

# *Prestige 2602HW Series*

*ADSL VoIP IAD with 802.11g Wireless*

## **User's Guide**

Version 3.40

1/2005





# 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.

## Certifications

Go to [www.zyxel.com](http://www.zyxel.com)

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



# Safety Warnings

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

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

# ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

## Note

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

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

# Customer Support

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

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

METHOD	SUPPORT E-MAIL	TELEPHONE <sup>A</sup>	WEB SITE	REGULAR MAIL
LOCATION	SALES E-MAIL	FAX	FTP SITE	
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	
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	
GERMANY	<a href="mailto:support@zyxel.de">support@zyxel.de</a>	+49-2405-6909-0	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
	sales@zyxel.de	+49-2405-6909-99		
FRANCE	<a href="mailto:info@zyxel.fr">info@zyxel.fr</a>	+33 (0)4 72 52 97 97	<a href="http://www.zyxel.fr">www.zyxel.fr</a>	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
		+33 (0)4 72 52 19 20		
SPAIN	support@zyxel.es	+34 902 195 420	<a href="http://www.zyxel.es">www.zyxel.es</a>	ZyXEL Communications Alejandro Villegas 33 1º, 28043 Madrid Spain
	<a href="mailto:sales@zyxel.es">sales@zyxel.es</a>	+34 913 005 345		
DENMARK	<a href="mailto:support@zyxel.dk">support@zyxel.dk</a>	+45 39 55 07 00	<a href="http://www.zyxel.dk">www.zyxel.dk</a>	ZyXEL Communications A/S Columbusvej 5 2860 Soeborg Denmark
	<a href="mailto:sales@zyxel.dk">sales@zyxel.dk</a>	+45 39 55 07 07		
NORWAY	<a href="mailto:support@zyxel.no">support@zyxel.no</a>	+47 22 80 61 80	<a href="http://www.zyxel.no">www.zyxel.no</a>	ZyXEL Communications A/S Nils Hansens vei 13 0667 Oslo Norway
	<a href="mailto:sales@zyxel.no">sales@zyxel.no</a>	+47 22 80 61 81		
SWEDEN	<a href="mailto:support@zyxel.se">support@zyxel.se</a>	+46 31 744 7700	<a href="http://www.zyxel.se">www.zyxel.se</a>	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden
	<a href="mailto:sales@zyxel.se">sales@zyxel.se</a>	+46 31 744 7701		
FINLAND	support@zyxel.fi	+358-9-4780-8411	<a href="http://www.zyxel.fi">www.zyxel.fi</a>	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland
	sales@zyxel.fi	+358-9-4780 8448		

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



# Table of Contents

<b>Copyright</b> .....	<b>3</b>
<b>Federal Communications Commission (FCC) Interference Statement</b> .....	<b>4</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>9</b>
<b>List of Figures</b> .....	<b>27</b>
<b>List of Tables</b> .....	<b>35</b>
<b>Preface</b> .....	<b>41</b>
<b>Introduction to DSL</b> .....	<b>43</b>
<b>Chapter 1</b>	
<b>Getting To Know Your Prestige</b> .....	<b>45</b>
1.1 Introducing the Prestige .....	45
1.2 Prestige 2602HW-L with Lifeline .....	46
1.3 Features of the Prestige .....	46
1.4 Applications for the Prestige .....	53
1.4.1 Internet Access .....	53
1.4.2 Making Calls via Internet Telephony Service Provider .....	54
1.4.3 Firewall for Secure Broadband Internet Access .....	55
1.4.4 LAN to LAN Application .....	55
1.5 Prestige Hardware Installation and Connection .....	56
<b>Chapter 2</b>	
<b>Introducing the Web Configurator</b> .....	<b>57</b>
2.1 Web Configurator Overview .....	57
2.1.1 Accessing the Prestige Web Configurator .....	57
2.1.2 Resetting the Prestige .....	58
2.1.2.1 Using The Reset Button .....	58
2.1.3 Navigating the Prestige Web Configurator .....	58

<b>Chapter 3</b>	
<b>Wizard Setup .....</b>	<b>63</b>
3.1 Wizard Setup Introduction .....	63
3.1.1 Encapsulation .....	63
3.1.1.1 ENET ENCAP .....	63
3.1.1.2 PPP over Ethernet .....	63
3.1.1.3 PPPoA .....	63
3.1.1.4 RFC 1483 .....	64
3.1.2 Multiplexing .....	64
3.1.2.1 VC-based Multiplexing .....	64
3.1.2.2 LLC-based Multiplexing .....	64
3.1.3 VPI and VCI .....	64
3.1.4 Internet Access Wizard Setup: First Screen .....	64
3.2 IP Address and Subnet Mask .....	65
3.2.1 IP Address Assignment .....	66
3.2.1.1 IP Assignment with PPPoA or PPPoE Encapsulation .....	66
3.2.1.2 IP Assignment with RFC 1483 Encapsulation .....	66
3.2.1.3 IP Assignment with ENET ENCAP Encapsulation .....	66
3.2.1.4 Private IP Addresses .....	67
3.2.2 Nailed-Up Connection (PPP) .....	67
3.2.3 NAT .....	67
3.2.4 Internet Access Wizard Setup: Second Screen .....	67
3.2.5 SIP Identities .....	71
3.2.5.1 SIP Number .....	71
3.2.5.2 SIP Service Domain .....	71
3.2.6 Internet Access Wizard Setup: Third Screen .....	71
3.2.7 DHCP Setup .....	73
3.2.7.1 IP Pool Setup .....	73
3.2.8 Internet Access Wizard Setup: Fourth Screen .....	73
3.2.9 Internet Access Wizard Setup: Connection Test .....	75
3.2.9.1 Test Your Internet Connection .....	76
<b>Chapter 4</b>	
<b>Password Setup .....</b>	<b>77</b>
4.1 Password Overview .....	77
4.1.1 Configuring Password .....	77
<b>Chapter 5</b>	
<b>LAN Setup .....</b>	<b>79</b>
5.1 LAN Overview .....	79
5.1.1 LANs, WANs and the Prestige .....	79
5.2 DNS Server Address .....	80
5.3 DNS Server Address Assignment .....	80

5.4 LAN TCP/IP .....	81
5.4.1 Factory LAN Defaults .....	81
5.4.2 IP Address and Subnet Mask .....	81
5.4.3 RIP Setup .....	81
5.4.4 Multicast .....	82
5.5 Any IP .....	82
5.5.1 How Any IP Works .....	83
5.6 Configuring LAN .....	84
5.7 Configuring Static DHCP .....	85

## **Chapter 6**

### **Wireless LAN Setup ..... 87**

6.1 Wireless LAN Introduction .....	87
6.1.1 Additional Installation Requirements for Using IEEE 802.1x .....	87
6.1.2 Channel .....	87
6.1.3 ESS ID .....	87
6.1.4 RTS/CTS .....	88
6.1.5 Fragmentation Threshold .....	89
6.2 Levels of Security .....	89
6.3 Data Encryption with WEP .....	90
6.4 Configuring Wireless LAN .....	90
6.5 Configuring MAC Filter .....	92
6.6 Network Authentication .....	94
6.6.1 EAP .....	94
6.6.1.1 RADIUS .....	94
6.6.1.2 Types of RADIUS Messages .....	94
6.6.2 EAP Authentication Overview .....	95
6.7 Introduction to WPA .....	96
6.7.1 User Authentication .....	96
6.7.2 Encryption .....	96
6.8 WPA-PSK Application Example .....	97
6.9 WPA with RADIUS Application Example .....	97
6.10 Security Parameters Summary .....	98
6.11 Wireless Client WPA Supplicants .....	99
6.12 Configuring 802.1x and WPA .....	99
6.12.1 Authentication Required: 802.1x .....	100
6.12.2 Authentication Required: WPA .....	102
6.12.3 Authentication Required: WPA-PSK .....	103
6.13 Configuring Local User Authentication .....	105
6.14 Configuring RADIUS .....	106

<b>Chapter 7</b>	
<b>WAN Setup</b>	<b>109</b>
7.1 WAN Overview	109
7.2 Metric	109
7.3 PPPoE Encapsulation	110
7.4 Traffic Shaping	110
7.5 Zero Configuration Internet Access	111
7.6 Configuring WAN Setup	111
7.7 Traffic Redirect	114
7.8 Configuring WAN Backup	115
<b>Chapter 8</b>	
<b>Network Address Translation (NAT) Screens</b>	<b>119</b>
8.1 NAT Overview	119
8.1.1 NAT Definitions	119
8.1.2 What NAT Does	120
8.1.3 How NAT Works	120
8.1.4 NAT Application	121
8.1.5 NAT Mapping Types	121
8.2 SUA (Single User Account) Versus NAT	122
8.3 SUA Server	123
8.3.1 Default Server IP Address	123
8.3.2 Port Forwarding: Services and Port Numbers	123
8.3.3 Configuring Servers Behind SUA (Example)	124
8.4 Selecting the NAT Mode	124
8.5 Configuring SUA Server	125
8.6 Configuring Address Mapping	127
8.7 Editing an Address Mapping Rule	128
<b>Chapter 9</b>	
<b>Introduction to VoIP</b>	<b>131</b>
9.1 Introduction to VoIP	131
9.2 SIP	131
9.2.1 SIP Identities	131
9.2.1.1 SIP Number	131
9.2.1.2 SIP Service Domain	132
9.2.2 SIP Call Progression	132
9.2.3 SIP Servers	132
9.2.3.1 SIP User Agent Server	133
9.2.3.2 SIP Proxy Server	133
9.2.3.3 SIP Redirect Server	134
9.2.3.4 SIP Register Server	135
9.2.4 RTP	135



9.3 SIP ALG .....	135
9.4 Pulse Code Modulation .....	135
9.5 Voice Coding .....	136
9.5.1 G.711 .....	136
9.5.2 G.729 .....	136
9.6 PSTN Call Setup Signaling .....	136
<b>Chapter 10</b>	
<b>Voice Screens .....</b>	<b>137</b>
10.1 Voice Screens Introduction .....	137
10.2 SIP Settings Configuration .....	137
10.3 Advanced Voice Settings Configuration .....	138
10.4 Quality of Service (QoS) .....	140
10.4.1 Type Of Service (ToS) .....	140
10.4.2 DiffServ .....	141
10.4.2.1 DSCP and Per-Hop Behavior .....	141
10.4.3 VLAN .....	141
10.5 QoS Configuration .....	141
10.6 Phone .....	142
10.6.1 Voice Activity Detection/Silence Suppression .....	143
10.6.2 Comfort Noise Generation .....	143
10.6.3 Echo Cancellation .....	143
10.7 Phone Configuration .....	143
10.8 Speed Dial .....	144
10.8.1 Peer-to-Peer Calls .....	144
10.9 Speed Dial Configuration .....	145
10.10 Lifeline (Prestige 2602HW-L) .....	146
10.11 Lifeline Configuration (Prestige 2602HW-L) .....	146
10.12 Common Phone Port Configuration .....	147
<b>Chapter 11</b>	
<b>Dynamic DNS Setup.....</b>	<b>149</b>
11.1 Dynamic DNS .....	149
11.1.1 DYNDNS Wildcard .....	149
11.2 Configuring Dynamic DNS .....	149
<b>Chapter 12</b>	
<b>Time and Date.....</b>	<b>151</b>
12.1 Pre-defined NTP Time Servers List .....	151
12.2 Configuring Time and Date .....	151

<b>Chapter 13</b>	
<b>Firewalls</b>	<b>155</b>
13.1 Firewall Overview	155
13.2 Types of Firewalls	155
13.2.1 Packet Filtering Firewalls	155
13.2.2 Application-level Firewalls	155
13.2.3 Stateful Inspection Firewalls	156
13.3 Introduction to ZyXEL's Firewall	156
13.3.1 Denial of Service Attacks	157
13.4 Denial of Service	157
13.4.1 Basics	157
13.4.2 Types of DoS Attacks	158
13.4.2.1 ICMP Vulnerability	160
13.4.2.2 Illegal Commands (NetBIOS and SMTP)	160
13.4.2.3 Traceroute	161
13.5 Stateful Inspection	161
13.5.1 Stateful Inspection Process	162
13.5.2 Stateful Inspection and the Prestige	163
13.5.3 TCP Security	163
13.5.4 UDP/ICMP Security	164
13.5.5 Upper Layer Protocols	164
13.6 Guidelines for Enhancing Security with Your Firewall	164
13.6.1 Security In General	165
13.7 Packet Filtering Vs Firewall	166
13.7.1 Packet Filtering:	166
13.7.1.1 When To Use Filtering	166
13.7.2 Firewall	166
13.7.2.1 When To Use The Firewall	166
<b>Chapter 14</b>	
<b>Firewall Configuration</b>	<b>169</b>
14.1 Access Methods	169
14.2 Firewall Policies Overview	169
14.3 Rule Logic Overview	170
14.3.1 Rule Checklist	170
14.3.2 Security Ramifications	170
14.3.3 Key Fields For Configuring Rules	171
14.3.3.1 Action	171
14.3.3.2 Service	171
14.3.3.3 Source Address	171
14.3.3.4 Destination Address	171
14.4 Connection Direction Example	171
14.4.1 LAN to WAN Rules	172

14.4.2 WAN to LAN Rules .....	172
14.4.3 Alerts .....	173
14.5 Configuring Basic Firewall Settings .....	173
14.6 Rule Summary .....	174
14.6.1 Configuring Firewall Rules .....	176
14.7 Customized Services .....	179
14.8 Creating/Editing A Customized Service .....	179
14.9 Example Firewall Rule .....	180
14.10 Predefined Services .....	184
14.11 Anti-Probing .....	186
14.12 DOS Thresholds .....	187
14.12.1 Threshold Values .....	188
14.12.2 Half-Open Sessions .....	188
14.12.2.1 TCP Maximum Incomplete and Blocking Time .....	188
<b>Chapter 15</b>	
<b>Content Filtering .....</b>	<b>191</b>
15.1 Content Filtering Overview .....	191
15.2 Configuring Keyword Blocking .....	191
15.3 Configuring the Schedule .....	192
15.4 Configuring Trusted Computers .....	193
<b>Chapter 16</b>	
<b>Introduction to IPSec .....</b>	<b>195</b>
16.1 VPN Overview .....	195
16.1.1 IPSec .....	195
16.1.2 Security Association .....	195
16.1.3 Other Terminology .....	195
16.1.3.1 Encryption .....	195
16.1.3.2 Data Confidentiality .....	196
16.1.3.3 Data Integrity .....	196
16.1.3.4 Data Origin Authentication .....	196
16.1.4 VPN Applications .....	196
16.2 IPSec Architecture .....	197
16.2.1 IPSec Algorithms .....	197
16.2.2 Key Management .....	197
16.3 Encapsulation .....	197
16.3.1 Transport Mode .....	198
16.3.2 Tunnel Mode .....	198
16.4 IPSec and NAT .....	198

<b>Chapter 17</b>	
<b>VPN Screens</b>	<b>201</b>
17.1 VPN/IPSec Overview	201
17.2 IPSec Algorithms	201
17.2.1 AH (Authentication Header) Protocol	201
17.2.2 ESP (Encapsulating Security Payload) Protocol	202
17.3 My IP Address	202
17.4 Secure Gateway Address	203
17.4.1 Dynamic Secure Gateway Address	203
17.5 VPN Summary Screen	203
17.6 Keep Alive	205
17.7 Remote DNS Server	205
17.8 NAT Traversal	206
17.8.1 NAT Traversal Configuration	207
17.9 ID Type and Content	207
17.9.1 ID Type and Content Examples	208
17.10 Pre-Shared Key	209
17.11 Editing VPN Policies	209
17.12 IKE Phases	214
17.12.1 Negotiation Mode	216
17.12.2 Diffie-Hellman (DH) Key Groups	216
17.12.3 Perfect Forward Secrecy (PFS)	216
17.13 Configuring Advanced IKE Settings	216
17.14 Manual Key Setup	219
17.14.1 Security Parameter Index (SPI)	219
17.15 Configuring Manual Key	220
17.16 Viewing SA Monitor	223
17.17 Configuring Global Setting	225
17.18 Telecommuter VPN/IPSec Examples	225
17.18.1 Telecommuters Sharing One VPN Rule Example	225
17.18.2 Telecommuters Using Unique VPN Rules Example	226
17.19 VPN and Remote Management	228
<b>Chapter 18</b>	
<b>Remote Management Configuration</b>	<b>229</b>
18.1 Remote Management Overview	229
18.1.1 Remote Management Limitations	229
18.1.2 Remote Management and NAT	230
18.1.3 System Timeout	230
18.2 Telnet	230
18.3 FTP	230
18.4 Web	231
18.5 Configuring Remote Management	231

<b>Chapter 19</b>	
<b>Universal Plug-and-Play (UPnP) .....</b>	<b>233</b>
19.1 Introducing Universal Plug and Play .....	233
19.1.1 How do I know if I'm using UPnP? .....	233
19.1.2 NAT Traversal .....	233
19.1.3 Cautions with UPnP .....	233
19.2 UPnP and ZyXEL .....	234
19.2.1 Configuring UPnP .....	234
19.3 Installing UPnP in Windows Example .....	235
19.4 Using UPnP in Windows XP Example .....	239
<b>Chapter 20</b>	
<b>Logs Screens.....</b>	<b>247</b>
20.1 Logs Overview .....	247
20.1.1 Alerts and Logs .....	247
20.2 Configuring Log Settings .....	247
20.3 Displaying the Logs .....	250
20.4 SMTP Error Messages .....	250
20.4.1 Example E-mail Log .....	251
<b>Chapter 21</b>	
<b>Maintenance .....</b>	<b>253</b>
21.1 Maintenance Overview .....	253
21.2 System Status Screen .....	253
21.2.1 System Statistics .....	256
21.3 DHCP Table Screen .....	257
21.4 Any IP Table Screen .....	258
21.5 Wireless Screen .....	259
21.5.1 Association List .....	259
21.6 Diagnostic Screens .....	260
21.6.1 Diagnostic General Screen .....	260
21.6.2 Diagnostic DSL Line Screen .....	260
21.7 Firmware Screen .....	262
<b>Chapter 22</b>	
<b>Introducing the SMT .....</b>	<b>265</b>
22.1 Introduction to the SMT .....	265
22.2 Accessing the SMT via the Console Port .....	265
22.2.1 Initial Screen .....	265
22.2.2 Entering the Password .....	266
22.2.3 Procedure for SMT Configuration via Telnet .....	266
22.2.4 Entering Password .....	267
22.3 Navigating the SMT Interface .....	267

22.3.1 System Management Terminal Interface Summary .....	268
22.3.2 SMT Menus Overview .....	269
22.4 Changing the System Password .....	270
<b>Chapter 23</b>	
<b>Menu 1 General Setup .....</b>	<b>273</b>
23.1 General Setup .....	273
23.2 Procedure To Configure Menu 1 .....	273
23.2.1 Procedure to Configure Dynamic DNS .....	274
<b>Chapter 24</b>	
<b>Menu 2 WAN Backup Setup .....</b>	<b>277</b>
24.1 Introduction to WAN Backup Setup .....	277
24.2 Configuring WAN Backup in Menu 2 .....	277
24.2.1 Traffic Redirect Setup .....	278
<b>Chapter 25</b>	
<b>Menu 3 LAN Setup .....</b>	<b>281</b>
25.1 LAN Setup .....	281
25.1.1 General Ethernet Setup .....	281
25.2 Protocol Dependent Ethernet Setup .....	281
25.3 TCP/IP Ethernet Setup and DHCP .....	282
<b>Chapter 26</b>	
<b>Wireless LAN Setup .....</b>	<b>285</b>
26.1 Wireless LAN Overview .....	285
26.2 Wireless LAN Setup .....	285
26.2.1 Wireless LAN MAC Address Filter .....	286
<b>Chapter 27</b>	
<b>Internet Access .....</b>	<b>289</b>
27.1 Internet Access Overview .....	289
27.2 IP Policies .....	289
27.3 IP Alias .....	289
27.4 IP Alias Setup .....	290
27.5 Route IP Setup .....	291
27.6 Internet Access Configuration .....	292
<b>Chapter 28</b>	
<b>Remote Node Configuration .....</b>	<b>295</b>
28.1 Remote Node Setup Overview .....	295
28.2 Remote Node Setup .....	295
28.2.1 Remote Node Profile .....	295

28.2.2 Encapsulation and Multiplexing Scenarios .....	296
28.2.2.1 Scenario 1: One VC, Multiple Protocols .....	296
28.2.2.2 Scenario 2: One VC, One Protocol (IP) .....	296
28.2.2.3 Scenario 3: Multiple VCs .....	296
28.2.3 Outgoing Authentication Protocol .....	298
28.3 Remote Node Network Layer Options .....	299
28.3.1 My WAN Addr Sample IP Addresses .....	300
28.4 Remote Node Filter .....	301
28.5 Editing ATM Layer Options .....	302
28.5.1 VC-based Multiplexing (non-PPP Encapsulation) .....	302
28.5.2 LLC-based Multiplexing or PPP Encapsulation .....	303
28.5.3 Advance Setup Options .....	303
<b>Chapter 29</b>	
<b>Static Route Setup .....</b>	<b>305</b>
29.1 IP Static Route Overview .....	305
29.2 Configuration .....	305
<b>Chapter 30</b>	
<b>Bridging Setup .....</b>	<b>309</b>
30.1 Bridging in General .....	309
30.2 Bridge Ethernet Setup .....	309
30.2.1 Remote Node Bridging Setup .....	309
30.2.2 Bridge Static Route Setup .....	311
<b>Chapter 31</b>	
<b>Network Address Translation (NAT) .....</b>	<b>313</b>
31.1 Using NAT .....	313
31.1.1 SUA (Single User Account) Versus NAT .....	313
31.2 Applying NAT .....	313
31.3 NAT Setup .....	315
31.3.1 Address Mapping Sets .....	315
31.3.1.1 SUA Address Mapping Set .....	316
31.3.1.2 User-Defined Address Mapping Sets .....	317
31.3.1.3 Ordering Your Rules .....	318
31.4 Configuring a Server behind NAT .....	319
31.5 General NAT Examples .....	321
31.5.1 Example 1: Internet Access Only .....	321
31.5.2 Example 2: Internet Access with an Inside Server .....	322
31.5.3 Example 3: Multiple Public IP Addresses With Inside Servers .....	323
31.5.4 Example 4: NAT Unfriendly Application Programs .....	326

<b>Chapter 32</b>	
<b>Enabling the Firewall .....</b>	<b>329</b>
32.1 Remote Management and the Firewall .....	329
32.2 Access Methods .....	329
32.3 Enabling the Firewall .....	329
<b>Chapter 33</b>	
<b>Filter Configuration .....</b>	<b>331</b>
33.1 About Filtering .....	331
33.1.1 The Filter Structure of the Prestige .....	332
33.2 Configuring a Filter Set for the Prestige .....	333
33.3 Filter Rules Summary Menus .....	334
33.4 Configuring a Filter Rule .....	335
33.4.1 TCP/IP Filter Rule .....	336
33.4.2 Generic Filter Rule .....	338
33.5 Filter Types and NAT .....	340
33.6 Example Filter .....	340
33.7 Applying Filters and Factory Defaults .....	342
33.7.1 Ethernet Traffic .....	343
33.7.2 Remote Node Filters .....	343
<b>Chapter 34</b>	
<b>SNMP Configuration .....</b>	<b>345</b>
34.1 About SNMP .....	345
34.2 Supported MIBs .....	346
34.3 SNMP Configuration .....	346
34.4 SNMP Traps .....	347
<b>Chapter 35</b>	
<b>System Security .....</b>	<b>349</b>
35.1 System Security .....	349
35.1.1 System Password .....	349
35.1.2 Configuring External RADIUS Server .....	349
35.1.3 IEEE802.1x .....	351
35.2 Creating User Accounts on the Prestige .....	353
<b>Chapter 36</b>	
<b>System Information and Diagnosis .....</b>	<b>355</b>
36.1 Overview .....	355
36.2 System Status .....	355
36.3 System Information .....	357
36.3.1 System Information .....	357
36.3.2 Console Port Speed .....	358



36.4 Log and Trace .....	359
36.4.1 Viewing Error Log .....	359
36.4.2 Syslog and Accounting .....	360
36.5 Diagnostic .....	362

## **Chapter 37**

### **Firmware and Configuration File Maintenance ..... 365**

37.1 Filename Conventions .....	365
37.2 Backup Configuration .....	366
37.2.1 Backup Configuration .....	366
37.2.2 Using the FTP Command from the Command Line .....	367
37.2.3 Example of FTP Commands from the Command Line .....	367
37.2.4 GUI-based FTP Clients .....	368
37.2.5 TFTP and FTP over WAN Management Limitations .....	368
37.2.6 Backup Configuration Using TFTP .....	369
37.2.7 TFTP Command Example .....	369
37.2.8 GUI-based TFTP Clients .....	369
37.2.9 Backup Via Console Port .....	370
37.3 Restore Configuration .....	371
37.3.1 Restore Using FTP .....	371
37.3.2 Restore Using FTP Session Example .....	372
37.3.3 Restore Via Console Port .....	373
37.4 Uploading Firmware and Configuration Files .....	374
37.4.1 Firmware File Upload .....	374
37.4.2 Configuration File Upload .....	374
37.4.3 FTP File Upload Command from the DOS Prompt Example .....	375
37.4.4 FTP Session Example of Firmware File Upload .....	376
37.4.5 TFTP File Upload .....	376
37.4.6 TFTP Upload Command Example .....	377
37.4.7 Uploading Via Console Port .....	377
37.4.8 Uploading Firmware File Via Console Port .....	377
37.4.9 Example Xmodem Firmware Upload Using HyperTerminal .....	378
37.4.10 Uploading Configuration File Via Console Port .....	378
37.4.11 Example Xmodem Configuration Upload Using HyperTerminal .....	379

## **Chapter 38**

### **System Maintenance..... 381**

38.1 Command Interpreter Mode .....	381
38.2 Call Control Support .....	382
38.2.1 Budget Management .....	382
38.3 Time and Date Setting .....	383
38.3.1 Resetting the Time .....	384

<b>Chapter 39</b>	
<b>Remote Management .....</b>	<b>387</b>
39.1 Remote Management Overview .....	387
39.2 Remote Management .....	387
39.2.1 Remote Management Setup .....	387
39.2.2 Remote Management Limitations .....	388
39.3 Remote Management and NAT .....	389
39.4 System Timeout .....	389
<b>Chapter 40</b>	
<b>IP Policy Routing.....</b>	<b>391</b>
40.1 IP Policy Routing Overview .....	391
40.2 Benefits of IP Policy Routing .....	391
40.3 Routing Policy .....	391
40.4 IP Routing Policy Setup .....	392
40.5 Applying an IP Policy .....	395
40.5.1 Ethernet IP Policies .....	395
40.6 IP Policy Routing Example .....	396
<b>Chapter 41</b>	
<b>Call Scheduling .....</b>	<b>399</b>
41.1 Introduction .....	399
<b>Chapter 42</b>	
<b>VPN/IPSec Setup.....</b>	<b>403</b>
42.1 VPN/IPSec Overview .....	403
42.2 IPSec Summary Screen .....	404
42.3 IPSec Setup .....	406
42.4 IKE Setup .....	410
42.5 Manual Setup .....	412
42.5.1 Active Protocol .....	412
42.5.2 Security Parameter Index (SPI) .....	412
<b>Chapter 43</b>	
<b>SA Monitor.....</b>	<b>415</b>
43.1 SA Monitor Overview .....	415
43.2 Using SA Monitor .....	415
<b>Chapter 44</b>	
<b>Troubleshooting .....</b>	<b>419</b>
44.1 Problems Starting Up the Prestige .....	419
44.2 Problems with the LAN LED .....	419
44.3 Problems with the DSL LED .....	420

44.4 Problems with the LAN Interface .....	420
44.5 Problems with the WAN Interface .....	420
44.6 Problems with Internet Access .....	421
44.7 Problems with the Password .....	421
44.8 Problems with the Web Configurator .....	422
44.9 Problems with Remote Management .....	422
44.10 Telephone Problems .....	423

**Appendix A**  
**Hardware Specifications .....** **425**

Prestige 2602HW Series Power Adaptor Specifications .....	427
---	-----

**Appendix B**  
**Setting up Your Computer's IP Address.....** **429**

Windows 95/98/Me.....	429
Configuring .....	431
Verifying Settings.....	432
Windows 2000/NT/XP .....	432
Verifying Settings.....	436
Macintosh OS 8/9.....	437
Verifying Settings.....	438
Macintosh OS X .....	438
Verifying Settings.....	440

**Appendix C**  
**IP Subnetting .....** **441**

IP Addressing.....	441
IP Classes .....	441
Subnet Masks .....	442
Subnetting .....	442
Example: Two Subnets .....	443
Example: Four Subnets.....	445
Example Eight Subnets.....	446
Subnetting With Class A and Class B Networks .....	447

**Appendix D**  
**PPPoE .....** **449**

PPPoE in Action.....	449
Benefits of PPPoE.....	449
Traditional Dial-up Scenario .....	449
How PPPoE Works .....	450
Prestige as a PPPoE Client .....	450

<b>Appendix E</b>	
<b>Wireless LAN and IEEE 802.11</b>	<b>451</b>
Benefits of a Wireless LAN	451
IEEE 802.11	451
Ad-hoc Wireless LAN Configuration	452
Infrastructure Wireless LAN Configuration	452
<b>Appendix F</b>	
<b>Wireless LAN With IEEE 802.1x</b>	<b>455</b>
Security Flaws with IEEE 802.11	455
Deployment Issues with IEEE 802.11	455
IEEE 802.1x	455
Advantages of the IEEE 802.1x	455
RADIUS Server Authentication Sequence	456
<b>Appendix G</b>	
<b>Types of EAP Authentication</b>	<b>457</b>
EAP-MD5 (Message-Digest Algorithm 5)	457
EAP-TLS (Transport Layer Security)	457
EAP-TTLS (Tunneled Transport Layer Service)	457
LEAP	458
<b>Appendix H</b>	
<b>Triangle Route</b>	<b>459</b>
The Ideal Setup	459
The "Triangle Route" Problem	459
The "Triangle Route" Solutions	460
IP Aliasing	460
Gateways on the WAN Side	461
<b>Appendix I</b>	
<b>Internal SPTGEN</b>	<b>463</b>
Internal SPTGEN Overview	463
The Configuration Text File Format	463
Internal SPTGEN File Modification - Important Points to Remember	463
Internal SPTGEN FTP Download Example	464
Internal SPTGEN FTP Upload Example	465
Command Examples	486
<b>Appendix J</b>	
<b>Command Interpreter</b>	<b>489</b>

Command Syntax.....	489
Command Usage .....	489
<b>Appendix K</b>	
<b>Firewall Commands .....</b>	<b>491</b>
Sys Firewall Commands .....	491
<b>Appendix L</b>	
<b>Boot Commands .....</b>	<b>493</b>
<b>Appendix M</b>	
<b>Log Descriptions .....</b>	<b>495</b>
Log Commands.....	504
Configuring What You Want the Prestige to Log .....	504
Displaying Logs .....	505
Log Command Example.....	506
<b>Index.....</b>	<b>507</b>



# List of Figures

Figure 1 Prestige Internet Access Application .....	54
Figure 2 Internet Telephony Service Provider Application .....	55
Figure 3 Firewall Application .....	55
Figure 4 Prestige LAN-to-LAN Application .....	56
Figure 5 Password Screen .....	57
Figure 6 Change Password at Login .....	58
Figure 7 Web Configurator SITE MAP Screen .....	59
Figure 8 Internet Access Wizard Setup: First Screen .....	65
Figure 9 Internet Connection with PPPoE .....	68
Figure 10 Internet Connection with RFC 1483 .....	69
Figure 11 Internet Connection with ENET ENCAP .....	69
Figure 12 Internet Connection with PPPoA .....	70
Figure 13 Internet Access Wizard Setup: Third Screen .....	72
Figure 14 Internet Access Wizard Setup: Fourth Screen .....	74
Figure 15 Internet Access Wizard Setup: LAN Configuration .....	75
Figure 16 Internet Access Wizard Setup: Connection Tests .....	76
Figure 17 Password .....	77
Figure 18 LAN and WAN IP Addresses .....	79
Figure 19 Any IP Example .....	83
Figure 20 LAN Setup .....	84
Figure 21 LAN: Static DHCP .....	86
Figure 22 RTS/CTS .....	88
Figure 23 Prestige Wireless Security Levels .....	89
Figure 24 Wireless LAN .....	91
Figure 25 MAC Address Filter .....	93
Figure 26 EAP Authentication .....	95
Figure 27 WPA - PSK Authentication .....	97
Figure 28 WPA with RADIUS Application Example .....	98
Figure 29 Wireless LAN: 802.1x/WPA .....	99
Figure 30 Wireless LAN: 802.1x/WPA for 802.1x Protocol .....	100
Figure 31 Wireless LAN: 802.1x/WPA for WPA Protocol .....	102
Figure 32 Wireless LAN: 802.1x/WPA for WPA-PSK Protocol .....	104
Figure 33 Local User Database .....	105
Figure 34 RADIUS .....	106
Figure 35 Example of Traffic Shaping .....	111
Figure 36 WAN Setup (PPPoE) .....	112
Figure 37 Traffic Redirect Example .....	115
Figure 38 Traffic Redirect LAN Setup .....	115

Figure 39 WAN Backup .....	116
Figure 40 How NAT Works .....	121
Figure 41 NAT Application With IP Alias .....	121
Figure 42 Multiple Servers Behind NAT Example .....	124
Figure 43 NAT Mode .....	125
Figure 44 Edit SUA/NAT Server Set .....	126
Figure 45 Address Mapping Rules .....	127
Figure 46 Address Mapping Rule Edit .....	128
Figure 47 SIP User Agent Server .....	133
Figure 48 SIP Proxy Server .....	134
Figure 49 SIP Redirect Server .....	135
Figure 50 SIP Settings .....	137
Figure 51 Voice Advanced Setup .....	139
Figure 52 DiffServ: Differentiated Service Field .....	141
Figure 53 QoS .....	142
Figure 54 Phone .....	143
Figure 55 Speed Dial .....	145
Figure 56 Lifeline .....	147
Figure 57 Phone Port Common .....	148
Figure 58 Dynamic DNS .....	150
Figure 59 Time and Date .....	152
Figure 60 Prestige Firewall Application .....	157
Figure 61 Three-Way Handshake .....	159
Figure 62 SYN Flood .....	159
Figure 63 Smurf Attack .....	160
Figure 64 Stateful Inspection .....	162
Figure 65 LAN to WAN Traffic .....	172
Figure 66 WAN to LAN Traffic .....	172
Figure 67 Firewall: Default Policy .....	173
Figure 68 Firewall: Rule Summary .....	175
Figure 69 Firewall: Edit Rule .....	177
Figure 70 Firewall: Customized Services .....	179
Figure 71 Firewall: Configure Customized Services .....	180
Figure 72 Firewall Example: Rule Summary .....	181
Figure 73 Firewall Example: Edit Rule: Destination Address .....	182
Figure 74 Edit Custom Port Example .....	182
Figure 75 Firewall Example: Edit Rule: Select Customized Services .....	183
Figure 76 Firewall Example: Rule Summary: My Service .....	184
Figure 77 Firewall: Anti Probing .....	187
Figure 78 Firewall: Threshold .....	189
Figure 79 Content Filter: Keyword .....	192
Figure 80 Content Filter: Schedule .....	193
Figure 81 Content Filter: Trusted .....	194



Figure 82 Encryption and Decryption .....	196
Figure 83 IPSec Architecture .....	197
Figure 84 Transport and Tunnel Mode IPSec Encapsulation .....	198
Figure 85 IPSec Summary Fields .....	203
Figure 86 VPN Summary .....	204
Figure 87 VPN Host using Intranet DNS Server Example .....	206
Figure 88 NAT Router Between IPSec Routers .....	206
Figure 89 VPN IKE .....	210
Figure 90 Two Phases to Set Up the IPSec SA .....	215
Figure 91 VPN IKE: Advanced Setup .....	217
Figure 92 VPN: Manual Key .....	220
Figure 93 VPN: SA Monitor .....	224
Figure 94 VPN: Global Setting .....	225
Figure 95 Telecommuters Sharing One VPN Rule Example .....	226
Figure 96 Telecommuters Using Unique VPN Rules Example .....	227
Figure 97 Telnet Configuration on a TCP/IP Network .....	230
Figure 98 Remote Management .....	231
Figure 99 Configuring UPnP .....	234
Figure 100 Add/Remove Programs: Windows Setup: Communication .....	236
Figure 101 Add/Remove Programs: Windows Setup: Communication: Components 236	
Figure 102 Network Connections .....	237
Figure 103 Windows Optional Networking Components Wizard .....	238
Figure 104 Networking Services .....	239
Figure 105 Network Connections .....	240
Figure 106 Internet Connection Properties .....	241
Figure 107 Internet Connection Properties: Advanced Settings .....	242
Figure 108 Internet Connection Properties: Advanced Settings: Add .....	242
Figure 109 System Tray Icon .....	243
Figure 110 Internet Connection Status .....	243
Figure 111 Network Connections .....	244
Figure 112 Network Connections: My Network Places .....	245
Figure 113 Network Connections: My Network Places: Properties: Example .....	245
Figure 114 Log Settings .....	248
Figure 115 View Logs .....	250
Figure 116 E-mail Log Example .....	252
Figure 117 System Status .....	254
Figure 118 System Status: Show Statistics .....	256
Figure 119 DHCP Table .....	258
Figure 120 Any IP Table .....	258
Figure 121 Association List .....	259
Figure 122 Diagnostic: General .....	260
Figure 123 Diagnostic: DSL Line .....	261

