule sets field available as shown next.

**Figure 191** Applying Schedule Set(s) to a Remote Node (PPPoE)

```
Menu 11.1 - Remote Node Profile

Rem Node Name= MyISP           Route= IP
Active= Yes                    Edit IP= No
Encapsulation= PPPoE          Telco Option:
Service Type= Standard        Allocated Budget (min)= 0
Service Name=                 Period(hr)= 0
Outgoing:                     Schedules= 1,2,3,4
  My Login=                   Nailed-Up Connection= No
  My Password= *****
  Retype to Confirm= *****
  Authen= CHAP/PAP

                               Session Options:
                               Edit Filter Sets= No
                               Idle Timeout(sec)= 100

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

You can apply up to four schedule sets, separated by commas, for one remote node. Change the schedule set numbers to your preference(s).



# CHAPTER 37

## Troubleshooting

This chapter covers potential problems and the corresponding remedies.

### 37.1 Problems Starting Up the Prestige

**Table 131** Troubleshooting the Start-Up of Your Prestige

PROBLEM	CORRECTIVE ACTION
None of the LEDs turn on when I turn on the Prestige.	Make sure that the Prestige's power adaptor is connected to the Prestige and an appropriate power source. Check that the power source is turned on.
	Disconnect the Prestige's power and reconnect it.
	If the error persists, you may have a hardware problem. In this case, you should contact your vendor.

### 37.2 Problems with the LAN Interface

**Table 132** Troubleshooting the LAN Interface

PROBLEM	CORRECTIVE ACTION
I cannot access the Prestige from the LAN.	Check your Ethernet cable connections. Refer to the Quick Start Guide for LAN connection instructions.
	Check for faulty Ethernet cables.
	Make sure the computer's Ethernet adapter is installed and functioning properly.
I cannot ping any computer on the LAN.	The <b>LAN</b> LED on the front panel should be on. If it is off, check the cables between the Prestige and your computer or switch.
	Verify that the IP address and the subnet mask of the Prestige's LAN port and the computers are on the same subnet.

## 37.3 Problems with the WAN Interface

**Table 133** Troubleshooting the WAN Interface

PROBLEM	CORRECTIVE ACTION
The Prestige cannot get a WAN IP address from the ISP.	The ISP provides the WAN IP address after authentication. Authentication may be through the user name and password, the MAC address or the host name. Use the following corrective actions to make sure the ISP can authenticate your connection.
	You need a user name and password if you're using PPPoE encapsulation. Make sure that you have entered the correct <b>Service Type</b> , <b>User Name</b> and <b>Password</b> (the user name and password are case sensitive). Refer to <a href="#">Section 6.2 on page 82</a> .
	If your ISP requires MAC address authentication, you can clone the MAC address from your computer on the LAN as the Prestige's WAN MAC address. Refer to <a href="#">Section 6.5 on page 88</a> .
	If your ISP requires host name authentication, configure your computer's name as the Prestige's system name. Refer to <a href="#">Section 4.3 on page 62</a> .

## 37.4 Problems with Internet Access

**Table 134** Troubleshooting Internet Access

PROBLEM	CORRECTIVE ACTION
I cannot access the Internet.	Make sure the Prestige is turned on and connected to the network.
	Verify your Ethernet settings (see <a href="#">Chapter 5 on page 72</a> and <a href="#">Chapter 6 on page 82</a> ).
	Make sure you entered the correct user name and password.
Internet connection disconnects.	Contact your ISP.

## 37.5 Problems with the Password

**Table 135** Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
I cannot access the Prestige.	The username is admin. The default password is 1234. The <b>Password</b> and <b>Username</b> fields are case-sensitive. Make sure that you enter the correct password and username using the proper casing. If you have changed the password and have now forgotten it, you will need to restore the default configuration file (see <a href="#">Section 2.3 on page 45</a> ). This restores all of the factory defaults including the password.

## 37.6 Problems with the Web Configurator

**Table 136** Troubleshooting the Web Configurator

PROBLEM	CORRECTIVE ACTION
I cannot access the web configurator.	<p>When NAT is enabled:</p> <ul style="list-style-type: none"> <li>• Use the Prestige's WAN IP address when configuring from the WAN.</li> <li>• Use the Prestige's LAN IP address when configuring from the LAN.</li> </ul> <p>If the Prestige's WAN or LAN IP address has changed, then enter the new one as the URL.</p> <p>You may also need to clear your Internet browser's cache.</p> <p>In Internet Explorer, click <b>Tools</b> and then <b>Internet Options</b> to open the <b>Internet Options</b> screen.</p> <p>In the <b>General</b> tab, click <b>Delete Files</b>. In the pop-up window, select the <b>Delete all offline content</b> check box and click <b>OK</b>. Click <b>OK</b> in the <b>Internet Options</b> screen to close it.</p> <p>If you disconnect your computer from one device and connect it to another device that has the same IP address, your computer's ARP (Address Resolution Protocol) table may contain an entry that maps the management IP address to the previous device's MAC address).</p> <p>In Windows, use <b>arp -d</b> at the command prompt to delete all entries in your computer's ARP table.</p>

## 37.7 Problems with a Telephone or the Telephone Port

**Table 137** Troubleshooting Telephone

PROBLEM	CORRECTIVE ACTION
There is no dial tone or I can't make calls.	<p>Check the telephone connections and telephone wire.</p> <p>Make sure you have the <b>VoIP</b> screen properly configured.</p> <p>You can also check the Prestige's IP addresses and VoIP status in the <b>Maintenance Status</b> screen.</p>
The dial tone beeps (pulses).	<p>Make sure you have the <b>VoIP</b> screens properly configured. The dial tone will be steady when the SIP account is registered.</p>
I cannot call from one of the Prestige's phone ports to the other phone port.	<p>You cannot use a phone connected to the Prestige to call the SIP number of one of the Prestige's SIP accounts.</p> <p>You can just press "<b>####</b>" on your phone's keypad to call the Prestige's other phone port.</p>

## 37.8 Problems with Voice Service

**Table 138** Troubleshooting Voice Service

PROBLEM	CORRECTIVE ACTION
After VoIP is configured and working, others are unable to call you or you lose your connection during a call. There is a NAT router between the Prestige and the SIP server.	<p>This could be caused by a short NAT UDP session timeout on the NAT router. When the SIP session's entry in the NAT table times out, the NAT router does not have any record to use for forwarding VoIP traffic to the Prestige.</p> <p>If possible, set the NAT router to use a longer NAT UDP session timeout.</p> <p>Otherwise, try one of the following:</p> <ul style="list-style-type: none"> <li>• Shorten the registration expiration period (see the <b>Expiration Duration</b> field in the <b>VoIP Advanced</b> screen) in order to cause the Prestige to re-register with the SIP register server more frequently. Note that this will not help if the SIP register server enforces a long registration expiration period (since the Prestige will also use the period set by the SIP register server).</li> <li>• Use STUN. If your VoIP service provider does not have a STUN server, you can still enable STUN and enter the IP address and port number of the SIP server in the STUN server fields. This causes the Prestige to send STUN requests to the SIP server. While this will not make STUN work (since there won't be any responses to the STUN requests), it should keep the NAT UDP session in the NAT router.</li> </ul>

## 37.9 Pop-up Windows, JavaScripts and Java Permissions

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

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

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

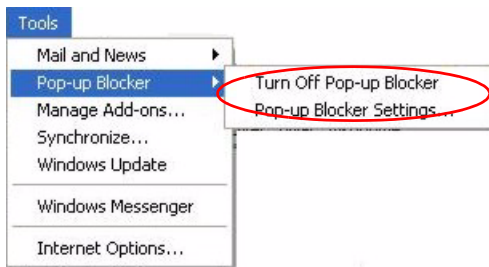
### 37.9.1 Internet Explorer Pop-up Blockers

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

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

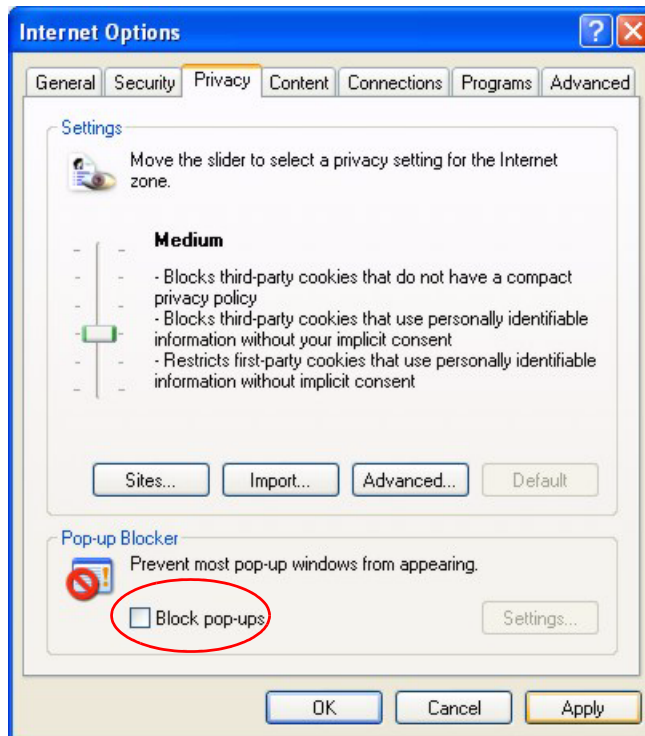
#### 37.9.1.1 Disable Pop-up Blockers

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

**Figure 192** Pop-up Blocker

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

- 1 In Internet Explorer, select **Tools, Internet Options, Privacy**.
- 2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

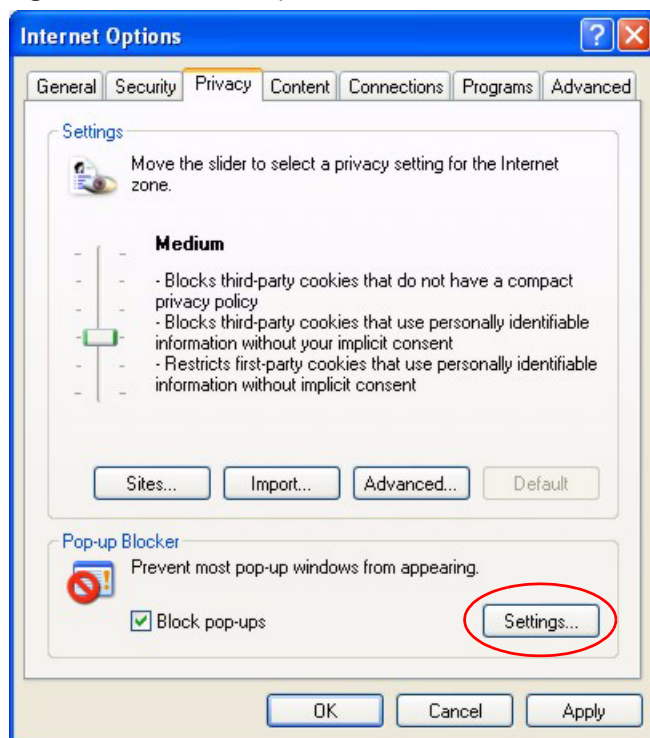
**Figure 193** Internet Options

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

### 37.9.1.2 Enable Pop-up Blockers with Exceptions

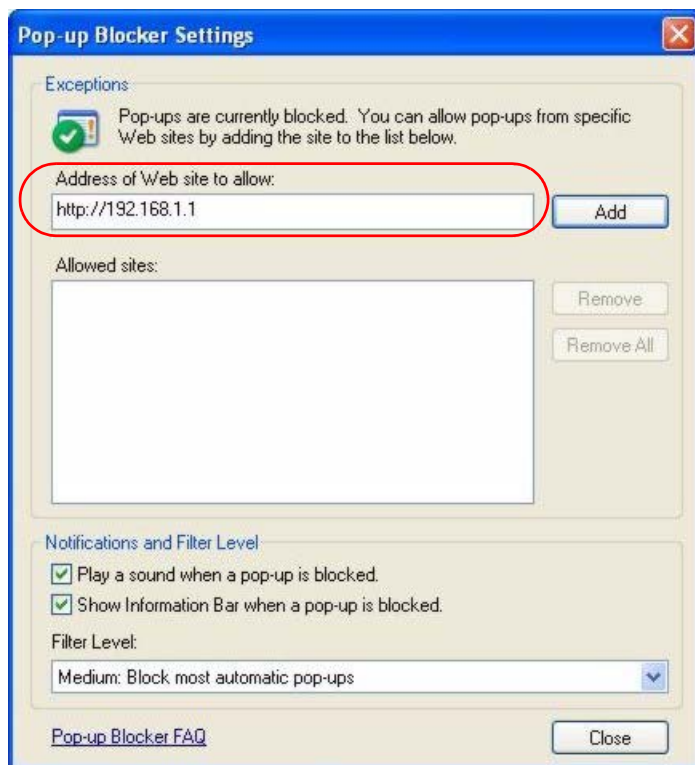
Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

- 1 In Internet Explorer, select **Tools, Internet Options** and then the **Privacy** tab.