Figure 124 Firmware Upgrade .....	262
Figure 125 Network Temporarily Disconnected .....	263
Figure 126 Error Message .....	263
Figure 127 Initial Screen .....	266
Figure 128 Password Screen .....	266
Figure 129 Login Screen .....	267
Figure 130 Menu 23.1 Change Password .....	271
Figure 131 Menu 1 General Setup .....	274
Figure 132 Menu 1.1 Configure Dynamic DNS .....	275
Figure 133 Menu 2 WAN Backup Setup .....	277
Figure 134 Menu 2.1Traffic Redirect Setup .....	278
Figure 135 Menu 3 LAN Setup .....	281
Figure 136 Menu 3.1 LAN Port Filter Setup .....	281
Figure 137 Menu 3.2 TCP/IP and DHCP Ethernet Setup .....	282
Figure 138 Menu 3.5 - Wireless LAN Setup .....	285
Figure 139 Menu 3.5.1 WLAN MAC Address Filtering .....	287
Figure 140 IP Alias Network Example .....	290
Figure 141 Menu 3.2 TCP/IP and DHCP Setup .....	290
Figure 142 Menu 3.2.1 IP Alias Setup .....	291
Figure 143 Menu 1 General Setup .....	292
Figure 144 Menu 4 Internet Access Setup .....	292
Figure 145 Menu 11 Remote Node Setup .....	296
Figure 146 Menu 11.1 Remote Node Profile .....	297
Figure 147 Menu 11.3 Remote Node Network Layer Options .....	299
Figure 148 Sample IP Addresses for a TCP/IP LAN-to-LAN Connection .....	301
Figure 149 Menu 11.5 Remote Node Filter (RFC 1483 or ENET Encapsulation) ..	302
Figure 150 Menu 11.5 Remote Node Filter (PPPoA or PPPoE Encapsulation) ....	302
Figure 151 Menu 11.6 for VC-based Multiplexing .....	303
Figure 152 Menu 11.6 for LLC-based Multiplexing or PPP Encapsulation .....	303
Figure 153 Menu 11.1 Remote Node Profile .....	304
Figure 154 Menu 11.8 Advance Setup Options .....	304
Figure 155 Sample Static Routing Topology .....	305
Figure 156 Menu 12 Static Route Setup .....	306
Figure 157 Menu 12.1 IP Static Route Setup .....	306
Figure 158 Menu 12.1.1 Edit IP Static Route .....	306
Figure 159 Menu 11.1 Remote Node Profile .....	310
Figure 160 Menu 11.3 Remote Node Network Layer Options .....	310
Figure 161 Menu 12.3.1 Edit Bridge Static Route .....	311
Figure 162 Menu 4 Applying NAT for Internet Access .....	314
Figure 163 Applying NAT in Menus 4 & 11.3 .....	314
Figure 164 Menu 15 NAT Setup .....	315
Figure 165 Menu 15.1 Address Mapping Sets .....	316
Figure 166 Menu 15.1.255 SUA Address Mapping Rules .....	316

Figure 167 Menu 15.1.1 First Set .....	317
Figure 168 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set .....	319
Figure 169 Menu 15.2 NAT Server Setup .....	320
Figure 170 Menu 15.2 NAT Server Setup .....	320
Figure 171 Multiple Servers Behind NAT Example .....	321
Figure 172 NAT Example 1 .....	321
Figure 173 Menu 4 Internet Access & NAT Example .....	322
Figure 174 NAT Example 2 .....	322
Figure 175 Menu 15.2.1 Specifying an Inside Server .....	323
Figure 176 NAT Example 3 .....	324
Figure 177 Example 3: Menu 11.3 .....	324
Figure 178 Example 3: Menu 15.1.1.1 .....	325
Figure 179 Example 3: Final Menu 15.1.1 .....	325
Figure 180 Example 3: Menu 15.2 .....	326
Figure 181 NAT Example 4 .....	326
Figure 182 Example 4: Menu 15.1.1.1 Address Mapping Rule .....	327
Figure 183 Example 4: Menu 15.1.1 Address Mapping Rules .....	327
Figure 184 Menu 21.2 Firewall Setup .....	330
Figure 185 Outgoing Packet Filtering Process .....	331
Figure 186 Filter Rule Process .....	332
Figure 187 Menu 21 Filter Set Configuration .....	333
Figure 188 NetBIOS_WAN Filter Rules Summary .....	333
Figure 189 NetBIOS_LAN Filter Rules Summary .....	334
Figure 190 IGMP Filter Rules Summary .....	334
Figure 191 Menu 21.1.x.1 TCP/IP Filter Rule .....	336
Figure 192 Executing an IP Filter .....	338
Figure 193 Menu 21.1.5.1 Generic Filter Rule .....	339
Figure 194 Protocol and Device Filter Sets .....	340
Figure 195 Sample Telnet Filter .....	341
Figure 196 Menu 21.1.6.1 Sample Filter .....	341
Figure 197 Menu 21.1.6.1 Sample Filter Rules Summary .....	342
Figure 198 Filtering Ethernet Traffic .....	343
Figure 199 Filtering Remote Node Traffic .....	343
Figure 200 SNMP Management Model .....	345
Figure 201 Menu 22 SNMP Configuration .....	347
Figure 202 Menu 23 – System Security .....	349
Figure 203 Menu 23 System Security .....	349
Figure 204 Menu 23.2 System Security: RADIUS Server .....	350
Figure 205 Menu 23 System Security .....	351
Figure 206 Menu 23.4 System Security: IEEE802.1x .....	351
Figure 207 Menu 14 Dial-in User Setup .....	354
Figure 208 Menu 14.1 Edit Dial-in User .....	354
Figure 209 Menu 24 System Maintenance .....	355

Figure 210 Menu 24.1 System Maintenance : Status .....	356
Figure 211 Menu 24.2 System Information and Console Port Speed .....	357
Figure 212 Menu 24.2.1 System Maintenance: Information .....	358
Figure 213 Menu 24.2.2 System Maintenance : Change Console Port Speed .....	359
Figure 214 Menu 24.3 System Maintenance: Log and Trace .....	359
Figure 215 Sample Error and Information Messages .....	360
Figure 216 Menu 24.3.2 System Maintenance: Syslog and Accounting .....	360
Figure 217 Syslog Example .....	361
Figure 218 Menu 24.4 System Maintenance : Diagnostic .....	362
Figure 219 Telnet in Menu 24.5 .....	367
Figure 220 FTP Session Example .....	368
Figure 221 System Maintenance: Backup Configuration .....	370
Figure 222 System Maintenance: Starting Xmodem Download Screen .....	370
Figure 223 Backup Configuration Example .....	371
Figure 224 Successful Backup Confirmation Screen .....	371
Figure 225 Telnet into Menu 24.6 .....	372
Figure 226 Restore Using FTP Session Example .....	372
Figure 227 System Maintenance: Restore Configuration .....	373
Figure 228 System Maintenance: Starting Xmodem Download Screen .....	373
Figure 229 Restore Configuration Example .....	373
Figure 230 Successful Restoration Confirmation Screen .....	374
Figure 231 Telnet Into Menu 24.7.1 Upload System Firmware .....	374
Figure 232 Telnet Into Menu 24.7.2 System Maintenance .....	375
Figure 233 FTP Session Example of Firmware File Upload .....	376
Figure 234 Menu 24.7.1 As Seen Using the Console Port .....	377
Figure 235 Example Xmodem Upload .....	378
Figure 236 Menu 24.7.2 As Seen Using the Console Port .....	378
Figure 237 Example Xmodem Upload .....	379
Figure 238 Command Mode in Menu 24 .....	381
Figure 239 Valid Commands .....	381
Figure 240 Menu 24.9 System Maintenance: Call Control .....	382
Figure 241 Menu 24.9.1 System Maintenance: Budget Management .....	382
Figure 242 Menu 24 System Maintenance .....	383
Figure 243 Menu 24.10 System Maintenance: Time and Date Setting .....	384
Figure 244 Menu 24.11 Remote Management Control .....	388
Figure 245 Menu 25 IP Routing Policy Setup .....	392
Figure 246 Menu 25.1 IP Routing Policy Setup .....	393
Figure 247 Menu 25.1.1 IP Routing Policy .....	394
Figure 248 Menu 3.2 TCP/IP and DHCP Ethernet Setup .....	396
Figure 249 Menu 11.3 Remote Node Network Layer Options .....	396
Figure 250 Example of IP Policy Routing .....	397
Figure 251 IP Routing Policy Example .....	397
Figure 252 IP Routing Policy Example .....	398

Figure 253 Applying IP Policies Example .....	398
Figure 254 Menu 26 Schedule Setup .....	399
Figure 255 Menu 26.1 Schedule Set Setup .....	400
Figure 256 Applying Schedule Set(s) to a Remote Node (PPPoE) .....	401
Figure 257 VPN SMT Menu Tree .....	403
Figure 258 Menu 27 VPN/IPSec Setup .....	404
Figure 259 Menu 27.1 IPSec Summary .....	404
Figure 260 Menu 27.1.1 IPSec Setup .....	407
Figure 261 Menu 27.1.1.1KE Setup .....	411
Figure 262 Menu 27.1.1.2 Manual Setup .....	413
Figure 263 Menu 27.2 SA Monitor .....	416
Figure 264 Ethernet Cable Pin Assignments .....	425
Figure 265 Prestige 2602HW-L DSL Port Pin Assignments .....	426
Figure 266 WIndows 95/98/Me: Network: Configuration .....	430
Figure 267 Windows 95/98/Me: TCP/IP Properties: IP Address .....	431
Figure 268 Windows 95/98/Me: TCP/IP Properties: DNS Configuration .....	432
Figure 269 Windows XP: Start Menu .....	433
Figure 270 Windows XP: Control Panel .....	433
Figure 271 Windows XP: Control Panel: Network Connections: Properties .....	434
Figure 272 Windows XP: Local Area Connection Properties .....	434
Figure 273 Windows XP: Advanced TCP/IP Settings .....	435
Figure 274 Windows XP: Internet Protocol (TCP/IP) Properties .....	436
Figure 275 Macintosh OS 8/9: Apple Menu .....	437
Figure 276 Macintosh OS 8/9: TCP/IP .....	438
Figure 277 Macintosh OS X: Apple Menu .....	439
Figure 278 Macintosh OS X: Network .....	439
Figure 279 Single-Computer per Router Hardware Configuration .....	450
Figure 280 Prestige as a PPPoE Client .....	450
Figure 281 Peer-to-Peer Communication in an Ad-hoc Network .....	452
Figure 282 ESS Provides Campus-Wide Coverage .....	453
Figure 283 Sequences for EAP MD5–Challenge Authentication .....	456
Figure 284 Ideal Setup .....	459
Figure 285 “Triangle Route” Problem .....	460
Figure 286 IP Alias .....	460
Figure 287 Gateways on the WAN Side .....	461
Figure 288 Configuration Text File Format: Column Descriptions .....	463
Figure 289 Invalid Parameter Entered: Command Line Example .....	464
Figure 290 Valid Parameter Entered: Command Line Example .....	464
Figure 291 Internal SPTGEN FTP Download Example .....	465
Figure 292 Internal SPTGEN FTP Upload Example .....	465
Figure 293 Option to Enter Debug Mode .....	493
Figure 294 Boot Module Commands .....	494
Figure 295 Displaying Log Categories Example .....	504

Figure 296 Displaying Log Parameters Example ..... 505  
Figure 297 Log Command Example ..... 506

# List of Tables

Table 1 ADSL Standards .....	45
Table 2 IEEE 802.11g .....	49
Table 3 Web Configurator Screens Summary .....	59
Table 4 Internet Access Wizard Setup: First Screen .....	65
Table 5 Internet Connection with PPPoE .....	68
Table 6 Internet Connection with RFC 1483 .....	69
Table 7 Internet Connection with ENET ENCAP .....	70
Table 8 Internet Connection with PPPoA .....	71
Table 9 Internet Access Wizard Setup: Voice Configuration .....	72
Table 10 Internet Access Wizard Setup: LAN Configuration .....	75
Table 11 Password .....	77
Table 12 LAN Setup .....	84
Table 13 LAN: Static DHCP .....	86
Table 14 Wireless LAN .....	91
Table 15 MAC Address Filter .....	93
Table 16 Wireless Security Relational Matrix .....	98
Table 17 Wireless LAN: 802.1x/WPA .....	100
Table 18 Wireless LAN: 802.1x/WPA for 802.1x Protocol .....	101
Table 19 Wireless LAN: 802.1x/WPA for WPA Protocol .....	103
Table 20 Wireless LAN: 802.1x/WPA for WPA-PSK Protocol .....	104
Table 21 Local User Database .....	106
Table 22 RADIUS .....	107
Table 23 WAN Setup .....	112
Table 24 WAN Backup .....	116
Table 25 NAT Definitions .....	119
Table 26 NAT Mapping Types .....	122
Table 27 Services and Port Numbers .....	123
Table 28 NAT Mode .....	125
Table 29 Edit SUA/NAT Server Set .....	126
Table 30 Address Mapping Rules .....	127
Table 31 Address Mapping Rule Edit .....	129
Table 32 SIP Call Progression .....	132
Table 33 SIP Settings .....	138
Table 34 Voice Advanced Setup .....	139
Table 35 QoS .....	142
Table 36 Phone .....	144
Table 37 Speed Dial .....	145
Table 38 Lifeline .....	147

Table 39 Phone Port Common .....	148
Table 40 Dynamic DNS .....	150
Table 41 Pre-defined NTP Time Servers .....	151
Table 42 Time and Date .....	152
Table 43 Common IP Ports .....	158
Table 44 ICMP Commands That Trigger Alerts .....	160
Table 45 Legal NetBIOS Commands .....	160
Table 46 Legal SMTP Commands .....	161
Table 47 Firewall: Default Policy .....	173
Table 48 Rule Summary .....	175
Table 49 Firewall: Edit Rule .....	178
Table 50 Customized Services .....	179
Table 51 Firewall: Configure Customized Services .....	180
Table 52 Predefined Services .....	184
Table 53 Firewall: Anti Probing .....	187
Table 54 Firewall: Threshold .....	189
Table 55 Content Filter: Keyword .....	192
Table 56 Content Filter: Schedule .....	193
Table 57 Content Filter: Trusted .....	194
Table 58 VPN and NAT .....	199
Table 59 AH and ESP .....	202
Table 60 VPN Summary .....	204
Table 61 Local ID Type and Content Fields .....	208
Table 62 Peer ID Type and Content Fields .....	208
Table 63 Matching ID Type and Content Configuration Example .....	208
Table 64 Mismatching ID Type and Content Configuration Example .....	209
Table 65 VPN IKE .....	211
Table 66 VPN IKE: Advanced Setup .....	217
Table 67 VPN: Manual Key .....	221
Table 68 VPN: SA Monitor .....	224
Table 69 VPN: Global Setting .....	225
Table 70 Telecommuters Sharing One VPN Rule Example .....	226
Table 71 Telecommuters Using Unique VPN Rules Example .....	227
Table 72 Remote Management .....	231
Table 73 Configuring UPnP .....	235
Table 74 Log Settings .....	249
Table 75 View Logs .....	250
Table 76 SMTP Error Messages .....	251
Table 77 System Status .....	255
Table 78 System Status: Show Statistics .....	256
Table 79 DHCP Table .....	258
Table 80 Any IP Table .....	258
Table 81 Association List .....	259



Table 82 Diagnostic: General .....	260
Table 83 Diagnostic: DSL Line .....	261
Table 84 Firmware Upgrade .....	262
Table 85 Navigating the SMT Interface .....	267
Table 86 SMT Main Menu .....	268
Table 87 Main Menu Summary .....	268
Table 88 SMT Menus Overview .....	269
Table 89 Menu 1 General Setup .....	274
Table 90 Menu 1.1 Configure Dynamic DNS .....	275
Table 91 Menu 2 WAN Backup Setup .....	277
Table 92 Menu 2.1Traffic Redirect Setup .....	278
Table 93 DHCP Ethernet Setup .....	282
Table 94 TCP/IP Ethernet Setup .....	283
Table 95 Menu 3.5 - Wireless LAN Setup .....	285
Table 96 Menu 3.5.1 WLAN MAC Address Filtering .....	287
Table 97 Menu 3.2.1 IP Alias Setup .....	291
Table 98 Menu 4 Internet Access Setup .....	293
Table 99 Menu 11.1 Remote Node Profile .....	297
Table 100 Menu 11.3 Remote Node Network Layer Options .....	299
Table 101 Menu 11.8 Advance Setup Options .....	304
Table 102 Menu12.1.1 Edit IP Static Route .....	307
Table 103 Remote Node Network Layer Options: Bridge Fields .....	310
Table 104 Menu 12.3.1 Edit Bridge Static Route .....	311
Table 105 Applying NAT in Menus 4 & 11.3 .....	315
Table 106 SUA Address Mapping Rules .....	316
Table 107 Menu 15.1.1 First Set .....	318
Table 108 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set .....	319
Table 109 Abbreviations Used in the Filter Rules Summary Menu .....	334
Table 110 Rule Abbreviations Used .....	335
Table 111 Menu 21.1.x.1 TCP/IP Filter Rule .....	336
Table 112 Menu 21.1.5.1 Generic Filter Rule .....	339
Table 113 Filter Sets Table .....	342
Table 114 Menu 22 SNMP Configuration .....	347
Table 115 SNMP Traps .....	347
Table 116 Ports and Permanent Virtual Circuits .....	348
Table 117 Menu 23.2 System Security: RADIUS Server .....	350
Table 118 Menu 23.4 System Security: IEEE802.1x .....	352
Table 119 Menu 14.1 Edit Dial-in User .....	354
Table 120 Menu 24.1 System Maintenance: Status .....	356
Table 121 Menu 24.2.1 System Maintenance: Information .....	358
Table 122 Menu 24.3.2 System Maintenance : Syslog and Accounting .....	360
Table 123 Menu 24.4 System Maintenance Menu: Diagnostic .....	363
Table 124 Filename Conventions .....	366

Table 125 General Commands for GUI-based FTP Clients .....	368
Table 126 General Commands for GUI-based TFTP Clients .....	370
Table 127 Menu 24.9.1 System Maintenance: Budget Management .....	383
Table 128 Menu 24.10 System Maintenance: Time and Date Setting .....	384
Table 129 Menu 24.11 Remote Management Control .....	388
Table 130 Menu 25.1 IP Routing Policy Setup .....	393
Table 131 Menu 25.1.1 IP Routing Policy .....	394
Table 132 Menu 26.1 Schedule Set Setup .....	400
Table 133 Menu 27.1 IPsec Summary .....	404
Table 134 Menu 27.1.1 IPsec Setup .....	407
Table 135 Menu 27.1.1.1 IKE Setup .....	411
Table 136 Active Protocol: Encapsulation and Security Protocol .....	412
Table 137 Menu 27.1.1.2 Manual Setup .....	413
Table 138 Menu 27.2 SA Monitor .....	416
Table 139 Troubleshooting the Start-Up of Your Prestige .....	419
Table 140 Troubleshooting the LAN LED .....	419
Table 141 Troubleshooting the DSL LED .....	420
Table 142 Troubleshooting the LAN Interface .....	420
Table 143 Troubleshooting the WAN Interface .....	420
Table 144 Troubleshooting Internet Access .....	421
Table 145 Troubleshooting the Password .....	421
Table 146 Troubleshooting the Web Configurator .....	422
Table 147 Troubleshooting Remote Management .....	422
Table 148 Troubleshooting Telephone .....	423
Table 149 Prestige 2602HW Series Power Adaptor Specifications .....	427
Table 150 Classes of IP Addresses .....	441
Table 151 Allowed IP Address Range By Class .....	442
Table 152 "Natural" Masks .....	442
Table 153 Alternative Subnet Mask Notation .....	443
Table 154 Two Subnets Example .....	443
Table 155 Subnet 1 .....	444
Table 156 Subnet 2 .....	444
Table 157 Subnet 1 .....	445
Table 158 Subnet 2 .....	445
Table 159 Subnet 3 .....	445
Table 160 Subnet 4 .....	446
Table 161 Eight Subnets .....	446
Table 162 Class C Subnet Planning .....	446
Table 163 Class B Subnet Planning .....	447
Table 164 Comparison of EAP Authentication Types .....	458
Table 165 Abbreviations Used in the Example Internal SPTGEN Screens Table ..	465
Table 166 Menu 1 General Setup (SMT Menu 1) .....	466
Table 167 Menu 3 (SMT Menu 3) .....	466

Table 168 Menu 4 Internet Access Setup (SMT Menu 4)	469
Table 169 Menu 12 (SMT Menu 12)	471
Table 170 Menu 15 SUA Server Setup (SMT Menu 15)	475
Table 171 Menu 21.1 Filter Set #1 (SMT Menu 21.1)	477
Table 172 Menu 21.1 Filer Set #2, (SMT Menu 21.1)	480
Table 173 Menu 23 System Menus (SMT Menu 23)	485
Table 174 Menu 24.11 Remote Management Control (SMT Menu 24.11)	486
Table 175 Command Examples	486
Table 176 Sys Firewall Commands	491
Table 177 System Maintenance Logs	495
Table 178 System Error Logs	496
Table 179 Access Control Logs	496
Table 180 TCP Reset Logs	497
Table 181 Packet Filter Logs	497
Table 182 ICMP Logs	497
Table 183 CDR Logs	498
Table 184 PPP Logs	498
Table 185 UPnP Logs	499
Table 186 Content Filtering Logs	499
Table 187 Attack Logs	499
Table 188 802.1X Logs	500
Table 189 ACL Setting Notes	501
Table 190 ICMP Notes	501
Table 191 Syslog Logs	502
Table 192 SIP Logs	502
Table 193 RTP Logs	503
Table 194 FSM Logs: Caller Side	503
Table 195 FSM Logs: Callee Side	503
Table 196 Lifeline Logs	503
Table 197 RFC-2408 ISAKMP Payload Types	504



# Preface

Congratulations on your purchase of the Prestige 2602HW Series ADSL VoIP IAD with 802.11g Wireless.

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

Your Prestige is easy to install and configure.

## About This User's Guide

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

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

## Related Documentation

- Supporting Disk

Refer to the included CD for support documents.

- Quick Start Guide

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

- Web Configurator Online Help

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

- ZyXEL Glossary and Web Site

Please refer to [www.zyxel.com](http://www.zyxel.com) for an online glossary of networking terms and additional support documentation.










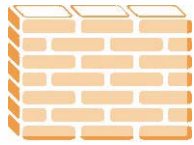

## User Guide Feedback

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 predefined choices.
- The SMT menu titles and labels are in **Bold Times New Roman** font. Predefined field choices are in **Bold Arial** font. Command and arrow keys are enclosed in square brackets. [ENTER] means the Enter, or carriage return key; [ESC] means the Escape key and [SPACE BAR] means the Space Bar.
- Mouse action sequences are denoted using a comma. For example, “click the Apple icon, **Control Panels** and then **Modem**” means first click the Apple icon, then point your mouse pointer to **Control Panels** and then click **Modem**.
- For brevity's sake, we will use “e.g.,” as a shorthand for “for instance”, and “i.e.,” for “that is” or “in other words” throughout this manual.
- The Prestige 2602HW series may be referred to as the Prestige in this user's guide. This refers to both models (ADSL over POTS and ADSL over ISDN) unless specifically identified.

## Graphics Icons Key

Prestige 	Computer 	Notebook Computer 
Server 	Switch 	Router 
Telephone 	DSLAM 	Trunking Gateway 
Firewall 	Wireless Signal 	

# Introduction to DSL

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

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

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

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

### **Introduction to ADSL**

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



# CHAPTER 1

## Getting To Know Your Prestige

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

### 1.1 Introducing the Prestige

The Prestige P2602HW ADSL VoIP IAD (Integrated Access Device) combines high-speed ADSL Internet access, a 4-port Ethernet switch, IEEE 802.11g wireless access, and Voice over IP (VoIP) communication capabilities. It is ideal for small networks.

VoIP is the sending of voice signals over the Internet. The Prestige lets you use a traditional analog telephone for VoIP calls. You can call any landline or mobile telephone as well as IP telephones (depending on your VoIP service provider). Calls received from IP telephones work exactly as you would expect from the traditional telephone service. The Prestige uses SIP (Session Initiated Protocol), an internationally recognized standard for implementing VoIP.

**Note:** The Prestige is ideal for high-speed Internet browsing and making LAN-to-LAN connections to remote networks. The Prestige is an ADSL router compatible with the ADSL/ADSL2/ADSL2+ standards. Maximum data rates attainable by the Prestige for each standard are shown in the next table.

**Table 1** ADSL Standards

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

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

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

Three Prestige models are included in this user's guide at the time of writing. In the Prestige product name, "H" denotes an integrated 4-port switch (hub) and "W" denotes an internal wireless card. The Prestige 2602HW provides 802.11g wireless LAN connectivity allowing users to enjoy the convenience and mobility of working anywhere within the coverage area.

**Note:** Models ending in “1”, for example Prestige 2602HW-61, denote a device that works over the analog telephone system, POTS (Plain Old Telephone Service). Models ending in “3” denote a device that works over ISDN (Integrated Synchronous Digital System). Models ending in “7” denote a device that works over T-ISDN (UR-2).

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

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

## 1.2 Prestige 2602HW-L with Lifeline

The Prestige 2602HW-L has all of the features of the Prestige 2602HW 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 of the Prestige

The following sections describe the features of the Prestige.

### PSTN Lifeline

The Prestige 2602HW-L has a **LINE** port for connecting 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 2602HW-L loses power.

### REN

A Ringer Equivalence Number is used to determine the number of devices that may be connected to the telephone line. The Prestige can support three devices per telephone port.

### 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.

### VoIP Standards Compliance

The Prestige complies with the following VoIP standards.

- SIP version 2 (RFC 3261)
- SDP (RFC 2327)
- RTP (RFC 1889)
- RTCP (RFC 1890)

## Multiple SIP Accounts

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

## 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 “silent packets” when you are not speaking.

## Comfort Noise Generation

When the Prestige uses VAD, it generates and sends comfort (background) noise when you are not speaking.

## 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.

## SIP ALG

The Prestige 2602HW is a SIP Application Layer Gateway (ALG). It allows VoIP calls to pass through NAT.

## Auto-provisioning

Auto-provisioning automatically updates your Prestige's configurable settings via a TFTP server.

## High Speed Internet Access

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

## Zero Configuration Internet Access

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

## Any IP

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

## Firewall

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

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

## IPSec VPN Capability

Establish a Virtual Private Network (VPN) to connect with business partners and branch offices using data encryption and the Internet to provide secure communications without the expense of leased site-to-site lines. The Prestige VPN is based on the IPSec standard and is fully interoperable with other IPSec-based VPN products.

The Prestige supports up to 20 simultaneous IPSec connections.

## Content Filtering

Content filtering allows you to block access to Internet web sites that contain key words (that you specify) in the URL. You can also schedule when the Prestige should perform the filtering and give trusted LAN IP addresses unfiltered Internet access.

## IEEE 802.11g Wireless LAN

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

**Table 2** IEEE 802.11g

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

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

## External Antenna

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

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

## Wireless LAN MAC Address Filtering

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

## WEP Encryption

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

## Wi-Fi Protected Access

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

## **Traffic Redirect**

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

## **Universal Plug and Play (UPnP)**

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

## **PPPoE Support (RFC2516)**

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

## **Network Address Translation (NAT)**

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

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

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

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

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

## **Dynamic DNS Support**

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

## **Multiple PVC (Permanent Virtual Circuits) Support**

Your Prestige supports up to 8 PVC's.

## ADSL Standards

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

## Protocol Support

- DHCP Support

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

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

## IP Alias

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

## IP Policy Routing (IPPR)

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

## Networking Compatibility

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

## Multiplexing

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

## Encapsulation

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

## Network Management

- Menu driven SMT (System Management Terminal) management
- Embedded web configurator
- CLI (Command Line Interpreter)
- Remote Management via Telnet or Web
- SNMP manageable
- DHCP Server/Client/Relay
- Built-in Diagnostic Tools
- Syslog
- Telnet Support (Password-protected telnet access to internal configuration manager)
- TFTP/FTP server, firmware upgrade and configuration backup/support supported
- Supports OAM F4/F5 loop-back, AIS and RDI OAM cells

## Other PPPoE Features

- PPPoE idle time out
- PPPoE dial on demand

## Diagnostics Capabilities

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

- FLASH memory



- ADSL circuitry
- RAM
- LAN port

### **Packet Filters**

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

### **Ease of Installation**

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

### **Housing**

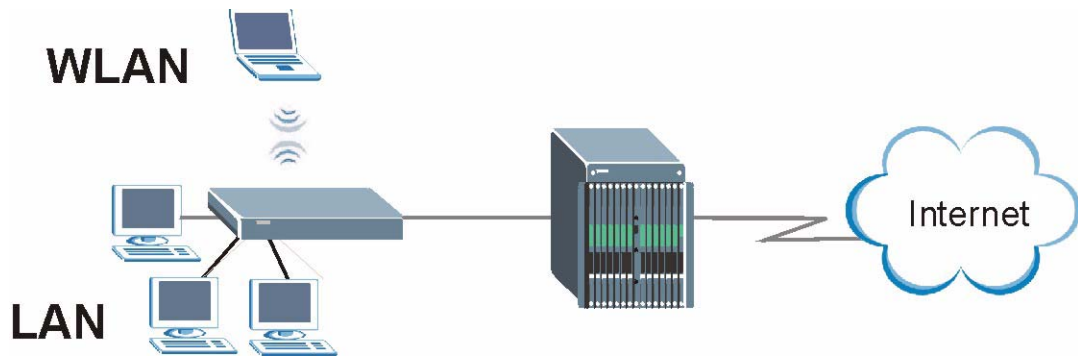
Your Prestige's compact and ventilated housing minimizes space requirements making it easy to position anywhere in your busy office.

## **1.4 Applications for the Prestige**

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

### **1.4.1 Internet Access**

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

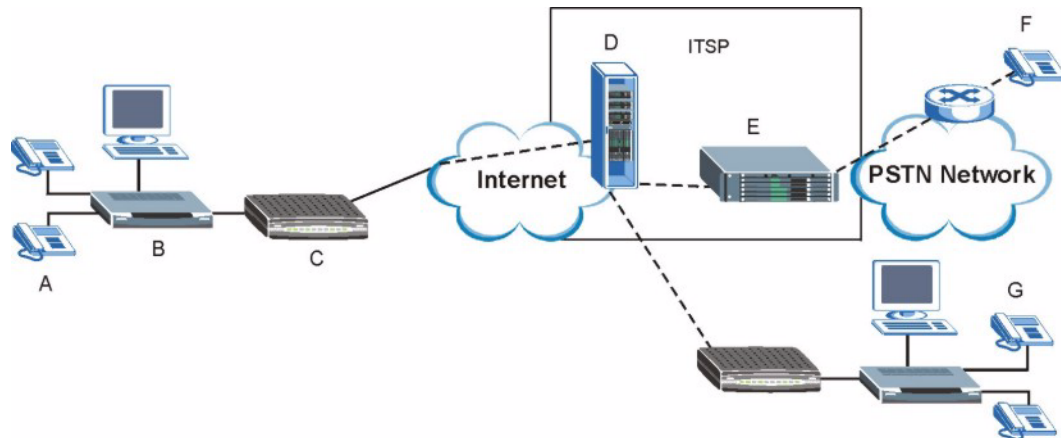
**Figure 1** Prestige Internet Access Application**Internet Single User Account**

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

**1.4.2 Making Calls via Internet Telephony Service Provider**

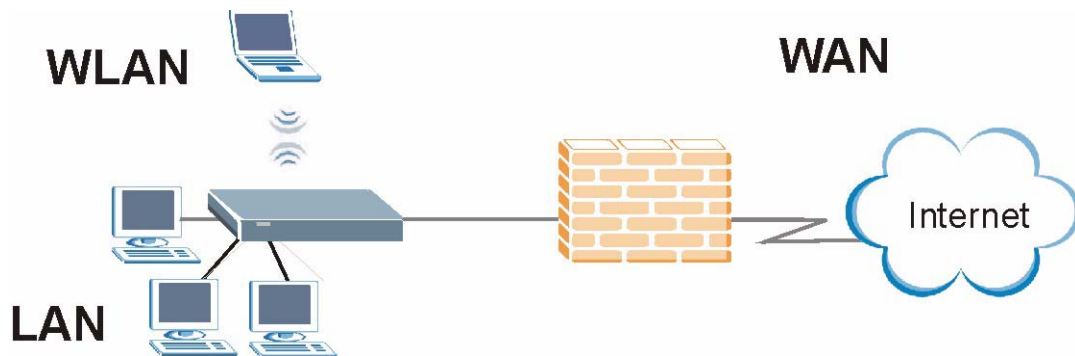
In a home or small office environment, you can use the Prestige to make and receive VoIP telephone calls through an Internet Telephony Service Provider (ITSP).

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. 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

### 1.4.3 Firewall for Secure Broadband Internet Access

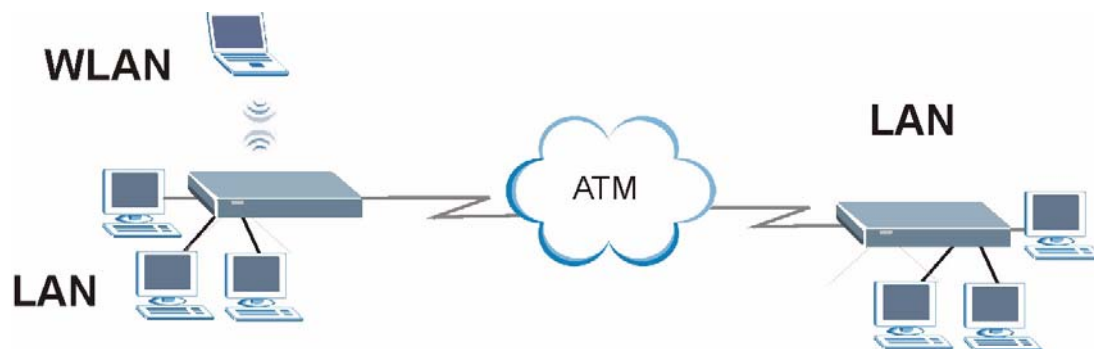
The Prestige provides protection from attacks by Internet hackers. By default, the firewall blocks all incoming traffic from the WAN. The firewall supports TCP/UDP inspection and DoS (Denial of Services) detection and prevention, as well as real time alerts, reports and logs.

**Figure 3** Firewall Application

### 1.4.4 LAN to LAN Application

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

**Figure 4** Prestige LAN-to-LAN Application



## 1.5 Prestige Hardware Installation and Connection

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

# CHAPTER 2

## Introducing the Web Configurator

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

### 2.1 Web Configurator Overview

The embedded web configurator allows you to manage the Prestige from anywhere through a browser such as Microsoft Internet Explorer or Netscape Navigator. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions with JavaScript enabled. It is recommended that you set your screen resolution to 1024 by 768 pixels

#### 2.1.1 Accessing the Prestige Web Configurator

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

**Figure 5** Password Screen



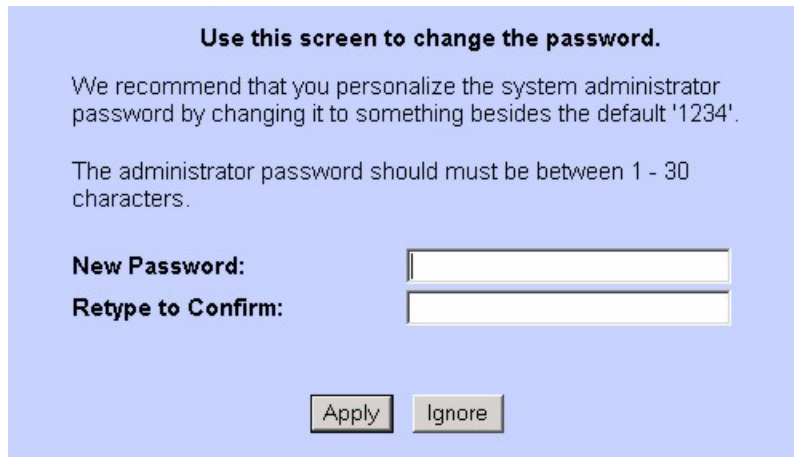
Prestige 2602HW-61

Enter Password and click Login.

Password:

Login Cancel

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

**Figure 6** Change Password at Login

**Use this screen to change the password.**

We recommend that you personalize the system administrator password by changing it to something besides the default '1234'.

The administrator password should must be between 1 - 30 characters.

**New Password:**

**Retype to Confirm:**

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

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

## 2.1.2 Resetting the Prestige

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

### 2.1.2.1 Using The Reset Button

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

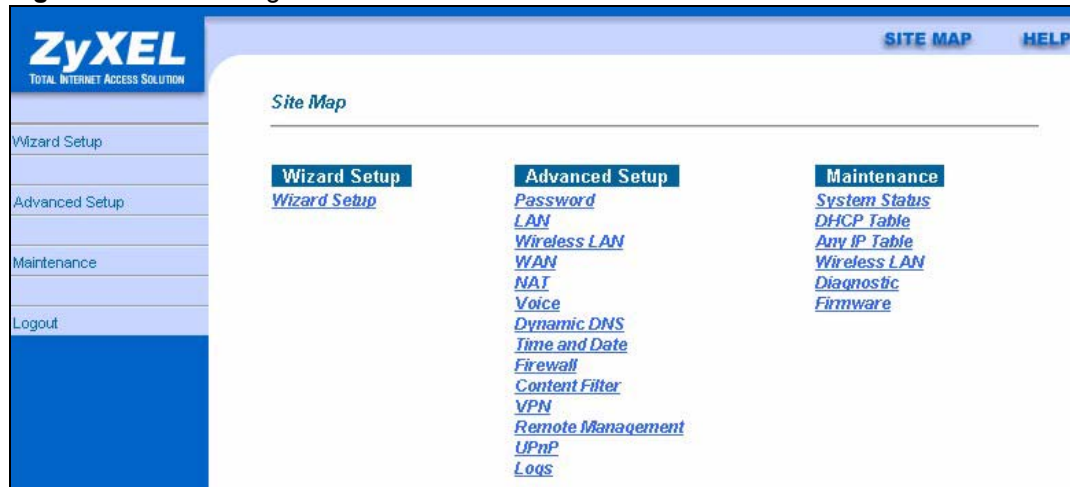
## 2.1.3 Navigating the Prestige Web Configurator

The following summarizes how to navigate the web configurator from the **SITE MAP** screen. We use the Prestige 2602HW-61 web screens in this guide as an example. Screens vary slightly for different Prestige models.

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

- Click **Logout** in the navigation panel when you have finished a Prestige management session.

**Figure 7** Web Configurator SITE MAP Screen



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

**Table 3** Web Configurator Screens Summary

LINK	SUB-LINK	FUNCTION
Wizard Setup	Wizard Setup	Use these screens for initial configuration including general setup, ISP parameters for Internet Access and WAN IP/DNS Server/MAC address assignment.
Advanced Setup		
Password		Use this screen to change your password.
LAN		Use this screen to configure LAN DHCP and TCP/IP settings.
Wireless LAN	Wireless	Use this screen to configure the wireless LAN settings.
	MAC Filter	Use this screen to change MAC filter settings on the Prestige
	802.1X	Use this screen to configure the Prestige's WLAN authentication settings
	Local User Database	Use this screen to set up built-in user profiles for wireless client authentication.
	RADIUS	Configure this screen to use an external server to authenticate wireless clients.
WAN	WAN Setup	Use this screen to change the Prestige's WAN remote node settings.
	WAN Backup	Use this screen to configure your traffic redirect properties and WAN backup settings.
NAT	SUA Only	Use this screen to configure servers behind the Prestige.
	Full Feature	Use this screen to configure network address translation mapping rules.

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

LINK	SUB-LINK	FUNCTION
Voice	SIP Settings	Use this screen to configure your Prestige's Session Initiation Protocol settings.
	QoS	Use this screen to configure your Prestige's Quality of Service settings.
	Phone	Use this screen to configure your Prestige's phone settings.
	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 2602HW-L only).
	Common	Use this screen to configure general phone port settings.
Dynamic DNS		Use this screen to set up dynamic DNS.
Time and Date		Use this screen to change your Prestige's time and date.
Firewall	Default Policy	Use this screen to activate/deactivate the firewall and the direction of network traffic to which to apply the rule.
	Rule Summary	This screen shows a summary of the firewall rules, and allows you to edit/add a firewall rule.
	Anti Probing	Use this screen to change your anti-probing settings.
	Threshold	Use this screen to configure the threshold for DoS attacks.
Content Filter	Keyword	Use this screen to block sites containing certain keywords in the URL.
	Schedule	Use this screen to set the days and times for the Prestige to perform content filtering.
	Trusted	Use this screen to exclude a range of users on the LAN from content filtering on your Prestige.
VPN	Setup	Use this screen to configure VPN connections and view the rule summary.
	Monitor	Use this screen to display and manage active VPN connections.
	Global Setting	Use this screen to allow NetBIOS packets through the VPN connections.
Remote Management		Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet/FTP/Web to manage the Prestige.
UPnP		Use this screen to enable UPnP on the Prestige.
Logs	Log Settings	Use this screen to change your Prestige's log settings.
	View Log	Use this screen to view the logs for the categories that you selected.
Maintenance		
System Status		This screen contains administrative and system-related information.
DHCP Table		This screen displays DHCP (Dynamic Host Configuration Protocol) related information and is READ-ONLY.
Any IP Table		This screen lists the devices that are using the Any IP feature to communicate with the Prestige.



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

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



# CHAPTER 3

## Wizard Setup

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

### 3.1 Wizard Setup Introduction

Use the Wizard Setup screens to configure your system for Internet access and Voice with the information provided by your ISP and voice service provider. Your ISP may have already configured some of the fields in the wizard screens for you.

#### 3.1.1 Encapsulation

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

##### 3.1.1.1 ENET ENCAP

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

##### 3.1.1.2 PPP over Ethernet

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

##### 3.1.1.3 PPPoA

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

### 3.1.1.4 RFC 1483

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

## 3.1.2 Multiplexing

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

### 3.1.2.1 VC-based Multiplexing

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

### 3.1.2.2 LLC-based Multiplexing

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

## 3.1.3 VPI and VCI

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

## 3.1.4 Internet Access Wizard Setup: First Screen

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

**Figure 8** Internet Access Wizard Setup: First Screen

The screenshot shows a configuration window titled "Connection Setup- ISP Parameters for Internet Access". It contains the following fields and values:

- Mode:** Routing
- Encapsulation:** ENET ENCAP
- Multiplex:** LLC
- Virtual Circuit ID:**
  - VPI: 8
  - VCI: 35
- Next:** A button at the bottom right.

The following table describes the fields in this screen.

**Table 4** Internet Access Wizard Setup: First Screen

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

## 3.2 IP Address and Subnet Mask

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

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

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

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

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

### 3.2.1 IP Address Assignment

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

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

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

#### 3.2.1.2 IP Assignment with RFC 1483 Encapsulation

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

#### 3.2.1.3 IP Assignment with ENET ENCAP Encapsulation

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

### 3.2.1.4 Private IP Addresses

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

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

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

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

### 3.2.2 Nailed-Up Connection (PPP)

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

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

### 3.2.3 NAT

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

### 3.2.4 Internet Access Wizard Setup: Second Screen

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

**Figure 9** Internet Connection with PPPoE

The following table describes the fields in this screen.

**Table 5** Internet Connection with PPPoE

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



**Figure 10** Internet Connection with RFC 1483

*Connection Setup- ISP Parameters for Internet Access*

---

IP Address

**Network Address Translation**  
 ▾

---

The following table describes the fields in this screen.

**Table 6** Internet Connection with RFC 1483

LABEL	DESCRIPTION
IP Address	This field is available if you select <b>Routing</b> in the <b>Mode</b> field. Type your ISP assigned IP address in this field.
Network Address Translation	Select <b>None</b> , <b>SUA Only</b> or <b>Full Feature</b> from the drop-down list box. Refer to <a href="#">Chapter 8 on page 119</a> for more details.
Back	Click <b>Back</b> to go back to the first wizard screen.
Next	Click <b>Next</b> to continue to the next wizard screen.

**Figure 11** Internet Connection with ENET ENCAP

*Connection Setup- ISP Parameters for Internet Access*

---

**IP Address**

Obtain an IP Address Automatically

Static IP Address

IP Address

Subnet Mask

ENET ENCAP Gateway

**Network Address Translation**  
 ▾

---

The following table describes the fields in this screen.

**Table 7** Internet Connection with ENET ENCAP

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

**Figure 12** Internet Connection with PPPoA

*Connection Setup- ISP Parameters for Internet Access*

---

User Name

Password

**IP Address**

Obtain an IP Address Automatically

Static IP Address

**Connection**

Connect on Demand: Max Idle Timeout  sec

Nailed-Up Connection

**Network Address Translation**

▼

---

The following table describes the fields in this screen.

**Table 8** Internet Connection with PPPoA

LABEL	DESCRIPTION
User Name	Enter the login name that your ISP gives you.
Password	Enter the password associated with the user name above.
IP Address	This option is available if you select <b>Routing</b> in the <b>Mode</b> field. A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Click <b>Obtain an IP Address Automatically</b> if you have a dynamic IP address; otherwise click <b>Static IP Address</b> and type your ISP assigned IP address in the IP Address text box below.
Connection	Select <b>Connect on Demand</b> when you don't want the connection up all the time and specify an idle time-out (in seconds) in the <b>Max. Idle Timeout</b> field. The default setting selects <b>Connection on Demand</b> with 0 as the idle time-out, which means the Internet session will not timeout. Select <b>Nailed-Up Connection</b> when you want your connection up all the time. The Prestige will try to bring up the connection automatically if it is disconnected. The schedule rule(s) in SMT menu 26 has priority over your <b>Connection</b> settings.
Network Address Translation	This option is available if you select <b>Routing</b> in the <b>Mode</b> field. Select <b>None</b> , <b>SUA Only</b> or <b>Full Feature</b> from the drop-down list box. Refer to <a href="#">Chapter 8 on page 119</a> for more details.
Back	Click <b>Back</b> to go back to the first wizard screen.
Next	Click <b>Next</b> to continue to the next wizard screen.

## 3.2.5 SIP Identities

A SIP account's Uniform Resource Identifier (URI) identifies the SIP account in a way similar to the way an e-mail address identifies an e-mail account. It is also known as a SIP identity or address. The format of a SIP identity is SIP-Number@SIP-Service-Domain.

### 3.2.5.1 SIP Number

A SIP number is the part of the SIP URI that comes before the "@" symbol. For example, if 1122334455@VoIP-provider.com was your SIP URI, "1122334455" would be your SIP number.

### 3.2.5.2 SIP Service Domain

A SIP service domain is the domain name that comes after the @ symbol in a SIP URI. For example, if 1122334455@VoIP-provider.com was your SIP URI, "VoIP-provider.com" is the SIP service domain.

## 3.2.6 Internet Access Wizard Setup: Third Screen

Use this screen to configure the voice settings (for the Prestige's SIP account one) with the information in the Voice Account Information table.

**Figure 13** Internet Access Wizard Setup: Third Screen

The screenshot shows the 'Wizard Setup - Voice Configuration' screen for 'SIP Account :SIP1'. It is divided into three main sections:

- SIP Settings:** Includes a checked 'Active' checkbox, 'SIP Number' (ChangeMe), 'SIP Local Port' (5060), 'SIP Server Address' (192.168.1.33), 'SIP Server Port' (5060), 'REGISTER Server Address' (192.168.1.33), 'REGISTER Server Port' (5060), and 'SIP Service Domain' (192.168.1.33).
- Authentication:** Includes 'User-ID' (ChangeMe) and a masked 'Password' field.
- Caller ID:** Includes a checked 'Send Caller ID' checkbox.

At the bottom, there are 'Back' and 'Next' buttons.

**Table 9** Internet Access Wizard Setup: Voice Configuration

LABEL	DESCRIPTION
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 95 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 of the SIP server in this field. It doesn't matter whether the SIP server is a proxy, redirect or register server.
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 address in this field. <b>If you were not given a register server address, then enter the address from the SIP Server Address field again here.</b>
REGISTER Server Port	Enter the SIP register server's listening port for SIP in this field. <b>If you were not given a register server port, then enter the port from the SIP Server Port field again here.</b>
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.

**Table 9** Internet Access Wizard Setup: Voice Configuration (continued)

LABEL	DESCRIPTION
Authentication Password	Type the password associated with the user name above. You can use up to 95 ASCII Extended set characters.
Send 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.
Back	Click <b>Back</b> to go back to the previous screen.
Next	Click <b>Next</b> to continue to the next wizard screen.

### 3.2.7 DHCP Setup

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

#### 3.2.7.1 IP Pool Setup

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

### 3.2.8 Internet Access Wizard Setup: Fourth Screen

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

**Figure 14** Internet Access Wizard Setup: Fourth Screen

*Wizard Setup - ISP Parameters for Internet Access*

---

**WAN Information:**  
Mode: **Routing**  
Encapsulation: **RFC 1483**  
Multiplexing: **LLC**  
VPI/VCI: **8/35**  
IP Address : **0.0.0.0**  
Network Address Translation: **SUA Only**

**Voice Information:**  
Active : **Yes**  
SIP Number: **ChangeMe**  
SIP Local Port: **5060**  
SIP Server Address: **192.168.1.33**  
SIP Server Port: **5060**  
REGISTER Server Address: **192.168.1.33**  
REGISTER Server Port: **5060**  
SIP Service Domain: **192.168.1.33**  
Authentication User-ID: **ChangeMe**  
Authentication Password: **\*\*\*\*\***  
Caller ID: **Send Caller ID**

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

Change LAN Configuration

---

Save Settings

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

**Figure 15** Internet Access Wizard Setup: LAN Configuration

*Connection Setup- ISP Parameters for Internet Access*

LAN IP Address: 192.168.1.1

LAN Subnet Mask: 255.255.255.0

**DHCP**

DHCP Server: ON

Client IP Pool Starting Address: 192.168.1.33

Size of Client IP Pool: 32

Primary DNS Server: 0.0.0.0

Secondary DNS Server: 0.0.0.0

Back Finish

The following table describes the fields in this screen.

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

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

### 3.2.9 Internet Access Wizard Setup: Connection Test

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

**Figure 16** Internet Access Wizard Setup: Connection Tests

**Wizard Setup - ISP Parameters for Internet Access**

Your DSL Gateway is now configured. Your device is capable of testing your DSL service. The individual tests are listed below. Click "Start Diagnose" button if you want to test; otherwise, click "Return to Main Menu" button.

<b>LAN connections</b>		
Test your Ethernet Connection		<b>PASS</b>
<b>WAN connections</b>		
Test ADSL synchronization		<b>N/A</b>
Test ADSL(ATM OAM) loopback test		<b>N/A</b>
<b>Voice connections</b>		
Test Voice Registration		<b>N/A</b>

Start Diagnose      Return to Main Menu

### 3.2.9.1 Test Your Internet Connection

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



# CHAPTER 4

## Password Setup

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

### 4.1 Password Overview

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

#### 4.1.1 Configuring Password

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

**Figure 17** Password

*Password*

Old Password

New Password

Retype to confirm

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

Apply Cancel

The following table describes the fields in this screen.

**Table 11** Password

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



# CHAPTER 5

## LAN Setup

This chapter describes how to configure LAN settings.

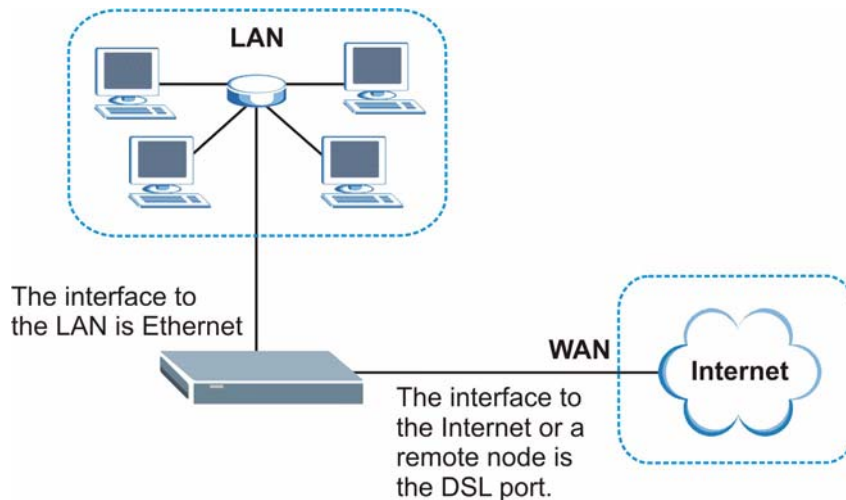
### 5.1 LAN Overview

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 and manage IP addresses.

#### 5.1.1 LANs, WANs and the Prestige

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

**Figure 18** LAN and WAN IP Addresses



## 5.2 DNS Server Address

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

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

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

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

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

## 5.3 DNS Server Address Assignment

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

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

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

## 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.

### 5.4.2 IP Address and Subnet Mask

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

### 5.4.3 RIP Setup

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

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

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

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

## 5.4.4 Multicast

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

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

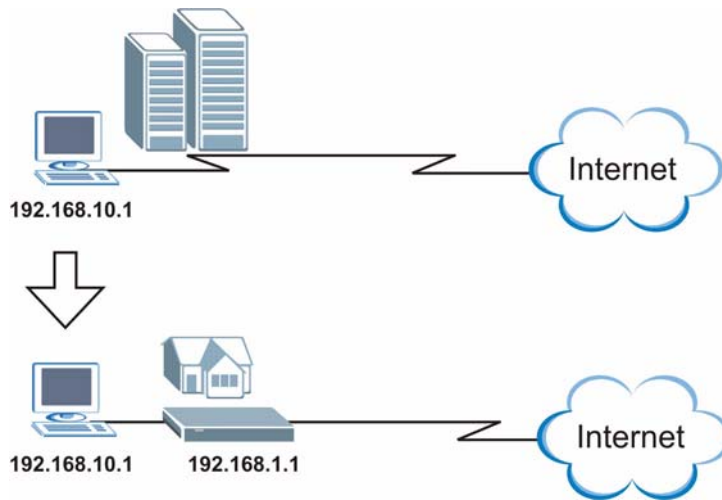
The Prestige supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the Prestige queries all directly connected networks to gather group membership. After that, the Prestige periodically updates this information. IP multicasting can be enabled/disabled on the Prestige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

## 5.5 Any IP

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

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

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

**Figure 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.

### 5.5.1 How Any IP Works

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

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

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

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

## 5.6 Configuring LAN

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

**Figure 20** LAN Setup

**LAN - LAN Setup**

**DHCP**

DHCP: Server

Client IP Pool Starting Address: 192.168.1.33

Size of Client IP Pool: 32

Primary DNS Server: 0.0.0.0

Secondary DNS Server: 0.0.0.0

Remote DHCP Server: N/A

**TCP/IP**

IP Address: 192.168.1.1

IP Subnet Mask: 255.255.255.0

RIP Direction: Both

RIP Version: RIP-1

Multicast: None

**Any IP Setup**

Active

Back Apply Cancel

The following table describes the fields in this screen.

**Table 12** LAN Setup

LABEL	DESCRIPTION
DHCP	
DHCP	<p>If set to <b>Server</b>, your Prestige can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client.</p> <p>If set to <b>None</b>, the DHCP server will be disabled.</p> <p>If set to <b>Relay</b>, the Prestige acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the <b>Remote DHCP Server</b> field in this case.</p> <p>When DHCP is used, the following items need to be set:</p>
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.



**Table 12** LAN Setup (continued)

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

## 5.7 Configuring Static DHCP

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

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

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

**Figure 21** LAN: Static DHCP

*LAN - Static DHCP*

#	MAC Address	IP Address
1	00:00:00:00:00:00	0.0.0.0
2	00:00:00:00:00:00	0.0.0.0
3	00:00:00:00:00:00	0.0.0.0
4	00:00:00:00:00:00	0.0.0.0
5	00:00:00:00:00:00	0.0.0.0
6	00:00:00:00:00:00	0.0.0.0
7	00:00:00:00:00:00	0.0.0.0
8	00:00:00:00:00:00	0.0.0.0
9	00:00:00:00:00:00	0.0.0.0
10	00:00:00:00:00:00	0.0.0.0

Back Apply Cancel

The following table describes the labels in this screen.

**Table 13** LAN: Static DHCP

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

# CHAPTER 6

## Wireless LAN Setup

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

### 6.1 Wireless LAN Introduction

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

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

#### 6.1.1 Additional Installation Requirements for Using IEEE 802.1x

- A computer with an IEEE 802.11b/g wireless LAN card and equipped with a web browser (with JavaScript enabled) and/or Telnet.
- A wireless station computer must be running IEEE 802.1x-compliant software. Currently, this is offered in Windows XP.
- An optional network RADIUS server for remote user authentication and accounting.

#### 6.1.2 Channel

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

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

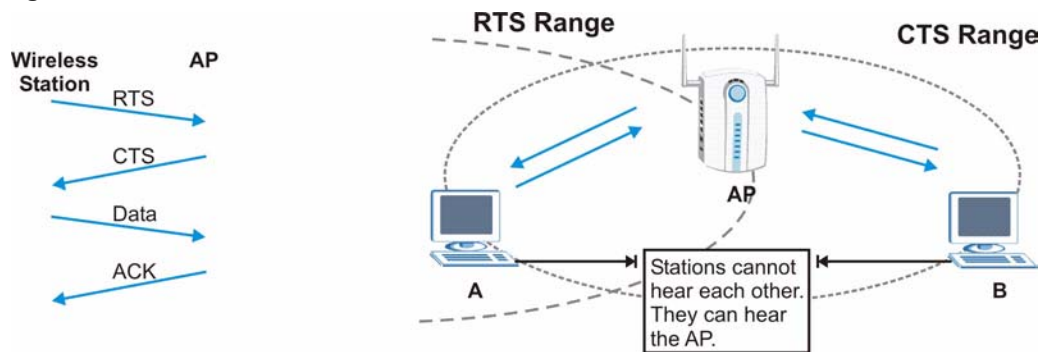
#### 6.1.3 ESS ID

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

## 6.1.4 RTS/CTS

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

**Figure 22** RTS/CTS



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

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

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

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

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

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

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

## 6.1.5 Fragmentation Threshold

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

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

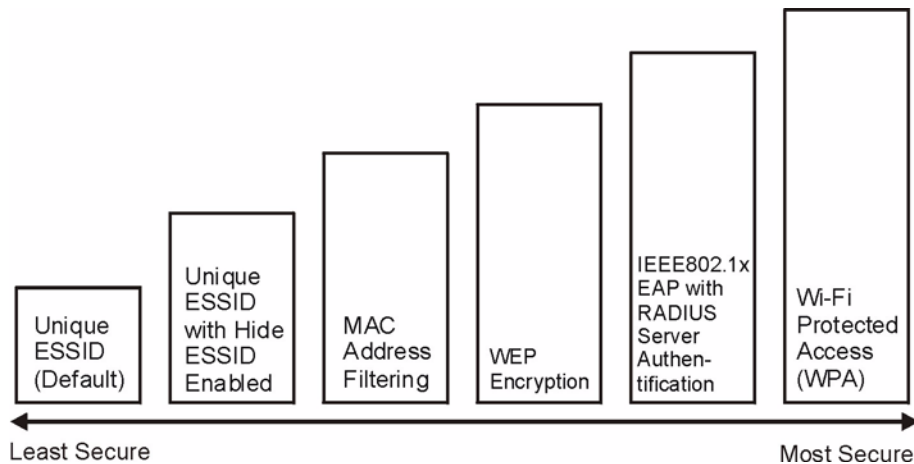
If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

## 6.2 Levels of Security

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

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

**Figure 23** Prestige Wireless Security Levels



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

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

## 6.3 Data Encryption with WEP

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

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

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

## 6.4 Configuring Wireless LAN

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

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

**Figure 24** Wireless LAN

**Wireless LAN- Wireless**

Enable Wireless LAN

ESSID

Hide ESSID

Channel ID

RTS/CTS Threshold  (0 ~ 2432)

Fragmentation Threshold  (256 ~ 2432)

WEP Encryption

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

Key1

Key2

Key3

Key4

The following table describes the fields in this screen.

**Table 14** Wireless LAN

LABEL	DESCRIPTION
Enable Wireless LAN	The wireless LAN is turned off by default, before you enable the wireless LAN you should configure some security by setting MAC filters and/or 802.1x security; otherwise your wireless LAN will be vulnerable upon enabling it. Select the check box to enable the wireless LAN.
ESSID	The ESSID (Extended Service Set Identification) is a unique name to identify the Prestige in the wireless LAN. Wireless stations associating to the Prestige must have the same ESSID. Enter a descriptive name (up to 32 characters).
Hide ESSID	Select <b>Yes</b> to hide the ESSID in so a station cannot obtain the ESSID through passive scanning. Select <b>No</b> to make the ESSID visible so a station can obtain the ESSID through passive scanning.
Channel ID	The radio frequency used by IEEE 802.11b wireless devices is called a channel. Select a channel from the drop-down list box.
RTS/CTS Threshold	The RTS (Request To Send) threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between 0 and 2432.
Fragmentation Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between 256 and 2432.

**Table 14** Wireless LAN (continued)

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

## 6.5 Configuring MAC Filter

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

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



**Figure 25** MAC Address Filter

*Wireless LAN- MAC Filter*

---

Active No ▾

Action Allow Association ▾

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

---

Back   Apply   Cancel

The following table describes the fields in this menu.

**Table 15** MAC Address Filter

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

**Table 15** MAC Address Filter (continued)

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

## 6.6 Network Authentication

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

### 6.6.1 EAP

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

#### 6.6.1.1 RADIUS

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

- Authentication  
Determines the identity of the users.
- Authorization  
Determines the network services available to authenticated users once they are connected to the network.
- Accounting  
Keeps track of the client's network activity.

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

#### 6.6.1.2 Types of RADIUS Messages

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

- Access-Request  
Sent by an access point requesting authentication.

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

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

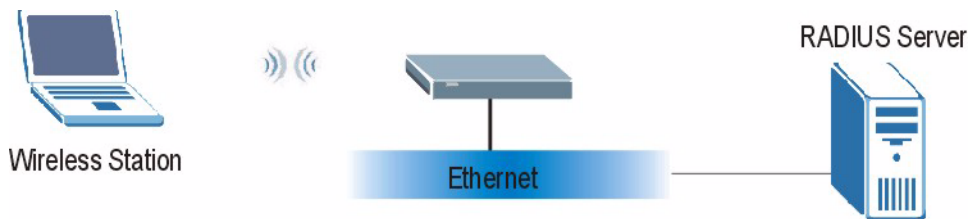
- **Accounting-Request**  
Sent by the access point requesting accounting.
- **Accounting-Response**  
Sent by the RADIUS server to indicate that it has started or stopped accounting.

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

## 6.6.2 EAP Authentication Overview

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

**Figure 26** EAP Authentication



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

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

- 3 The wireless station replies with identity information, including username and password.
- 4 The RADIUS server checks the user information against its user profile database and determines whether or not to authenticate the wireless station.

## 6.7 Introduction to WPA

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

### 6.7.1 User Authentication

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

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

### 6.7.2 Encryption

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

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

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

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

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

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

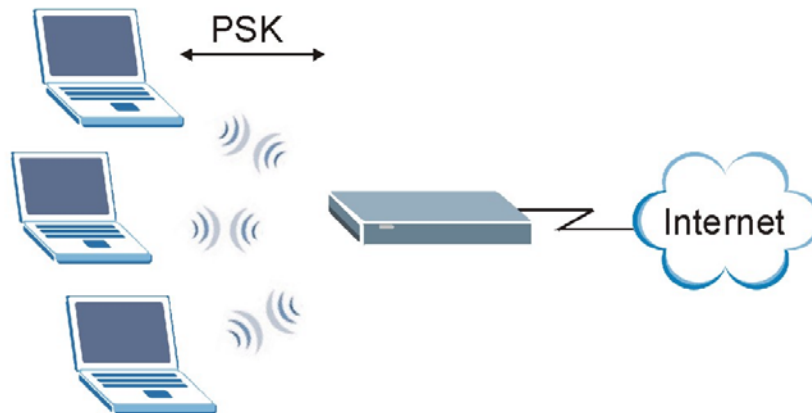
The encryption mechanisms used for WPA and WPA-PSK are the same. The only difference between the two is that WPA-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA-PSK susceptible to brute-force password-guessing attacks but it's still an improvement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

## 6.8 WPA-PSK Application Example

A WPA-PSK application looks as follows.

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

**Figure 27** WPA - PSK Authentication



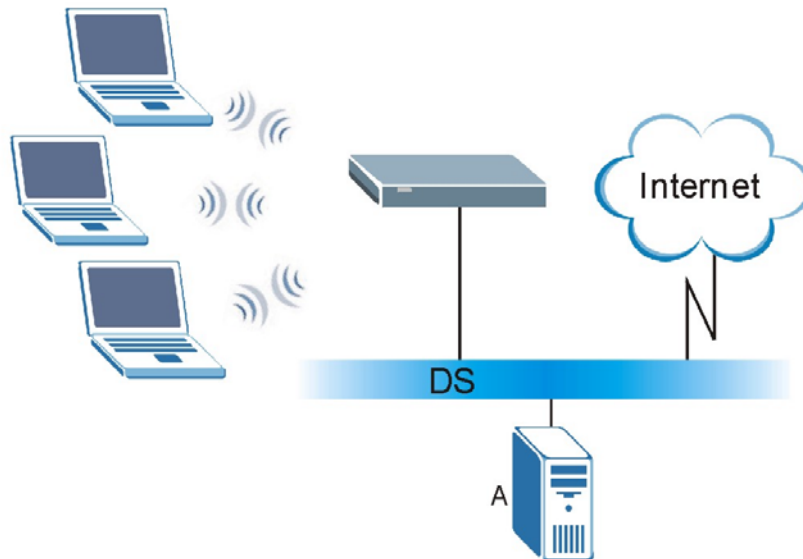
## 6.9 WPA with RADIUS Application Example

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

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

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

**Figure 28** WPA with RADIUS Application Example



## 6.10 Security Parameters Summary

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

**Table 16** Wireless Security Relational Matrix

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

**Table 16** Wireless Security Relational Matrix (continued)

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

## 6.11 Wireless Client WPA Supplicants

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

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

The Funk Software's Odyssey client is bundled free (at the time of writing) with the client wireless adaptor(s).

## 6.12 Configuring 802.1x and WPA

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

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

**Figure 29** Wireless LAN: 802.1x/WPA

The screenshot shows a configuration window titled "Wireless LAN - 802.1x/WPA". Below the title bar, there is a section labeled "802.1x Authentication". Inside this section, the text "Wireless Port Control" is followed by a dropdown menu that currently displays "No Authentication Required". At the bottom of the window, there are three buttons: "Back", "Apply", and "Cancel".

The following table describes the label in this screen.

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

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

### 6.12.1 Authentication Required: 802.1x

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

**Figure 30** Wireless LAN: 802.1x/WPA for 802.1x Protocol

*Wireless LAN - 802.1x/WPA*

---

**802.1x Authentication**

Wireless Port Control: Authentication Required

ReAuthentication Timer: 1800 (In Seconds)

Idle Timeout: 3600 (In Seconds)

---

Key Management Protocol: 802.1x

Dynamic WEP Key Exchange: Disable

---

Authentication Databases: Local User Database Only

---

Back    Apply    Cancel

The following table describes the labels in this screen.



**Table 18** Wireless LAN: 802.1x/WPA for 802.1x Protocol

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

**Table 18** Wireless LAN: 802.1x/WPA for 802.1x Protocol (continued)

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

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

### 6.12.2 Authentication Required: WPA

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

**Figure 31** Wireless LAN: 802.1x/WPA for WPA Protocol

*Wireless LAN - 802.1x/WPA*

---

**802.1x Authentication**

Wireless Port Control: Authentication Required

ReAuthentication Timer: 1800 (In Seconds)

Idle Timeout: 3600 (In Seconds)

---

Key Management Protocol: WPA

WPA Mixed Mode

Group Data Privacy: TKIP

WPA Group Key Update Timer: 1800 (In Seconds)

---

Authentication Databases: RADIUS Only

---

Back Apply Cancel

The following table describes the labels not previously discussed

**Table 19** Wireless LAN: 802.1x/WPA for WPA Protocol

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

### 6.12.3 Authentication Required: WPA-PSK

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

**Figure 32** Wireless LAN: 802.1x/WPA for WPA-PSK Protocol

The following table describes the labels not previously discussed.

**Table 20** Wireless LAN: 802.1x/WPA for WPA-PSK Protocol

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

## 6.13 Configuring Local User Authentication

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

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

**Figure 33** Local User Database

*Wireless LAN - Local User DataBase*

#	Active	User Name	Password
1	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
2	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
3	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
4	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
5	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
6	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
7	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
8	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
9	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
10	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
11	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
12	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
13	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
14	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
15	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
16	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
17	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
18	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
19	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
20	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
21	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
22	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
23	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
24	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
25	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
26	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
27	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
28	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
29	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
30	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
31	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
32	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

Back Apply Cancel

The following table describes the fields in this screen.

**Table 21** Local User Database

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

## 6.14 Configuring RADIUS

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

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

**Figure 34** RADIUS

The following table describes the fields in this screen.

**Table 22** RADIUS

LABEL	DESCRIPTION
Authentication Server	
Active	Select <b>Yes</b> from the drop-down list box to enable user authentication through an external authentication server.
Server IP Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port Number	The default port of the RADIUS server for authentication is <b>1812</b> . You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the access points. The key is not sent over the network. This key must be the same on the external authentication server and Prestige.
Accounting Server	
Active	Select <b>Yes</b> from the drop-down list box to enable user authentication through an external accounting server.
Server IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port Number	The default port of the RADIUS server for accounting is <b>1813</b> . You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the access points. The key is not sent over the network. This key must be the same on the external accounting server and the Prestige.
Back	Click <b>Back</b> to go to the main wireless LAN setup screen.
Apply	Click <b>Apply</b> to save these settings back to the Prestige.
Cancel	Click <b>Cancel</b> to begin configuring this screen again.





# CHAPTER 7

## WAN Setup

This chapter describes how to configure WAN settings.

### 7.1 WAN Overview

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

See [Chapter 3 on page 63](#) for more information on the fields in the WAN screens.

### 7.2 Metric

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

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

- Normal route: designated by the ISP (see [Section 7.6 on page 111](#))
- Traffic-redirect route (see [Section 7.7 on page 114](#))

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

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

IP Policy Routing overrides the default routing behavior and takes priority over all of the routes mentioned above (see [Chapter 40 on page 391](#)).

## 7.3 PPPoE Encapsulation

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

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

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

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

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

## 7.4 Traffic Shaping

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

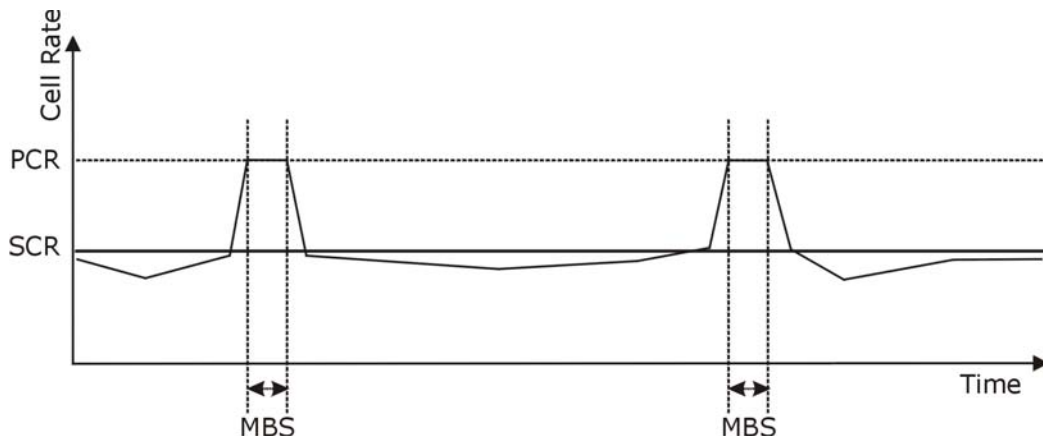
Peak Cell Rate (PCR) is the maximum rate at which the sender can send cells. This parameter may be lower (but not higher) than the maximum line speed. 1 ATM cell is 53 bytes (424 bits), so a maximum speed of 832Kbps gives a maximum PCR of 1962 cells/sec. This rate is not guaranteed because it is dependent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

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

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

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

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

**Figure 35** Example of Traffic Shaping

## 7.5 Zero Configuration Internet Access

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

Zero configuration for Internet access is disabled when

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

## 7.6 Configuring WAN Setup

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

**Figure 36** WAN Setup (PPPoE)

**WAN - WAN Setup**

---

**Name**

**Mode**

**Encapsulation**

**Multiplex**

**Virtual Circuit ID**

VPI

VCI

**ATM QoS Type**

**Cell Rate**

Peak Cell Rate  cell/sec

Sustain Cell Rate  cell/sec

Maximum Burst Size

**Login Information**

Service Name

User Name

Password

**IP Address**

Obtain an IP Address Automatically

Static IP Address

IP Address

**Connection**

Nailed-Up Connection

Connect on Demand

Max Idle Timeout  sec

**PPPoE Pass Through**

**Zero Configuration**

---

The following table describes the fields in this screen.

**Table 23** WAN Setup

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

**Table 23** WAN Setup (continued)

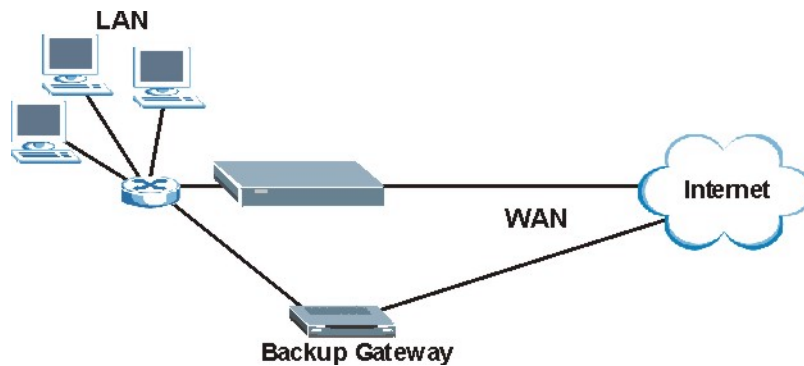
LABEL	DESCRIPTION
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. Choices vary depending on the mode you select in the <b>Mode</b> field. If you select <b>Bridge</b> in the <b>Mode</b> field, select either <b>PPPoA</b> or <b>RFC 1483</b> . If you select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

**Table 23** WAN Setup (continued)

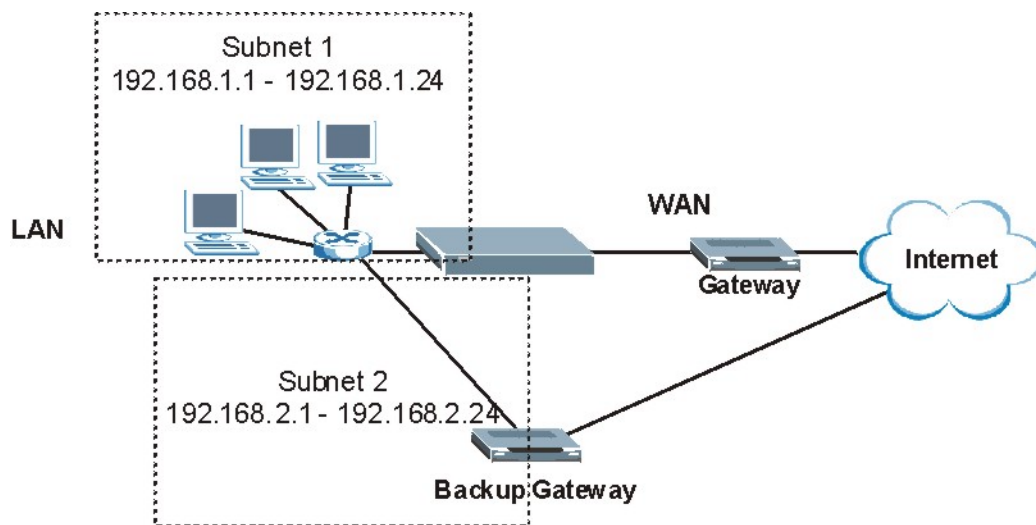
LABEL	DESCRIPTION
Connect on Demand	Select <b>Connect on Demand</b> when you don't want the connection up all the time and specify an idle time-out in the <b>Max Idle Timeout</b> field.
Max Idle Timeout	Specify an idle time-out in the <b>Max Idle Timeout</b> field when you select <b>Connect on Demand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

## 7.7 Traffic Redirect

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

**Figure 37** Traffic Redirect Example

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

**Figure 38** Traffic Redirect LAN Setup

## 7.8 Configuring WAN Backup

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

**Figure 39** WAN Backup

**WAN - WAN Backup Setup**

Backup Type: DSL Link

Check WAN IP Address1: 0.0.0.0

Check WAN IP Address2: 0.0.0.0

Check WAN IP Address3: 0.0.0.0

Fail Tolerance: 0

Recovery Interval: 0 sec

Timeout: 0 sec

**Traffic Redirect**

Active

Metric: 15

Backup Gateway: 0.0.0.0

Back Apply Cancel

The following table describes the fields in this screen.