- 2 Select **Settings...** to open the **Pop-up Blocker Settings** screen.

**Figure 194** Internet Options

- 3** Type the IP address of your device (the web page that you do not want to have blocked) with the prefix “http://”. For example, http://192.168.1.1.
- 4** Click **Add** to move the IP address to the list of **Allowed sites**.



**Figure 195** Pop-up Blocker Settings

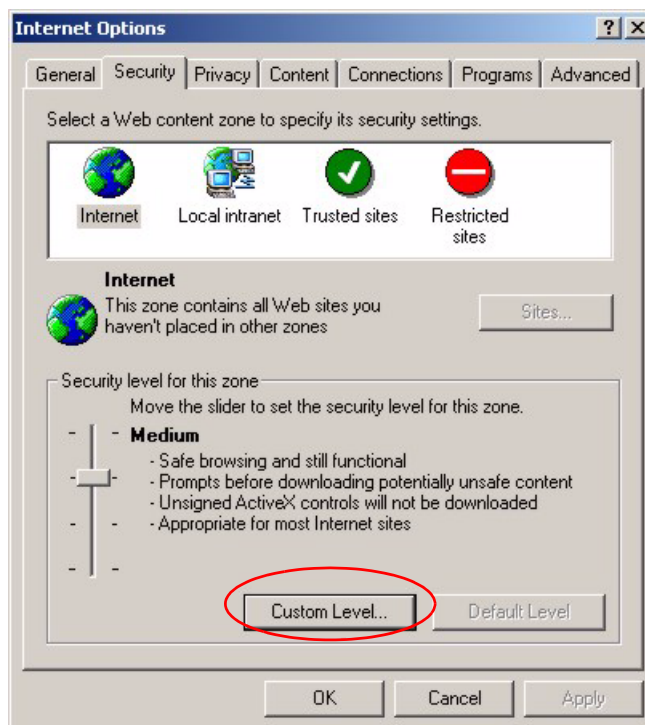
**5** Click **Close** to return to the **Privacy** screen.

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

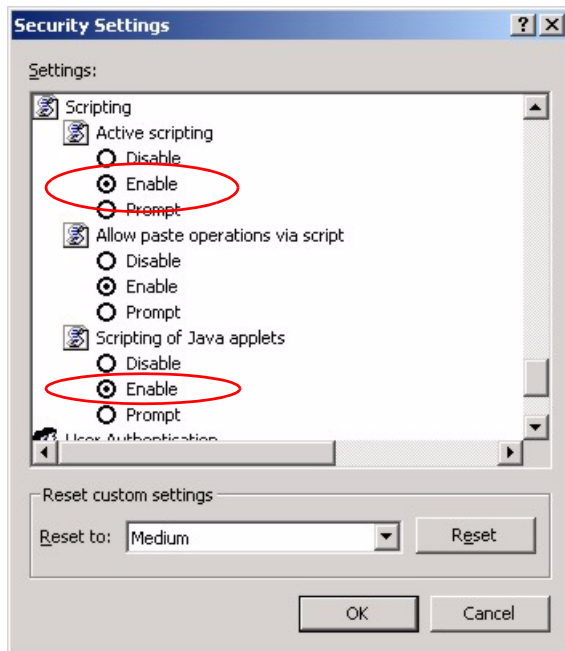
## 37.9.2 JavaScripts

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

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

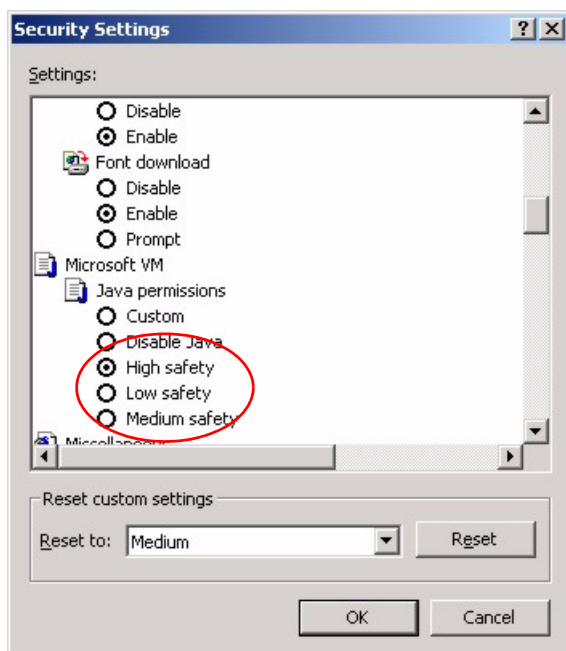
**Figure 196** Internet Options

- 2** Click the **Custom Level...** button.
- 3** Scroll down to **Scripting**.
- 4** Under **Active scripting** make sure that **Enable** is selected (the default).
- 5** Under **Scripting of Java applets** make sure that **Enable** is selected (the default).
- 6** Click **OK** to close the window.

**Figure 197** Security Settings - Java Scripting

### 37.9.3 Java Permissions

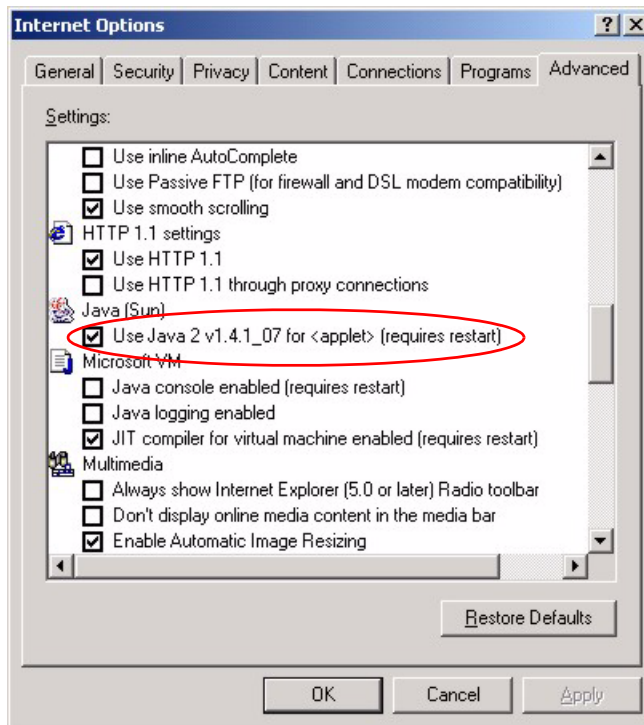
- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.
- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Microsoft VM**.
- 4 Under **Java permissions** make sure that a safety level is selected.
- 5 Click **OK** to close the window.

**Figure 198** Security Settings - Java

### 37.9.3.1 JAVA (Sun)

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

Figure 199 Java (Sun)





# APPENDIX A

## Product Specifications

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

### Specification Tables

**Table 139** Device Specifications

Default IP Address	192.168.1.1
Default Management Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234
Dimensions	109 (Wide) x 105 (Deep) x 22 (High) mm
Weight	312 g
Ethernet Ports	Two RJ-45, 10/100Mbps Half / Full Auto-negotiation, Auto-crossover Ethernet ports
Phone Ports	Two FXS (Foreign Exchange Station) POTS ports
Feeding Voltage	On hook: -48V; Minimum Voltage: -20V Off hook: -24V
Ringing Voltage	P2302R: 40V RMS at 5 REN P2302RL: 40V RMS at 3 REN
Line Ports (P2302RL Only)	One FXO (Foreign Exchange Office) lifeline port
Operation Temperature	0° C ~ 40° C
Storage Temperature	0° ~ 60° C
Operation Humidity	10% ~ 85% RH
Storage Humidity	10% ~ 90% RH

**Table 140** Feature Specifications

Voice Functions	<p>SIP (RFC 3261) version 2  SDP (RFC 2327)  RTP (RFC 1889)  RTCP (RFC 1890)  G.168 Echo Cancellation  VAD (Voice Activity Detection)  Silence Suppression  CNG (Comfort Noise Generation)  QoS Supports TOS and Diffserv Tagging  Compression: G.711 (PCM), G.729 (ADPCM)  Loop Start Signaling Support  Modem and Fax Tone Detection and Pass Through  DTMF Detection  Point to Point Calling (Direct IP to IP Calling)  Speed Dial Phonebook  Lifeline Support (Prestige 2302RL)  Support NAT Traversal / RFC 3489- IETF Simple Traversal of UDP Through NAT (STUN)  Caller ID  Dialing Type: Tone, Pulse (Auto detection)  Tip/ring polarity reversal</p>
Protocol Support	<p>PPP over Ethernet (RFC 2516)  Transparent bridging for unsupported network layer protocols.  DHCP Client</p>
Management	<p>Embedded Web Configurator  CLI (Command Line Interpreter)  Remote Management via Telnet or Web  SNMP manageable  FTP/TFTP for firmware downloading, configuration backup and restoration  Syslog  Built-in Diagnostic Tools for FLASH memory, RAM and LAN port</p>
Firewall	<p>Stateful Packet Inspection.  Prevent Denial of Service attacks such as Ping of Death, SYN Flood, LAND, Smurf etc.  Real time E-mail alerts.  Reports and logs.</p>
Content Filtering	<p>Service blocking.  Web page blocking by URL keyword.</p>
NAT/SUA	<p>Port Forwarding  1024 NAT sessions  Multimedia application.  PPTP under NAT/SUA.  IPSec passthrough  SIP ALG passthrough.</p>



**Table 140** Feature Specifications (continued)

Static Routes	16 IP and 4 Bridge
Other Features	Internal SPTGEN DNS Proxy Dynamic DNS Any IP IP Alias Traffic Redirect

## Wall Mounting Specifications

Use two M4 x 30 mm screws to wall-mount the Prestige.

The centers of the holes for the wall-mounting screws should be 109 mm apart.

## Power Adaptor Specifications

**Table 141** Prestige Power Adaptor Specifications

<b>NORTH AMERICAN PLUG STANDARDS</b>	
AC Power Adapter Model	DV-1215A
Input Power	AC120Volts/60Hz/30W
Output Power	AC12Volts/1.25A
Power Consumption	11 W
Safety Standards	UL, CUL, CSA (UL 1310, CSA C22.2 No.223)
<b>NORTH AMERICAN PLUG STANDARDS</b>	
AC Power Adapter Model	AA-121A25
Input Power	AC120Volts/60Hz/19W
Output Power	AC 12Volts/ 1.25A
Power Consumption	11W
Safety Standards	UL, CUL (UL 1310, CSA C22.2 No.223)
<b>EUROPEAN PLUG STANDARDS</b>	
AC Power Adapter Model	AA-121A3BN
Input Power	AC230Volts/50Hz/140mA
Output Power	AC12Volts/1.3A
Power Consumption	11W
Safety Standards	ITS-GS, CE (EN 60950)



# APPENDIX B

## Wall-mounting Instructions

Do the following to hang your Prestige on a wall.

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

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

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

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



# APPENDIX C

## Setting up Your Computer's IP Address

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

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

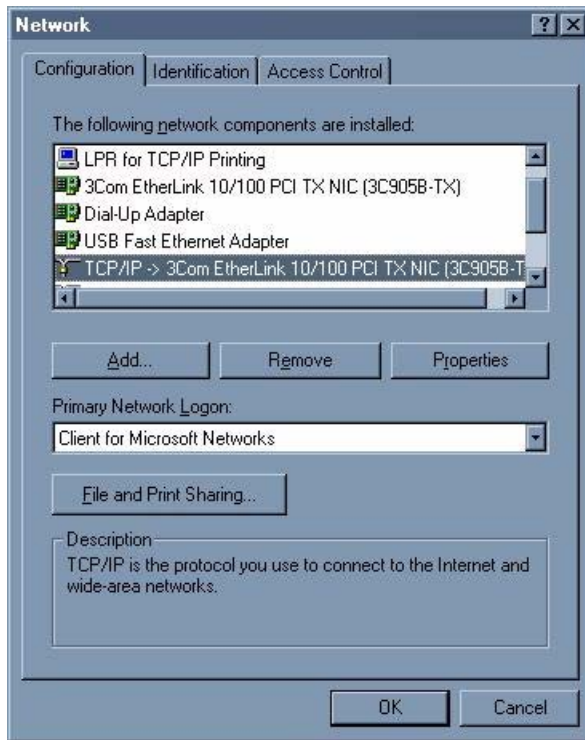
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

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

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

### Windows 95/98/Me

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

**Figure 200** Windows 95/98/Me: Network: Configuration

## Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

- 1 In the **Network** window, click **Add**.