**Table 24** WAN Backup

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



**Table 24** WAN Backup (continued)

LABEL	DESCRIPTION
Timeout	Type the number of seconds (3 recommended) for your Prestige to wait for a ping response from one of the IP addresses in the <b>Check WAN IP Address</b> field before timing out the request. The WAN connection is considered "down" after the Prestige times out the number of times specified in the <b>Fail Tolerance</b> field. Use a higher value in this field if your network is busy or congested.
Traffic Redirect	
Active	Select this check box to have the Prestige use traffic redirect if the normal WAN connection goes down.  <b>Note:</b> If you activate traffic redirect, you must configure at least one Check WAN IP Address.
Metric	This field sets this route's priority among the routes the Prestige uses. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".
Backup Gateway	Type the IP address of your backup gateway in dotted decimal notation. The Prestige automatically forwards traffic to this IP address if the Prestige's Internet connection terminates.
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save the changes.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.



# CHAPTER 8

## Network Address Translation (NAT) Screens

This chapter discusses how to configure NAT on the Prestige.

### 8.1 NAT Overview

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

#### 8.1.1 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 25** NAT Definitions

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

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

## 8.1.2 What NAT Does

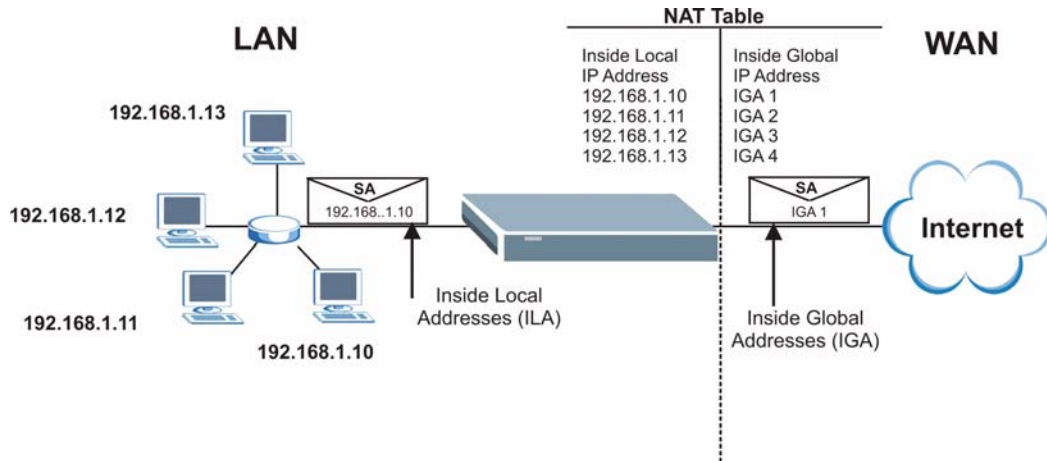
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address)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

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping – see [Table 26 on page 122](#)), 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)*.

## 8.1.3 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.

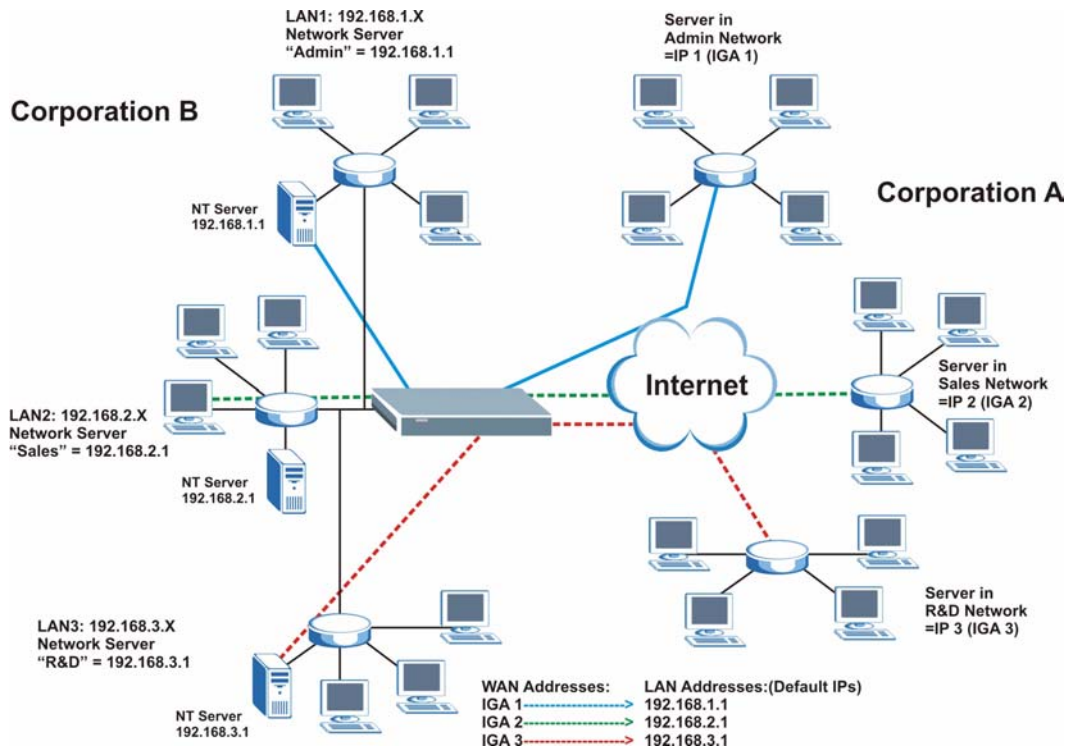
**Figure 40** How NAT Works



### 8.1.4 NAT Application

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

**Figure 41** NAT Application With IP Alias



### 8.1.5 NAT Mapping Types

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

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

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

The following table summarizes these types.

**Table 26** NAT Mapping Types

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

## 8.2 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. The Prestige also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types as outlined in [Table 26 on page 122](#).

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

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

## 8.3 SUA Server

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

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

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

### 8.3.1 Default Server IP Address

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

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

### 8.3.2 Port Forwarding: Services and Port Numbers

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

**Table 27** Services and Port Numbers

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

**Table 27** Services and Port Numbers (continued)

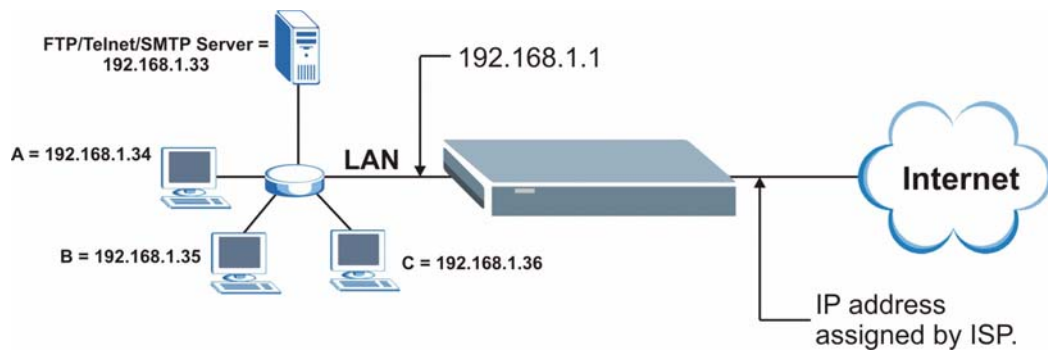
SERVICES	PORT NUMBER
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

### 8.3.3 Configuring Servers Behind SUA (Example)

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

IP address assigned by ISP.

**Figure 42** Multiple Servers Behind NAT Example



## 8.4 Selecting the NAT Mode

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

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



**Figure 43** NAT Mode

**NAT - Mode**

---

Network Address Translation

None

SUA Only [Edit Details](#)

Full Feature [Edit Details](#)

---

The following table describes the labels in this screen.

**Table 28** NAT Mode

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

## 8.5 Configuring SUA Server

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

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

Refer to [Table 27 on page 123](#) for port numbers commonly used for particular services.

**Figure 44** Edit SUA/NAT Server Set

*NAT - Edit SUA/NAT Server Set*

	Start Port No.	End Port No.	IP Address
1	All ports	All ports	0.0.0.0
2	0	0	0.0.0.0
3	0	0	0.0.0.0
4	0	0	0.0.0.0
5	0	0	0.0.0.0
6	0	0	0.0.0.0
7	0	0	0.0.0.0
8	0	0	0.0.0.0
9	0	0	0.0.0.0
10	0	0	0.0.0.0
11	0	0	0.0.0.0
12	0	0	0.0.0.0

The following table describes the fields in this screen.

**Table 29** Edit SUA/NAT Server Set

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

## 8.6 Configuring Address Mapping

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

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

**Figure 45** Address Mapping Rules

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

Back

The following table describes the fields in this screen.

**Table 30** Address Mapping Rules

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

**Table 30** Address Mapping Rules (continued)

LABEL	DESCRIPTION
Type	<p><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.</p> <p><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.</p> <p><b>M-M Ov (Overload):</b> Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses.</p> <p><b>MM No (No Overload):</b> Many-to-Many No Overload mode maps each local IP address to unique global IP addresses.</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>
Back	Click <b>Back</b> to return to the <b>NAT Mode</b> screen.

## 8.7 Editing an Address Mapping Rule

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

**Figure 46** Address Mapping Rule Edit

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

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

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

The following table describes the fields in this screen.

**Table 31** Address Mapping Rule Edit

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



# CHAPTER 9

## Introduction to VoIP

This chapter provides background information on VoIP and SIP.

### 9.1 Introduction to VoIP

VoIP 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.

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.

### 9.2 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.

#### 9.2.1 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.

##### 9.2.1.1 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).

### 9.2.1.2 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.

### 9.2.2 SIP Call Progression

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

**Table 32** SIP Call Progression

<b>A</b>		<b>B</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.

### 9.2.3 SIP Servers

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.

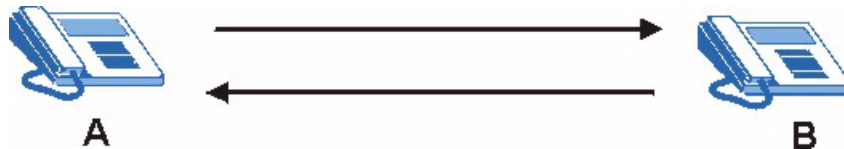
When you use SIP to make a VoIP call, it originates at a client and terminates at a server. A SIP client could be a computer or a SIP phone. One device can act as both a SIP client and a SIP server.



### 9.2.3.1 SIP User Agent Server

A SIP user agent server 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 server to receive the call.

**Figure 47** SIP User Agent Server

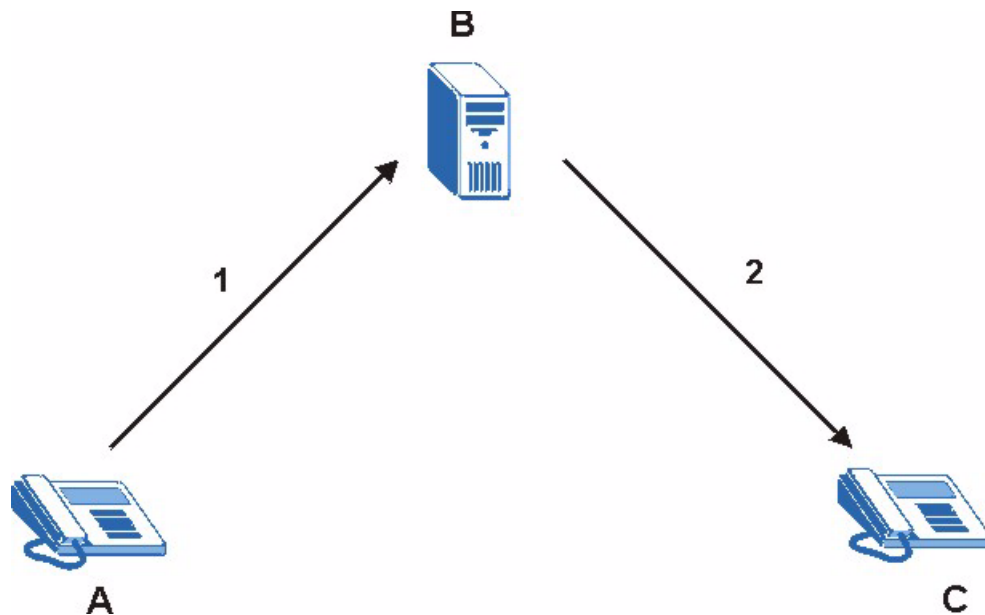


### 9.2.3.2 SIP Proxy Server

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.

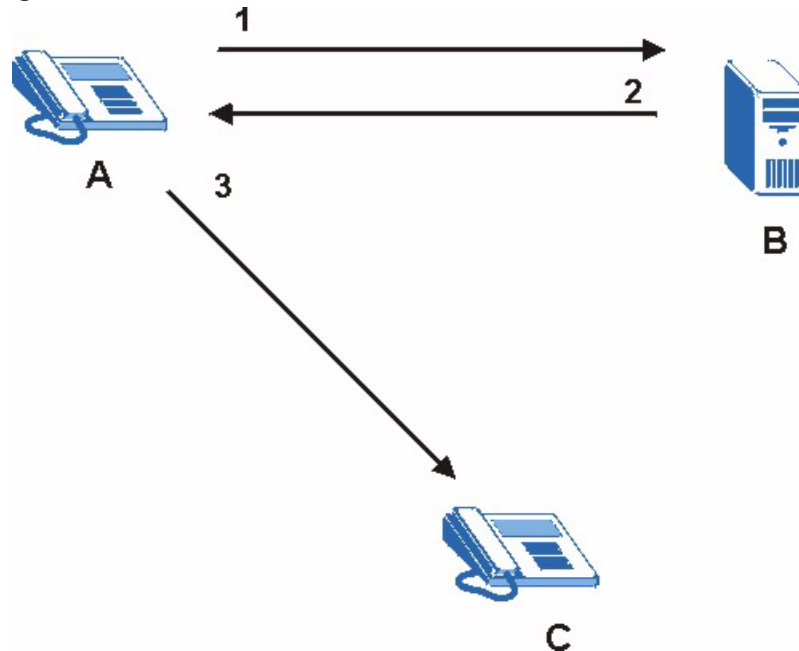
**Figure 48** SIP Proxy Server

### 9.2.3.3 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 49** SIP Redirect Server

#### 9.2.3.4 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.

#### 9.2.4 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.

### 9.3 SIP ALG

The Prestige 2602HW is a SIP Application Layer Gateway (ALG). A SIP ALG allows VoIP calls to pass through NAT by examining and translating IP addresses embedded in the data stream. When a VoIP device behind the Prestige registers with the SIP register server, the Prestige translates the device's private IP address inside the SIP data stream to a public IP address. You do not need to use STUN with a VoIP device that is behind the Prestige 2602HW.

### 9.4 Pulse Code Modulation

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

## 9.5 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.

### 9.5.1 G.711

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

### 9.5.2 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.

## 9.6 PSTN Call Setup Signaling

Dual-Tone MultiFrequency (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>

---

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

# CHAPTER 10

## Voice Screens

This chapter describes how to configure advanced VoIP, QoS, phone and phone book settings.

### 10.1 Voice Screens Introduction

This chapter covers the configuration of the **VoIP** screens.

### 10.2 SIP Settings Configuration

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

**Figure 50** SIP Settings

**Voice - SIP Settings** SIP Account : SIP1

**SIP Settings**

Active SIP

SIP Number

SIP Local Port  (1024-65535)

SIP Server Address

SIP Server Port  (1024-65535)

REGISTER Server Address

REGISTER Server Port  (1024-65535)

SIP Service Domain

**Authentication**

User-ID

Password

**Caller ID**  Send Caller ID

**Incoming Call apply to**  Phone1  Phone2

**Advanced Settings**

**Table 33** SIP Settings

LABEL	DESCRIPTION
SIP Account	You can configure the Prestige to use multiple SIP accounts. Select one to configure its settings on the Prestige.
Active SIP	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 95 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 of the SIP server in this field. It doesn't matter whether the SIP server is a proxy, redirect or register server.
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 address in this field. <b>If you were not given a register server address, then enter the address from the SIP Server Address field again here.</b>
REGISTER Server Port	Enter the SIP register server's listening port for SIP in this field. <b>If you were not given a register server port, then enter the port from the SIP Server Port field again here.</b>
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.
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.
Password	Type the password associated with the user name above. You can use up to 95 ASCII Extended set characters.
Send 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	<b>Phone 1</b> and <b>Phone 2</b> correspond to the Prestige's physical PHONE 1 and 2 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.
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save your changes back to the Prestige.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 10.3 Advanced Voice Settings Configuration

Click **Voice** in the navigation panel and then **SIP Settings** to open the **SIP Settings** screen. Select a SIP account and then click **Settings** to display the following screen.

**Figure 51** Voice Advanced Setup

*Voice - Advanced Setting*
**SIP Account :SIP1**

---

**SIP Server Settings**

URL Type

Expiration Duration  (20-65535) sec

Register Re-send timer  (1-65535) sec

Session Expires  (30-3600) sec

Min-SE  (20-1800) sec

**RTP Port Range**

From  (1025-65535)

To  (1025-65535)

**Others**

Preferred Compression Type

**Dual-Tone-Multi-Frequency**

DTMF Mode

---

The following table describes the labels in this screen.

**Table 34** Voice Advanced Setup

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 Resend 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.

**Table 34** Voice Advanced Setup (continued)

LABEL	DESCRIPTION
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.
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>
DTMF Mode	<p>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.</p> <p>Select <b>RFC 2833</b> to send the DTMF tones in RTP packets.</p> <p>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.</p> <p>Select <b>SIP INFO</b> to send the DTMF tones in SIP messages.</p>
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save your changes back to the Prestige.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 10.4 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.

### 10.4.1 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.



## 10.4.2 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>

### 10.4.2.1 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 52** 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.

## 10.4.3 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.

## 10.5 QoS Configuration

Click **Voice** in the navigation panel and then **Qos** to display the following screen.

---

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

**Figure 53** QoS

The following table describes the labels in this screen.

**Table 35** 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. Priorities 6 and 7 are reserved for network control traffic. It is recommended that you use priority 5 for SIP.
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. Priorities 6 and 7 are reserved for network control traffic. It is recommended that you use priority 5 for RTP.
Voice VLAN ID	<p>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.</p> <p>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.</p> <p>Disable VLAN tagging if the Prestige does not need to be a member of a VLAN group to communicate with the SIP server.</p>
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save your changes back to the Prestige.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 10.6 Phone

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.

## 10.6.1 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.

## 10.6.2 Comfort Noise Generation

When using VAD, the Prestige generates and sends comfort noise when you are not speaking. Comfort noise uses the lowest possible transmission bandwidth to match the background noise. The comfort noise lets the person at the other end of the connection know that the line is still connected (total silence would easily be mistaken for a lost connection).

## 10.6.3 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.

## 10.7 Phone Configuration

Click **Voice** in the navigation panel and then **Phone** to display the following screen.

**Figure 54** Phone

**Voice - Phone** Phone Port Settings: Phone1

**Voice Volume Control**

Speaking Volume: -1 (Min.)

Listening Volume: -1 (Min.)

**Outgoing Call use**

SIP1  SIP2

**Echo Cancellation**

G.168 Active

**Voice Active Detector**

VAD Support

**Dialing Interval**: 3

Back Apply Cancel

The following table describes the labels in this screen.

**Table 36** Phone

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	<p><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.</p> <p>You cannot call the SIP number of the SIP account that you are using to make a call. The Prestige generates a busy tone and does not attempt to establish a call if the SIP number you dial matches the outgoing SIP number of the phone port you are using.</p> <p>For example, if you set <b>Phone 1</b> to use SIP account 1 and set <b>Phone 2</b> to use SIP account 2, then you can use <b>Phone 1</b> to call to SIP account 2's SIP number or <b>Phone 2</b> to call to SIP account 1's SIP number.</p>
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) to reduce the bandwidth that a call uses. The Prestige will generate and send comfort noise when you are not talking.
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.
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save your changes back to the Prestige.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 10.8 Speed Dial

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

### 10.8.1 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 on the Prestige 2602HW in order to make a peer-to-peer VoIP call. You must still configure a SIP account on the Prestige 2602HW-L in order to make a peer-to-peer VoIP call.

## 10.9 Speed Dial Configuration

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

**Figure 55** Speed Dial

The screenshot shows the 'Voice - Speed Dial' configuration interface. It is divided into two main sections: 'Add New Entry' and 'Speed Dial Phone Book'.

**Add New Entry Section:**

Speed Dial	SIP Number	Name	Type	
#01			<input checked="" type="radio"/> Use Proxy <input type="radio"/> Non-Proxy (Use IP or URL)	Add

**Speed Dial Phone Book Section:**

Speed Dial	SIP Number	Name	Destination	
#01				Delete Edit
#02				Delete Edit
#03				Delete Edit
#04				Delete Edit
#05				Delete Edit
#06				Delete Edit
#07				Delete Edit
#08				Delete Edit
#09				Delete Edit
#10				Delete Edit

At the bottom of the 'Speed Dial Phone Book' section, there is a button labeled 'Clear' with the text 'Push Button to Clear Phone Book' above it.

The following table describes the labels in this screen.

**Table 37** 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.
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 95 ASCII characters.
Name	Enter a descriptive name to identify the party that you will use this entry to call. You can use up to 95 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.

**Table 37** Speed Dial (continued)

<b>LABEL</b>	<b>DESCRIPTION</b>
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.
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.
SIP Number	This is the SIP number of the party that you will call.
Name	This is the descriptive name of the party that you will use this speed dial entry to call.
Destination	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.

## 10.10 Lifeline (Prestige 2602HW-L)

With lifeline you can make and receive regular phone calls. Use a prefix number to make a regular call. When the Prestige 2602HW-L 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).

## 10.11 Lifeline Configuration (Prestige 2602HW-L)

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

**Figure 56** Lifeline

The following table describes the labels in this screen.

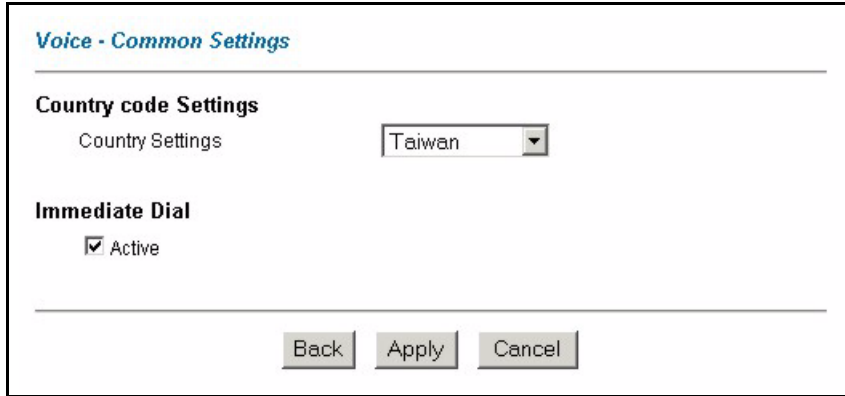
**Table 38** Lifeline

LABEL	DESCRIPTION
PSTN Pre-fix Number	Specify the prefix number for dialing regular calls when VoIP service is available.
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.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 10.12 Common Phone Port 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 57** Phone Port Common



The following table describes the labels in this screen.

**Table 39** Phone Port Common

LABEL	DESCRIPTION
Country Settings	Use the drop-down list box to select the country where your Prestige is located.
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).
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save your changes back to the Prestige.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.



# CHAPTER 11

## Dynamic DNS Setup

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

### 11.1 Dynamic DNS

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

First of all, you need to have registered a dynamic DNS account with [www.dyndns.org](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.

#### 11.1.1 DYNDNS Wildcard

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

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

### 11.2 Configuring Dynamic DNS

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

**Figure 58** Dynamic DNS

The following table describes the fields in this screen.

**Table 40** Dynamic DNS

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

# CHAPTER 12

## Time and Date

Use this screen to configure the Prestige's time and date settings.

### 12.1 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 41** 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

### 12.2 Configuring Time and Date

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

**Figure 59** Time and Date

The following table describes the fields in this screen.

**Table 42** Time and Date

LABEL	DESCRIPTION
Time Server	
Use Protocol when Bootup	Select the time service protocol that your time server sends when you turn on the Prestige. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main difference between them is the format. <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. <b>NTP (RFC 1305)</b> is similar to <b>Time (RFC 868)</b> . Select <b>None</b> to enter the time and date manually.
IP Address or URL	Enter the IP address or URL of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time and Date	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Select this option if you use daylight savings time. Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.

**Table 42** Time and Date (continued)

LABEL	DESCRIPTION
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> .
Synchronize system clock with Time Server now.	Select this option to have your Prestige use the time server (that you configured above) to set its internal system clock. Please wait for up to 60 seconds while the Prestige locates the time server. If the Prestige cannot find the time server, please check the time server protocol and its IP address. If the IP address was entered correctly, try pinging it for example to test the connection.
Date	
Current Date	This field displays the date of your Prestige. Each time you reload this page, the Prestige synchronizes the time with the time server.
New Date (yyyy-mm-dd)	This field displays the last updated date from the time server. When you select <b>None</b> in the <b>Use Protocol when Bootup</b> field, enter the new date in this field and then click <b>Apply</b> .
Time	
Current Time	This field displays the time of your Prestige. Each time you reload this page, the Prestige synchronizes the time with the time server.
New Time	This field displays the last updated time from the time server. When you select <b>None</b> in the <b>Use Protocol when Bootup</b> field, enter the new time in this field and then click <b>Apply</b> .
Apply	Click <b>Apply</b> to save your changes back to the Prestige.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.



# CHAPTER 13

## Firewalls

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

### 13.1 Firewall Overview

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

### 13.2 Types of Firewalls

There are three main types of firewalls:

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

#### 13.2.1 Packet Filtering Firewalls

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

#### 13.2.2 Application-level Firewalls

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

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

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

### 13.2.3 Stateful Inspection Firewalls

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also "inspect" the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency, however, they may lack the granular application level access control or caching that some proxies support. See [Section 13.5 on page 161](#) for more information on Stateful Inspection.

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

## 13.3 Introduction to ZyXEL's Firewall

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

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

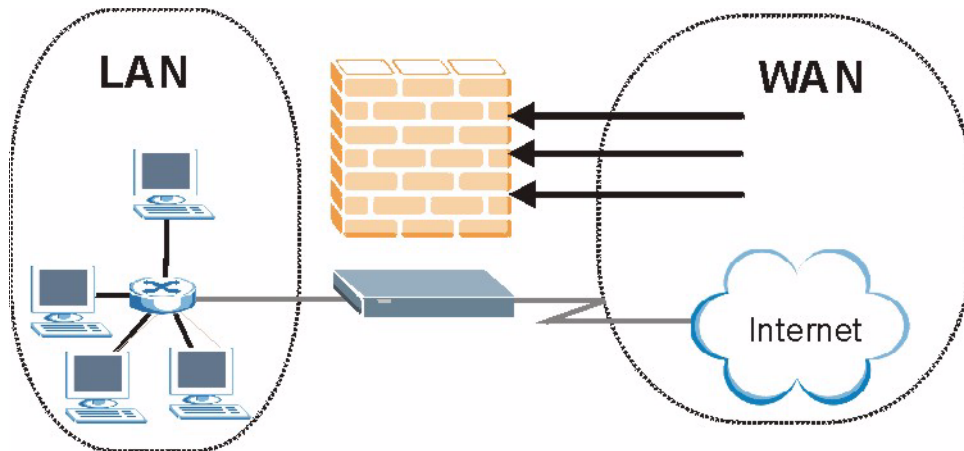
The Prestige has one DSL/ISDN port and one Ethernet LAN port, which physically separate the network into two areas.

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



### 13.3.1 Denial of Service Attacks

Figure 60 Prestige Firewall Application



## 13.4 Denial of Service

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

### 13.4.1 Basics

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

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

Some of the most common IP ports are:

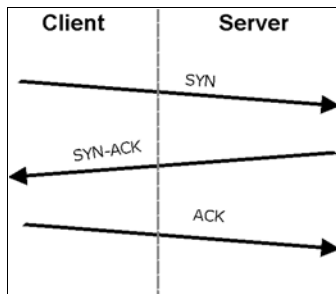
**Table 43** Common IP Ports

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

## 13.4.2 Types of DoS Attacks

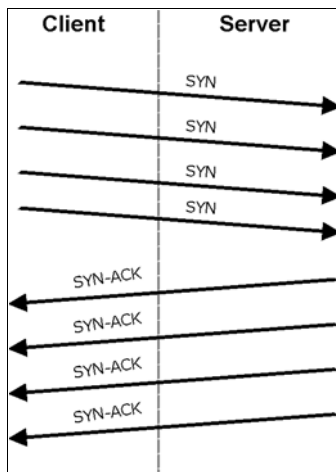
There are four types of DoS attacks:

- 1 Those that exploit bugs in a TCP/IP implementation.
- 2 Those that exploit weaknesses in the TCP/IP specification.
- 3 Brute-force attacks that flood a network with useless data.
- 4 IP Spoofing.
- 5 **"Ping of Death"** and **"Teardrop"** attacks exploit bugs in the TCP/IP implementations of various computer and host systems.
  - Ping of Death uses a "ping" utility to create an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. The oversize packet is then sent to an unsuspecting system. Systems may crash, hang or reboot.
  - Teardrop attack exploits weaknesses in the re-assembly of IP packet fragments. As data is transmitted through a network, IP packets are often broken up into smaller chunks. Each fragment looks like the original IP packet except that it contains an offset field that says, for instance, "This fragment is carrying bytes 200 through 400 of the original (non fragmented) IP packet." The Teardrop program creates a series of IP fragments with overlapping offset fields. When these fragments are reassembled at the destination, some systems will crash, hang, or reboot.
- 6 Weaknesses in the TCP/IP specification leave it open to **"SYN Flood"** and **"LAND"** attacks. These attacks are executed during the handshake that initiates a communication session between two applications.

**Figure 61** Three-Way Handshake

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

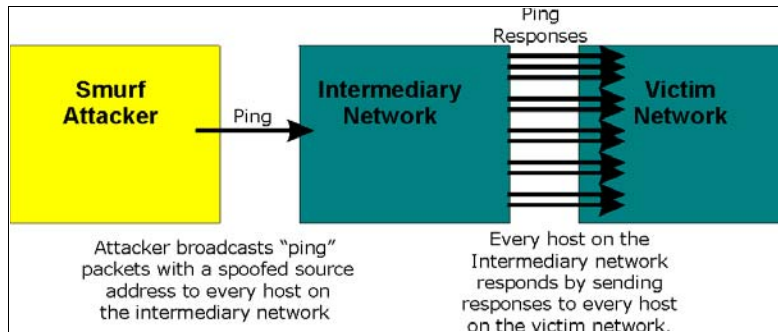
- **SYN Attack** floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on what is known as a backlog queue. SYN-ACKs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

**Figure 62** SYN Flood

- In a **LAND Attack**, hackers flood SYN packets into the network with a spoofed source IP address of the targeted system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.
- 7 A **brute-force** attack, such as a "Smurf" attack, targets a feature in the IP specification known as directed or subnet broadcasting, to quickly flood the target network with useless data. A Smurf hacker floods a router with Internet Control Message Protocol (ICMP) echo request packets (pings). Since the destination IP address of each packet is the broadcast address of the network, the router will broadcast the ICMP echo request packet to all hosts on the network. If there are numerous hosts, this will create a large

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

**Figure 63** Smurf Attack



### 13.4.2.1 ICMP Vulnerability

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

**Table 44** ICMP Commands That Trigger Alerts

5	REDIRECT
13	TIMESTAMP_REQUEST
14	TIMESTAMP_REPLY
17	ADDRESS_MASK_REQUEST
18	ADDRESS_MASK_REPLY

### 13.4.2.2 Illegal Commands (NetBIOS and SMTP)

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

**Table 45** Legal NetBIOS Commands

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

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

**Table 46** Legal SMTP Commands

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

### 13.4.2.3 Traceroute

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

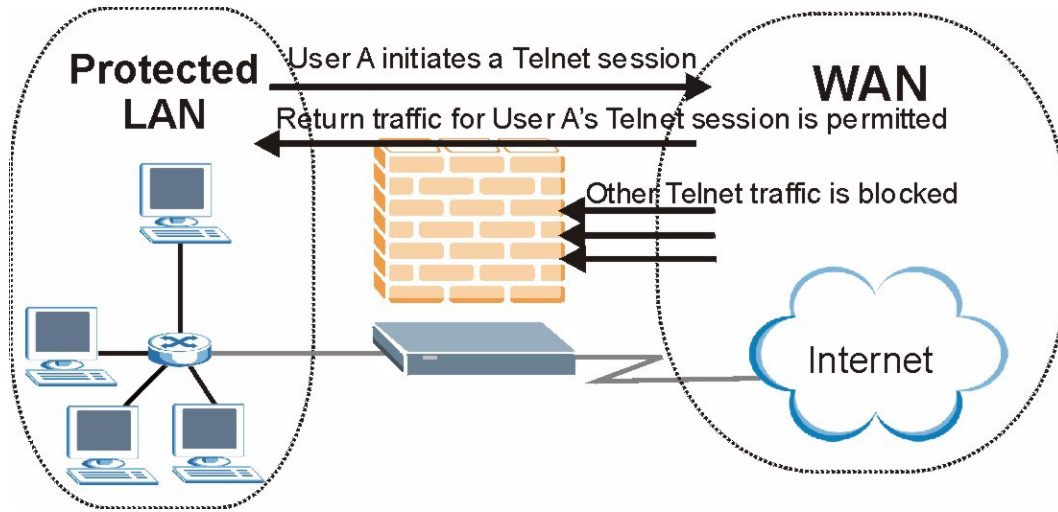
Often, many DoS attacks also employ a technique known as "**IP Spoofing**" as part of their attack. IP Spoofing may be used to break into systems, to hide the hacker's identity, or to magnify the effect of the DoS attack. IP Spoofing is a technique used to gain unauthorized access to computers by tricking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

## 13.5 Stateful Inspection

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

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

Figure 64 Stateful Inspection



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

### 13.5.1 Stateful Inspection Process

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

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

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

- 8 Any additional inbound or outbound packets that belong to the connection are inspected to update the state table entry and to modify the temporary inbound access list entries as required, and are forwarded through the interface.
- 9 When the connection terminates or times out, the connection's state table entry is deleted and the connection's temporary inbound access list entries are deleted.

## 13.5.2 Stateful Inspection and the Prestige

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

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

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

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

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

## 13.5.3 TCP Security

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

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

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

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

### 13.5.4 UDP/ICMP Security

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

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

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

### 13.5.5 Upper Layer Protocols

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

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

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

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

## 13.6 Guidelines for Enhancing Security with Your Firewall

- Change the default password via SMT or web configurator.



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

### 13.6.1 Security In General

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

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

- Always shred confidential information, particularly about your computer, before throwing it away. Some hackers dig through the trash of companies or individuals for information that might help them in an attack.

## 13.7 Packet Filtering Vs Firewall

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

### 13.7.1 Packet Filtering:

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

#### 13.7.1.1 When To Use Filtering

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

### 13.7.2 Firewall

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

#### 13.7.2.1 When To Use The Firewall

- To prevent DoS attacks and prevent hackers cracking your network.

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



# CHAPTER 14

## Firewall Configuration

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

### 14.1 Access Methods

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

### 14.2 Firewall Policies Overview

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

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

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

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

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

- WAN to LAN
- WAN to WAN/ Router

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

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

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

For example, you may create rules to:

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

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

## 14.3 Rule Logic Overview

**Note:** Study these points carefully before configuring rules.

### 14.3.1 Rule Checklist

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

- 1 Is the intent of the rule to forward or block traffic?
- 2 What direction of traffic does the rule apply to (refer to [Section 14.2 on page 169](#))?
- 3 What IP services will be affected?
- 4 What computers on the LAN are to be affected (if any)?
- 5 What computers on the Internet will be affected? The more specific, the better. For example, if traffic is being allowed from the Internet to the LAN, it is better to allow only certain machines on the Internet to access the LAN.

### 14.3.2 Security Ramifications

- 1 Once the logic of the rule has been defined, it is critical to consider the security ramifications created by the rule:
- 2 Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?
- 3 Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?

- 4 Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.
- 5 Does this rule conflict with any existing rules?
- 6 Once these questions have been answered, adding rules is simply a matter of plugging the information into the correct fields in the web configurator screens.

### 14.3.3 Key Fields For Configuring Rules

#### 14.3.3.1 Action

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

**Note:** “Block” means the firewall silently discards the packet.

#### 14.3.3.2 Service

Select the service from the **Service** scrolling list box. If the service is not listed, it is necessary to first define it. See [Section 14.10 on page 184](#) for more information on predefined services.

#### 14.3.3.3 Source Address

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

#### 14.3.3.4 Destination Address

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

## 14.4 Connection Direction Example

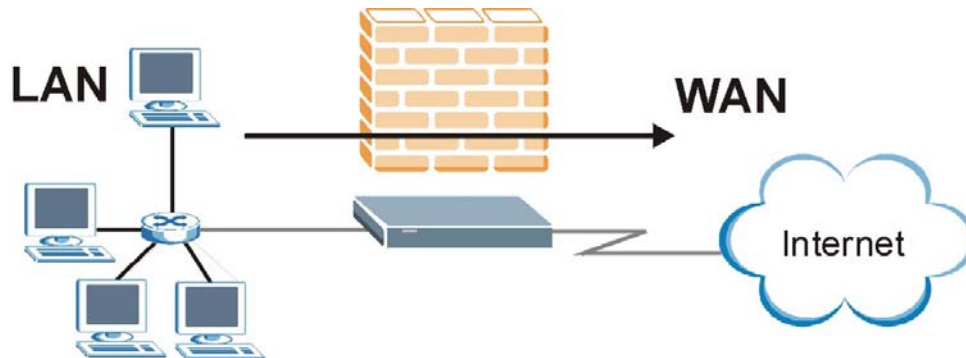
This section describes examples for firewall rules for connections going from LAN to WAN and from WAN to LAN.

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

### 14.4.1 LAN to WAN Rules

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

**Figure 65** LAN to WAN Traffic

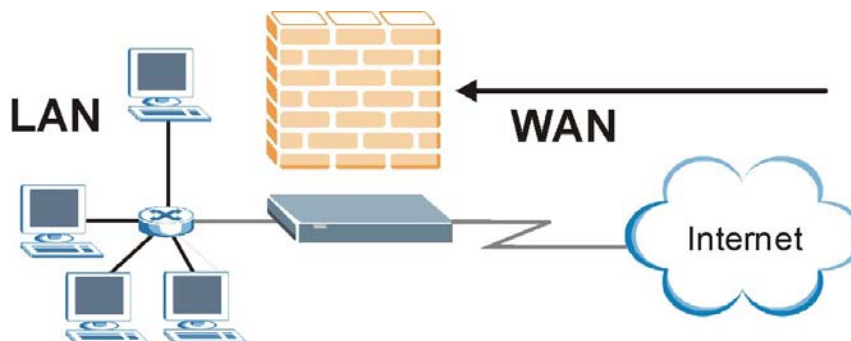


### 14.4.2 WAN to LAN Rules

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

See the following figure.

**Figure 66** WAN to LAN Traffic





### 14.4.3 Alerts

Alerts are reports on events, such as attacks, that you may want to know about right away. You can choose to generate an alert when an attack is detected in the **Edit Rule** screen (select the **Send Alert Message to Administrator When Matched** check box) or when a rule is matched in the **Edit Rule** screen (see [Section 14.6.1 on page 176](#)). When an event generates an alert, a message can be immediately sent to an e-mail account that you specify in the **Log Settings** screen (see the chapter on logs).

## 14.5 Configuring Basic Firewall Settings

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

**Figure 67** Firewall: Default Policy

Packet Direction	Default Action	Log
LAN to LAN / Router	<input type="radio"/> Block <input checked="" type="radio"/> Forward	<input type="checkbox"/>
LAN to WAN	<input type="radio"/> Block <input checked="" type="radio"/> Forward	<input checked="" type="checkbox"/>
WAN to LAN	<input checked="" type="radio"/> Block <input type="radio"/> Forward	<input checked="" type="checkbox"/>
WAN to WAN / Router	<input checked="" type="radio"/> Block <input type="radio"/> Forward	<input checked="" type="checkbox"/>

The following table describes the labels in this screen.

**Table 47** Firewall: Default Policy

LABEL	DESCRIPTION
Firewall Enabled	Select this check box to activate the firewall. The Prestige performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Allow Asymmetrical Route	Select this check box to have the Prestige firewall permit the use of triangle route topology on the network. See the appendix for more on triangle route topology.
Packet Direction	This is the direction of travel of packets ( <b>LAN to LAN/Router</b> , <b>LAN to WAN</b> , <b>WAN to WAN/Router</b> or <b>WAN to LAN</b> ). Firewall rules are grouped based on the direction of travel of packets to which they apply. For example, <b>LAN to LAN/Router</b> means packets traveling from a computer/subnet on the LAN to either another computer/subnet on the LAN interface of the Prestige or the Prestige itself.

**Table 47** Firewall: Default Policy (continued)

LABEL	DESCRIPTION
Default Action	Use the radio buttons to select whether to <b>Block</b> (silently discard) or <b>Forward</b> (allow the passage of) packets that are traveling in the selected direction.
Log	Select the check box to create a log (when the above action is taken) for packets that are traveling in the selected direction and do not match any of the rules below.
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save your changes back to the Prestige.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

## 14.6 Rule Summary

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

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

**Figure 68** Firewall: Rule Summary

*Firewall - Rule Summary*

---

Firewall Rules Storage Space in Use (1%)

0%  100%

Packet Direction: LAN to LAN / Router

Default Policy: Forward, None Log

Rule	Active	Source IP	Destination IP	Service	Action	Schedule	Log	Alert
1	Y	Any	Any	Any(UDP)	Forward	No	Disable	No

Create Rule: Insert new rule before rule number

Rules Reorder: Move rule number  to rule number

---

**Table 48** Rule Summary

LABEL	DESCRIPTION
Firewall Rules Storage Space in Use	This read-only bar shows how much of the Prestige's memory for recording firewall rules it is currently using. When you are using 80% or less of the storage space, the bar is green. When the amount of space used is over 80%, the bar is red.
Packet Direction	Use the drop-down list box to select a direction of travel of packets for which you want to configure firewall rules.
Default Policy	This field displays the default action and log policy you selected in the <b>Default Rule</b> screen for the packet direction shown in the field above.
	The following read-only fields summarize the rules you have created that apply to traffic traveling in the selected packet direction. The firewall rules that you configure (summarized below) take priority over the general firewall action settings above.
Rule	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn. Click a rule's number to go to the <b>Firewall Edit Rule</b> screen to configure or edit a firewall rule.
Active	This field displays whether a firewall is turned on ( <b>Y</b> ) or not ( <b>N</b> ).
Source IP	This drop-down list box displays the source addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to <b>Any</b> .
Destination IP	This drop-down list box displays the destination addresses or ranges of addresses to which this firewall rule applies. Please note that a blank source or destination address is equivalent to <b>Any</b> .
Service	This drop-down list box displays the services to which this firewall rule applies. Please note that a blank service type is equivalent to <b>Any</b> . See for more information.
Action	This is the specified action for that rule, either <b>Block</b> or <b>Forward</b> . Note that <b>Block</b> means the firewall silently discards the packet.

**Table 48** Rule Summary (continued)

LABEL	DESCRIPTION
Schedule	This field tells you whether a schedule is specified ( <b>Yes</b> ) or not ( <b>No</b> ).
Log	This field shows you whether a log is created when packets match this rule ( <b>Enabled</b> ) or not ( <b>Disable</b> ).
Alert	This field tells you whether this rule generates an alert ( <b>Yes</b> ) or not ( <b>No</b> ) when the rule is matched.
Insert/Append	Type the index number for where you want to put a rule. For example, if you type "6", your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7. Click <b>Insert</b> to add a new firewall rule before the specified index number. Click <b>Append</b> to add a new firewall rule after the specified index number.
Move	Type a rule's index number and the number for where you want to put that rule. Click <b>Move</b> to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save your changes back to the Prestige.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.

### 14.6.1 Configuring Firewall Rules

Follow these directions to create a new rule.

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

**Figure 69** Firewall: Edit Rule

**Firewall - Edit Rule 1**

---

Active

Action for Matched Packets:  Block  Forward

**Source Address:**

Address Type: Any Address

Start IP Address:  Add >>

End IP Address:  Edit <<

Subnet Mask:  Delete

Source Address List: 

Any

**Destination Address:**

Address Type: Any Address

Start IP Address:  Add >>

End IP Address:  Edit <<

Subnet Mask:  Delete

Destination Address List: 

Any

**Service:**

Available Services:

AIM/NEW-ICQ(TCP:5190)  
 AUTH(TCP:113)  
 BGP(TCP:179)  
 BOOTP\_CLIENT(UDP:68)  
 BOOTP\_SERVER(UDP:67)

Add >> Remove

[Edit Customized Services](#)

Selected Services: 

Any(UDP)  
Any(TCP)

**Schedule:**

Day to Apply:

Everyday

Sun  Mon  Tue  Wed  Thu  Fri  Sat

Time of Day to Apply: (24-Hour Format)

All day

Start  hour  minute End  hour  minute

**Log:**

Log Packet Detail Information.

**Alert:**

Send Alert Message to Administrator When Matched.

---

Back Apply Cancel Delete

The following table describes the labels in this screen.

**Table 49** Firewall: Edit Rule

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

## 14.7 Customized Services

Configure customized services and port numbers not predefined by the Prestige. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. For further information on these services, please read [Section 14.10 on page 184](#). Click the **Edit Customized Services** link while editing a firewall rule to configure a custom service port. This displays the following screen.

**Figure 70** Firewall: Customized Services

No.	Name:	Protocol	Port
<a href="#">1</a>			
<a href="#">2</a>			
<a href="#">3</a>			
<a href="#">4</a>			
<a href="#">5</a>			
<a href="#">6</a>			
<a href="#">7</a>			
<a href="#">8</a>			
<a href="#">9</a>			
<a href="#">10</a>			

**Table 50** Customized Services

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

## 14.8 Creating/Editing A Customized Service

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

**Figure 71** Firewall: Configure Customized Services

The screenshot shows a configuration window titled "Firewall - Customized Services - Config". It contains the following elements:

- Service Name:** A text input field.
- Service Type:** A dropdown menu currently showing "TCP/UDP".
- Port Configuration:** A section with two radio buttons: "Single" (selected) and "Range".
- Port Number:** Two text input fields separated by a hyphen, both containing the number "0".
- Buttons:** Four buttons at the bottom: "Back", "Apply", "Cancel", and "Delete".

The following table describes the labels in this screen.

**Table 51** Firewall: Configure Customized Services

LABEL	DESCRIPTION
Service Name	Type a unique name for your custom port.
Service Type	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.
Port Configuration	
Type	Click <b>Single</b> to specify one port only or <b>Range</b> to specify a span of ports that define your customized service.
Port Number	Type a single port number or the range of port numbers that define your customized service.
Back	Click <b>Back</b> to return to the <b>Firewall Customized Services</b> screen.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Cancel	Click <b>Cancel</b> to return to the previously saved settings.
Delete	Click <b>Delete</b> to delete the current rule.

## 14.9 Example Firewall Rule

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

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



**Figure 72** Firewall Example: Rule Summary

The screenshot shows the 'Firewall - Rule Summary' window. At the top, it displays 'Firewall Rules Storage Space in Use (1%)' with a progress bar from 0% to 100%. Below this, the 'Packet Direction' is set to 'WAN to LAN' in a dropdown menu, and the 'Default Policy' is 'Block, Log'. There are two rows of controls: the first row has a dropdown for 'Create Rule: Insert new rule before rule number', followed by 'Insert' and 'Append' buttons; the second row has a dropdown for 'Rules Reorder: Move rule number', followed by a text input field containing '0', a dropdown for 'to rule number', another text input field containing '0', and a 'Move' button. At the bottom of the window are 'Back', 'Apply', and 'Cancel' buttons.

- 3** In the **Rule Summary** screen, type the index number for where you want to put the rule. For example, if you type “6”, your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7.
- 4** Click **Insert** to display the firewall rule configuration screen.
- 5** Select **Any** in the **Destination Address** box and then click **Delete**.
- 6** Configure the destination address screen as follows and click **Add**.

**Figure 73** Firewall Example: Edit Rule: Destination Address

**Firewall - Edit Rule 1**

Active  
 Action for Matched Packets:  Block  Forward

**Source Address:**

Address Type: Any Address  
 Start IP Address: 0.0.0.0  
 End IP Address: 0.0.0.0  
 Subnet Mask: 0.0.0.0

Source Address List: Any

**Destination Address:**

Address Type: Range Address  
 Start IP Address: 10.0.0.10  
 End IP Address: 10.0.0.15  
 Subnet Mask: 0.0.0.0

Destination Address List:

**Service:**

Available Services: AIM/NEW-ICQ(TCP:5190), AUTH(TCP:113)  
 Selected Services: Any(UDP), Any(TCP)

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

**8** Click the number of a customized service to open the configuration screen. Configure it as follows and click **Apply**.

**Figure 74** Edit Custom Port Example

**Firewall - Customized Services - Config**

Service Name: MyService  
 Service Type: TCP/UDP

**Port Configuration**

Type:  Single  Range  
 Port Number: 123 - 0

Back Apply Cancel Delete

**9** Click **Back** in the **Customized Services** screen to return to the **Edit Rule** screen.

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

**Figure 75** Firewall Example: Edit Rule: Select Customized Services

**Firewall - Edit Rule 1**

Active  
 Action for Matched Packets:  Block  Forward

**Source Address:**

Address Type:    
 Start IP Address:    
 End IP Address:    
 Subnet Mask:

Source Address List:

**Destination Address:**

Address Type:    
 Start IP Address:    
 End IP Address:    
 Subnet Mask:

Destination Address List:

**Service:**

Available Services:    
 Any(UDP)  
 AIM/NEW-ICQ(TCP:5190)  
 AUTH(TCP:113)  
 BGP(TCP:179)   
[Edit Customized Services](#)

Selected Services:

**Schedule:**

Day to Apply:  
 Everyday  
 Sun  Mon  Tue  Wed  Thu  Fri  Sat

Time of Day to Apply: (24-Hour Format)  
 All day  
 Start  hour  minute End  hour  minute

**Log:**  
 Log Packet Detail Information.

**Alert:**  
 Send Alert Message to Administrator When Matched.

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

On completing the configuration procedure for this Internet firewall rule, the **Rule Summary** screen should look like the following.

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

**Figure 76** Firewall Example: Rule Summary: My Service

The screenshot shows the 'Firewall - Rule Summary' configuration page. At the top, there is a progress bar for 'Firewall Rules Storage Space in Use (1%)' showing 0% usage. Below this, the 'Packet Direction' is set to 'WAN to LAN' and the 'Default Policy' is 'Block, Log'. A table lists the rule configuration:

Rule	Active	Source IP	Destination IP	Service	Action	Schedule	Log	Alert
1	Y	Any	10.0.0.10 - 10.0.0.15	*MyService(TCP/UDP:123)	Forward	No	Disable	No

Below the table, there are controls for 'Create Rule' (Insert new rule before rule number 1, with 'Insert' and 'Append' buttons) and 'Rules Reorder' (Move rule number 0 to rule number 0, with a 'Move' button). At the bottom, there are 'Back', 'Apply', and 'Cancel' buttons.

## 14.10 Predefined Services

The **Available Services** list box in the **Edit Rule** screen (see [Section 14.6.1 on page 176](#)) displays all predefined services that the Prestige already supports. Next to the name of the service, two fields appear in brackets. The first field indicates the IP protocol type (TCP, UDP, or ICMP). The second field indicates the IP port number that defines the service. (Note that there may be more than one IP protocol type. For example, look at the default configuration labeled “(DNS)”. **(UDP/TCP:53)** means UDP port 53 and TCP port 53. Up to 128 entries are supported. Custom service ports may also be configured using the **Customized Services** function discussed previously.

**Table 52** Predefined Services

SERVICE	DESCRIPTION
AIM/NEW_ICQ(TCP:5190)	AOL's Internet Messenger service, used as a listening port by ICQ.
AUTH(TCP:113)	Authentication protocol used by some servers.
BGP(TCP:179)	Border Gateway Protocol.
BOOTP_CLIENT(UDP:68)	DHCP Client.
BOOTP_SERVER(UDP:67)	DHCP Server.
CU-SEEME(TCP/UDP:7648, 24032)	A popular videoconferencing solution from White Pines Software.
DNS(UDP/TCP:53)	Domain Name Server, a service that matches web names (e.g. www.zyxel.com) to IP numbers.
FINGER(TCP:79)	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP(TCP:20.21)	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323(TCP:1720)	Net Meeting uses this protocol.

**Table 52** Predefined Services (continued)

SERVICE	DESCRIPTION
HTTP(TCP:80)	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	HTTPS is a secured http session often used in e-commerce.
ICQ(UDP:4000)	This is a popular Internet chat program.
IPSEC_TRANSPORT/ TUNNEL(AH:0)	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
IPSEC_TUNNEL(ESP:0)	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
IRC(TCP/UDP:6667)	This is another popular Internet chat program.
MSN Messenger(TCP:1863)	Microsoft Networks' messenger service uses this protocol.
MULTICAST(IGMP:0)	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
NEWS(TCP:144)	A protocol for news groups.
NFS(UDP:2049)	Network File System - NFS is a client/server distributed file service that provides transparent file-sharing for network environments.
NNTP(TCP:119)	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING(ICMP:0)	Packet Internet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3(TCP:110)	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP(TCP:1723)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL(GRE:0)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the data channel.
RCMD(TCP:512)	Remote Command Service.
REAL_AUDIO(TCP:7070)	A streaming audio service that enables real time sound over the web.
REXEC(TCP:514)	Remote Execution Daemon.
RLOGIN(TCP:513)	Remote Login.
RTELNET(TCP:107)	Remote Telnet.
RTSP(TCP/UDP:554)	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP(TCP:115)	Simple File Transfer Protocol.
SMTP(TCP:25)	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP(TCP/UDP:161)	Simple Network Management Program.
SNMP-TRAPS (TCP/ UDP:162)	Traps for use with the SNMP (RFC:1215).
SQL-NET(TCP:1521)	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSDP(UDP:1900)	Simple Service Discovery Protocol (SSDP) is a discovery service searching for Universal Plug and Play devices on your home network or upstream Internet gateways using DUDP port 1900.

**Table 52** Predefined Services (continued)

SERVICE	DESCRIPTION
SSH(TCP/UDP:22)	Secure Shell Remote Login Program.
STRMWORKS(UDP:1558)	Stream Works Protocol.
SYSLOG(UDP:514)	Syslog allows you to send system logs to a UNIX server.
TACACS(UDP:49)	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET(TCP:23)	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP(UDP:69)	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE(TCP:7000)	Another videoconferencing solution.

## 14.11 Anti-Probing

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

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

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

**Figure 77** Firewall: Anti Probing

The following table describes the labels in this screen.

**Table 53** Firewall: Anti Probing

LABEL	DESCRIPTION
Respond to PING on	The Prestige does 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. Note that the probing packets must first traverse the Prestige 's firewall mechanism before reaching this anti-probing mechanism. Therefore if the firewall mechanism blocks a probing packet, the Prestige reacts based on the firewall policy, which by default, is to send a TCP reset packet for a blocked TCP packet. You can use the command "sys firewall tcprst rst [on off]" to change this policy. When the firewall mechanism blocks a UDP packet, it drops the packet without sending a response packet.
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save your changes back to the Prestige.
Reset	Click <b>Reset</b> to begin configuring this screen afresh.

## 14.12 DOS Thresholds

For DoS attacks, the Prestige uses thresholds to determine when to drop sessions that do not become fully established. These thresholds apply globally to all sessions.

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

## 14.12.1 Threshold Values

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

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

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

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

## 14.12.2 Half-Open Sessions

An unusually high number of half-open sessions (either an absolute number or measured as the arrival rate) could indicate that a Denial of Service attack is occurring. For TCP, "half-open" means that the session has not reached the established state-the TCP three-way handshake has not yet been completed (see [Figure 61 on page 159](#)). For UDP, "half-open" means that the firewall has detected no return traffic.

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

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

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

### 14.12.2.1 TCP Maximum Incomplete and Blocking Time

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



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

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

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

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

**Figure 78** Firewall: Threshold

The screenshot shows a configuration window titled "Firewall - Threshold". It is divided into two main sections. The first section, "Denial of Service Thresholds", contains five rows of settings, each with a text input field and a unit label in parentheses: "One Minute Low" (80 Sessions per Minute), "One Minute High" (100 Sessions per Minute), "Maximum Incomplete Low" (80 Sessions), "Maximum Incomplete High" (100 Sessions), and "TCP Maximum Incomplete" (10 Sessions). The second section, "Action taken when TCP Maximum Incomplete reached threshold", has two radio button options: "Delete the Oldest Half Open Session when New Connection Request Comes." (which is selected) and "Deny New Connection Request for" followed by a text input field containing "10" and the label "Minutes(1~255)". At the bottom of the window are three buttons: "Back", "Apply", and "Cancel".

The following table describes the labels in this screen.

**Table 54** Firewall: Threshold

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

**Table 54** Firewall: Threshold (continued)

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

# CHAPTER 15

## Content Filtering

This chapter covers how to configure content filtering.

### 15.1 Content Filtering Overview

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

### 15.2 Configuring Keyword Blocking

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

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

**Figure 79** Content Filter: Keyword

The following table describes the labels in this screen.

**Table 55** Content Filter: Keyword

LABEL	DESCRIPTION
Enable Keyword Blocking	Select this check box to enable this feature.
Block Websites that contain these keywords in the URL:	This box contains the list of all the keywords that you have configured the Prestige to block.
Delete	Highlight a keyword in the box and click <b>Delete</b> to remove it.
Clear All	Click <b>Clear All</b> to remove all of the keywords from the list.
Keyword	Type a keyword in this field. You may use any character (up to 127 characters). Wildcards are not allowed.
Add Keyword	Click <b>Add Keyword</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.
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save your changes back to the Prestige.
Cancel	Click <b>Cancel</b> to return to the previously saved settings.

## 15.3 Configuring the Schedule

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

**Figure 80** Content Filter: Schedule

The following table describes the labels in this screen.

**Table 56** Content Filter: Schedule

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

## 15.4 Configuring Trusted Computers

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

**Figure 81** Content Filter: Trusted

The following table describes the labels in this screen.

**Table 57** Content Filter: Trusted

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

# CHAPTER 16

## Introduction to IPSec

This chapter introduces the basics of IPSec VPNs.

### 16.1 VPN Overview

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

#### 16.1.1 IPSec

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

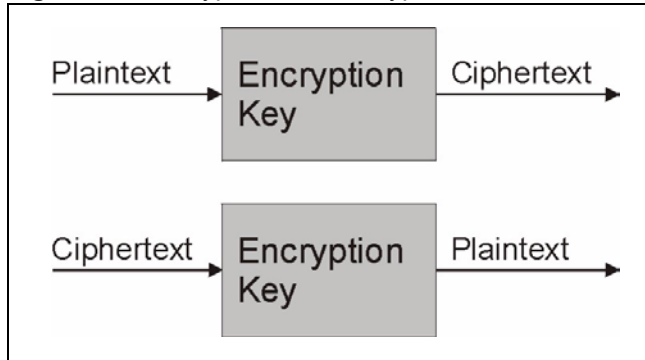
#### 16.1.2 Security Association

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

#### 16.1.3 Other Terminology

##### 16.1.3.1 Encryption

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

**Figure 82** Encryption and Decryption

### 16.1.3.2 Data Confidentiality

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

### 16.1.3.3 Data Integrity

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

### 16.1.3.4 Data Origin Authentication

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

## 16.1.4 VPN Applications

The Prestige supports the following VPN applications.

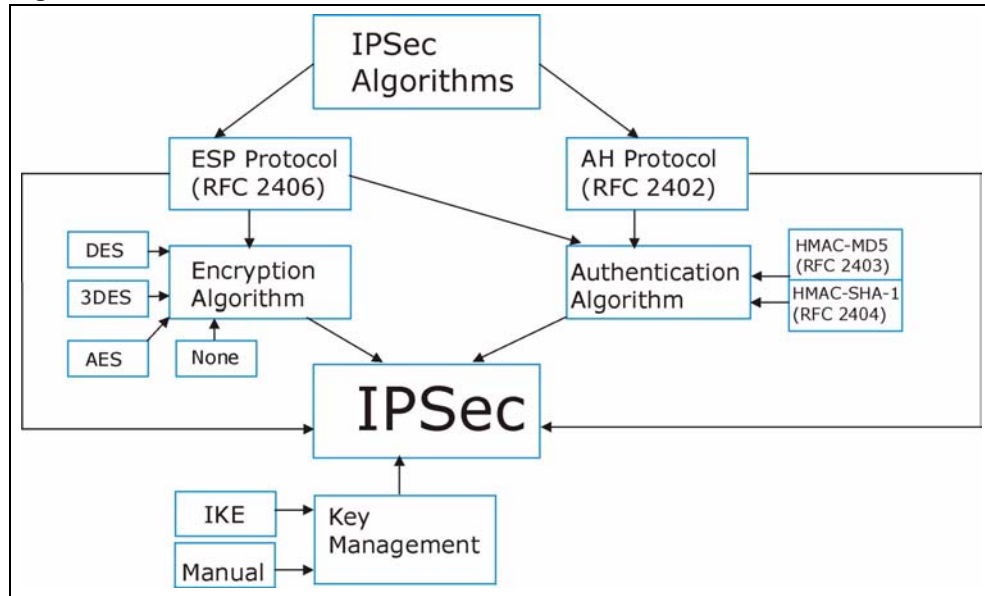
- **Linking Two or More Private Networks Together**  
Connect branch offices and business partners over the Internet with significant cost savings and improved performance when compared to leased lines between sites.
- **Accessing Network Resources When NAT Is Enabled**  
When NAT is enabled, remote users are not able to access hosts on the LAN unless the host is designated a public LAN server for that specific protocol. Since the VPN tunnel terminates inside the LAN, remote users will be able to access all computers that use private IP addresses on the LAN.
- **Unsupported IP Applications**  
A VPN tunnel may be created to add support for unsupported emerging IP applications.



## 16.2 IPsec Architecture

The overall IPsec architecture is shown as follows.

**Figure 83** IPsec Architecture



### 16.2.1 IPsec Algorithms

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

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

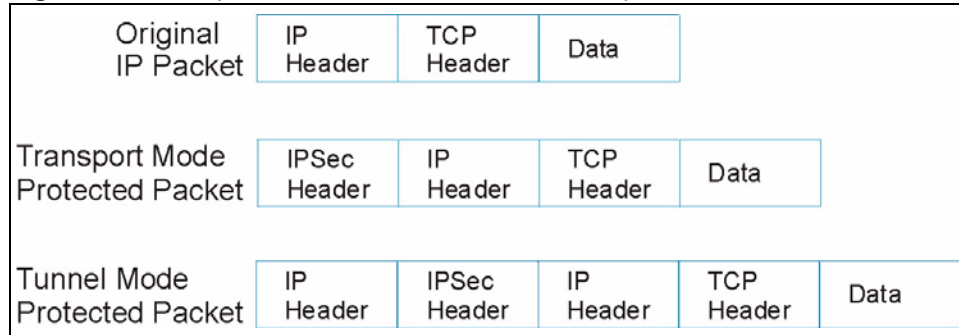
The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404), provide an authentication mechanism for the **AH** and **ESP** protocols. Please see [Section 17.2 on page 201](#) for more information.

### 16.2.2 Key Management

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

## 16.3 Encapsulation

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

**Figure 84** Transport and Tunnel Mode IPSec Encapsulation

### 16.3.1 Transport Mode

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

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

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

### 16.3.2 Tunnel Mode

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

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

## 16.4 IPSec and NAT

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

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

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

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

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

**Transport** mode **ESP** with authentication is not compatible with NAT, although NAT traversal provides a way to use **Transport** mode **ESP** when there is a NAT router between the IPsec endpoints (see [Section 17.8 on page 206](#) for details).

**Table 58** VPN and NAT

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



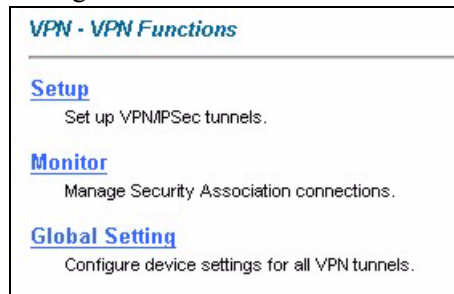
# CHAPTER 17

## VPN Screens

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

### 17.1 VPN/IPSec Overview

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



### 17.2 IPSec Algorithms

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

#### 17.2.1 AH (Authentication Header) Protocol

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

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

## 17.2.2 ESP (Encapsulating Security Payload) Protocol

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

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

**Table 59** AH and ESP

	<b>ESP</b>	<b>AH</b>
<b>ENCRYPTION</b>	<b>DES</b> (default) Data Encryption Standard (DES) is a widely used method of data encryption using a private (secret) key. DES applies a 56-bit key to each 64-bit block of data.	<b>MD5</b> (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
	<b>3DES</b> Triple DES (3DES) is a variant of DES, which iterates three times with three separate keys (3 x 56 = 168 bits), effectively doubling the strength of DES.	<b>SHA1</b> SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.
	<b>AES</b> Advanced Encryption Standard is a newer method of data encryption that also uses a secret key. This implementation of AES applies a 128-bit key to 128-bit blocks of data. AES is faster than 3DES.	
	Select <b>NULL</b> to set up a phase 2 tunnel without encryption.	
<b>AUTHENTICATION</b>	<b>MD5</b> (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.	<b>MD5</b> (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
	<b>SHA1</b> SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.	<b>SHA1</b> SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.
	Select <b>MD5</b> for minimal security and <b>SHA1</b> for maximum security.	

## 17.3 My IP Address

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

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

- The Prestige uses the current Prestige WAN IP address (static or dynamic) to set up the VPN tunnel.

- If the WAN connection goes down, the Prestige uses the dial backup IP address for the VPN tunnel when using dial backup or the LAN IP address when using traffic redirect. See the chapter on WAN for details on dial backup and traffic redirect.

## 17.4 Secure Gateway Address

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

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

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

### 17.4.1 Dynamic Secure Gateway Address

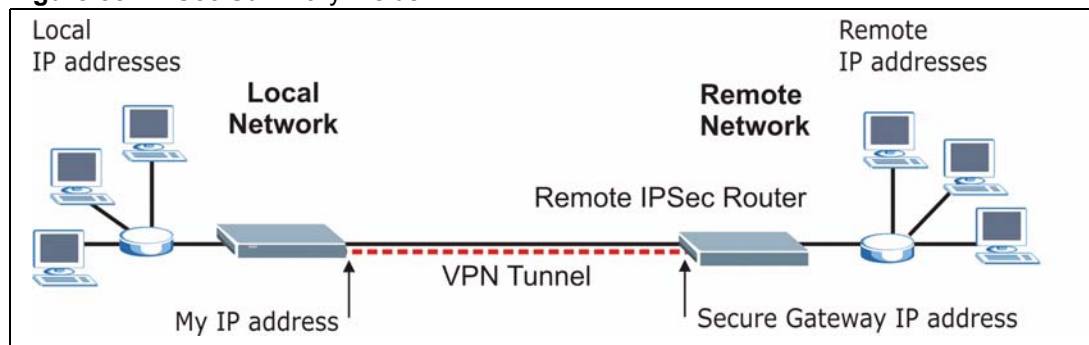
If the remote secure gateway has a dynamic WAN IP address and does not use DDNS, enter 0.0.0.0 as the secure gateway's address. In this case only the remote secure gateway can initiate SAs. This may be useful for telecommuters initiating a VPN tunnel to the company network (see [Section 17.18 on page 225](#) for configuration examples).

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

## 17.5 VPN Summary Screen

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

**Figure 85** IPSec Summary Fields



Local and remote IP addresses must be static.

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

**Figure 86** VPN Summary

No.	Name	Active	Local Address	Remote Address	Encap.	IPSec Algorithm	Secure Gateway IP
<a href="#">1</a>	-	-	-	-	-	-	...
<a href="#">2</a>	-	-	-	-	-	-	...
<a href="#">3</a>	-	-	-	-	-	-	...
<a href="#">4</a>	-	-	-	-	-	-	...
<a href="#">5</a>	-	-	-	-	-	-	...
<a href="#">6</a>	-	-	-	-	-	-	...
<a href="#">7</a>	-	-	-	-	-	-	...
<a href="#">8</a>	-	-	-	-	-	-	...
<a href="#">9</a>	-	-	-	-	-	-	...
<a href="#">10</a>	-	-	-	-	-	-	...
<a href="#">11</a>	-	-	-	-	-	-	...
<a href="#">12</a>	-	-	-	-	-	-	...
<a href="#">13</a>	-	-	-	-	-	-	...
<a href="#">14</a>	-	-	-	-	-	-	...
<a href="#">15</a>	-	-	-	-	-	-	...
<a href="#">16</a>	-	-	-	-	-	-	...
<a href="#">17</a>	-	-	-	-	-	-	...
<a href="#">18</a>	-	-	-	-	-	-	...
<a href="#">19</a>	-	-	-	-	-	-	...
<a href="#">20</a>	-	-	-	-	-	-	...

Back

The following table describes the fields in this screen.

**Table 60** VPN Summary

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



**Table 60** VPN Summary (continued)

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

## 17.6 Keep Alive

When you initiate an IPSec tunnel with keep alive enabled, the Prestige automatically renegotiates the tunnel when the IPSec SA lifetime period expires (see [Section 17.12 on page 214](#) for more on the IPSec SA lifetime). In effect, the IPSec tunnel becomes an “always on” connection after you initiate it. Both IPSec routers must have a Prestige-compatible keep alive feature enabled in order for this feature to work.

If the Prestige has its maximum number of simultaneous IPSec tunnels connected to it and they all have keep alive enabled, then no other tunnels can take a turn connecting to the Prestige because the Prestige never drops the tunnels that are already connected. Refer to [Section 1.3 on page 46](#) to see how many simultaneous IPSec SAs your Prestige model can support.

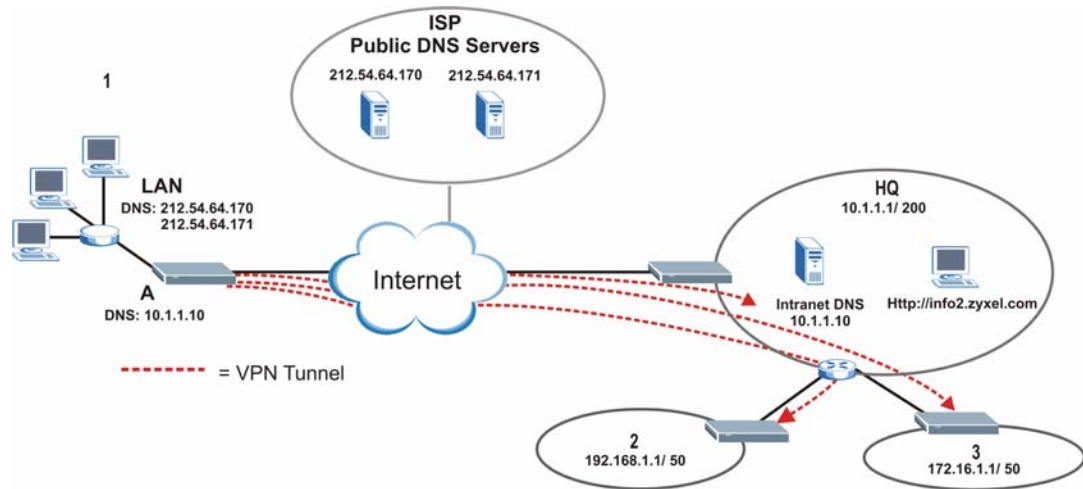
When there is outbound traffic with no inbound traffic, the Prestige automatically drops the tunnel after two minutes.

## 17.7 Remote DNS Server

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

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

**Figure 87** VPN Host using Intranet DNS Server Example



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

## 17.8 NAT Traversal

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

**Figure 88** NAT Router Between IPsec Routers



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

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

## 17.8.1 NAT Traversal Configuration

For NAT traversal to work you must:

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

In order for IPSec router A (see [Figure 88 on page 206](#)) to receive an initiating IPSec packet from IPSec router B, set the NAT router to forward UDP port 500 to IPSec router A.

## 17.9 ID Type and Content

With aggressive negotiation mode (see [Section 17.12.1 on page 216](#)), the Prestige identifies incoming SAs by ID type and content since this identifying information is not encrypted. This enables the Prestige to distinguish between multiple rules for SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. Telecommuters can use separate passwords to simultaneously connect to the Prestige from IPSec routers with dynamic IP addresses (see [Section 17.18 on page 225](#) for a telecommuter configuration example).

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

With main mode (see [Section 17.12.1 on page 216](#)), the ID type and content are encrypted to provide identity protection. In this case the Prestige can only distinguish between up to 12 different incoming SAs that connect from remote IPSec routers that have dynamic WAN IP addresses. The Prestige can distinguish up to 12 incoming SAs because you can select between three encryption algorithms (DES, 3DES and AES), two authentication algorithms (MD5 and SHA1) and two key groups (DH1 and DH2) when you configure a VPN rule (see [Section 17.13 on page 216](#)). The ID type and content act as an extra level of identification for incoming SAs.

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

**Table 61** Local ID Type and Content Fields

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

**Table 62** Peer ID Type and Content Fields

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

### 17.9.1 ID Type and Content Examples

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

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

**Table 63** Matching ID Type and Content Configuration Example

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

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

**Table 64** Mismatching ID Type and Content Configuration Example

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

## 17.10 Pre-Shared Key

A pre-shared key identifies a communicating party during a phase 1 IKE negotiation (see [Section 17.12 on page 214](#) for more on IKE phases). It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.

## 17.11 Editing VPN Policies

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

**Figure 89** VPN IKE

**VPN - IKE**

---

**IPSec Setup**

Active
  Keep Alive
  NAT Traversal

Name

IPSec Key Mode

Negotiation Mode

Encapsulation Mode

DNS Server (for IPSec VPN)

**Local**

Local Address Type

IP Address Start

End / Subnet Mask

**Remote**

Remote Address Type

IP Address Start

End / Subnet Mask

**Address Information**

Local ID Type

Content

My IP Address

Peer ID Type

Content

Secure Gateway Address

**Security Protocol**

VPN Protocol

Pre-Shared Key

Encryption Algorithm

Authentication Algorithm

---

The following table describes the fields in this screen.