- 2 Select **Adapter** and then click **Add**.
- 3 Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

- 1 In the **Network** window, click **Add**.
- 2 Select **Protocol** and then click **Add**.
- 3 Select **Microsoft** from the list of **manufacturers**.
- 4 Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

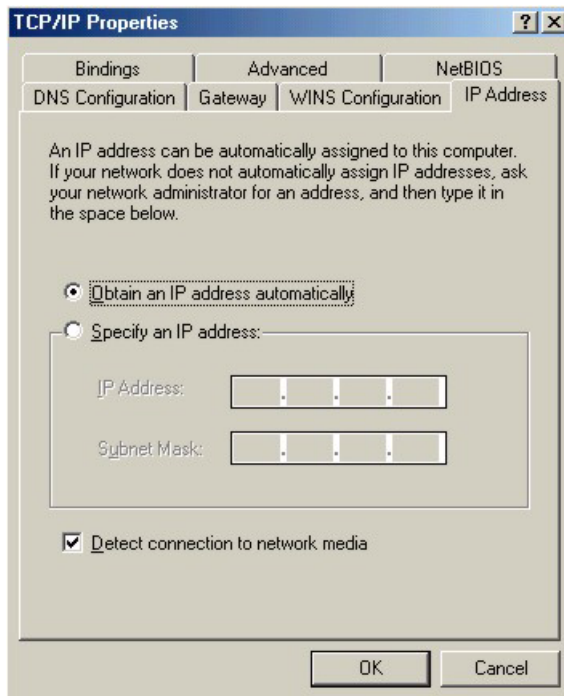
- 1 Click **Add**.
- 2 Select **Client** and then click **Add**.

- 3 Select **Microsoft** from the list of manufacturers.
- 4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
- 5 Restart your computer so the changes you made take effect.

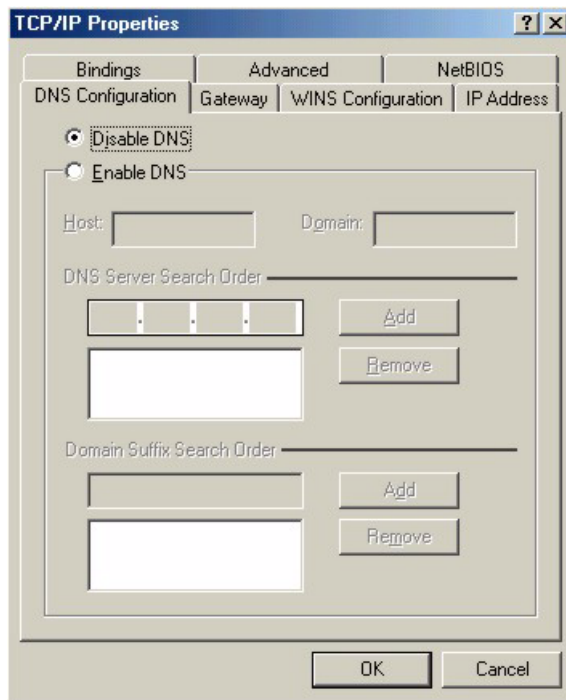
## Configuring

- 1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**
- 2 Click the **IP Address** tab.
  - If your IP address is dynamic, select **Obtain an IP address automatically**.
  - If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

**Figure 201** Windows 95/98/Me: TCP/IP Properties: IP Address



- 3 Click the **DNS Configuration** tab.
  - If you do not know your DNS information, select **Disable DNS**.
  - If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

**Figure 202** Windows 95/98/Me: TCP/IP Properties: DNS Configuration**4** Click the **Gateway** tab.

- If you do not know your gateway's IP address, remove previously installed gateways.
- If you have a gateway IP address, type it in the **New gateway field** and click **Add**.

**5** Click **OK** to save and close the **TCP/IP Properties** window.**6** Click **OK** to close the **Network** window. Insert the Windows CD if prompted.**7** Turn on your Prestige and restart your computer when prompted.

## Verifying Settings

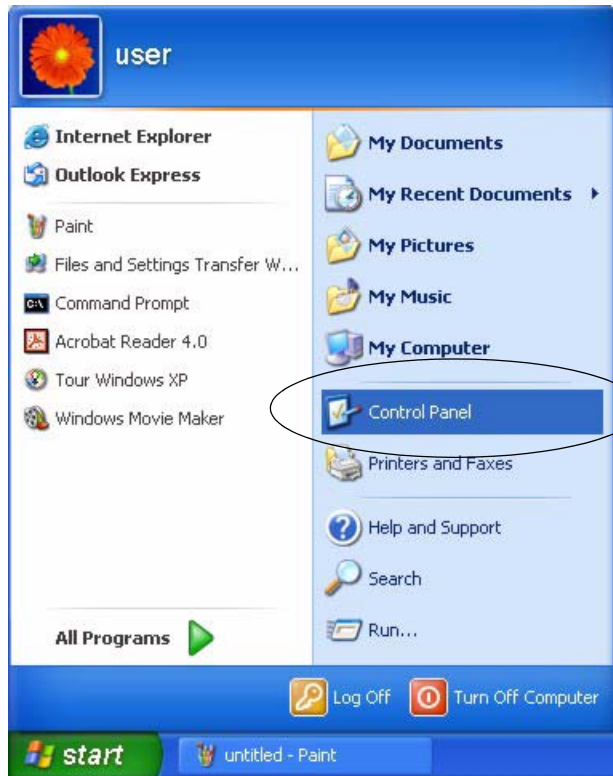
**1** Click **Start** and then **Run**.**2** In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.**3** Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

## Windows 2000/NT/XP

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

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

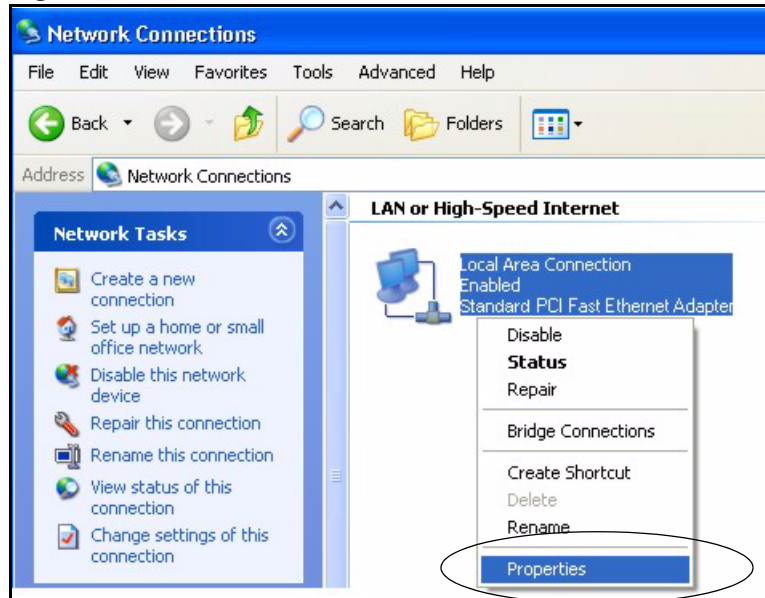


**Figure 203** Windows XP: Start Menu

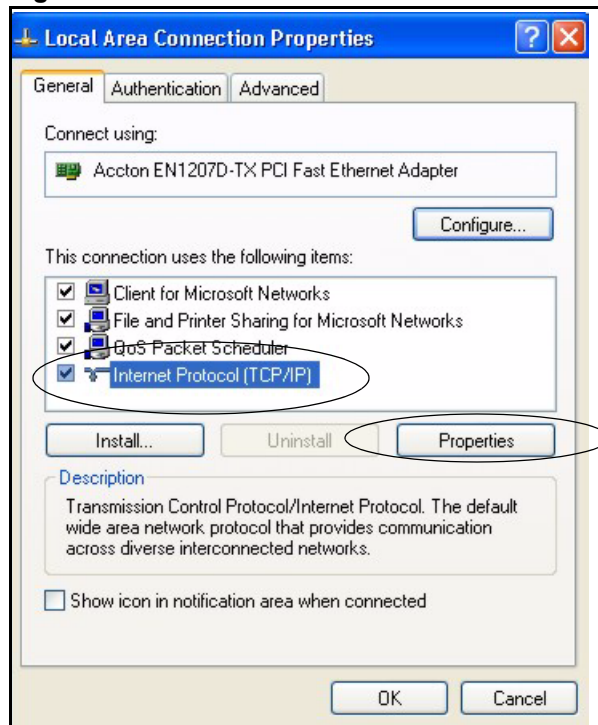
**2** In the **Control Panel**, double-click **Network Connections (Network and Dial-up Connections)** in Windows 2000/NT).

**Figure 204** Windows XP: Control Panel

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

**Figure 205** Windows XP: Control Panel: Network Connections: Properties

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

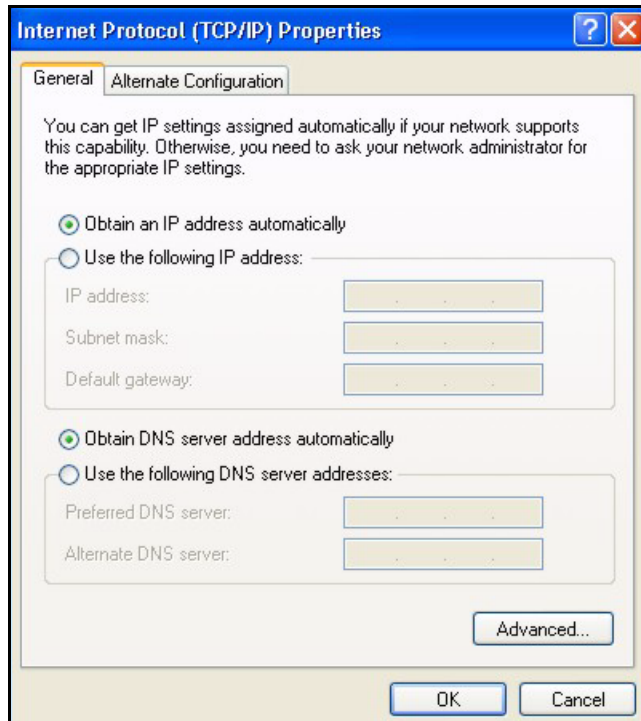
**Figure 206** Windows XP: Local Area Connection Properties

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

- If you have a dynamic IP address click **Obtain an IP address automatically**.

- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.
- Click **Advanced**.