**Table 65** VPN IKE

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

**Table 65** VPN IKE (continued)

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



**Table 65** VPN IKE (continued)

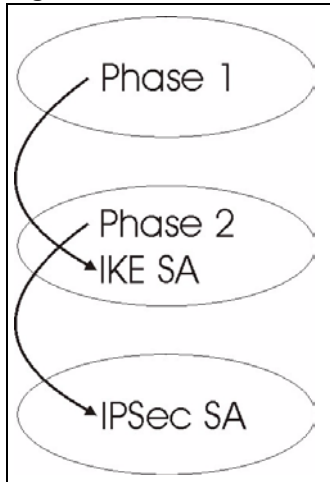
LABEL	DESCRIPTION
My IP Address	<p>Enter the WAN IP address of your Prestige. The VPN tunnel has to be rebuilt if this IP address changes.</p> <p>The following applies if this field is configured as <b>0.0.0.0</b>:            The Prestige uses the current Prestige WAN IP address (static or dynamic) to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

**Table 65** VPN IKE (continued)

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

## 17.12 IKE Phases

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

**Figure 90** Two Phases to Set Up the IPsec SA

In phase 1 you must:

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

In phase 2 you must:

- Choose which protocol to use (**ESP** or **AH**) for the IKE key exchange.
- Choose an encryption algorithm.
- Choose an authentication algorithm
- Choose whether to enable Perfect Forward Secrecy (PFS) using Diffie-Hellman public-key cryptography – see [Section 17.12.3 on page 216](#). Select **None** (the default) to disable PFS.
- Choose **Tunnel** mode or **Transport** mode.
- Set the IPsec SA lifetime. This field allows you to determine how long the IPsec SA should stay up before it times out. The Prestige automatically renegotiates the IPsec SA if there is traffic when the IPsec SA lifetime period expires. The Prestige also automatically renegotiates the IPsec SA if both IPsec routers have keep alive enabled, even if there is no traffic. If an IPsec SA times out, then the IPsec router must renegotiate the SA the next time someone attempts to send traffic.

## 17.12.1 Negotiation Mode

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

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

## 17.12.2 Diffie-Hellman (DH) Key Groups

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

## 17.12.3 Perfect Forward Secrecy (PFS)

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

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

## 17.13 Configuring Advanced IKE Settings

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

**Figure 91** VPN IKE: Advanced Setup

*VPN - IKE - Advanced Setup*

---

**VPN - IKE**

Protocol

Enable Replay Detection

Local Start Port  End

Remote Start Port  End

**Phase1**

Negotiation Mode

Pre-Shared Key

Encryption Algorithm

Authentication Algorithm

SA Life Time (Seconds)

Key Group

**Phase2**

Active Protocol

Encryption Algorithm

Authentication Algorithm

SA Life Time (Seconds)

Encapsulation

Perfect Forward Secrecy (PFS)

---

The following table describes the fields in this screen.

**Table 66** VPN IKE: Advanced Setup

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

**Table 66** VPN IKE: Advanced Setup (continued)

LABEL	DESCRIPTION
Remote Start Port	0 is the default and signifies any port. Type a port number from 0 to 65535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
End	Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. If <b>Remote Start Port</b> is left at 0, <b>End</b> will also remain at 0.
Phase 1	
Negotiation Mode	Select <b>Main</b> or <b>Aggressive</b> from the drop-down list box. Multiple SAs connecting through a secure gateway must have the same negotiation mode.
Pre-Shared Key	<p>Type your pre-shared key in this field. A pre-shared key identifies a communicating party during a phase 1 IKE negotiation. It is called "pre-shared" because you have to share it with another party before you can communicate with them over a secure connection.</p> <p>Type from 8 to 31 case-sensitive ASCII characters or from 16 to 62 hexadecimal ("0-9", "A-F") characters. You must precede a hexadecimal key with a "0x" (zero x), which is not counted as part of the 16 to 62-character range for the key. For example, in "0x0123456789ABCDEF", "0x" denotes that the key is hexadecimal and "0123456789ABCDEF" is the key itself.</p> <p>Both ends of the VPN tunnel must use the same pre-shared key. You will receive a "PYLD_MALFORMED" (payload malformed) packet if the same pre-shared key is not used on both ends.</p>
Encryption Algorithm	<p>Select <b>DES</b>, <b>3DES</b> or <b>AES</b> from the drop-down list box.</p> <p>When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (<b>3DES</b>) is a variation on <b>DES</b> that uses a 168-bit key. As a result, <b>3DES</b> is more secure than <b>DES</b>. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of AES uses a 128-bit key. <b>AES</b> is faster than <b>3DES</b>.</p>
Authentication Algorithm	Select <b>SHA1</b> or <b>MD5</b> from the drop-down list box. <b>MD5</b> (Message Digest 5) and <b>SHA1</b> (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The <b>SHA1</b> algorithm is generally considered stronger than <b>MD5</b> , but is slower. Select <b>MD5</b> for minimal security and <b>SHA-1</b> for maximum security.
SA Life Time (Seconds)	<p>Define the length of time before an IKE SA automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days).</p> <p>A short SA Life Time increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.</p>
Key Group	You must choose a key group for phase 1 IKE setup. <b>DH1</b> (default) refers to Diffie-Hellman Group 1 a 768 bit random number. <b>DH2</b> refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number.
Phase 2	
Active Protocol	Use the drop-down list box to choose from <b>ESP</b> or <b>AH</b> .

**Table 66** VPN IKE: Advanced Setup (continued)

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

## 17.14 Manual Key Setup

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

### 17.14.1 Security Parameter Index (SPI)

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

Current ZyXEL implementation assumes identical outgoing and incoming SPIs.

## 17.15 Configuring Manual Key

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

**Figure 92** VPN: Manual Key

*VPN - Manual Key*

---

**IPSec Setup**

Active

Name

IPSec Key Mode

SPI

Encapsulation Mode

DNS Server (for IPSec VPN)

**Local**

Local Address Type

IP Address Start

End / Subnet Mask

**Remote**

Remote Address Type

IP Address Start

End / Subnet Mask

**Address Information**

My IP Address

Secure Gateway Address

**Security Protocol**

IPSec Protocol

Encryption Algorithm

Encapsulation Key

Authentication Algorithm

Authentication Key

---

The following table describes the fields in this screen.



**Table 67** VPN: Manual Key

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

**Table 67** VPN: Manual Key (continued)

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

## 17.16 Viewing SA Monitor

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

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

When there is outbound traffic but no inbound traffic, the SA times out automatically after two minutes. A tunnel with no outbound or inbound traffic is "idle" and does not timeout until the SA lifetime period expires. See [Section 17.6 on page 205](#) on keep alive to have the Prestige renegotiate an IPSec SA when the SA lifetime expires, even if there is no traffic.

**Figure 93** VPN: SA Monitor

*VPN - SA Monitor*

No.	Name	Encapsulation	IP Sec Algorithm	Disconnect
1	-	-	-	<input type="radio"/>
2	-	-	-	<input type="radio"/>
3	-	-	-	<input type="radio"/>
4	-	-	-	<input type="radio"/>
5	-	-	-	<input type="radio"/>
6	-	-	-	<input type="radio"/>
7	-	-	-	<input type="radio"/>
8	-	-	-	<input type="radio"/>
9	-	-	-	<input type="radio"/>
10	-	-	-	<input type="radio"/>
11	-	-	-	<input type="radio"/>
12	-	-	-	<input type="radio"/>
13	-	-	-	<input type="radio"/>
14	-	-	-	<input type="radio"/>
15	-	-	-	<input type="radio"/>
16	-	-	-	<input type="radio"/>
17	-	-	-	<input type="radio"/>
18	-	-	-	<input type="radio"/>
19	-	-	-	<input type="radio"/>
20	-	-	-	<input type="radio"/>

Back    Apply    Refresh

The following table describes the fields in this screen.

**Table 68** VPN: SA Monitor

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

## 17.17 Configuring Global Setting

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

**Figure 94** VPN: Global Setting

The following table describes the fields in this screen.

**Table 69** VPN: Global Setting

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

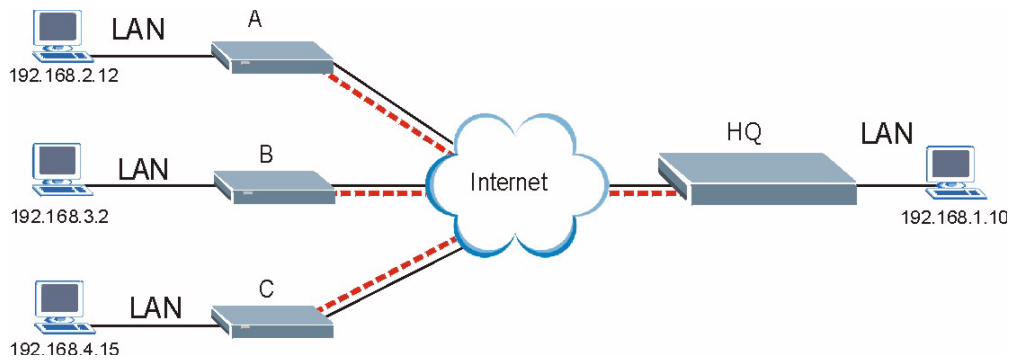
## 17.18 Telecommuter VPN/IPSec Examples

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

### 17.18.1 Telecommuters Sharing One VPN Rule Example

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

**Figure 95** Telecommuters Sharing One VPN Rule Example



**Table 70** Telecommuters Sharing One VPN Rule Example

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

### 17.18.2 Telecommuters Using Unique VPN Rules Example

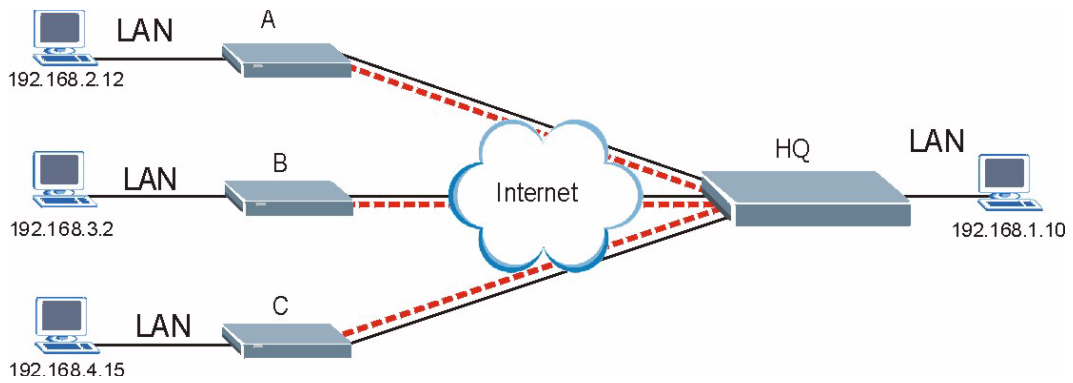
In this example the telecommuters (A, B and C in the figure) use IPsec routers with domain names that are mapped to their dynamic WAN IP addresses (use Dynamic DNS to do this).

With aggressive negotiation mode (see [Section 17.12.1 on page 216](#)), the Prestige can use the ID types and contents to distinguish between VPN rules. Telecommuters can each use a separate VPN rule to simultaneously access a Prestige at headquarters. They can use different IPsec parameters. The local IP addresses (or ranges of addresses) of the rules configured on the Prestige at headquarters can overlap. The local IP addresses of the rules configured on the telecommuters' IPsec routers should not overlap.

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

The Prestige at headquarters can also initiate VPN connections to the telecommuters since it can find the telecommuters by resolving their domain names.

**Figure 96** Telecommuters Using Unique VPN Rules Example



**Table 71** Telecommuters Using Unique VPN Rules Example

TELECOMMUTERS	HEADQUARTERS
All Telecommuter Rules:	All Headquarters Rules:
My IP Address 0.0.0.0	My IP Address: bigcompanyhq.com
Secure Gateway Address: bigcompanyhq.com	Local IP Address: 192.168.1.10
Remote IP Address: 192.168.1.10	Local ID Type: E-mail
Peer ID Type: E-mail	Local ID Content: bob@bigcompanyhq.com
Peer ID Content: bob@bigcompanyhq.com	
Telecommuter A (telecommutera.dydns.org)	Headquarters Prestige Rule 1:
Local ID Type: IP	Peer ID Type: IP
Local ID Content: 192.168.2.12	Peer ID Content: 192.168.2.12
Local IP Address: 192.168.2.12	Secure Gateway Address: telecommuter1.com
	Remote Address 192.168.2.12
Telecommuter B (telecommuterb.dydns.org)	Headquarters Prestige Rule 2:
Local ID Type: DNS	Peer ID Type: DNS
Local ID Content: telecommuterb.com	Peer ID Content: telecommuterb.com
Local IP Address: 192.168.3.2	Secure Gateway Address: telecommuterb.com
	Remote Address 192.168.3.2
Telecommuter C (telecommuterc.dydns.org)	Headquarters Prestige Rule 3:
Local ID Type: E-mail	Peer ID Type: E-mail
Local ID Content: myVPN@myplace.com	Peer ID Content: myVPN@myplace.com
Local IP Address: 192.168.4.15	Secure Gateway Address: telecommuterc.com
	Remote Address 192.168.4.15

## 17.19 VPN and Remote Management

If a VPN tunnel uses Telnet, FTP, WWW, then you should configure remote management (**Remote Management**) to allow access for that service.



# CHAPTER 18

## Remote Management Configuration

This chapter provides information on configuring remote management.

### 18.1 Remote Management Overview

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

When you configure remote management to allow management from the WAN, you still need to configure a firewall rule to allow access. See the firewall chapters for details on configuring firewall rules.

You may manage your Prestige from a remote location via:

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

When you Choose **WAN only** or **ALL** (LAN & WAN), you still need to configure a firewall rule to allow access.

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

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

- 1 Telnet
- 2 HTTP

#### 18.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

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

## 18.1.2 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.

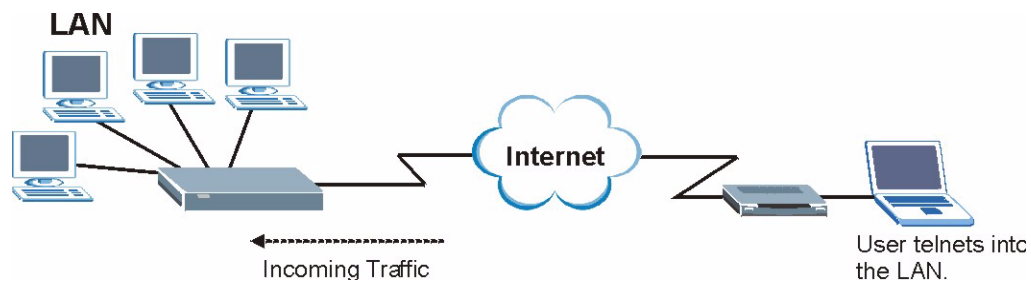
## 18.1.3 System Timeout

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.

## 18.2 Telnet

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

**Figure 97** Telnet Configuration on a TCP/IP Network



## 18.3 FTP

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

## 18.4 Web

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

## 18.5 Configuring Remote Management

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

**Figure 98** Remote Management

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

The following table describes the fields in this screen.

**Table 72** Remote Management

LABEL	DESCRIPTION
Server Type	Each of these labels denotes a service that you may use to remotely manage the Prestige.
Access Status	Select the access interface. Choices are <b>All</b> , <b>LAN Only</b> , <b>WAN Only</b> and <b>Disable</b> .
Port	This field shows the port number for the remote management service. You may change the port number for a service in this field, but you must use the same port number to use that service for remote management.
Secured Client IP	The default 0.0.0.0 allows any client to use this service to remotely manage the Prestige. Type an IP address to restrict access to a client with a matching IP address.
Apply	Click <b>Apply</b> to save your settings back to the Prestige.
Cancel	Click <b>Cancel</b> to begin configuring this screen afresh.



# CHAPTER 19

## Universal Plug-and-Play (UPnP)

This chapter introduces the UPnP feature in the web configurator.

### 19.1 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.

#### 19.1.1 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.

#### 19.1.2 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 8 on page 119](#) for further information about NAT.

#### 19.1.3 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.

## 19.2 UPnP and ZyXEL

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

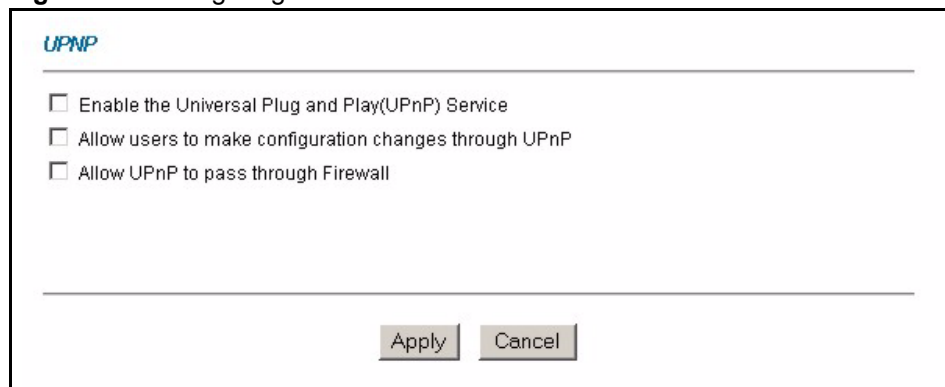
The Prestige only sends UPnP multicasts to the LAN.

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

### 19.2.1 Configuring UPnP

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

**Figure 99** Configuring UPnP



The screenshot shows a window titled "UPnP" with a horizontal line at the top. Below the line are three checkboxes, all of which are unchecked:

- Enable the Universal Plug and Play(UPnP) Service
- Allow users to make configuration changes through UPnP
- Allow UPnP to pass through Firewall

At the bottom of the window, there are two buttons: "Apply" and "Cancel".

The following table describes the fields in this screen.

**Table 73** Configuring UPnP

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

## 19.3 Installing UPnP in Windows Example

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

### Installing UPnP in Windows Me

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

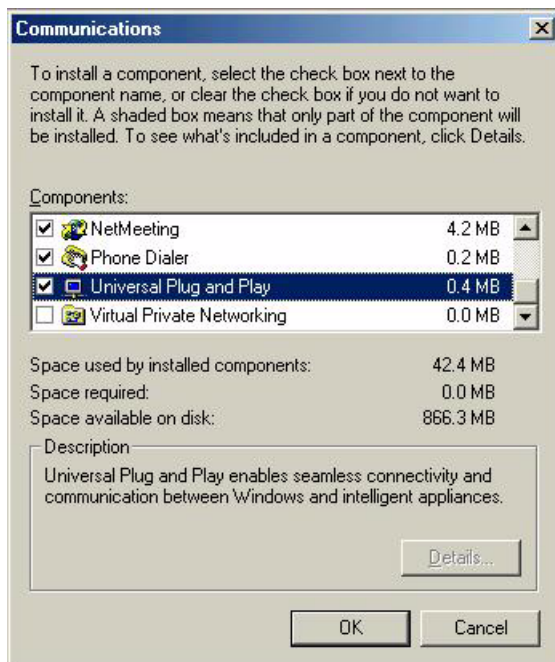
- 1** Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.
- 2** Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.

**Figure 100** 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 101** Add/Remove Programs: Windows Setup: Communication: Components



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

**5** Restart the computer when prompted.



## Installing UPnP in Windows XP

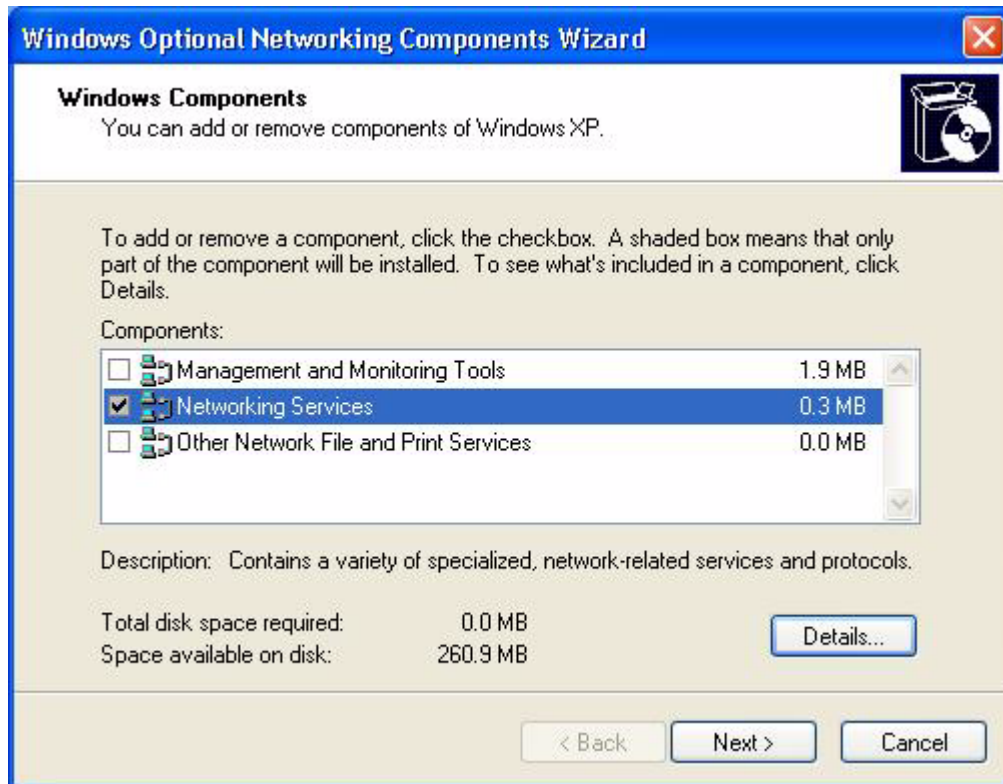
Follow the steps below to install the UPnP in Windows XP.

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

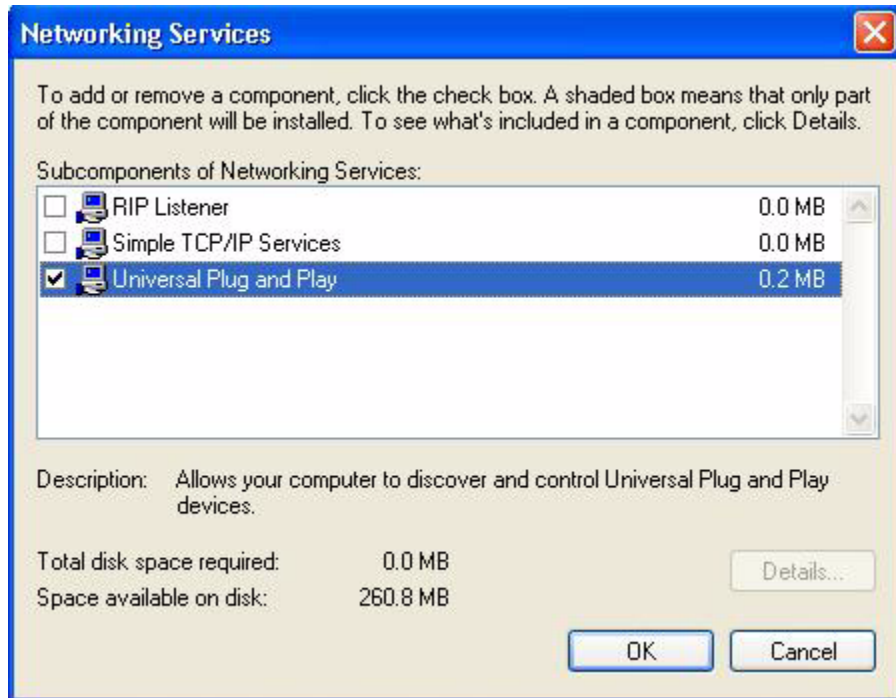
**Figure 102** Network Connections



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

**Figure 103** Windows Optional Networking Components Wizard

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

**Figure 104** Networking Services

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

## 19.4 Using UPnP in Windows XP Example

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

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

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

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

**Figure 105** Network Connections

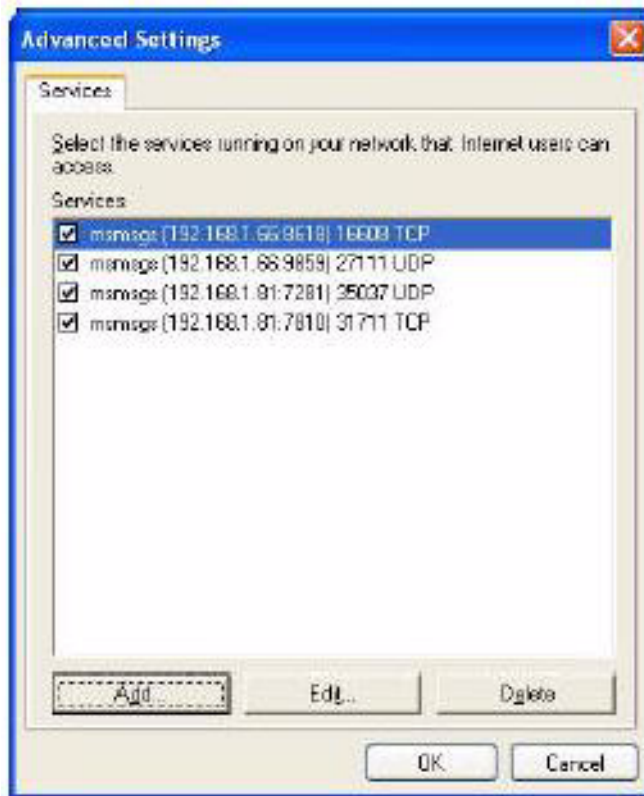


**3** In the **Internet Connection Properties** window, click **Settings** to see the port mappings there were automatically created.

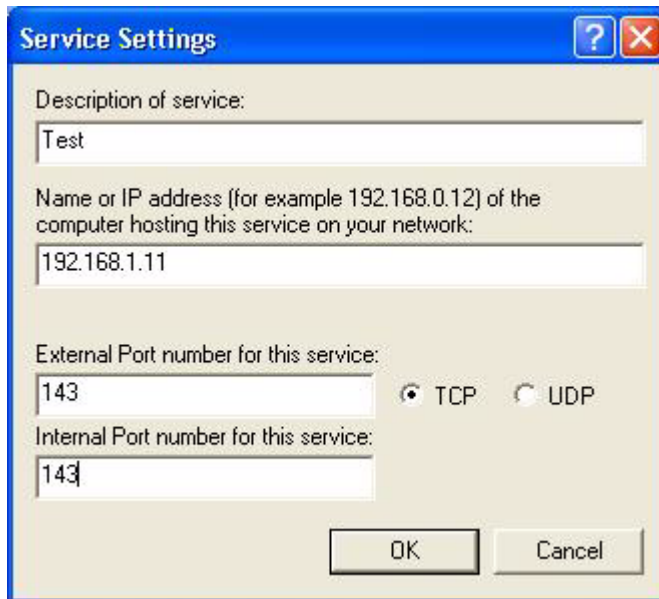
**Figure 106** Internet Connection Properties

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

**Figure 107** Internet Connection Properties: Advanced Settings



**Figure 108** 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 109** System Tray Icon

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

**Figure 110** Internet Connection Status

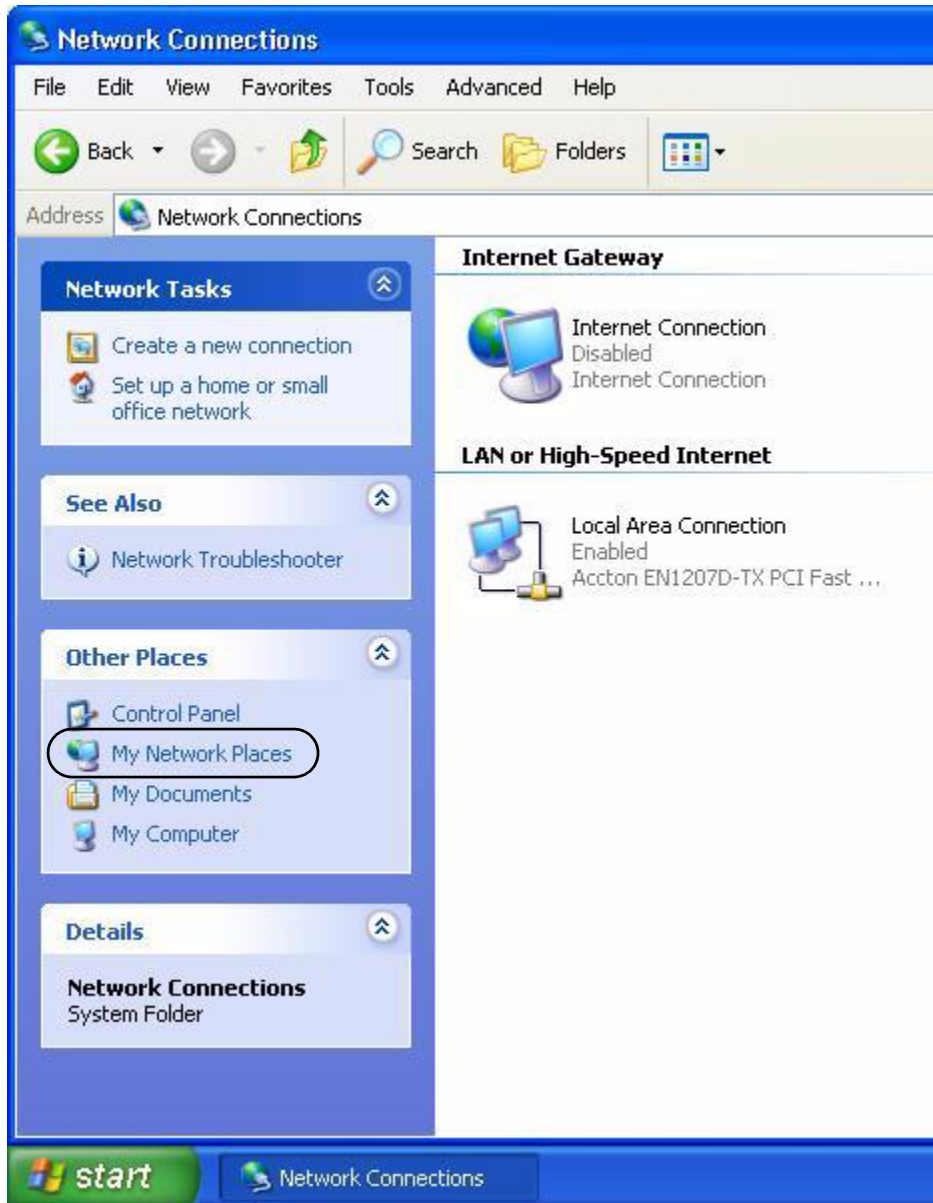
### Web Configurator Easy Access

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

Follow the steps below to access the web configurator.

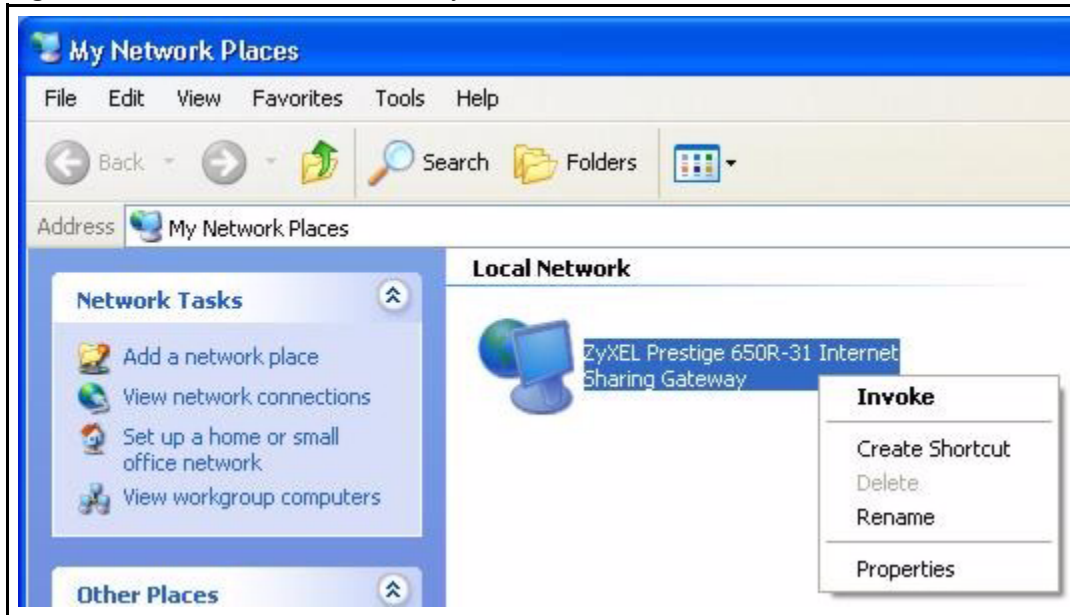
- 1 Click **Start** and then **Control Panel**.
- 2 Double-click **Network Connections**.
- 3 Select **My Network Places** under **Other Places**.

**Figure 111** 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 112** 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 113** Network Connections: My Network Places: Properties: Example



# CHAPTER 20

## Logs Screens

This chapter contains information about configuring general log settings and viewing the Prestige's logs. Refer to the appendix for example log message explanations.

### 20.1 Logs Overview

The web configurator allows you to choose which categories of events and/or alerts to have the Prestige log and then display the logs or have the Prestige send them to an administrator (as e-mail) or to a syslog server.

#### 20.1.1 Alerts and Logs

An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

### 20.2 Configuring Log Settings

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

To change your Prestige's log settings, click **Logs**, then the **Log Settings**. The screen appears as shown.

Alerts are e-mailed as soon as they happen. Logs may be e-mailed as soon as the log is full (see **Log Schedule**). Selecting many alert and/or log categories (especially **Access Control**) may result in many e-mails being sent.

**Figure 114** Log Settings

**Logs - 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)

**UNIX Syslog:**

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)

---

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"/> UPnP	<input type="checkbox"/> Attacks
<input checked="" type="checkbox"/> Forward Web Sites	<input type="checkbox"/> IPsec
<input checked="" type="checkbox"/> Blocked Web Sites	<input type="checkbox"/> IKE
<input checked="" type="checkbox"/> Attacks	
<input type="checkbox"/> IPsec	
<input type="checkbox"/> IKE	
<input checked="" type="checkbox"/> Any IP	
<input checked="" type="checkbox"/> 802.1x	
<input type="checkbox"/> SIP	
<input type="checkbox"/> RTP	
<input type="checkbox"/> FSM	

---

The following table describes the fields in this screen.

**Table 74** Log Settings

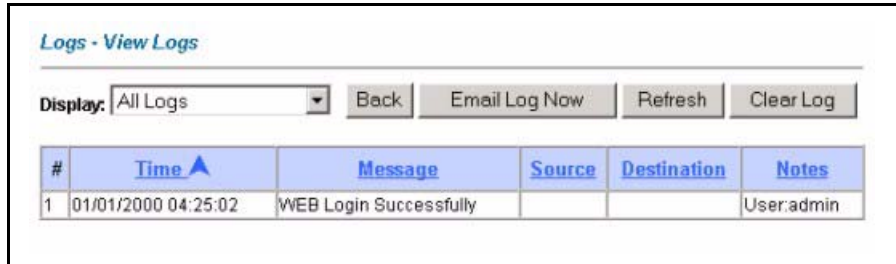
LABEL	DESCRIPTION
Address Info	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via e-mail.
Mail Subject	Type a title that you want to be in the subject line of the log 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	Alerts are sent to the e-mail address specified in this field. If this field is left blank, alerts will not be sent via e-mail.
UNIX Syslog	Syslog logging sends a log to an external syslog server used to store logs.
Active	Click <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 you select <b>Weekly</b> or <b>Daily</b>, specify a time of day when the E-mail should be sent. If you select <b>Weekly</b>, then also specify which day of the week the E-mail should be sent. If you select <b>When Log is Full</b>, 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	Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Log	Select the categories of logs that you want to record. Logs include alerts.
Send Immediate Alert	Select the categories of alerts for which you want the Prestige to instantly e-mail alerts to the e-mail address specified in the <b>Send Alerts To</b> field.
Back	Click <b>Back</b> to return to the previous screen.
Apply	Click <b>Apply</b> to save your customized settings and exit this screen.
Cancel	Click <b>Cancel</b> to return to the previously saved settings.

## 20.3 Displaying the Logs

Click **Logs** and then **View Log** to open the **View Logs** screen. Use the **View Logs** screen to see the logs for the categories that you selected in the **Log Settings** screen (see [Section 20.2 on page 247](#)).

Log entries in red indicate alerts. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.

**Figure 115** View Logs



The following table describes the fields in this screen.

**Table 75** View Logs

LABEL	DESCRIPTION
Display	The categories that you select in the <b>Log Settings</b> screen (see <i>section</i> ) display in the drop-down list box. Select a category of logs to view; select <b>All Logs</b> to view logs from all of the log categories that you selected in the <b>Log Settings</b> page.
Time	This field displays the time the log was recorded. See the chapter on system maintenance and information to configure the Prestige's time and date.
Message	This field states the reason for the log.
Source	This field lists the source IP address and the port number of the incoming packet.
Destination	This field lists the destination IP address and the port number of the incoming packet.
Notes	This field displays additional information about the log entry.
Back	Click <b>Back</b> to return to the previous screen
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 (make sure that you have first filled in the <b>Address Info</b> fields in <b>Log Settings</b> , see <a href="#">Section 20.2 on page 247</a> ).
Refresh	Click <b>Refresh</b> to renew the log screen.
Clear Log	Click <b>Clear Log</b> to delete all the logs.

## 20.4 SMTP Error Messages

If there are difficulties in sending e-mail the following error messages appear.

E-mail error messages appear in SMT menu 24.3.1 as "SMTP action request failed. ret= ??". The "??" are described in the following table.

**Table 76** SMTP Error Messages

-1 means Prestige out of socket
-2 means tcp SYN fail
-3 means smtp server OK fail
-4 means HELO fail
-5 means MAIL FROM fail
-6 means RCPT TO fail
-7 means DATA fail
-8 means mail data send fail

### 20.4.1 Example E-mail Log

An "End of Log" message displays for each mail in which a complete log has been sent. The following is an example of a log sent by e-mail.

- You may edit the subject title.
- The date format here is Day-Month-Year.
- The date format here is Month-Day-Year. The time format is Hour-Minute-Second.
- "End of Log" message shows that a complete log has been sent.

**Figure 116** E-mail Log Example

```

Subject:
    Firewall Alert From Prestige
Date:
    Fri, 07 Apr 2000 10:05:42
From:
    user@zyxel.com
To:
    user@zyxel.com
1|Apr 7 00 |From:192.168.1.1      To:192.168.1.255  |default policy
|forward
| 09:54:03 |UDP      src port:00520 dest port:00520  |<1,00>          |
2|Apr 7 00 |From:192.168.1.131  To:192.168.1.255  |default policy
|forward
| 09:54:17 |UDP      src port:00520 dest port:00520  |<1,00>          |
3|Apr 7 00 |From:192.168.1.6    To:10.10.10.10   |match           |forward
| 09:54:19 |UDP      src port:03516 dest port:00053  |<1,01>          |
.....{snip}.....
.....{snip}.....
126|Apr 7 00 |From:192.168.1.1    To:192.168.1.255  |match           |forward
| 10:05:00 |UDP      src port:00520 dest port:00520  |<1,02>          |
127|Apr 7 00 |From:192.168.1.131  To:192.168.1.255  |match           |forward
| 10:05:17 |UDP      src port:00520 dest port:00520  |<1,02>          |
128|Apr 7 00 |From:192.168.1.1    To:192.168.1.255  |match           |forward
| 10:05:30 |UDP      src port:00520 dest port:00520  |<1,02>          |
End of Firewall Log

```



# CHAPTER 21

## Maintenance

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

### 21.1 Maintenance Overview

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

### 21.2 System Status Screen

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

**Figure 117** System Status

*System Status*

---

**System Status**

System Name:  
 ZyNOS FW Version: V3.40(MF.2) | 12/8/2004  
 DSL FW Version: TI AR7 01.01.00.00  
 Standard: NORMAL

**WAN Information**

IP Address: 0.0.0.0  
 IP Subnet Mask: 0.0.0.0  
 Default Gateway: 0.0.0.0  
 VPI/VCI: 8/35

**LAN Information**

MAC Address: 00:a0:c5:00:00:01  
 IP Address: 192.168.1.1  
 IP Subnet Mask: 255.255.255.0  
 DHCP: Server  
 DHCP Start IP: 192.168.1.33  
 DHCP Pool Size: 32

**WLAN Information**

ESSID: Wireless  
 Channel: 6  
 WEP: Disable

**Voice Information**

SIP1 URI: ChangeMe@192.168.1.33	
SIP1 Registration Status: Not Register	<input type="button" value="Register"/>
Used Port: 5060/UDP	
SIP2 URI: ChangeMe@192.168.1.33	
SIP2 Registration Status: Not Register	<input type="button" value="Register"/>
Used Port: 5060/UDP	

The following table describes the fields in this screen.

**Table 77** System Status

LABEL	DESCRIPTION
System Status	
System Name	This is the name of your Prestige. It is for identification purposes.
ZyNOS Firmware Version	This is the ZyNOS firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design.
DSL FW Version	This is the DSL firmware version associated with your Prestige.
Standard	This is the standard that your Prestige is using.
WAN Information	
IP Address	This is the WAN port IP address.
IP Subnet Mask	This is the WAN port IP subnet mask.
Default Gateway	This is the IP address of the default gateway, if applicable.
VPI/VCI	This is the Virtual Path Identifier and Virtual Channel Identifier that you entered in the first Wizard screen.
LAN Information	
MAC Address	This is the MAC (Media Access Control) or Ethernet address unique to your Prestige.
IP Address	This is the LAN port IP address.
IP Subnet Mask	This is the LAN port IP subnet mask.
DHCP	This is the WAN port DHCP role - <b>Server</b> , <b>Relay</b> (not all Prestige models) or <b>None</b> .
DHCP Start IP	This is the first of the contiguous addresses in the IP address pool.
DHCP Pool Size	This is the number of IP addresses in the IP address pool.
WLAN Information	
ESSID	This is the descriptive name used to identify the Prestige in the wireless LAN.
Channel	This is the channel number used by the Prestige now.
WEP	This displays the status of WEP data encryption.
Voice Information	
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 Registered</b> when the Prestige has not successfully registered the SIP account with the SIP register server.
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.
Used Port	This field displays the Prestige's listening port for SIP traffic on this SIP account.
Show Statistics	Click <b>Show Statistics</b> to see the performance statistics such as number of packets sent and number of packets received for each port.

## 21.2.1 System Statistics

Click **Show Statistics** in the **System Status** screen to open the following screen. Read-only information here includes port status and packet specific statistics. Also provided are "system up time" and "poll interval(s)". The **Poll Interval(s)** field is configurable.

**Figure 118** System Status: Show Statistics

**System up Time: 4:37:26**  
CPU Load: 3.63%

**WAN Port Statistics:**  
Link Status: **Down**  
Upstream Speed: **0 kbps**  
Downstream Speed: **0 kbps**

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

LAN Port Statistics:

Interface:	Status	TxPkts	RxPkts	Collisions
Ethernet	100M/Full Duplex	5369	4361	0
Wireless	54M	1334	454	0

Voice Statistics:

Phone	Status	TxPkts	RxPkts	Tx B/s	Rx B/s	Talk Time
1	OnHook	0	0	0	0	0:00:00
2	OnHook	0	0	0	0	0:00:00

**Poll Interval(s) :**

The following table describes the fields in this screen.

**Table 78** System Status: Show Statistics

LABEL	DESCRIPTION
System up Time	This is the elapsed time the system has been up.
CPU Load	This field specifies the percentage of CPU utilization.
LAN or WAN Port Statistics	This is the WAN or LAN port.
Link Status	This is the status of your WAN link.
Upstream Speed	This is the upstream speed of your Prestige.
Downstream Speed	This is the downstream speed of your Prestige.
Node-Link	This field displays the remote node index number and link type. Link types are PPPoA, ENET, RFC 1483 and PPPoE.
Interface	This field displays the type of port.

**Table 78** System Status: Show Statistics (continued)

LABEL	DESCRIPTION
Status	For the WAN port, 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. For a LAN port, this shows the port speed and duplex setting.
TxPkts	This field displays the number of packets transmitted on this port.
RxPkts	This field displays the number of packets received on this port.
Errors	This field displays the number of error packets on this port.
Tx B/s	This field displays the number of bytes transmitted in the last second.
Rx B/s	This field displays the number of bytes received in the last second.
Up Time	This field displays the elapsed time this port has been up.
Collisions	This is the number of collisions on this port.
Voice Statistics	The voice statistics fields apply to calls currently being made or received on a telephone connected to one of the Prestige's phone ports.
Phone	This field displays the Prestige's phone port number.
Status	Status This field displays <b>Onhook</b> when the telephone handset is in it's cradle and <b>Offhook</b> when telephone handset is out of it's cradle.
TxPkts	This field displays a call's number of RTP (Real time Transport Protocol) packets that have been transmitted. RTP is used to handle voice data transfer. This field displays 0 again after the call ends.
RxPkts	This field displays a call's number of RTP packets received. This field displays 0 again after the call ends.
Tx B/s	This field displays a call's number of bytes of RTP traffic transmitted in the last second. This field displays 0 again after the call ends.
Rx B/s	This field displays a call's number of bytes of RTP traffic received in the last second. This field displays 0 again after the call ends.
Talk Time	This field displays a call's duration. This field displays 0 again after the call ends.
Poll Interval(s)	Type the time interval for the browser to refresh system statistics.
Set Interval	Click this button to apply the new poll interval you entered in the <b>Poll Interval</b> field above.
Stop	Click this button to halt the refreshing of the system statistics.

## 21.3 DHCP Table Screen

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the Prestige as a DHCP server or disable it. When configured as a server, the Prestige provides the TCP/IP configuration for the clients. If set to **None**, DHCP service will be disabled and you must have another DHCP server on your LAN, or else the computer must be manually configured.

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

**Figure 119** DHCP Table

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

The following table describes the fields in this screen.

**Table 79** DHCP Table

LABEL	DESCRIPTION
Host Name	This is the name of the host computer.
IP Address	This field displays the IP address relative to the <b>Host Name</b> field.
MAC Address	This field displays the MAC (Media Access Control) address of the computer with the displayed host name.  Every Ethernet device has a unique MAC address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

## 21.4 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 5.5 on page 82](#) for more information.

**Figure 120** Any IP Table

Any IP Table		
#	IP Address	MAC Address
1	192.168.10.1	00:50:ba:ad:4f:81

Refresh

The following table describes the labels in this screen.

**Table 80** Any IP Table

LABEL	DESCRIPTION
#	This field displays the index number.
IP Address	This field displays the IP address of the network device.

**Table 80** Any IP Table

LABEL	DESCRIPTION
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.

## 21.5 Wireless Screen

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

### 21.5.1 Association List

This screen displays the MAC address(es) of the wireless stations that are currently logged in to the network. Click **Wireless LAN** and then **Association List** to open the screen shown next.

**Figure 121** Association List

<i>Wireless LAN - Association List</i>		
#	MAC Address	Association Time
001	00:a0:c5:00:07:27	00:27:37 2000/01/01
002	00:a0:c5:00:00:07	07:15:45 2000/01/01

The following table describes the fields in this screen.

**Table 81** Association List

LABEL	DESCRIPTION
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC (Media Access Control) address of an associated wireless station. Every Ethernet device has a unique MAC address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
Association Time	This field displays the time a wireless station is associated to the Prestige.
Back	Click <b>Back</b> to return to the previous screen.
Refresh	Click <b>Refresh</b> to renew the information in the table.

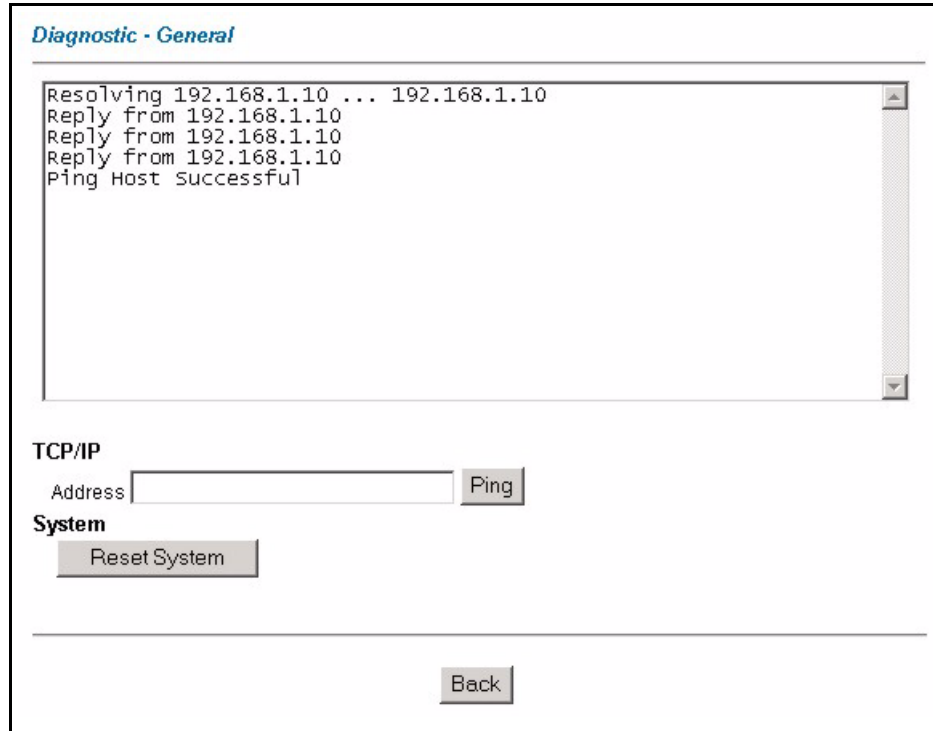
## 21.6 Diagnostic Screens

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

### 21.6.1 Diagnostic General Screen

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

**Figure 122** Diagnostic: General



The following table describes the fields in this screen.

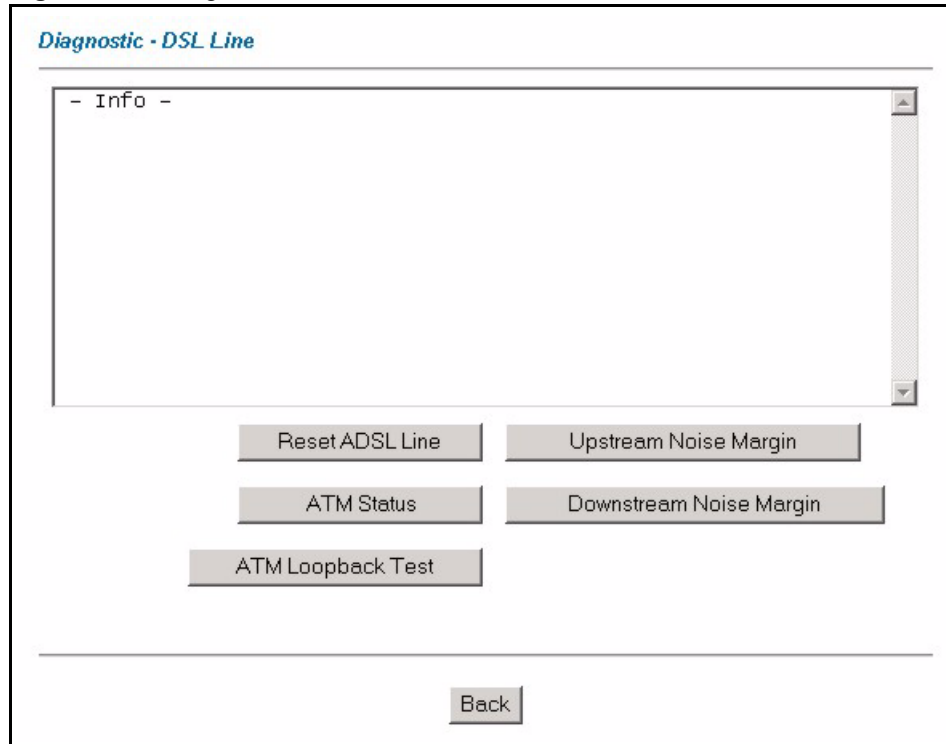
**Table 82** Diagnostic: General

LABEL	DESCRIPTION
TCP/IP Address	Type the IP address of a computer that you want to ping in order to test a connection.
Ping	Click this button to ping the IP address that you entered.
Reset System	Click this button to reboot the Prestige. A warning dialog box is then displayed asking you if you're sure you want to reboot the system. Click <b>OK</b> to proceed.
Back	Click this button to go back to the main <b>Diagnostic</b> screen.

### 21.6.2 Diagnostic DSL Line Screen

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



**Figure 123** Diagnostic: DSL Line

The following table describes the fields in this screen.

**Table 83** Diagnostic: DSL Line

LABEL	DESCRIPTION
Reset ADSL Line	Click this button to reinitialize the ADSL line. The large text box above then displays the progress and results of this operation, for example: "Start to reset ADSL Loading ADSL modem F/W... Reset ADSL Line Successfully!"
ATM Status	Click this button to view ATM status.
ATM Loopback Test	Click this button to start the ATM loopback test. Make sure you have configured at least one PVC with proper VPIs/VCI before you begin this test. The Prestige sends an OAM F5 packet to the DSLAM/ATM switch and then returns it (loops it back) to the Prestige. The ATM loopback test is useful for troubleshooting problems with the DSLAM and ATM network.
Upstream Noise Margin	Click this button to display the upstream noise margin.
Downstream Noise Margin	Click this button to display the downstream noise margin.
Back	Click this button to go back to the main <b>Diagnostic</b> screen.

## 21.7 Firmware 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. See [Chapter 37 on page 365](#) for upgrading firmware using FTP/TFTP commands.

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

Click **Firmware** to open the following screen. Follow the instructions in this screen to upload firmware to your Prestige.

**Figure 124** Firmware Upgrade

**FIRMWARE**

---

**Firmware Upgrade**

To upgrade the internal router firmware, browse to the location of the binary (.BIN) upgrade file and click **UPLOAD**.

File Path:  **Browse...** **Upload**

---

**CONFIGURATION FILE**

Click **Reset** to clear all user-defined configurations and return to the factory defaults.

**Reset**

The following table describes the labels in this screen.

**Table 84** Firmware Upgrade

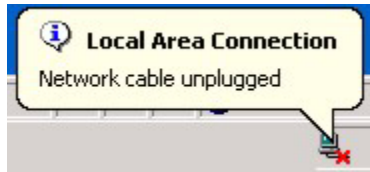
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click <b>Browse ...</b> to find it.
Browse...	Click <b>Browse...</b> to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click <b>Upload</b> to begin the upload process. This process may take up to two minutes.
Reset	Click this button to clear all user-entered configuration information and return the Prestige to its factory defaults. Refer to the <i>Resetting the Prestige</i> section.

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

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

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

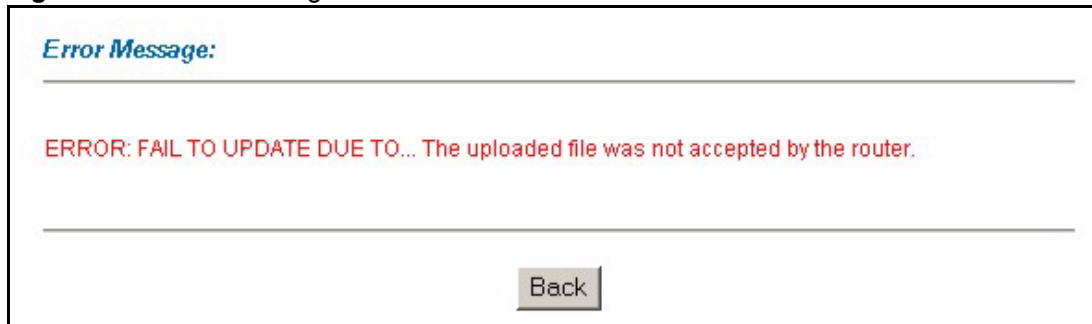
**Figure 125** Network Temporarily Disconnected



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

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

**Figure 126** Error Message





# CHAPTER 22

## Introducing the SMT

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

### 22.1 Introduction to the SMT

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

### 22.2 Accessing the SMT via the Console Port

Make sure you have the physical connection properly set up as described in the *Quick Start Guide*.

When configuring using the console port, you need a computer equipped with communications software configured to the following parameters:

- VT100 terminal emulation.
- 9600 Baud.
- No parity, 8 data bits, 1 stop bit, flow control set to none.

#### 22.2.1 Initial Screen

When you turn on your Prestige, it performs several internal tests as well as line initialization.

After the tests, the Prestige asks you to press [ENTER] to continue, as shown next.

**Figure 127** Initial Screen

```
Copyright (c) 1994 - 2004 ZyXEL Communications Corp.
initialize ch =0, ethernet address: 00:A0:C5:7A:86:D5
initialize ch =1, ethernet address: 00:A0:C5:7A:86:D6
initialize ch =2, ethernet address: 00:A0:C5:7A:86:D7
initialize ch =3, ethernet address: 00:00:00:00:00:00
AUX port init . done
Modem init . inactive

Press ENTER to continue...
```

## 22.2.2 Entering the Password

The login screen appears after you press [ENTER], prompting you to enter the password, as shown below.

For your first login, enter the default password “1234”. As you type the password, the screen displays an “X” for each character you type.

Please note that if there is no activity for longer than five minutes after you log in, your Prestige will automatically log you out and display a blank screen. If you see a blank screen, press [ENTER] to bring up the login screen again.

**Figure 128** Password Screen

```
Enter Password : XXXX
```

## 22.2.3 Procedure for SMT Configuration via Telnet

The following procedure details how to telnet into your Prestige.

- 1** In Windows, click **Start** (usually in the bottom left corner), **Run** and then type "telnet 192.168.1.1" (the default IP address) and click **OK**.
- 2** Enter “1234” in the **Password** field.
- 3** After entering the password you will see the main menu.

Please note that if there is no activity for longer than five minutes (default timeout period) after you log in, your Prestige will automatically log you out. You will then have to telnet into the Prestige again.

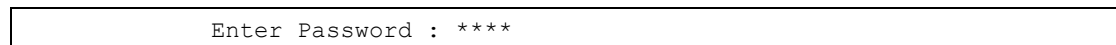
## 22.2.4 Entering Password

The login screen appears after you press [ENTER], prompting you to enter the password, as shown next.

For your first login, enter the default password "1234". As you type the password, the screen displays an asterisk "\*" for each character you type.

Please note that if there is no activity for longer than five minutes after you log in, your Prestige will automatically log you out.

**Figure 129** Login Screen



## 22.3 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 85** Navigating the SMT Interface

OPERATION	KEY STROKE	DESCRIPTION
Move down to another menu	[ENTER]	To move forward to a submenu, type in the number of the desired submenu and press [ENTER].
Move up to a previous menu	[ESC]	Press [ESC] to move back to the previous menu.
Move to a hidden menu	Press [SPACE BAR] to change <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> , then press [ENTER] to go to the "hidden" menu.
Move the cursor	[ENTER] or [UP]/[DOWN] arrow keys.	Within a menu, press [ENTER] to move to the next field. You can also use the [UP]/[DOWN] arrow keys to move to the previous and the next field, respectively.
Entering information	Type in or press [SPACE BAR], then press [ENTER].	You need to fill in two types of fields. The first requires you to type in the appropriate information. The second allows you to cycle through the available choices by pressing [SPACE BAR].
Required fields	<? > or <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.

**Table 85** Navigating the SMT Interface

OPERATION	KEY STROKE	DESCRIPTION
Save your configuration	[ENTER]	Save your configuration by pressing [ENTER] at the message "Press ENTER to confirm or ESC to cancel". Saving the data on the screen will take you, in most cases to the previous menu.
Exit the SMT		Type 99, then press [ENTER]. Type 99 at the main menu prompt and press [ENTER] to exit the SMT interface.

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

**Table 86** SMT Main Menu

Copyright (c) 1994 - 2004 ZyXEL Communications Corp.	
Prestige 2602HW-61 Main Menu	
Getting Started	Advanced Management
1. General Setup	21. Filter and Firewall Setup
2. WAN Backup Setup	22. SNMP Configuration
3. LAN Setup	23. System Security
4. Internet Access Setup	24. System Maintenance
	25. IP Routing Policy Setup
Advanced Applications	26. Schedule Setup
11. Remote Node Setup	27. VPN/IPSec Setup
12. Static Routing Setup	
14. Dial-in User Setup	99. Exit
15. NAT Setup	
Enter Menu Selection Number:	

### 22.3.1 System Management Terminal Interface Summary

**Table 87** Main Menu Summary

#	MENU TITLE	DESCRIPTION
1	General Setup	Use this menu to set up your general information.
2	WAN Backup Setup	Use this menu to setup traffic redirect and dial-back up.
3	LAN Setup	Use this menu to set up your wireless LAN and LAN connection.
4	Internet Access Setup	A quick and easy way to set up an Internet connection.
11	Remote Node Setup	Use this menu to set up the Remote Node for LAN-to-LAN connection, including Internet connection.
12	Static Routing Setup	Use this menu to set up static routes.
14	Dial-in User Setup	Use this menu to set up local user profiles on the Prestige.
15	NAT Setup	Use this menu to specify inside servers when NAT is enabled.
21	Filter and Firewall Setup	Use this menu to configure filters, activate/deactivate the firewall and view the firewall log.
22	SNMP Configuration	Use this menu to set up SNMP related parameters.
23	System Security	Use this menu to set up wireless security and change your password.



**Table 87** Main Menu Summary

#	MENU TITLE	DESCRIPTION
24	System Maintenance	This menu provides system status, diagnostics, software upload, etc.
25	IP Routing Policy Setup	Use this menu to configure your IP routing policy.
26	Schedule Setup	Use this menu to schedule outgoing calls.
27	VPN/IPSec Setup	Use this menu to configure VPN connections.
99	Exit	Use this to exit from SMT and return to a blank screen.

## 22.3.2 SMT Menus Overview

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

**Table 88** SMT Menus Overview

MENUS	SUB MENUS		
1 General Setup	1.1 Configure Dynamic DNS		
2 WAN Backup Setup	2.1 Traffic Redirect Setup		
3 LAN Setup	3.1 LAN Port Filter Setup		
	3.2 TCP/IP and DHCP Setup	3.2.1 IP Alias Setup	
	3.5 Wireless LAN Setup	3.5.1 WLAN MAC Address Filter	
4 Internet Access Setup			
11 Remote Node Setup	11.1 Remote Node Profile		
	11.3 Remote Node Network Layer Options		
	11.5 Remote Node Filter		
	11.6 Remote Node ATM Layer Options		
	11.8 Advance Setup Options		
12 Static Routing Setup	12.1 Edit Static Route Setup	12.1.1 Edit IP Static Route	
	12.3 Bridge Static Route	12.3.1 Edit Bridge Static Route	
14 Dial-in User Setup	14.1 Edit Dial-in User		
15 NAT Setup	15.1 Address Mapping Sets	15.1.1 Address Mapping Rules	15.1.1.x Address Mapping Rule
	15.2 NAT Server Sets	15.2.x NAT Server Setup	

**Table 88** SMT Menu Overview (continued)

MENUS	SUB MENUS		
21 Filter and Firewall Rule Setup	21.1 Filter Setup	21.1 Filter Rules Summary	21.1.x.1 Generic Filter Rule
			21.1.x.1 TCP/IP Filter Rule
	21.1 Firewall Setup		
22 SNMP Configuration			
23 System Security	23.1 Change Password		
	23.2 RADIUS Server		
	23.4 IEEE802.1X		
24 System Maintenance	24.1 Status		
	24.2 System Information and Console Port Speed	24.2.1 Information	
		24.2.2 Change Console Port Speed	
	24.3 Log and Trace	24.3.1 View Error Log	
		24.3.2 UNIX Syslog	
	24.4 Diagnostic		
	24.5 Backup Configuration		
	24.6 Restore Configuration		
	24.7 Upload Firmware	24.7.1 Upload System Firmware	
		24.7.2 Upload System Configuration File	
	24.8 Command Interpreter Mode		
	24.9 Call Control	24.9.1 Budget Management	
24.10 Time and Date Setting			
24.11 Remote Management Control			
25 IP Routing Policy Setup	25.1 IP Policy Routing Setup	25.1.1 IP Routing Policy	
26 Schedule Setup	26.1 Schedule Setup		
27 VPN/IPSec Setup	27.1 IPSec Summary	27.1.1 IPSec Setup	27.1.1.1 IKE Setup
			27.1.1.2 Manual Setup
	27.1 SA Monitor		

## 22.4 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 Security**.
- 2** Enter 1 to display **Menu 23.1 - System Security - Change Password** as shown next.
- 3** Type your existing system password in the **Old Password** field, for example "1234", and press [ENTER].

**Figure 130** Menu 23.1 Change Password

```
Menu 23.1 - System Security - Change Password
Old Password= ?
New Password= ?
Retype to confirm= ?
Enter here to CONFIRM or ESC to CANCEL:
```

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

**Note:** Note that as you type a password, the screen displays an "\*" for each character you type.



# CHAPTER 23

## Menu 1 General Setup

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

### 23.1 General Setup

**Menu 1 — General Setup** contains administrative and system-related information (shown next). The **System Name** field is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

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

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

### 23.2 Procedure To Configure Menu 1

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

**Figure 131** Menu 1 General Setup

```

Menu 1 General Setup
System Name= ?
Location=
Contact Person's Name=
Domain Name=
Edit Dynamic DNS= No

Route IP= Yes
Bridge= No
Press ENTER to Confirm or ESC to Cancel:
    
```

Fill in the required fields. Refer to the table shown next for more information about these fields.

**Table 89** Menu 1 General Setup

FIELD	DESCRIPTION
System Name	Choose a descriptive name for identification purposes. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Location (optional)	Enter the geographic location (up to 31 characters) of your Prestige.
Contact Person's Name (optional)	Enter the name (up to 30 characters) of the person in charge of this Prestige.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. You can go to menu 24.8 and type "sys domainname" to see the current domain name used by your gateway. If you want to clear this field just press the [SPACE BAR]. The domain name entered by you is given priority over the ISP assigned domain name.
Edit Dynamic DNS	Press the [SPACE BAR] to select <b>Yes</b> or <b>No</b> (default). Select <b>Yes</b> to configure <b>Menu 1.1 — Configure Dynamic DNS</b> (discussed next).
Route IP	Set this field to <b>Yes</b> to enable or <b>No</b> to disable IP routing. You must enable IP routing for Internet access.
Bridge	Turn on/off bridging for protocols not supported (for example, SNA) or not turned on in the previous <b>Route IP</b> field. Select <b>Yes</b> to turn bridging on; select <b>No</b> to turn bridging off.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm or ESC to Cancel:" to save your configuration, or press [ESC] at any time to cancel.	

### 23.2.1 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 132** Menu 1.1 Configure Dynamic DNS

```

Menu 1.1 - Configure Dynamic DNS
Service Provider= WWW.DynDNS.ORG
Active= No
Host=
EMAIL=
USER=
Password= *****
Enable Wildcard= No
Press ENTER to Confirm or ESC to Cancel:

```

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

**Table 90** 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.
Host	Enter the domain name assigned to your Prestige by your dynamic DNS provider.
EMAIL	Enter your e-mail address.
User	Enter your user name.
Password	Enter the password assigned to you.
Enable Wildcard	Your Prestige supports DYNDNS Wildcard. Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> or <b>No</b> . This field is <b>N/A</b> when you choose DDNS client as your service provider.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm or ESC to Cancel:" to save your configuration, or press [ESC] at any time to cancel.	





# CHAPTER 24

## Menu 2 WAN Backup Setup

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

### 24.1 Introduction to WAN Backup Setup

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

### 24.2 Configuring WAN Backup in Menu 2

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

**Figure 133** Menu 2 WAN Backup Setup

```

Menu 2 - Wan Backup Setup
Check Mechanism = DSL Link
Check WAN IP Address1 = 0.0.0.0
Check WAN IP Address2 = 0.0.0.0
Check WAN IP Address3 = 0.0.0.0
  KeepAlive Fail Tolerance = 0
  Recovery Interval(sec) = 0
  ICMP Timeout(sec) = 0
  Traffic Redirect = No
Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the fields in this menu.

**Table 91** Menu 2 WAN Backup Setup

FIELD	DESCRIPTION
Check Mechanism	Press [SPACE BAR] and then press [ENTER] to select the method that the Prestige uses to check the DSL connection. Select <b>DSL Link</b> to have the Prestige check the DSL connection's physical layer. Select <b>ICMP</b> to have the Prestige periodically ping the IP addresses configured in the <b>Check WAN IP Address</b> fields.
Check WAN IP Address1-3	Configure this field to test your Prestige's WAN accessibility. Type the IP address of a reliable nearby computer (for example, your ISP's DNS server address). When using a WAN backup connection, the Prestige periodically pings the addresses configured here and uses the other WAN backup connection (if configured) if there is no response.

**Table 91** Menu 2 WAN Backup Setup (continued)

FIELD	DESCRIPTION
KeepAlive Fail Tolerance	Type the number of times (2 recommended) that your Prestige may ping the IP addresses configured in the <b>Check WAN IP Address</b> field without getting a response before switching to a WAN backup connection (or a different WAN backup connection).
Recovery Interval(sec)	When the Prestige is using a lower priority connection (usually a WAN backup connection), it periodically checks to whether or not it can use a higher priority connection. Type the number of seconds (30 recommended) for the Prestige to wait between checks. Allow more time if your destination IP address handles lots of traffic.
ICMP Timeout	Type the number of seconds for an ICMP session to wait for the ICMP response
Traffic Redirect	Press [SPACE BAR] to select <b>Yes</b> or <b>No</b> . Select <b>Yes</b> and press [ENTER] to configure <b>Menu 2.1 Traffic Redirect Setup</b> . Select <b>No</b> (default) if you do not want to configure this feature.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm or ESC to Cancel:" to save your configuration, or press [ESC] at any time to cancel.	

## 24.2.1 Traffic Redirect Setup

Configure parameters that determine when the Prestige will forward WAN traffic to the backup gateway using **Menu 2.1 — Traffic Redirect Setup**.

**Figure 134** Menu 2.1Traffic Redirect Setup

```

Menu 2.1 - Traffic Redirect Setup
Active= No
Configuration:
Backup Gateway IP Address= 0.0.0.0
Metric= 15
Press ENTER to Confirm or ESC to Cancel:
    
```

The following table describes the fields in this menu.

**Table 92** Menu 2.1Traffic 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.

**Table 92** Menu 2.1Traffic Redirect Setup

FIELD	DESCRIPTION
Metric	This field sets this route's priority among the routes the Prestige uses. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost"
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm or ESC to Cancel:" to save your configuration, or press [ESC] at any time to cancel.	



# CHAPTER 25

## Menu 3 LAN Setup

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

### 25.1 LAN Setup

This section describes how to configure the Ethernet using **Menu 3 — LAN Setup**. From the main menu, enter 3 to display menu 3.

**Figure 135** Menu 3 LAN Setup

```
Menu 3 - LAN Setup
1. LAN Port Filter Setup
2. TCP/IP and DHCP Setup

5. Wireless LAN Setup
Enter Menu Selection Number:
```

#### 25.1.1 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 136** 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 33 on page 331](#) first, then return to this menu to define the filter sets.

### 25.2 Protocol Dependent Ethernet Setup

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

- For TCP/IP Ethernet setup refer to [Section 27.6 on page 292](#).
- For bridging Ethernet setup refer to [Chapter 30 on page 309](#).

## 25.3 TCP/IP Ethernet Setup and DHCP

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

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

**Figure 137** Menu 3.2 TCP/IP and DHCP Ethernet Setup

```

Menu 3.2 - TCP/IP and DHCP Setup
DHCP Setup
DHCP= Server
Client IP Pool Starting Address= 192.168.1.33
Size of Client IP Pool= 32
Primary DNS Server= 0.0.0.0
Secondary DNS Server= 0.0.0.0
Remote DHCP Server= N/A
TCP/IP Setup:
IP Address= 192.168.1.1
IP Subnet Mask= 255.255.255.0
RIP Direction= None
Version= N/A
Multicast= None
IP Policies=
Edit IP Alias= No
Press ENTER to Confirm or ESC to Cancel:
    
```

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

**Table 93** DHCP Ethernet Setup

FIELD	DESCRIPTION
DHCP Setup	
DHCP	<p>If set to <b>Server</b>, your Prestige can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client.</p> <p>If set to <b>None</b>, the DHCP server will be disabled.</p> <p>If set to <b>Relay</b>, the Prestige acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the Remote DHCP Server in this case.</p> <p>When DHCP server is used, the following items need to be set:</p>
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.

**Table 93** DHCP Ethernet Setup (continued)

FIELD	DESCRIPTION
Size of Client IP Pool	This field specifies the size or count of the IP address pool.
Primary DNS Server Secondary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Remote DHCP Serve	If <b>Relay</b> is selected in the <b>DHCP</b> field above then enter the IP address of the actual remote DHCP server here.

Follow the instructions in the following table to configure TCP/IP parameters for the Ethernet port.

**Table 94** TCP/IP Ethernet Setup

FIELD	DESCRIPTION
TCP/IP Setup	
IP Address	Enter the (LAN) IP address of your Prestige in dotted decimal notation
IP Subnet Mask	Your Prestige will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Prestige (refer to the appendix on IP subnetting for more information).
RIP Direction	Press [SPACE BAR] to select the RIP direction. Choices are <b>Both</b> , <b>In Only</b> , <b>Out Only</b> or <b>None</b> .
Version	Press [SPACE BAR] to select the RIP version. Choices are <b>RIP-1</b> , <b>RIP-2B</b> or <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 version 2 ( <b>IGMP-v2</b> ). Press the [SPACE BAR] to enable IP Multicasting or select <b>None</b> to disable it.
IP Policies	Create policies using SMT menu 25 (see <a href="#">Chapter 40 on page 391</a> ) and apply them on the Prestige LAN interface here. You can apply up to four IP Policy sets (from twelve) by entering their numbers separated by commas.
Edit IP Alias	The Prestige supports three logical LAN interfaces via its single physical Ethernet interface with the Prestige itself as the gateway for each LAN network. Press [SPACE BAR] to change <b>No</b> to <b>Yes</b> and press [ENTER] to display Menu 3.2.1.





# CHAPTER 26

## Wireless LAN Setup

This chapter covers how to configure wireless LAN settings in SMT menu 3.5.

### 26.1 Wireless LAN Overview

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

### 26.2 Wireless LAN Setup

Use menu 3.5 to set up your Prestige as the wireless access point. To edit menu 3.5, enter 3 from the main menu to display **Menu 3 – LAN Setup**. When menu 3 appears, press 5 and then press [ENTER] to display **Menu 3.5 – Wireless LAN Setup** as shown next.

**Figure 138** Menu 3.5 - Wireless LAN Setup

```

Menu 3.5- Wireless LAN Setup
      ESSID= Wireless
      Hide ESSID= No
      Channel ID= CH06 2437MHz
      RTS Threshold= 2432
      Frag. Threshold= 2432
      WEP= Disable
          Default Key= N/A
          Key1= N/A
          Key2= N/A
          Key3= N/A
          Key4= N/A
      Edit MAC Address Filter= No

Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the fields in this menu.

**Table 95** Menu 3.5 - Wireless LAN Setup

FIELD	DESCRIPTION
ESSID	The ESSID (Extended Service Set Identifier) identifies the AP to which the wireless stations associate. Wireless stations associating to the Access Point must have the same ESSID. Enter a descriptive name of up to 32 printable 7-bit ASCII characters.
Hide ESSID	Press [SPACE BAR] and select <b>Yes</b> to hide the ESSID in the outgoing beacon frame so a station cannot obtain the ESSID through passive scanning.