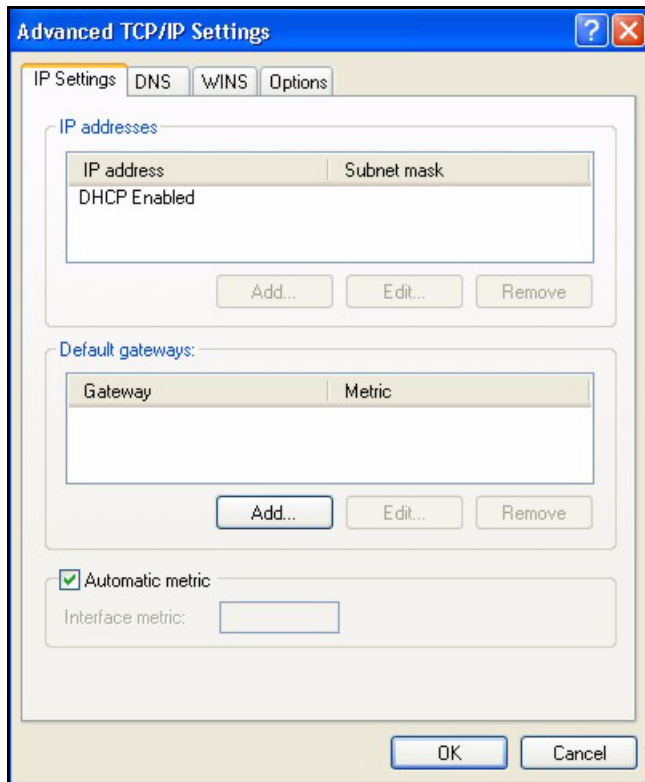
**Figure 207** Windows XP: Internet Protocol (TCP/IP) Properties



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

Do one or more of the following if you want to configure additional IP addresses:

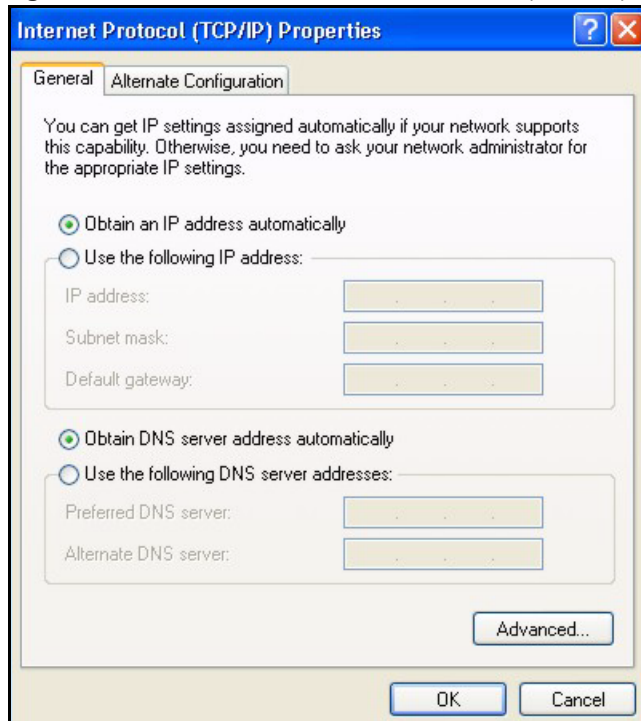
- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

**Figure 208** Windows XP: Advanced TCP/IP Properties

**7** In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

**Figure 209** Windows XP: Internet Protocol (TCP/IP) Properties

- 8** Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 9** Click **Close (OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.
- 10** Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).
- 11** Turn on your Prestige and restart your computer (if prompted).

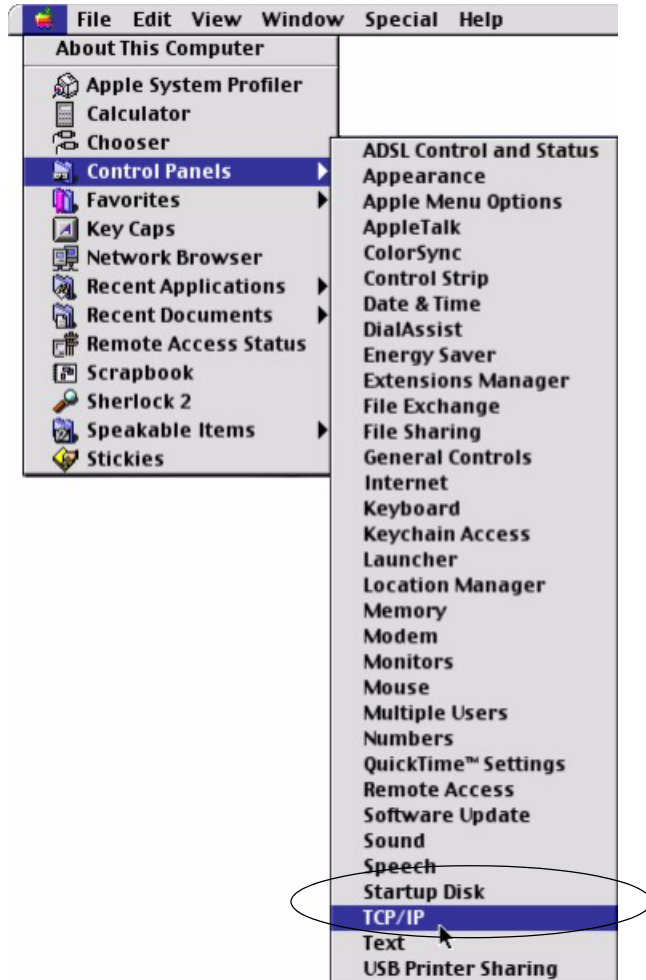
## Verifying Settings

- 1** Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.
- 2** In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

## Macintosh OS 8/9

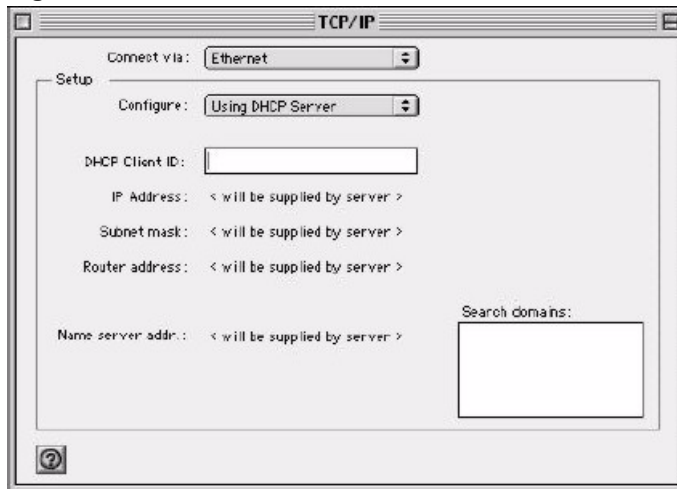
- 1** Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

**Figure 210** Macintosh OS 8/9: Apple Menu



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

**Figure 211** Macintosh OS 8/9: TCP/IP



**3** For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

- 4 For statically assigned settings, do the following:
  - From the **Configure** box, select **Manually**.
  - Type your IP address in the **IP Address** box.
  - Type your subnet mask in the **Subnet mask** box.
  - Type the IP address of your Prestige in the **Router address** box.
- 5 Close the **TCP/IP Control Panel**.
- 6 Click **Save** if prompted, to save changes to your configuration.
- 7 Turn on your Prestige and restart your computer (if prompted).

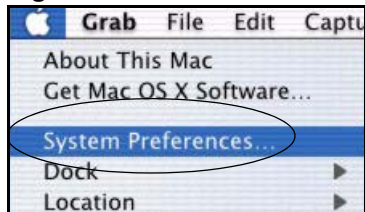
## Verifying Settings

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

## Macintosh OS X

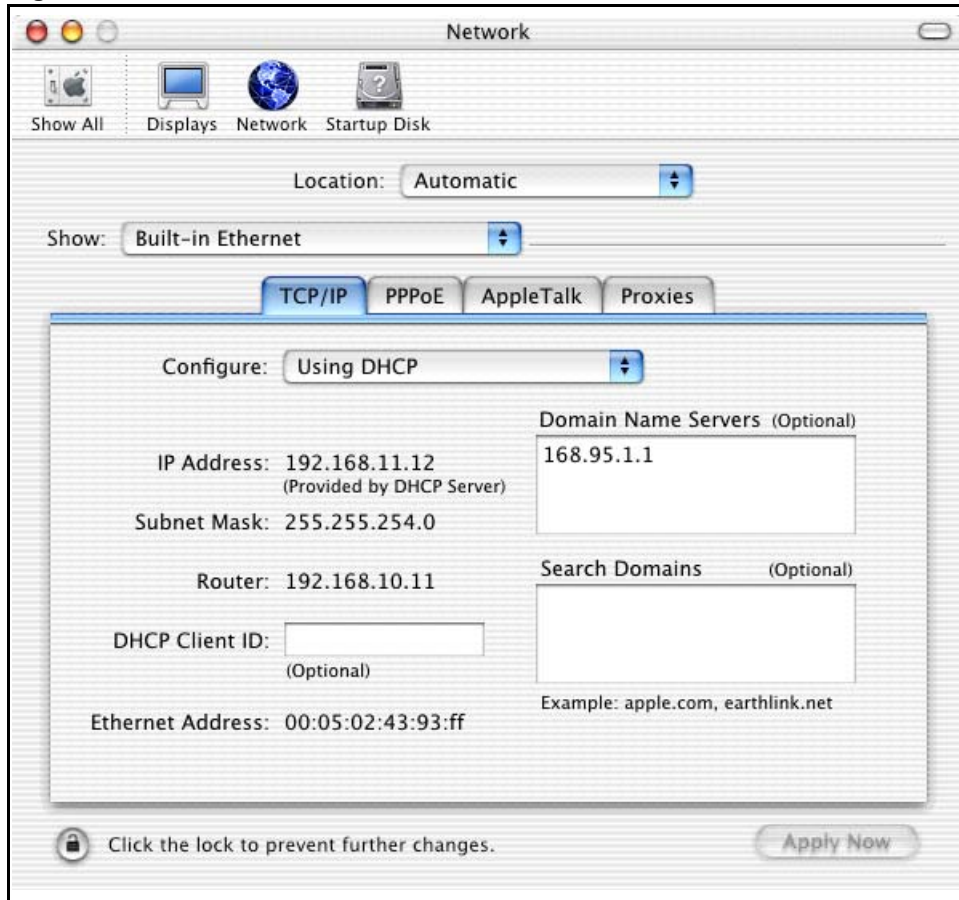
- 1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

**Figure 212** Macintosh OS X: Apple Menu



- 2 Click **Network** in the icon bar.
  - Select **Automatic** from the **Location** list.
  - Select **Built-in Ethernet** from the **Show** list.
  - Click the **TCP/IP** tab.
- 3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.



**Figure 213** Macintosh OS X: Network

**4** For statically assigned settings, do the following:

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

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

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

## Verifying Settings

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



# APPENDIX D

## IP Subnetting

### IP Addressing

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

### IP Classes

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

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

**Table 142** Classes of IP Addresses

IP ADDRESS:		OCTET 1	OCTET 2	OCTET 3	OCTET 4
Class A	0	Network number	Host ID	Host ID	Host ID
Class B	10	Network number	Network number	Host ID	Host ID
Class C	110	Network number	Network number	Network number	Host ID

**Note:** Host IDs of all zeros or all ones are not allowed.

Therefore:

A class “C” network (8 host bits) can have  $2^8 - 2$  or 254 hosts.

A class “B” address (16 host bits) can have  $2^{16} - 2$  or 65534 hosts.

A class “A” address (24 host bits) can have  $2^{24} - 2$  hosts (approximately 16 million hosts).

Since the first octet of a class “A” IP address must contain a “0”, the first octet of a class “A” address can have a value of 0 to 127.

Similarly the first octet of a class “B” must begin with “10”, therefore the first octet of a class “B” address has a valid range of 128 to 191. The first octet of a class “C” address begins with “110”, and therefore has a range of 192 to 223.

**Table 143** Allowed IP Address Range By Class

CLASS	ALLOWED RANGE OF FIRST OCTET (BINARY)	ALLOWED RANGE OF FIRST OCTET (DECIMAL)
Class A	00000000 to 01111111	0 to 127
Class B	10000000 to 10111111	128 to 191
Class C	11000000 to 11011111	192 to 223
Class D	11100000 to 11101111	224 to 239

## Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). A subnet mask has 32 is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

Subnet masks are expressed in dotted decimal notation just as IP addresses are. The “natural” masks for class A, B and C IP addresses are as follows.

**Table 144** “Natural” Masks

CLASS	NATURAL MASK
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

## Subnetting

With subnetting, the class arrangement of an IP address is ignored. For example, a class C address no longer has to have 24 bits of network number and 8 bits of host ID. With subnetting, some of the host ID bits are converted into network number bits. By convention, subnet masks always consist of a continuous sequence of ones beginning from the left most bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a “/” followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with mask 255.255.255.128.

The following table shows all possible subnet masks for a class “C” address using both notations.

**Table 145** Alternative Subnet Mask Notation

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

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

## Example: Two Subnets

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

**Table 146** Two Subnets Example

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

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

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

**Note:** In the following charts, shaded/bolded last octet bit values indicate host ID bits “borrowed” to form network ID bits. The number of “borrowed” host ID bits determines the number of subnets you can have. The remaining number of host ID bits (after “borrowing”) determines the number of hosts you can have on each subnet.

**Table 147** Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	<b>00000000</b>
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	<b>10000000</b>
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

**Table 148** Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	<b>10000000</b>
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	<b>10000000</b>
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

The remaining 7 bits determine the number of hosts each subnet can have. Host IDs of all zeros represent the subnet itself and host IDs of all ones are the broadcast address for that subnet, so the actual number of hosts available on each subnet in the example above is  $2^7 - 2$  or 126 hosts for each subnet.

192.168.1.0 with mask 255.255.255.128 is the subnet itself, and 192.168.1.127 with mask 255.255.255.128 is the directed broadcast address for the first subnet. Therefore, the lowest IP address that can be assigned to an actual host for the first subnet is 192.168.1.1 and the highest is 192.168.1.126. Similarly the host ID range for the second subnet is 192.168.1.129 to 192.168.1.254.

## Example: Four Subnets

The above example illustrated using a 25-bit subnet mask to divide a class “C” address space into two subnets. Similarly to divide a class “C” address into four subnets, you need to “borrow” two host ID bits to give four possible combinations of 00, 01, 10 and 11. The subnet mask is 26 bits (11111111.11111111.11111111.11000000) or 255.255.255.192. Each subnet contains 6 host ID bits, giving  $2^6-2$  or 62 hosts for each subnet (all 0’s is the subnet itself, all 1’s is the broadcast address on the subnet).

**Table 149** Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

**Table 150** Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	01000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

**Table 151** Subnet 3

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

**Table 152** Subnet 4

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	11000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

## Example Eight Subnets

Similarly use a 27-bit mask to create 8 subnets (001, 010, 011, 100, 101, 110).

The following table shows class C IP address last octet values for each subnet.

**Table 153** Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

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

**Table 154** Class C Subnet Planning

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

## Subnetting With Class A and Class B Networks.

For class “A” and class “B” addresses the subnet mask also determines which bits are part of the network number and which are part of the host ID.

A class “B” address has two host ID octets available for subnetting and a class “A” address has three host ID octets (see [Table 142 on page 356](#)) available for subnetting.

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

**Table 155** Class B Subnet Planning

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





# APPENDIX E

## PPPoE

### PPPoE in Action

An ADSL modem bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your computer to an ATM PVC (Permanent Virtual Circuit) which connects to a DSL Access Concentrator where the PPP session terminates (see [Figure 214 on page 365](#)). One PVC can support any number of PPP sessions from your LAN. PPPoE provides access control and billing functionality in a manner similar to dial-up services using PPP.

### Benefits of PPPoE

PPPoE offers the following benefits:

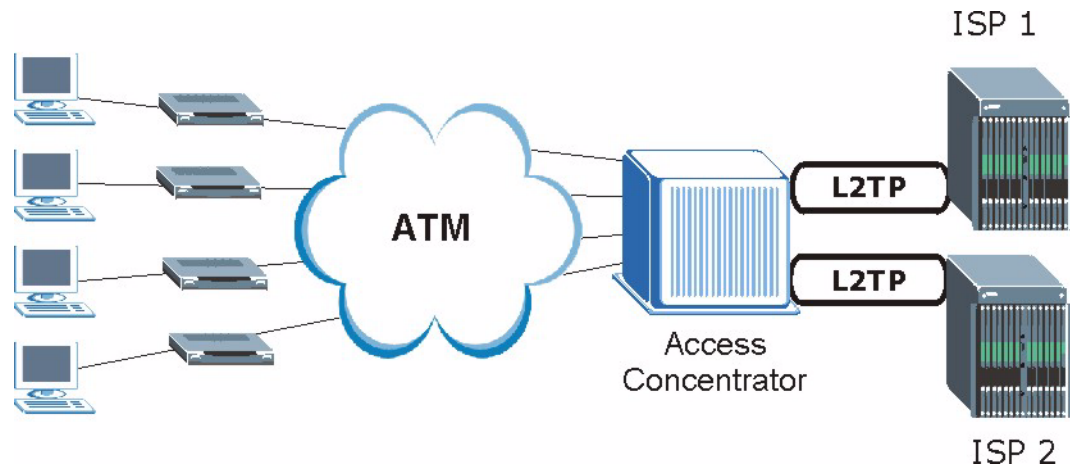
It provides you with a familiar dial-up networking (DUN) user interface.

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

It allows the ISP to use the existing dial-up model to authenticate and (optionally) to provide differentiated services.

### Traditional Dial-up Scenario

The following diagram depicts a typical hardware configuration where the computers use traditional dial-up networking.

**Figure 214** Single-Computer per Router Hardware Configuration

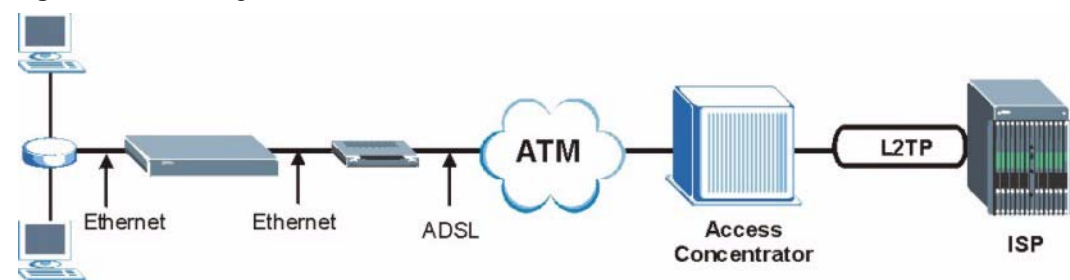
## How PPPoE Works

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

With PPPoE, the VC (Virtual Circuit) is equivalent to the dial-up connection and is between the modem and the AC, as opposed to all the way to the ISP. However, the PPP negotiation is between the computer and the ISP.

## Prestige as a PPPoE Client

When using the Prestige as a PPPoE client, the computers on the LAN see only Ethernet and are not aware of PPPoE. This alleviates the administrator from having to manage the PPPoE clients on the individual computers.

**Figure 215** Prestige as a PPPoE Client

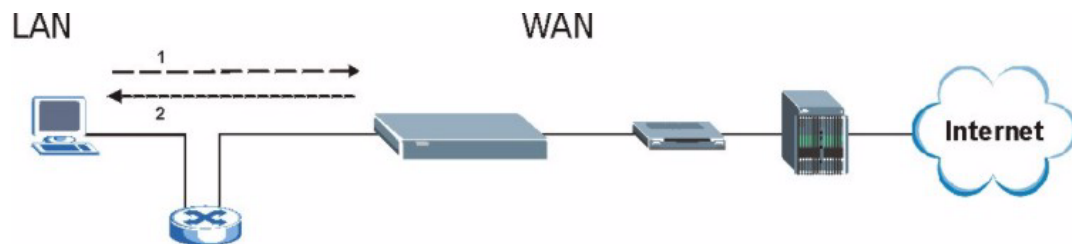
# APPENDIX F

## Triangle Route

### The Ideal Setup

When the firewall is on, your Prestige acts as a secure gateway between your LAN and the Internet. In an ideal network topology, all incoming and outgoing network traffic passes through the Prestige to protect your LAN against attacks.

**Figure 216** Ideal Setup

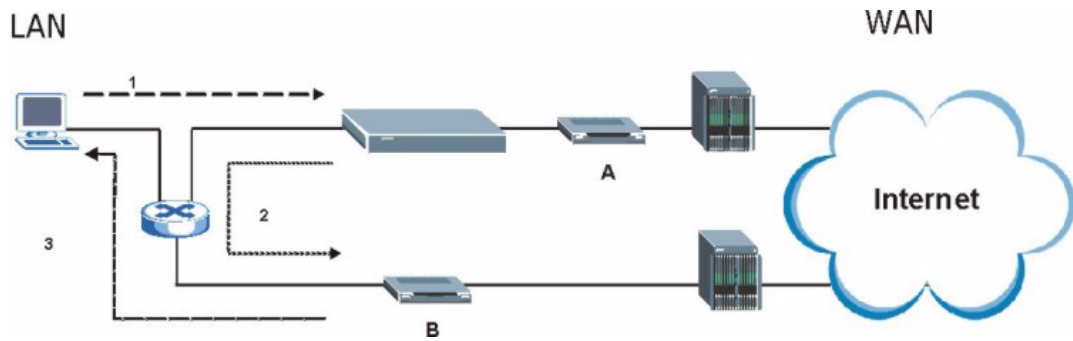


### The “Triangle Route” Problem

A traffic route is a path for sending or receiving data packets between two Ethernet devices. Some companies have more than one alternate route to one or more ISPs. If the LAN and ISP(s) are in the same subnet, the “triangle route” problem may occur. The steps below describe the “triangle route” problem.

- 1** A computer on the LAN initiates a connection by sending out a SYN packet to a receiving server on the WAN.
- 2** The Prestige reroutes the SYN packet through Gateway **B** on the LAN to the WAN.
- 3** The reply from the WAN goes directly to the computer on the LAN without going through the Prestige.

As a result, the Prestige resets the connection, as the connection has not been acknowledged.

**Figure 217** “Triangle Route” Problem

## The “Triangle Route” Solutions

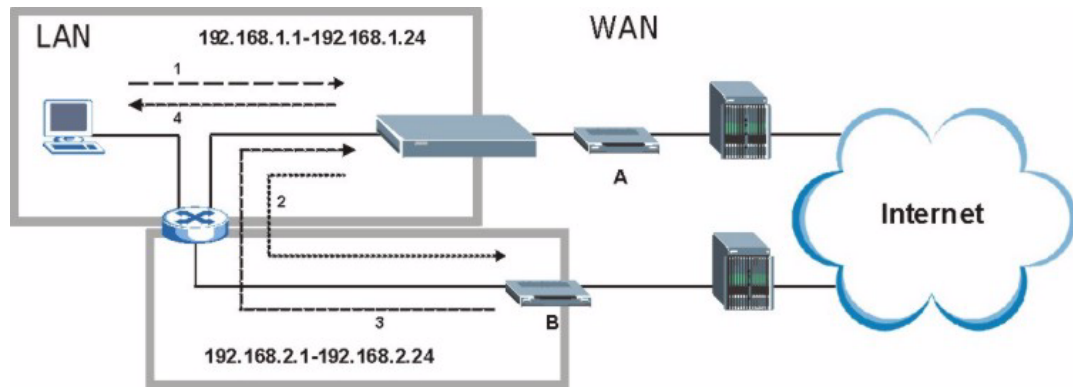
This section presents you two solutions to the “triangle route” problem.

### IP Aliasing

IP alias allows you to partition your network into logical sections over the same Ethernet interface. Your Prestige supports up to three logical LAN interfaces with the Prestige being the gateway for each logical network. By putting your LAN and Gateway **B** in different subnets, all returning network traffic must pass through the Prestige to your LAN. The following steps describe such a scenario.

- 1** A computer on the LAN initiates a connection by sending a SYN packet to a receiving server on the WAN.
- 2** The Prestige reroutes the packet to Gateway B, which is in the 192.168.2.1 to 192.168.2.24 subnet.
- 3** The reply from WAN goes through the Prestige to the computer on the LAN in the 192.168.1.1 to 192.168.1.24 subnet.

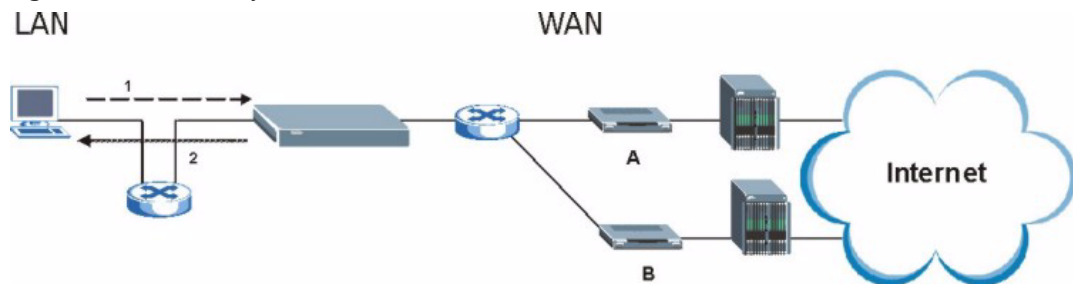
Figure 218 IP Alias



## Gateways on the WAN Side

A second solution to the “triangle route” problem is to put all of your network gateways on the WAN side as the following figure shows. This ensures that all incoming network traffic passes through your Prestige to your LAN. Therefore your LAN is protected.

Figure 219 Gateways on the WAN Side



## Configuring Triangle Route via Commands

- 1 From the SMT main menu, enter 24.
- 2 Enter “8” in menu 24 to enter CI command mode.
- 3 Use the following command to allow triangle route:

```
sys firewall ignore triangle all on
```

or this command to disallow triangle route:

```
sys firewall ignore triangle all off
```



# APPENDIX G

## SIP Passthrough

### Enabling/Disabling the SIP ALG

You can turn off the Prestige SIP ALG to avoid retranslating the IP address of an existing SIP device that is using STUN. If you want to use STUN with a SIP client device (a SIP phone or IP phone for example) behind the Prestige, use the `ip alg disable ALG_SIP` command to turn off the SIP ALG.

### Signaling Session Timeout

Most SIP clients have an “expire” mechanism indicating the lifetime of signaling sessions. The SIP UA sends registration packets to the SIP server periodically and keeps the session alive in the Prestige.

If the SIP client does not have this mechanism and makes no call during the Prestige SIP timeout default (60 minutes), the Prestige SIP ALG drops any incoming calls after the timeout period. You can use the `ip alg siptimeout` command to change the timeout value.

### Audio Session Timeout

If no voice packets go through the SIP ALG before the timeout period default (5 minutes) expires, the SIP ALG does not drop the call but blocks all voice traffic and deletes the audio session. You cannot hear anything and you will need to make a new call to continue your conversation.





# Index

## Numerics

10/100 Mbps Ethernet [35](#)  
 110V AC [5](#)  
 230V AC [5](#)  
 64kbps [58](#), [107](#)  
 8kbps [58](#), [107](#)

## A

Abnormal Working Conditions [6](#)  
 About This User's Guide [32](#)  
 AbS [101](#)  
 AC [5](#)  
 Accept [124](#)  
 Access methods [274](#)  
 Accessories [5](#)  
 ACK Message [91](#)  
 Active [247](#)  
 ActiveX [155](#)  
 Acts of God [6](#)  
 Address Mapping [135](#)  
 Address Resolution Protocol (ARP) [76](#)  
 Administrator Inactivity Timer [64](#)  
 ADPCM [339](#)  
 Advanced Setup Call Forwarding [124](#)  
 Airflow [5](#)  
 ALG [35](#), [99](#)  
 Allocated Budget [250](#)  
 Alternative Subnet Mask Notation [358](#)  
 American Wire Gauge [5](#)  
 Analog Telephone [34](#)  
 Analysis-by-Synthesis [101](#)  
 Any IP [35](#), [75](#)  
   How it works [76](#)  
   note [76](#)  
 Any IP Setup [79](#)  
 Any IP Table [216](#)  
 Application Layer Gateway [35](#), [99](#)  
 AT Command [305](#)  
 Authen [250](#)  
 Authentication Password [58](#), [104](#)

Authentication Protocol [249](#)  
 Authentication User ID [58](#), [104](#)  
 Authority [3](#)  
 Auto Firmware Upgrade [37](#), [127](#)  
 Auto-crossover [35](#)  
 Auto-discovering UPnP-enabled Network Devices [176](#)  
 Automatic Log Out [45](#)  
 Auto-negotiating [35](#)  
 Auto-provisioning [37](#), [127](#)  
 AWG [5](#)

## B

Backup [305](#)  
 Backup Configuration [220](#)  
 Bandwidth Borrowing [202](#)  
 Bandwidth Class [198](#)  
 Bandwidth Filter [198](#), [207](#)  
 Bandwidth Management [35](#), [198](#)  
 Bandwidth Management Statistics [208](#)  
 Bandwidth Manager Class Configuration [206](#)  
 Bandwidth Manager Class Setup [205](#)  
 Bandwidth Manager Monitor [209](#)  
 Bandwidth Manager Summary [203](#)  
 Basement [5](#)  
 Block [124](#)  
 Budget Management [315](#), [316](#)  
 Buffer, Jitter [36](#)  
 Busy [124](#)  
 BYE Request [91](#)

## C

Cable, Ethernet [35](#)  
 Cables, Connecting [5](#)  
 Call Control [315](#)  
 Call Forward [122](#)  
 Call Forward Table [109](#)  
 Call History [316](#)  
 Call Hold [115](#), [117](#)  
 Call Scheduling [322](#)

Maximum Number of Schedule Sets [322](#)  
PPPoE [324](#)  
Precedence [322](#)  
Precedence Example [322](#)  
Call Service Mode [114](#), [116](#), [118](#)  
Call to Phone Port Mapping [104](#)  
Call Transfer [116](#), [117](#)  
Call Waiting [115](#), [117](#)  
Caller ID [104](#), [339](#)  
Call-Triggering Packet [299](#)  
CDR [298](#)  
CDR (Call Detail Record) [296](#)  
Certifications [3](#)  
Change Password [45](#)  
Changes or Modifications [3](#)  
Charge [6](#)  
Checking the Prestige's IP Address [126](#)  
Circuit [3](#)  
Circuit-switched Telephone Networks [90](#)  
Class B [3](#)  
Class of Service [110](#)  
Class of Service (CoS) [110](#)  
Clicks [101](#)  
Client Server, SIP [91](#)  
Client-server Protocol [91](#)  
CNG [339](#)  
Codec [58](#), [100](#), [107](#)  
Codecs [37](#)  
Coder/Decoder [58](#), [100](#), [107](#)  
Comfort Noise Generation [112](#), [339](#)  
Command Interpreter Mode [314](#)  
Comments [32](#)  
Communications [3](#)  
Community [166](#), [290](#)  
Compliance, FCC [3](#)  
Components [6](#)  
Compression [339](#)  
Computer [33](#)  
Computer Name [62](#)  
Condition [6](#), [124](#)  
Configuration [73](#), [215](#)  
Configuration Screen [220](#)  
Configuration Upload Successful [221](#)  
Configuring Address Mapping [137](#)  
Connecting Cables [5](#)  
Consequential Damages [6](#)  
Console Port [295](#)  
Contact Information [7](#)  
Contacting Customer Support [7](#)  
Content Filtering [154](#)

Days and Times [154](#)  
Restrict Web Features [154](#)  
Cookies [155](#)  
Copyright [2](#)  
Correcting Interference [3](#)  
Corrosive Liquids [5](#)  
CoS [110](#)  
Cost Of Transmission [257](#)  
Covers [5](#)  
Crossover Ethernet Cable [35](#)  
Customer Support [7](#)

## D

Damage [5](#)  
Dampness [5](#)  
Danger [5](#)  
Date [69](#)  
Date Setting [317](#)  
Daylight Saving [319](#)  
Daylight Savings [70](#)  
Daytime (RFC 867) [319](#)  
Daytime RFC 867 [69](#)  
Dealer [3](#)  
Decoder [100](#)  
Deep [338](#)  
Default  
    LAN IP Address [44](#)  
    Password [44](#)  
Default LAN IP address [44](#)  
Default Management IP Address [338](#)  
Default Management Subnet Mask [338](#)  
Default Password [44](#), [338](#)  
Default Server [134](#)  
Default Server IP Address [132](#)  
Default Settings [36](#)  
Defective [6](#)  
Denial of Service [274](#)  
Denmark, Contact Information [7](#)  
Device Name [172](#)  
DHCP [38](#), [63](#), [65](#), [73](#), [215](#), [295](#)  
DHCP (Dynamic Host Configuration Protocol) [38](#)  
DHCP Client [339](#)  
DHCP Clients [63](#)  
Diagnostic Tools [339](#)  
Dialing Interval [114](#)  
Dialing Type [339](#)  
Dial-up Networking User Interface, See PPPoE [39](#)

Differentiated Services [37, 110](#)  
 DiffServ [37, 110](#)  
 Diffserv [339](#)  
 DiffServ Code Point (DSCP) [110](#)  
 DiffServ Code Points [110](#)  
 DiffServ marking rule [110](#)  
 Dimensions [338](#)  
 Disclaimer [2](#)  
 Discretion [6](#)  
 DNS [133, 167](#)  
 DNS Device Port [167](#)  
 DNS Proxy [340](#)  
 DNS Server Address [73](#)  
 Domain Name [63, 64](#)  
 Domain Name System [73, 133](#)  
 DS Field [110](#)  
 DS field [110](#)  
 DSCPs [110](#)  
 DTMF [101](#)  
 DTMF Detection [339](#)  
 DTMF Mode [59, 108](#)  
 Dual-Tone Multi-Frequency [59, 101, 108](#)  
 Dust [5](#)  
 Dynamic DNS [65, 231](#)  
 Dynamic DNS Support [38](#)  
 Dynamic Domain Name System [38](#)  
 Dynamic Host Configuration Protocol [38](#)  
 Dynamic Jitter Buffer [36](#)  
 DYNDNS Wildcard [65](#)

## E

ECHO [132](#)  
 Echo Cancellation [37, 112](#)  
 Edit IP [248](#)  
 Electric Shock [5](#)  
 Electrical Pipes [5](#)  
 Electrocutation [5](#)  
 Embedded FTP and TFTP Servers [39](#)  
 Embedded Web Configurator [339](#)  
 Emergency Numbers [120](#)  
 Encapsulation [247](#)  
 Equal or Higher Value [6](#)  
 Ethernet [51, 52, 339](#)  
 Ethernet Cable [35](#)  
 Ethernet Encapsulation [132, 246, 247](#)  
 Ethernet Ports [338](#)  
 Europe [5](#)

Europe Type [118](#)  
 Europe Type Call Service Mode [114](#)  
 Expiration Duration [107](#)  
 Exposure [5](#)  
 External IP Addresses [94](#)

## F

Factory Defaults [222](#)  
 Factory LAN Defaults [73](#)  
 Factory-default Configuration [45](#)  
 Fail Tolerance [254](#)  
 Failure [6](#)  
 Fairness-based Scheduler [200](#)  
 Fast Ethernet Interfaces [35](#)  
 Fax [37](#)  
 Fax Pass Through [339](#)  
 Fax Pass-through [37](#)  
 Fax Tone Detection [37, 339](#)  
 FCC [3](#)

- Compliance [3](#)
  - Rules, Part 15 [3](#)

 FCC Rules [3](#)  
 Features [34](#)  
 Federal Communications Commission [3](#)  
 Feedback [32](#)  
 Feeding Voltage [338](#)  
 File Transfer Protocol [132](#)  
 Filename Conventions [304](#)  
 Filter [236, 252](#)

- Applying [288](#)
- Example [286](#)
- Generic Filter Rule [284](#)
- Generic Rule [285](#)
- NAT [288](#)
- Remote Node [289](#)
- Structure [277](#)

 Finger [133](#)  
 Finland, Contact Information [7](#)  
 Firewall [146, 147](#)

- Access Methods [274](#)
- Remote Management [274](#)
- SMT menus [274](#)

 Firmware [217, 294](#)  
 Firmware Upgrades [39](#)  
 Firmware Upload Error [219](#)  
 Firmware Upload In Process [219](#)  
 Fitness [6](#)  
 Flash Key [114](#)  
 Flashing [114](#)

Foreign Exchange Office [338](#)  
Foreign Exchange Station [338](#)  
Forward to Number [124](#)  
Forwarding Service Requests, See Port Forwarding [38](#)  
France, Contact Information [7](#)  
Frequency Pairs [101](#)  
FTP [65](#), [131](#), [132](#), [158](#), [160](#), [339](#)  
FTP File Transfer [310](#)  
FTP Restrictions [158](#)  
FTP Server [39](#), [268](#)  
Full Cone NAT [96](#)  
Functionally Equivalent [6](#)  
FXO [338](#)  
FXS [338](#)

## G

G.168 [37](#), [112](#)  
G.168 Active [113](#)  
G.168 Echo Cancellation [339](#)  
G.711 [37](#), [58](#), [101](#), [107](#), [339](#)  
G.729 [37](#), [58](#), [101](#), [107](#), [339](#)  
Gas Pipes [5](#)  
Gateway [143](#), [257](#)  
Gateway IP Addr [251](#)  
Gateway IP Address [144](#), [243](#)  
General Setup [62](#)  
Germany, Contact Information [7](#)  
Get [163](#)  
Get Community [166](#)  
GetNext [163](#)  
Global [128](#)  
Global End IP [136](#), [138](#)  
Global Start IP [136](#), [138](#)  
Glossary [32](#)  
God, act of [6](#)

## H

Harmful Interference [3](#)  
Help [32](#)  
Help Icon [46](#)  
Hidden Menus [225](#)  
High [338](#)  
High Voltage Points [5](#)  
Hop Count [257](#)

Host [68](#)  
Host IDs [356](#)  
HTTP [133](#), [217](#)  
Hybrid, Waveform Codec [101](#)  
Hyper Text Transfer Protocol [133](#)  
Hypertext Transfer Protocol [217](#)

## I

ICMP [169](#)  
Idle Management Session [45](#)  
Idle Timeout [159](#), [249](#), [250](#)  
IEEE 802.1Q VLAN [110](#)  
IGA [128](#), [136](#)  
IGD 1.0 [171](#)  
IGMP [38](#), [75](#)  
ILA [128](#), [136](#)  
Immediate Dial [118](#), [124](#)  
Incoming Call Mapping [104](#)  
Incoming Call Number [124](#)  
Incoming Lifeline Call Mapping [118](#)  
Indirect Damages [6](#)  
Inside [128](#)  
Inside Global Address [128](#), [136](#)  
Inside Local Address [128](#), [136](#)  
Install UPnP [172](#)  
    Windows Me [172](#)  
    Windows XP [174](#)  
Insurance [6](#)  
Interference [3](#)  
Interference Correction Measures [3](#)  
Interference Statement [3](#)  
Internal Calls [126](#)  
Internal IP Addresses [94](#)  
Internal SPTGEN [340](#)  
Internet Access [242](#)  
    ISP's Name [243](#)  
Internet access [242](#)  
Internet Access Problems [327](#)  
Internet Access Setup [243](#), [258](#)  
Internet Control Message Protocol [169](#)  
Internet Explorer [44](#)  
Internet Explorer Pop-up Blockers [329](#)  
Internet Gateway Device [171](#)  
Internet Group Management Protocol [38](#)  
Internet Protocol Private Branch Exchange [41](#)  
Internet Telephony Service Provider [40](#), [90](#)  
Introduction to Filters [276](#)

IP Address [72](#), [133](#), [134](#), [238](#), [243](#), [251](#), [257](#), [295](#)  
 IP Address Assignment [251](#)  
 IP Addressing [356](#)  
 IP Alias [38](#), [130](#)  
 IP Classes [356](#)  
 IP Multicast [38](#)  
 IP Pool [237](#)  
 IP Pool Setup [73](#)  
 IP Static Route [142](#)  
 IP Static Route Setup [256](#)  
 IP to IP Calling [339](#)  
 IP to IP Calls [42](#)  
 IP-PBX [41](#), [90](#)  
 ITSP [40](#), [90](#)  
 ITU-T [112](#)

## J

JAVA [335](#)  
 Java [155](#)  
 Java Permissions [44](#), [329](#), [334](#)  
 JavaScripts [44](#), [329](#), [332](#)  
 Jitter Buffer [36](#)

## K

Keep Alive Interval [108](#)

## L

Labor [6](#)  
 LAN Interface Problems [326](#)  
 LAN IP Address, Default [44](#)  
 LAN Setup [72](#), [82](#)  
 LAN TCP/IP [73](#)  
 LEDs [39](#)  
 Legal Rights [6](#)  
 Liability [2](#)  
 License [2](#)  
 Lifeline [34](#), [120](#), [339](#)  
 Lifeline Screen [125](#)  
 Lightning [5](#)  
 Limitations, WAN Management [307](#)  
 Line Ports [338](#)

Liquids, Corrosive [5](#)  
 Listening Port [57](#), [59](#), [103](#), [108](#)  
 Listening Port, Register Server's [58](#), [104](#)  
 Listening Port, SIP Server's [57](#), [104](#)  
 Listening Volume [113](#)  
 Local [128](#)  
 Local End IP [136](#), [138](#)  
 Local Start IP [136](#), [137](#)  
 Log Facility [297](#)  
 Log Out [45](#)  
 Logging [39](#)  
 Login [44](#)  
 Login Name [243](#)  
 Logs [184](#)  
 Loop Start Signaling [339](#)

## M

MAC Address [234](#)  
 Maintenance [212](#)  
 Management [339](#)  
 Management Information Base (MIB) [163](#)  
 Management IP Address, Default [338](#)  
 Management Limitations [307](#)  
 Management Restrictions [321](#)  
 Management Session Idle [45](#)  
 Management Subnet Mask, Default [338](#)  
 Many to Many No Overload [130](#), [137](#)  
 Many to Many Overload [130](#), [137](#)  
 Many-to-One [130](#), [137](#)  
 Mapping  
   NAT, Many One-to-One [130](#), [137](#)  
   NAT, Many-to-Many Overload [130](#), [137](#)  
   NAT, Many-to-One [130](#), [137](#)  
   NAT, One-to-One [130](#), [137](#)  
   NAT, Server [130](#), [137](#)  
 Mapping, Call to Port [113](#)  
 Mapping, Phone Ports [104](#)  
 Materials [6](#)  
 Maximize Bandwidth Usage [200](#), [204](#)  
 Merchantability [6](#)  
 Message Logging [296](#)  
 Message Waiting Indication [101](#), [108](#)  
 Metric [144](#), [251](#), [257](#)  
 Min-SE [107](#)  
 Model [213](#)  
 Model Name [213](#)  
 Modem [33](#), [339](#)  
 Modifications [3](#)

Mouse Action Sequences [32](#)  
Multicast [38, 75, 238, 252](#)  
Multicast Groups [38](#)  
Multimedia [90](#)  
Multiple SIP Accounts [36](#)  
Multiple Telephones [36](#)  
Multiple Voice Channels [36](#)  
MWI [101, 108](#)  
My Login [247](#)  
My Login Name [243](#)  
My Password [243, 247](#)

## N

Nailed-Up Connection [250](#)  
Nailed-up Connection [249](#)  
NAT [38, 72, 94, 128, 131, 132, 251, 288](#)  
  Address Mapping [135](#)  
  and Remote Management [159](#)  
  Application [130](#)  
  Applying NAT in the SMT Menus [258](#)  
  Configuring [259](#)  
  Definitions [128](#)  
  Examples [265](#)  
  Full Cone [96](#)  
  Global End IP [136, 138](#)  
  Global Start IP [136, 138](#)  
  How NAT Works [129](#)  
  Local End IP [136, 138](#)  
  Local Start IP [136, 137](#)  
  Mapping Types [130](#)  
  Non NAT Friendly Application Programs [270](#)  
  Ordering Rules [262](#)  
  Server Sets [132](#)  
  Symmetric [98](#)  
  What NAT does [129](#)  
NAT Keep Alive [108](#)  
NAT Mapping [130, 137](#)  
  Many One-to-One [130, 137](#)  
  Many-to-Many Overload [130, 137](#)  
  Many-to-One [130, 137](#)  
  One-to-One [130, 137](#)  
  Server [130, 137](#)  
NAT Mapping Type [136](#)  
NAT Routers [100](#)  
NAT Traversal [170, 339](#)  
NAT Types [95](#)  
NAT With IP Alias [130](#)  
NAT, Global [128](#)  
NAT, Incoming [95](#)  
NAT, Inside [128](#)  
NAT, Local [128](#)

NAT, Outgoing [94](#)  
NAT, Outside [128](#)  
Navigating Web Configurator [46](#)  
Netscape Navigator [44](#)  
Network Address Translation [94, 128](#)  
Network Address Translation (NAT) [38, 258](#)  
Network Address Translators [100](#)  
Network Management [133](#)  
Network News Transport Protocol [133](#)  
Network Temporarily Disconnected [219, 221](#)  
Networking Terms, Glossary of [32](#)  
New [6](#)  
NNTP [133](#)  
No Answer [124](#)  
No Answer Forward to Number [124](#)  
No Answer Waiting Time [124](#)  
Non-Proxy [121](#)  
North America [5](#)  
North America Contact Information [7](#)  
Norway, Contact Information [7](#)  
Notebook Computer [33](#)  
NTP (RFC-1305) [319](#)  
NTP RFC 1305 [69](#)  
NTP Time Servers [68](#)

## O

OK Response [91](#)  
One-to-One [130, 137](#)  
Online Help [32](#)  
Opening [5](#)  
Operating Condition [6](#)  
Operation Humidity [338](#)  
Operation Temperature [338](#)  
Outbound Proxy [36, 99, 100, 108](#)  
Outbound Proxy Server [100](#)  
Outbound Proxy, SIP [100](#)  
Out-dated Warranty [6](#)  
Outgoing Call use [113](#)  
Outlet [3](#)  
Outside [128](#)

## P

Parts [6](#)  
Password [44, 67, 224, 228, 243, 290, 338](#)

Change [45](#)  
Password Problems [327](#)  
Password, Authentication [58](#), [104](#)  
Password, Default [36](#)  
Patent [2](#)  
PBX Services [90](#)  
PCM [101](#), [339](#)  
PCM G.711 [37](#)  
Peer to Peer Calls [42](#)  
Peer-to-Peer Calls [120](#)  
Peer-to-peer Calls [42](#)  
Per-Hop Behavior [110](#)  
Period(hr) [250](#)  
Permission [2](#)  
PHB (Per-Hop Behavior) [110](#)  
PHONE 1 and 2 Ports [104](#), [118](#)  
Phone Book [120](#)  
Phone Port Call Mapping [113](#)  
Phone Port Mapping [104](#)  
Phone Port Screen [113](#), [118](#)  
Phone Port Settings [59](#), [113](#), [118](#), [124](#)  
Phone Ports [338](#)  
Phone Settings [112](#)  
Photocopying [2](#)  
Ping [169](#), [301](#)  
Pipes [5](#)  
Point to Point Calling [339](#)  
Point to Point Calls [42](#)  
Point-to-Point Protocol over Ethernet [39](#)  
Point-to-Point Tunneling Protocol [133](#)  
Polarity Reversal [339](#)  
Pool [5](#)  
POP3 [133](#)  
Pop-up Blockers [329](#)  
Pop-up Blocking [44](#)  
Pop-up Windows [329](#)  
Port [94](#)  
Port Forwarding [38](#), [132](#)  
Port Forwarding, Port Numbers [132](#)  
Port Forwarding, Services [132](#)  
Port Numbers [132](#)  
Port Restricted Cone NAT [97](#)  
Post Office Protocol [133](#)  
Postage Prepaid. [6](#)  
Power Adaptor [5](#)  
Power Cord [5](#)  
Power Outlet [5](#)  
Power Supply [5](#)  
Power Supply, repair [5](#)  
PPPoE [39](#), [52](#), [364](#)

PPPoE Encapsulation [244](#), [246](#), [249](#), [250](#)  
PPTP [133](#)  
Pre-defined NTP Time Servers List [68](#)  
Preferred Codec [58](#), [107](#)  
Prestige [33](#)  
Prestige 2302R [33](#)  
Priority-based Scheduler [200](#)  
Private [144](#), [252](#), [257](#)  
Private IP Addresses [94](#)  
Probing [169](#)  
Problems [326](#)  
Product Model [7](#)  
Product Page [3](#)  
Product Serial Number [7](#)  
Products [6](#)  
Proof of Purchase [6](#)  
Proper Operating Condition [6](#)  
Proportional Bandwidth Allocation [199](#)  
Protocol Support [339](#)  
Proxy Server, SIP [92](#)  
PSTN [34](#), [101](#)  
PSTN Lifeline [36](#)  
PSTN Pre-fix Number [125](#)  
Public IP Addresses [94](#)  
Public Switched Telephone Network [34](#), [101](#)  
Pulse Code Modulation [101](#)  
Pulse Dialing [101](#)  
Purchase, Proof of [6](#)  
Purchaser [6](#)

## Q

QoS [37](#), [109](#), [111](#), [339](#)  
Qualified Service Personnel [5](#)  
Quality of Service [37](#), [109](#)  
Quality of Service (QOS) [37](#)  
Questions [32](#)  
Quick Start Guide [32](#)

## R

Radio Communications [3](#)  
Radio Frequency Energy [3](#)  
Radio Interference [3](#)  
Radio Reception [3](#)  
Radio Technician [3](#)

RAS [295](#)  
Real Time [317](#)  
Real time Transport Protocol [93](#), [107](#)  
Receiving Antenna [3](#)  
Redirect Server, SIP [93](#)  
Register [214](#)  
Register Resend Timer [107](#)  
REGISTER Server Address [58](#), [104](#)  
REGISTER Server Port [58](#), [104](#)  
Register Server, SIP [93](#)  
Registered [2](#)  
Registered Trademark [2](#)  
Regular Mail [7](#)  
Related Documentation [32](#)  
Relay to PSTN [125](#)  
Relocate [3](#)  
Rem Node Name [247](#)  
Re-manufactured [6](#)  
Remote Management [158](#), [339](#)  
    Firewall [274](#)  
Remote Management and NAT [159](#)  
Remote Management Limitations [158](#)  
Remote Node Filter [252](#)  
Removing [5](#)  
REN [36](#)  
Reorient [3](#)  
Repair [5](#), [6](#)  
Replace [6](#)  
Replacement [6](#)  
Reproduction [2](#)  
Required Bandwidth [101](#)  
Required fields [225](#)  
RESET Button [45](#)  
Reset Button [36](#)  
Reset button [222](#)  
Reset Warning Message [222](#)  
Resetting the Time [70](#)  
Resetting to Factory Defaults [45](#)  
Restart Screen [223](#)  
Restore [6](#)  
Restore Configuration [221](#), [309](#)  
Restrict Web Features [155](#)  
Restricted Cone NAT [96](#)  
Return Material Authorization (RMA) Number [6](#)  
Returned Products [6](#)  
Returns [6](#)  
RFC 1213 [164](#)  
RFC 1215 [164](#)  
RFC 1305 [69](#), [319](#)  
RFC 1631 [128](#)

RFC 1889 [93](#), [339](#)  
RFC 1890 [339](#)  
RFC 2327 [339](#)  
RFC 2516 [339](#)  
RFC 3261 [339](#)  
RFC 3489 [100](#), [339](#)  
RFC 3842 [101](#)  
RFC 867 [69](#), [319](#)  
RFC 868 [69](#)  
RFC-868 [319](#)  
Rights [2](#)  
Rights, Legal [6](#)  
Ringer Equivalence Number [36](#)  
Ringing Voltage [338](#)  
RIP [252](#)  
    Version [252](#)  
RIPSee Routing Information Protocol [74](#)  
Risk [5](#)  
Risks [5](#)  
RMA [6](#)  
RoadRunner [39](#)  
Root Class [205](#)  
Route [248](#)  
Router [33](#)  
Routing Information Protocol [74](#)  
    Direction [74](#)  
    Version [74](#)  
RTCP (RFC 1890) [339](#)  
RTP [93](#)  
RTP (RFC 1889) [339](#)  
RTP Port Range [107](#)  
RTP TOS Priority [111](#)

## S

Safety Warnings [5](#)  
Schedule Sets  
    Duration [323](#)  
Schedule Setup [322](#)  
Scheduler [200](#), [204](#)  
Schedules [250](#)  
SDP (RFC 2327) [339](#)  
Secured Client IP Address [160](#), [161](#), [162](#), [167](#), [168](#)  
Security [169](#)  
Separation Between Equipment and Receiver [3](#)  
Serial Number [7](#)  
Server [33](#), [69](#), [130](#), [131](#), [137](#), [243](#), [247](#), [259](#), [261](#), [263](#),  
    [264](#), [266](#), [267](#)  
Server Access [160](#), [161](#), [162](#), [167](#)



- Server IP [247](#)
- Server Port [160](#), [161](#), [162](#), [167](#)
- Server, Outbound Proxy [100](#)
- Service [5](#), [6](#)
- Service Access [166](#)
- Service Name [250](#)
- Service Pack 2 [329](#)
- Service Personnel [5](#)
- Service Port [166](#)
- Service Request Forwarding, See Port Forwarding [38](#)
- Service Type [243](#), [247](#)
- Services [132](#), [150](#)
- Session Expires [107](#)
- Session Initiation Protocol [34](#), [90](#)
- Set [163](#)
- Set Community [166](#)
- Shipping [6](#)
- Shock, Electric [5](#)
- Silence Suppression [37](#), [112](#), [339](#)
- Silent Packets [112](#)
- Simple Mail Transfer Protocol [132](#)
- Simple Network Management Protocol [39](#), [133](#), [162](#)
- Single User Account [131](#)
- SIP [34](#), [90](#)
- SIP (RFC 3261) version 2 [339](#)
- SIP Account [90](#), [103](#)
- SIP Accounts [36](#)
- SIP ACK Message [91](#)
- SIP ALG [35](#), [99](#)
- SIP Application Layer Gateway [35](#), [99](#)
- SIP BYE Request [91](#)
- SIP Call Progression [91](#)
- SIP Client [91](#)
- SIP Client Server [91](#)
- SIP Identities [90](#)
- SIP INVITE Request [91](#)
- SIP Local Port [57](#), [103](#)
- SIP Number [57](#), [90](#), [103](#), [121](#)
- SIP OK Response [91](#)
- SIP Outbound Proxy [100](#)
- SIP Proxy Server [92](#)
- SIP Redirect Server [93](#)
- SIP Register Server [93](#)
- SIP Registration Status [214](#)
- SIP Server Address [57](#), [103](#)
- SIP Server Port [57](#), [104](#)
- SIP Server Settings [107](#)
- SIP Servers [91](#)
- SIP Service Domain [58](#), [91](#), [104](#)
- SIP URI [90](#), [121](#), [124](#)
- SIP User Agent [92](#)
- SIP, Advanced Settings [104](#)
- SIP, Authentication Password [58](#), [104](#)
- SIP, Authentication User ID [58](#), [104](#)
- SIP, Incoming Call Mapping [104](#)
- SIP, Outgoing Call Mapping [113](#)
- SMT Menu Overview [227](#)
- SMTP [132](#)
- SNMP [39](#), [133](#), [147](#), [162](#), [339](#)
  - Community [290](#)
  - Configuration [166](#), [290](#)
  - Manager [163](#)
  - MIBs [164](#)
  - Service Port [166](#)
  - Trusted Host [290](#)
- SNMPv1 [39](#), [162](#)
- SNMPv2 [39](#), [162](#)
- Sound Quality [101](#)
- Spain, Contact Information [8](#)
- Speaking Volume [113](#)
- Speed Dial [120](#), [121](#), [126](#)
- Speed Dial Phonebook [339](#)
- Speed Dial Screen [120](#)
- Start Up Problems [326](#)
- Stateful Inspection [146](#)
- Static Route [142](#)
- Static Routes [340](#)
- Status Screen [212](#)
- Storage Humidity [338](#)
- Storage Temperature [338](#)
- Straight-through Ethernet Cable [35](#)
- STUN [36](#), [99](#), [100](#), [107](#), [339](#)
- SUA [132](#), [133](#)
- SUA (Single User Account) [131](#)
- SUA Server Set [131](#)
- Sub-class Layers [205](#)
- Subnet Mask [72](#), [238](#), [243](#), [251](#), [257](#), [295](#)
- Subnet Masks [357](#)
- Subnetting [357](#)
- Suggestions [32](#)
- Sun [335](#)
- Supplementary Phone Services [114](#)
- Supplementary Services [114](#)
- Supply Voltage [5](#)
- Support E-mail [7](#)
- Supporting Disk [32](#)
- Sweden, Contact Information [8](#)
- Swimming Pool [5](#)
- Switch [33](#)
- Symmetric NAT [98](#)
- Symmetric NAT, Outgoing [99](#)

Syntax Conventions [32](#)  
Syslog [39](#), [296](#), [297](#), [339](#)  
Syslog IP Address [297](#)  
Syslog Server [296](#)  
System  
  Console Port Speed [295](#)  
  Diagnostic [300](#)  
  Log and Trace [296](#)  
  Syslog and Accounting [296](#)  
  System Information [294](#)  
System Information [294](#)  
System Information & Diagnosis [292](#)  
System Maintenance [292](#), [294](#), [296](#), [301](#), [305](#), [308](#), [312](#),  
  [314](#), [315](#), [316](#), [318](#)  
System Name [62](#), [64](#), [213](#), [230](#)  
System Timeout [159](#)

## T

Table Number [124](#)  
Tampering [6](#)  
TCP/IP [281](#), [282](#), [283](#), [285](#), [288](#)  
TCP/IP filter rule [281](#)  
Telecommunication Line Cord. [5](#)  
Telephone [7](#), [33](#)  
Telephone Keys [101](#)  
Telephone Port Problems [328](#)  
Telephone Problems [328](#)  
Television Interference [3](#)  
Television Reception [3](#)  
Telnet [159](#), [339](#)  
TFTP [339](#)  
TFTP and FTP over WAN Management Limitations [307](#)  
TFTP File Transfer [312](#)  
TFTP Restrictions [158](#)  
TFTP Server [39](#)  
Three-Way Conference [116](#), [117](#)  
Thunderstorm [5](#)  
Time [68](#)  
  Daylight Saving [319](#)  
  Resetting [70](#)  
  Zone [319](#)  
Time (RFC-868) [319](#)  
Time and Date Setting [317](#), [318](#), [319](#)  
Time Protocol [69](#), [319](#)  
Time RFC 868 [69](#)  
Time Server [69](#)  
Time Server Address [319](#)  
Time Zone [68](#), [70](#), [319](#)

Timeout [244](#), [250](#)  
Tip/ring Polarity Reversal [339](#)  
TOS [111](#), [339](#)  
ToS [37](#), [110](#)  
Touch Tone® [101](#)  
Trace Records [296](#)  
Tracing [39](#)  
Trademark [2](#)  
Trademark Owners [2](#)  
Trademarks [2](#)  
Translation [2](#)  
Trap [163](#), [166](#)  
Trap Community [166](#)  
Trap Destination [166](#)  
Trigger Port [140](#)  
Trigger Port Forwarding [138](#), [271](#)  
  Process [138](#)  
Troubleshooting [326](#)  
Trusted Computer [160](#), [161](#), [162](#), [167](#), [168](#)  
TV Technician [3](#)  
Type Of Service [110](#)  
Type of Service [37](#), [111](#)

## U

UIC [171](#)  
Unauthorized Services [169](#)  
Unconditional [124](#)  
Undesired Operations [3](#)  
Uniform Resource Identifier [90](#)  
Universal Plug and Play [170](#)  
  Application [170](#)  
  Security issues [170](#)  
Universal Plug and Play (UPnP) [38](#)  
Universal Plug and Play Forum [171](#)  
Unregister [214](#)  
Unused Ports [169](#)  
Upload Firmware [310](#)  
UPnP [170](#), [172](#)  
  Auto-discovery [176](#)  
  Installing Example [172](#)  
UPnP Certification [171](#)  
URL Keyword Blocking [156](#)  
URL Type [107](#)  
USA Type [118](#)  
USA Type Call Service Mode [116](#)  
Use NAT [99](#), [108](#)  
Use Proxy [121](#)  
Used Port [214](#)

User Agent, SIP [92](#)  
User Guide Feedback [32](#)  
User ID, Authentication [58](#), [104](#)  
User Name [66](#), [232](#)  
User Specified IP Addr [233](#)  
Using Speed Dial [126](#)

## V

VAD [37](#), [112](#), [113](#), [339](#)  
Vendor [5](#)  
Ventilation Slots [5](#)  
VID [111](#)  
Viewing Certifications [3](#)  
Virtual Local Area Network [110](#)  
VLAN [110](#)  
VLAN Group [110](#)  
VLAN ID [110](#)  
VLAN ID Tags [110](#)  
VLAN Tag [110](#), [111](#)  
Voice Account [102](#)  
Voice Activity Detection [37](#), [112](#), [113](#), [339](#)  
Voice Channels [36](#)  
Voice Coding [37](#), [100](#)  
Voice Functions [339](#)  
Voice Mail [90](#)  
Voice over IP [34](#), [90](#)  
Voice Priority [111](#)  
Voice VLAN ID [111](#)  
VoIP [34](#), [90](#)  
VoIP Advanced Screen [106](#)  
VoIP Screen [102](#)  
VoIP Status [214](#)  
Voltage [338](#)  
Voltage Supply [5](#)  
Voltage, High [5](#)

## W

Wall Mount [5](#)  
WAN DHCP [301](#), [302](#)  
WAN Interface Problems [327](#)  
WAN Management Limitations [307](#)  
WAN Setup [234](#)  
Warnings [5](#)  
Warranty [6](#)

Warranty Information [7](#)  
Warranty Period [6](#)  
Water [5](#)  
Water Pipes [5](#)  
Waveform Codec [101](#)  
Web [161](#)  
Web Configurator [44](#), [46](#), [275](#)  
Web Configurator Online Help [32](#)  
Web Configurator Problems [328](#)  
Web Proxy [155](#)  
Web Site [7](#)  
Weight [338](#)  
Wet Basement [5](#)  
Wide [338](#)  
Windows XP [329](#)  
Workmanship [6](#)  
Worldwide Contact Information [7](#)  
Written Permission [2](#)  
WWW [133](#), [161](#)  
[www.dyndns.org](#) [232](#)

## Z

Zone, Time [319](#)  
ZyNOS [2](#), [294](#), [305](#)  
ZyNOS F/W Version [294](#), [305](#)  
ZyNOS Firmware Version [213](#)  
ZyXEL Communications Corporation [2](#)  
ZyXEL Home Page [3](#)  
ZyXEL Limited Warranty  
Note [6](#)  
ZyXEL Network Operating System [2](#)