**Table 95** Menu 3.5 - Wireless LAN Setup (continued)

FIELD	DESCRIPTION
Channel ID	Press [SPACE BAR] to select a channel. This allows you to set the operating frequency/channel depending on your particular region.
RTS Threshold	RTS (Request To Send) threshold (number of bytes) enables RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC Service Data Unit) size turns off the RTS/CTS handshake. Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between 0 and 2432.
Frag. Threshold	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between 256 and 2432.
WEP	WEP (Wired Equivalent Privacy) provides data encryption to prevent wireless stations from accessing data transmitted over the wireless network. Select <b>Disable</b> allows wireless stations to communicate with the access points without any data encryption. Select <b>64-bit WEP</b> , <b>128-bit WEP</b> or <b>256-bit WEP</b> to for the type of data encryption. WEP causes performance degradation.
Default Key	Enter the number of the key as an active key.
Key 1 to Key 4	If you chose <b>64-bit WEP</b> in the <b>WEP Encryption</b> field, then enter 5 characters or 10 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key (1-4). If you chose <b>128-bit WEP</b> in the <b>WEP Encryption</b> field, then enter 13 characters or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key (1-4). If you chose <b>256-bit WEP</b> in the <b>WEP Encryption</b> field, then enter 29 characters or 58 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key (1-4). There are four data encryption keys to secure your data from eavesdropping by unauthorized wireless users. The values for the keys must be set up exactly the same on the access points as they are on the wireless stations.
Edit MAC Address Filter	To edit MAC address filtering table, press [SPACE BAR] to select <b>Yes</b> and press [ENTER] to open menu 3.5.1.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm or ESC to Cancel:" to save your configuration, or press [ESC] at any time to cancel.	

## 26.2.1 Wireless LAN MAC Address Filter

The next layer of security is MAC address filter. To allow a wireless station to associate with the Prestige, enter the MAC address of the wireless LAN adapter on that wireless station in the MAC address table.

**Figure 139** Menu 3.5.1 WLAN MAC Address Filtering

Menu 3.5.1 - WLAN MAC Address Filter					
Active= No					
Filter Action= Allowed Association					
1=	00:00:00:00:00:00	13=	00:00:00:00:00:00	25=	00:00:00:00:00:00
2=	00:00:00:00:00:00	14=	00:00:00:00:00:00	26=	00:00:00:00:00:00
3=	00:00:00:00:00:00	15=	00:00:00:00:00:00	27=	00:00:00:00:00:00
4=	00:00:00:00:00:00	16=	00:00:00:00:00:00	28=	00:00:00:00:00:00
5=	00:00:00:00:00:00	17=	00:00:00:00:00:00	29=	00:00:00:00:00:00
6=	00:00:00:00:00:00	18=	00:00:00:00:00:00	30=	00:00:00:00:00:00
7=	00:00:00:00:00:00	19=	00:00:00:00:00:00	31=	00:00:00:00:00:00
8=	00:00:00:00:00:00	20=	00:00:00:00:00:00	32=	00:00:00:00:00:00
9=	00:00:00:00:00:00	21=	00:00:00:00:00:00		
10=	00:00:00:00:00:00	22=	00:00:00:00:00:00		
11=	00:00:00:00:00:00	23=	00:00:00:00:00:00		
12=	00:00:00:00:00:00	24=	00:00:00:00:00:00		
-----					
Enter here to CONFIRM or ESC to CANCEL:					

The following table describes the fields in this menu.

**Table 96** Menu 3.5.1 WLAN MAC Address Filtering

FIELD	DESCRIPTION
Active	To enable MAC address filtering, press [SPACE BAR] to select <b>Yes</b> and press [ENTER].
Filter Action	Define the filter action for the list of MAC addresses in the MAC address filter table. To deny access to the Prestige, press [SPACE BAR] to select <b>Deny Association</b> and press [ENTER]. MAC addresses not listed will be allowed to access the router. The default action, <b>Allowed Association</b> , permits association with the Prestige. MAC addresses not listed will be denied access to the router.
MAC Address Filter	
Address 1.	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless stations that are allowed or denied access to the Prestige in these address fields.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm or ESC to Cancel:" to save your configuration, or press [ESC] at any time to cancel.	



# CHAPTER 27

## Internet Access

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

### 27.1 Internet Access Overview

Refer to the chapters on the web configurator's wizard, LAN and WAN screens for more background information on fields in the SMT screens covered in this chapter.

### 27.2 IP Policies

Traditionally, routing is based on the destination address *only* and the router takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing. Create policies using SMT menu 25 (see [Chapter 40 on page 391](#)) and apply them on the Prestige LAN and/or WAN interfaces using menus 3.2 (LAN) and 11.3 (WAN).

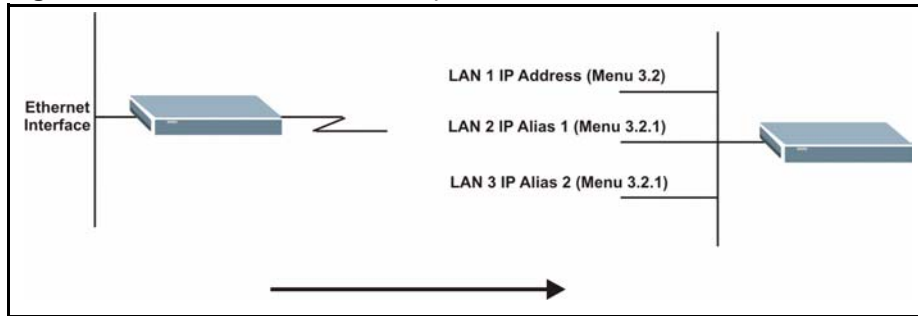
### 27.3 IP Alias

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

When you use IP alias, you can also configure firewall rules to control access between the LAN's logical networks (subnets).

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

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

**Figure 140** IP Alias Network Example

Use menu 3.2.1 to configure IP Alias on your Prestige.

## 27.4 IP Alias Setup

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

**Figure 141** Menu 3.2 TCP/IP and DHCP Setup

```

Menu 3.2 - TCP/IP and DHCP Setup
DHCP Setup
DHCP= Server
Client IP Pool Starting Address= 192.168.1.33
Size of Client IP Pool= 32
Primary DNS Server= 0.0.0.0
Secondary DNS Server= 0.0.0.0
Remote DHCP Server= N/A
TCP/IP Setup:
IP Address= 192.168.1.1
IP Subnet Mask= 255.255.255.0
RIP Direction= None
Version= N/A
Multicast= None
IP Policies=
Edit IP Alias= No

Press ENTER to Confirm or ESC to Cancel:

```

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

**Figure 142** Menu 3.2.1 IP Alias Setup

```

Menu 3.2.1 - IP Alias Setup
  IP Alias 1= No
    IP Address= N/A
    IP Subnet Mask= N/A
    RIP Direction= N/A
    Version= N/A
    Incoming protocol filters= N/A
    Outgoing protocol filters= N/A
  IP Alias 2= No
    IP Address= N/A
    IP Subnet Mask= N/A
    RIP Direction= N/A
    Version= N/A
    Incoming protocol filters= N/A
    Outgoing protocol filters= N/A

Enter here to CONFIRM or ESC to CANCEL:

```

Follow the instructions in the following table to configure IP Alias parameters.

**Table 97** Menu 3.2.1 IP Alias Setup

FIELD	DESCRIPTION
IP Alias	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] to select the RIP direction. Choices are <b>None</b> , <b>Both</b> , <b>In Only</b> or <b>Out Only</b> .
Version	Press [SPACE BAR] to select the RIP version. Choices 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.
Outgoing Protocol Filters	Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the Prestige.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm or ESC to Cancel:" to save your configuration, or press [ESC] at any time to cancel.	

## 27.5 Route IP Setup

The first step is to enable the IP routing in **Menu 1 — General Setup**.

To edit menu 1, type 1 in the main menu and press [ENTER]. Set the **Route IP** field to **Yes** by pressing [SPACE BAR].

**Figure 143** Menu 1 General Setup

```
Menu 1 - General Setup
    System Name= ?
    Location= location
    Contact Person's Name=
    Domain Name=
    Edit Dynamic DNS= No
    Route IP= Yes
    Bridge= No

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

## 27.6 Internet Access Configuration

Menu 4 allows you to enter the Internet Access information in one screen. Menu 4 is actually a simplified setup for one of the remote nodes that you can access in menu 11. Before you configure your Prestige for Internet access, you need to collect your Internet account information.

Use the *Internet Account Information* table in the *Quick Start Guide* to record your. Note that if you are using PPPoA or PPPoE encapsulation, then the only ISP information you need is a login name and password. You only need to know the Ethernet Encapsulation Gateway IP address if you are using ENET ENCAP encapsulation.

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

**Figure 144** Menu 4 Internet Access Setup

```
Menu 4 - Internet Access Setup
    ISP's Name= MyISP
    Encapsulation= RFC 1483
    Multiplexing= LLC-based
    VPI #= 8
    VCI #= 35
    ATM QoS Type= CBR
        Peak Cell Rate (PCR)= 0
        Sustain Cell Rate (SCR)= 0
        Maximum Burst Size (MBS)= 0
    My Login= N/A
    My Password= N/A
    ENET ENCAP Gateway= N/A
    IP Address Assignment= Static
        IP Address= 0.0.0.0
    Network Address Translation= SUA Only
        Address Mapping Set= N/A

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

The following table contains instructions on how to configure your Prestige for Internet access



**Table 98** Menu 4 Internet Access Setup

FIELD	DESCRIPTION
ISP's Name	Enter the name of your Internet Service Provider (ISP). This information is for identification purposes only.
Encapsulation	Press [SPACE BAR] to select the method of encapsulation used by your ISP. Choices are <b>PPPoE</b> , <b>PPPoA</b> , <b>RFC 1483</b> or <b>ENET ENCAP</b> .
Multiplexing	Press [SPACE BAR] to select the method of multiplexing used by your ISP. Choices are <b>VC-based</b> or <b>LLC-based</b> .
VPI #	Enter the Virtual Path Identifier (VPI) assigned to you.
VCI #	Enter the Virtual Channel Identifier (VCI) assigned to you.
ATM QoS Type	Press [SPACE BAR] and select <b>CBR</b> (Continuous Bit Rate) to specify fixed (always-on) bandwidth. Select <b>UBR</b> (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select <b>VBR</b> (Variable Bit Rate) for bursty traffic and bandwidth sharing with other applications.
Peak Cell Rate (PCR)	This is the maximum rate at which the sender can send cells. Type the PCR.
Sustain Cell Rate (SCR)= 0	Sustained Cell Rate is the mean cell rate of a bursty, on-off traffic source that can be sent at the peak rate, and a parameter for burst-traffic. Type the SCR; it must be less than the PCR.
Maximum Burst Size (MBS)= 0	Refers to the maximum number of cells that can be sent at the peak rate. Type the MBS. The MBS must be less than 65535.
My Login	Configure the <b>My Login</b> and <b>My Password</b> fields for PPPoA and PPPoE encapsulation only. Enter the login name that your ISP gives you. If you are using PPPoE encapsulation, then this field must be of the form user@domain where domain identifies your PPPoE service name.
My Password	Enter the password associated with the login name above.
ENET ENCAP Gateway	Enter the gateway IP address supplied by your ISP when you are using <b>ENET ENCAP</b> encapsulation.
Idle Timeout	This value specifies the number of idle seconds that elapse before the Prestige automatically disconnects the PPPoE session.
IP Address Assignment	Press [SPACE BAR] to select <b>Static</b> or <b>Dynamic</b> address assignment.
IP Address	Enter the IP address supplied by your ISP if applicable.
Network Address Translation	Press [SPACE BAR] to select <b>None</b> , <b>SUA Only</b> or <b>Full Feature</b> . Please see <a href="#">Chapter 31 on page 313</a> for more details on the SUA (Single User Account) feature.
Address Mapping Set	Type the numbers of mapping sets (1-8) to use with NAT. See <a href="#">Chapter 31 on page 313</a> for details.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm or ESC to Cancel:" to save your configuration, or press [ESC] at any time to cancel.	

If all your settings are correct your Prestige should connect automatically to the Internet. If the connection fails, note the error message that you receive on the screen and take the appropriate troubleshooting steps.



# CHAPTER 28

## Remote Node Configuration

This chapter covers remote node configuration.

### 28.1 Remote Node Setup Overview

This section describes the protocol-independent parameters for a remote node. A remote node is required for placing calls to a remote gateway. A remote node represents both the remote gateway and the network behind it across a WAN connection. When you use menu 4 to set up Internet access, you are configuring one of the remote nodes.

You first choose a remote node in **Menu 11- Remote Node Setup**. You can then edit that node's profile in menu 11.1, as well as configure specific settings in three submenus: edit IP and bridge options in menu 11.3; edit ATM options in menu 11.6; and edit filter sets in menu 11.5.

### 28.2 Remote Node Setup

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

#### 28.2.1 Remote Node Profile

To configure a remote node, follow these steps:

- 1 From the main menu, enter 11 to display **Menu 11 - Remote Node Setup**.
- 2 When menu 11 appears, as shown in the following figure, type the number of the remote node that you want to configure.

**Figure 145** Menu 11 Remote Node Setup

```
Menu 11 - Remote Node Setup
1. MyISP (ISP, SUA)
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____

Enter Node # to Edit:
```

## 28.2.2 Encapsulation and Multiplexing Scenarios

For Internet access you should use the encapsulation and multiplexing methods used by your ISP. Consult your telephone company for information on encapsulation and multiplexing methods for LAN-to-LAN applications, for example between a branch office and corporate headquarters. There must be prior agreement on encapsulation and multiplexing methods because they cannot be automatically determined. What method(s) you use also depends on how many VCs you have and how many different network protocols you need. The extra overhead that ENET ENCAP encapsulation entails makes it a poor choice in a LAN-to-LAN application. Here are some examples of more suitable combinations in such an application.

### 28.2.2.1 Scenario 1: One VC, Multiple Protocols

**PPPoA** (RFC-2364) encapsulation with **VC-based** multiplexing is the best combination because no extra protocol identifying headers are needed. The **PPP** protocol already contains this information.

### 28.2.2.2 Scenario 2: One VC, One Protocol (IP)

Selecting **RFC-1483** encapsulation with **VC-based** multiplexing requires the least amount of overhead (0 octets). However, if there is a potential need for multiple protocol support in the future, it may be safer to select **PPPoA** encapsulation instead of **RFC-1483**, so you do not need to reconfigure either computer later.

### 28.2.2.3 Scenario 3: Multiple VCs

If you have an equal number (or more) of VCs than the number of protocols, then select **RFC-1483** encapsulation and **VC-based** multiplexing.

**Figure 146** Menu 11.1 Remote Node Profile

```

Menu 11.1 - Remote Node Profile
Rem Node Name= MyISP                Route= IP
Active= Yes                          Bridge= No
Encapsulation= RFC 1483              Edit IP/Bridge= No
Multiplexing= LLC-based              Edit ATM Options= No
Service Name= N/A                    Edit Advance Options= N/A
Incoming:                             Telco Option:
  Rem Login= N/A                      Allocated Budget (min)= N/A
  Rem Password= N/A                  Period(hr)= N/A
Outgoing:                              Schedule Sets= N/A
  My Login= N/A                      Nailed-Up Connection= N/A
  My Password= N/A                  Session Options:
  Authen= N/A                        Edit Filter Sets= No
                                      Idle Timeout(sec)= N/A

Press ENTER to Confirm or ESC to Cancel:

```

In **Menu 11.1 – Remote Node Profile**, fill in the fields as described in the following table.

**Table 99** Menu 11.1 Remote Node Profile

FIELD	DESCRIPTION
Rem Node Name	Type a unique, descriptive name of up to eight characters for this node.
Active	Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> to activate or <b>No</b> to deactivate this node. Inactive nodes are displayed with a minus sign – in SMT menu 11.
Encapsulation	<b>PPPoA</b> refers to RFC-2364 (PPP Encapsulation over ATM Adaptation Layer 5). If RFC-1483 (Multiprotocol Encapsulation over ATM Adaptation Layer 5) of <b>ENET ENCAP</b> are selected, then the <b>Rem Login</b> , <b>Rem Password</b> , <b>My Login</b> , <b>My Password</b> and <b>Authen</b> fields are not applicable ( <b>N/A</b> ).
Multiplexing	Press [SPACE BAR] and then [ENTER] to select the method of multiplexing that your ISP uses, either <b>VC-based</b> or <b>LLC-based</b> .
Service Name	When using <b>PPPoE</b> encapsulation, type the name of your PPPoE service here.
Incoming:	
Rem Login	Type the login name that this remote node will use to call your Prestige. The login name and the <b>Rem Password</b> will be used to authenticate this node.
Rem Password	Type the password used when this remote node calls your Prestige.
Outgoing:	
My Login	Type the login name assigned by your ISP when the Prestige calls this remote node.
My Password	Type the password assigned by your ISP when the Prestige calls this remote node.
Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are:
	<b>CHAP/PAP</b> – Your Prestige will accept either <b>CHAP</b> or <b>PAP</b> when requested by this remote node.
	<b>CHAP</b> – accept <b>CHAP</b> (Challenge Handshake Authentication Protocol) only.

**Table 99** Menu 11.1 Remote Node Profile (continued)

FIELD	DESCRIPTION
	<b>PAP</b> – accept PAP (Password Authentication Protocol) only.
Route	This field determines the protocol used in routing. Options are <b>IP</b> and <b>None</b> .
Bridge	When bridging is enabled, your Prestige will forward any packet that it does not route to this remote node; otherwise, the packets are discarded. Select <b>Yes</b> to enable and <b>No</b> to disable.
Edit IP/Bridge	Press [SPACE BAR] to select <b>Yes</b> and press [ENTER] to display <b>Menu 11.3 – Remote Node Network Layer Options</b> .
Edit ATM Options	Press [SPACE BAR] to select <b>Yes</b> and press [ENTER] to display <b>Menu 11.6 – Remote Node ATM Layer Options</b> .
Edit Advance Options	This field is only available when you select <b>PPPoE</b> in the <b>Encapsulation</b> field. Press [SPACE BAR] to select <b>Yes</b> and press [ENTER] to display <b>Menu 11.8 – Advance Setup Options</b> .
Telco Option	
Allocated Budget (min)	This sets a ceiling for outgoing call time for this remote node. The default for this field is 0 meaning no budget control.
Period (hr)	This field is the time period that the budget should be reset. For example, if we are allowed to call this remote node for a maximum of 10 minutes every hour, then the <b>Allocated Budget</b> is (10 minutes) and the <b>Period (hr)</b> is 1 (hour).
Schedule Sets	This field is only applicable for <b>PPPoE</b> and <b>PPPoA</b> encapsulation. You can apply up to four schedule sets here. For more details please refer to <a href="#">Chapter 41 on page 399</a> .
Nailed up Connection	This field is only applicable for <b>PPPoE</b> and <b>PPPoA</b> encapsulation. This field specifies if you want to make the connection to this remote node a nailed-up connection. More details are given earlier in this section.
Session Options	
Edit Filter Sets	Use [SPACE BAR] to choose <b>Yes</b> and press [ENTER] to open menu 11.5 to edit the filter sets. See the <i>Remote Node Filter</i> section for more details.
Idle Timeout (sec)	Type the number of seconds (0-9999) that can elapse when the Prestige is idle (there is no traffic going to the remote node), before the Prestige automatically disconnects the remote node. 0 means that the session will not timeout.
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm or ESC to Cancel:” to save your configuration, or press [ESC] at any time to cancel.	

### 28.2.3 Outgoing Authentication Protocol

For obvious reasons, you should employ the strongest authentication protocol possible. However, some vendors' implementation includes specific authentication protocol in the user profile. It will disconnect if the negotiated protocol is different from that in the user profile, even when the negotiated protocol is stronger than specified. If the peer disconnects right after a successful authentication, make sure that you specify the correct authentication protocol when connecting to such an implementation.

## 28.3 Remote Node Network Layer Options

For the TCP/IP parameters, perform the following steps to edit **Menu 11.3 – Remote Node Network Layer Options** as shown next.

- 1 In menu 11.1, make sure **IP** is among the protocols in the **Route** field.
- 2 Move the cursor to the **Edit IP/Bridge** field, press [SPACE BAR] to select **Yes**, then press [ENTER] to display **Menu 11.3 – Remote Node Network Layer Options**.

**Figure 147** Menu 11.3 Remote Node Network Layer Options

```

Menu 11.3 - Remote Node Network Layer Options
IP Options:                               Bridge Options:
  IP Address Assignment = Static           Ethernet Addr Timeout(min)= N/A
  Rem IP Addr = 0.0.0.0
  Rem Subnet Mask= 0.0.0.0
  My WAN Addr= 0.0.0.0
  NAT= SUA Only
    Address Mapping Set= N/A
  Metric= 2
  Private= No
  RIP Direction= None
    Version= RIP-1
  Multicast= None
  IP Policies=

Enter here to CONFIRM or ESC to CANCEL:

```

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

**Table 100** Menu 11.3 Remote Node Network Layer Options

FIELD	DESCRIPTION
IP Address Assignment	Press [SPACE BAR] and then [ENTER] to select <b>Dynamic</b> if the remote node is using a dynamically assigned IP address or <b>Static</b> if it is using a static (fixed) IP address. You will only be able to configure this in the ISP node (also the one you configure in menu 4), all other nodes are set to <b>Static</b> .
Rem IP Addr	This is the IP address you entered in the previous menu.
Rem Subnet Mask	Type the subnet mask assigned to the remote node.
My WAN Addr	Some implementations, especially UNIX derivatives, require separate IP network numbers for the WAN and LAN links and each end to have a unique address within the WAN network number. In that case, type the IP address assigned to the WAN port of your Prestige. NOTE: Refers to local Prestige address, not the remote router address.
NAT	Press [SPACE BAR] and then [ENTER] to select <b>Full Feature</b> if you have multiple public WAN IP addresses for your Prestige.
	Select <b>SUA Only</b> if you have just one public WAN IP address for your Prestige. The SMT uses Address Mapping Set 255 (see <a href="#">Figure 165 on page 316</a> ). Select <b>None</b> to disable NAT.

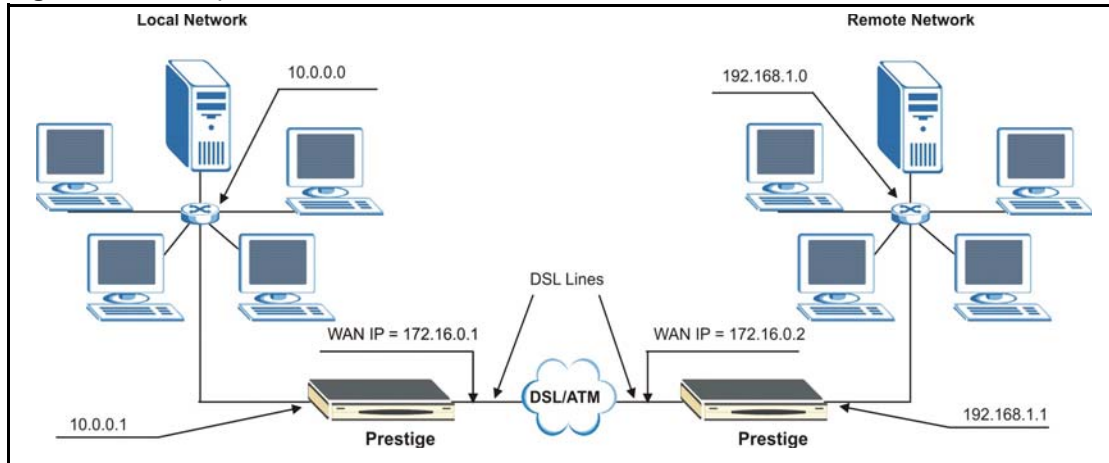
**Table 100** Menu 11.3 Remote Node Network Layer Options (continued)

FIELD	DESCRIPTION
Address Mapping Set	When <b>Full Feature</b> is selected in the <b>NAT</b> field, configure address mapping sets in menu 15.1. Select one of the NAT server sets (2-10) in menu 15.2 (see <a href="#">Chapter 31 on page 313</a> for details) and type that number here. When <b>SUA Only</b> is selected in the NAT field, the SMT uses NAT server set 1 in menu 15.2 (see <a href="#">Chapter 31 on page 313</a> for details).
Metric	The metric represents the cost of transmission for routing purposes. IP routing uses hop count as the cost measurement, with a minimum of 1 for directly connected networks. Type a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Private	This determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to <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. 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	<b>IGMP-v1</b> sets IGMP to version 1, <b>IGMP-v2</b> sets IGMP to version 2 and <b>None</b> disables IGMP.
IP Policies	You can apply up to four IP Policy sets (from 12) by typing in their numbers separated by commas. Configure the filter sets in menu 25 first (see <a href="#">Chapter 40 on page 391</a> ) and then apply them here.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm or ESC to Cancel:" to save your configuration, or press [ESC] at any time to cancel.	

### 28.3.1 My WAN Addr Sample IP Addresses

The following figure uses sample IP addresses to help you understand the field of **My WAN Addr** in menu 11.3. Refer to the previous [Figure 18 on page 79](#) in the web configurator chapter on LAN setup for a brief review of what a WAN IP is. **My WAN Addr** indicates the local Prestige WAN IP (172.16.0.1 in the following figure) while **Rem IP Addr** indicates the peer WAN IP (172.16.0.2 in the following figure).



**Figure 148** Sample IP Addresses for a TCP/IP LAN-to-LAN Connection

## 28.4 Remote Node Filter

Move the cursor to the **Edit Filter Sets** field in menu 11.1, then press [SPACE BAR] to select **Yes**. Press [ENTER] to display **Menu 11.5 – Remote Node Filter**.

Use **Menu 11.5 – Remote Node Filter** to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the Prestige and also to prevent certain packets from triggering calls. You can specify up to 4 filter sets separated by comma, for example, 1, 5, 9, 12, in each filter field.

Note that spaces are accepted in this field. The Prestige has a prepackaged filter set, **NetBIOS\_WAN**, that blocks NetBIOS packets. Include this in the call filter sets if you want to prevent NetBIOS packets from triggering calls to a remote node.

**Figure 149** Menu 11.5 Remote Node Filter (RFC 1483 or ENET Encapsulation)

```
Menu 11.5 - Remote Node Filter
Input Filter Sets:
  protocol filters=
  device filters=
Output Filter Sets:
  protocol filters=
  device filters=

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

**Figure 150** Menu 11.5 Remote Node Filter (PPPoA or PPPoE Encapsulation)

```
Menu 11.5 - Remote Node Filter
Input Filter Sets:
  protocol filters=
  device filters=
Output Filter Sets:
  protocol filters=
  device filters=
Call Filter Sets:
  protocol filters=
  device filters=

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

## 28.5 Editing ATM Layer Options

Follow the steps shown next to edit **Menu 11.6 – Remote Node ATM Layer Options**.

In menu 11.1, move the cursor to the **Edit ATM Options** field and then press [SPACE BAR] to select **Yes**. Press [ENTER] to display **Menu 11.6 – Remote Node ATM Layer Options**.

There are two versions of menu 11.6 for the Prestige, depending on whether you chose **VC-based/LLC-based** multiplexing and **PPP** encapsulation in menu 11.1.

### 28.5.1 VC-based Multiplexing (non-PPP Encapsulation)

For **VC-based** multiplexing, by prior agreement, a protocol is assigned a specific virtual circuit, for example, VC1 will carry IP. Separate VPI and VCI numbers must be specified for each protocol.

**Figure 151** Menu 11.6 for VC-based Multiplexing

```

Menu 11.6 - Remote Node ATM Layer Options
VPI/VCI (VC-Multiplexing)

VC Options for IP:                VC Options for Bridge:
VPI #= 8                        VPI #= 1
VCI #= 35                          VCI #= 36
ATM QoS Type= UBR                  ATM QoS Type= N/A
Peak Cell Rate (PCR)= 0            Peak Cell Rate (PCR)= N/A
Sustain Cell Rate (SCR)= 0         Sustain Cell Rate (SCR)= N/A
Maximum Burst Size (MBS)= 0        Maximum Burst Size (MBR)= N/A

Enter here to CONFIRM or ESC to CANCEL:

```

## 28.5.2 LLC-based Multiplexing or PPP Encapsulation

For **LLC-based** multiplexing or **PPP** encapsulation, one VC carries multiple protocols with protocol identifying information being contained in each packet header.

**Figure 152** Menu 11.6 for LLC-based Multiplexing or PPP Encapsulation

```

Menu 11.6 - Remote Node ATM Layer Options
VPI/VCI (LLC-Multiplexing or PPP-Encapsulation)
VPI #= 8
VCI #= 35
ATM QoS Type= UBR
Peak Cell Rate (PCR)= 0
Sustain Cell Rate (SCR)= 0
Maximum Burst Size (MBS)= 0

ENTER here to CONFIRM or ESC to CANCEL:

```

In this case, only one set of VPI and VCI numbers need be specified for all protocols. The valid range for the VPI is 0 to 255 and for the VCI is 32 to 65535 (1 to 31 is reserved for local management of ATM traffic).

## 28.5.3 Advance Setup Options

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

**Figure 153** Menu 11.1 Remote Node Profile

```

Menu 11.1 - Remote Node Profile
Rem Node Name= MyISP           Route= IP
Active= Yes                    Bridge= No
Encapsulation= PPPoE        Edit IP/Bridge= No
Multiplexing= LLC-based       Edit ATM Options= No
Service Name=                 Edit Advance Options= Yes
Incoming:                     Telco Option:
  Rem Login=                   Allocated Budget(min)= 0
  Rem Password= *****      Period(hr)= 0
Outgoing:                      Schedule Sets=
  My Login= ?                 Nailed-Up Connection= No
  My Password= ?             Session Options:
  Authen= CHAP/PAP           Edit Filter Sets= No
                              Idle Timeout(sec)= 0

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

Move the cursor to the **Edit Advance Options** field, press [SPACE BAR] to select **Yes**, then press [ENTER] to display **Menu 11.8 – Advance Setup Options**.

**Figure 154** Menu 11.8 Advance Setup Options

```

Menu 11.8 - Advance Setup Options

PPPoE pass-through= No

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

The following table describes the fields in this menu.

**Table 101** Menu 11.8 Advance Setup Options

FIELD	DESCRIPTION
PPPoE pass-through	<p>Press [SPACE BAR] to select <b>Yes</b> and press [ENTER] to enable PPPoE pass through. In addition to the Prestige's built-in PPPoE client, you can enable PPPoE pass through to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the Prestige. Each host can have a separate account and a public WAN IP address.</p> <p>PPPoE pass through is an alternative to NAT for applications where NAT is not appropriate.</p> <p>Press [SPACE BAR] to select <b>No</b> and press [ENTER] to disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.</p>
<p>When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm or ESC to Cancel:" to save your configuration, or press [ESC] at any time to cancel.</p>	

# CHAPTER 29

## Static Route Setup

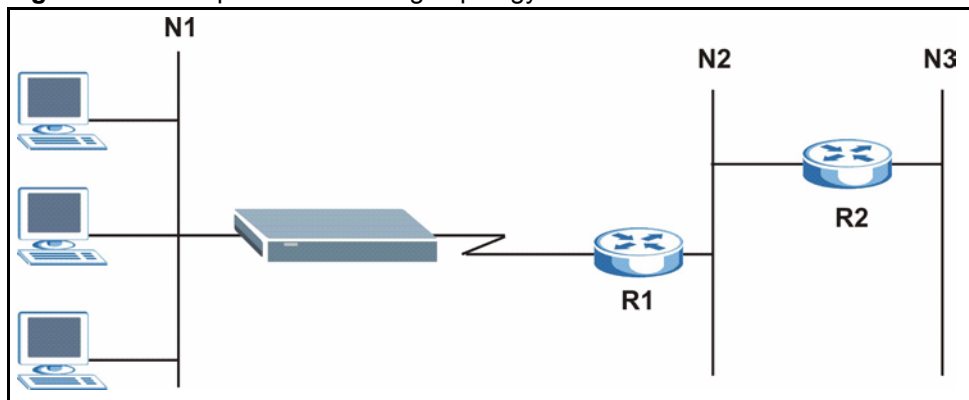
This chapter shows how to setup IP static routes.

### 29.1 IP Static Route Overview

Static routes tell the Prestige routing information that it cannot learn automatically through other means. This can arise in cases where RIP is disabled on the LAN or a remote network is beyond the one that is directly connected to a remote node.

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

**Figure 155** Sample Static Routing Topology



### 29.2 Configuration

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

**Figure 156** Menu 12 Static Route Setup

```
Menu 12 - Static Route Setup

1. IP Static Route
3. Bridge Static Route

Please enter selection:
```

From menu 12, select 1 to open **Menu 12.1 — IP Static Route Setup** (shown next).

**Figure 157** Menu 12.1 IP Static Route Setup

```
Menu 12.1 - IP Static Route Setup

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____
11. _____
12. _____
13. _____
14. _____
15. _____
16. _____

Enter selection number:
```

Now, type the route number of a static route you want to configure.

**Figure 158** Menu12.1.1 Edit IP Static Route

```
Menu 12.1.1 - Edit IP Static Route

Route #: 1
Route Name= ?
Active= No
Destination IP Address= ?
IP Subnet Mask= ?
Gateway IP Address= ?
Metric= 2
Private= No

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

The following table describes the fields for **Menu 12.1.1 – Edit IP Static Route Setup**.

**Table 102** Menu12.1.1 Edit IP Static Route

FIELD	DESCRIPTION
Route #	This is the index number of the static route that you chose in menu 12.1.
Route Name	Type a descriptive name for this route. This is for identification purpose only.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Type the subnet mask for this destination. See <a href="#">Section 5.4.2 on page 81</a> 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] at any time to cancel.	





# CHAPTER 30

## Bridging Setup

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

### 30.1 Bridging in General

Bridging bases the forwarding decision on the MAC (Media Access Control), or hardware address, while routing does it on the network layer (IP) address. Bridging allows the Prestige to transport packets of network layer protocols that it does not route, for example, SNA, from one network to another. The caveat is that, compared to routing, bridging generates more traffic for the same network layer protocol, and it also demands more CPU cycles and memory.

For efficiency reasons, do *not* turn on bridging unless you need to support protocols other than IP on your network. For IP, enable the routing if you need it; do not bridge what the Prestige can route.

### 30.2 Bridge Ethernet Setup

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

#### 30.2.1 Remote Node Bridging Setup

Follow the procedure in another section to configure the protocol-independent parameters in **Menu 11.1 – Remote Node Profile**. For bridging-related parameters, you need to configure **Menu 11.3 – Remote Node Network Layer Options**.

- 1 To setup **Menu 11.3 – Remote Node Network Layer Options** shown in the next figure, follow these steps:
- 2 In menu 11.1, make sure the **Bridge** field is set to **Yes**.

**Figure 159** Menu 11.1 Remote Node Profile

```

Menu 11.1 - Remote Node Profile
Rem Node Name= ?
Active= Yes
Encapsulation= ENET ENCAP
Multiplexing= VC-based
Service Name= N/A
Incoming:
  Rem Login= N/A
  Rem Password= N/A
Outgoing:
  My Login= N/A
  My Password= N/A
  Authen= N/A
Route= IP
Bridge= Yes
Edit IP/Bridge= No
Edit ATM Options= No
Edit Advance Options= N/A
Telco Option:
  Allocated Budget (min)= N/A
  Period(hr)= N/A
  Schedule Sets= N/A
  Nailed-Up Connection= N/A
Session Options:
  Edit Filter Sets= No
  Idle Timeout(sec)= N/A

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

**3** Move the cursor to the **Edit IP/Bridge** field, then press [SPACE BAR] to set the value to **Yes** and press [ENTER] to edit **Menu 11.3 – Remote Node Network Layer Options**.

**Figure 160** Menu 11.3 Remote Node Network Layer Options

```

Menu 11.3 - Remote Node Network Layer Options
IP Options:
  IP Address Assignment= Static
  Rem IP Addr: 0.0.0.0
  Rem Subnet Mask= 0.0.0.0
  My WAN Addr= 0.0.0.0
  NAT= Full Feature
  Address Mapping Set=2
  Metric= 2
  Private= No
  RIP Direction= Both
  Version= RIP-2B
  Multicast= IGMP-v2
  IP Policies=
Bridge Options:
  Ethernet Addr Timeout (min)= 0

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

**Table 103** Remote Node Network Layer Options: Bridge Fields

FIELD	DESCRIPTION
Bridge (menu 11.1)	Make sure this field is set to <b>Yes</b> .
Edit IP/Bridge (menu 11.1)	Press [SPACE BAR] to select <b>Yes</b> and press [ENTER] to display menu 11.3.
Ethernet Addr Timeout (min.) (menu 11.3)	Type the time (in minutes) for the Prestige to retain the Ethernet Address information in its internal tables while the line is down. If this information is retained, your Prestige will not have to recompile the tables when the line comes back up.

## 30.2.2 Bridge Static Route Setup

Similar to network layer static routes, a bridging static route tells the Prestige the route to a node before a connection is established. You configure bridge static routes in menu 12.3.1 (go to menu 12, choose option 3, then choose a static route to edit) as shown next.

**Figure 161** Menu 12.3.1 Edit Bridge Static Route

```

Menu 12.3.1 - Edit Bridge Static Route
Route #: 1
Route Name=
Active= No
Ether Address= ?
IP Address=
Gateway Node= 1

Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the **Edit Bridge Static Route** menu.

**Table 104** Menu 12.3.1 Edit Bridge Static Route

FIELD	DESCRIPTION
Route #	This is the route index number you typed in <b>Menu 12.3 – Bridge Static Route Setup</b> .
Route Name	Type a name for the bridge static route for identification purposes.
Active	Indicates whether the static route is active ( <b>Yes</b> ) or not ( <b>No</b> ).
Ether Address	Type the MAC address of the destination computer that you want to bridge the packets to.
IP Address	If available, type the IP address of the destination computer that you want to bridge the packets to.
Gateway Node	Press [SPACE BAR] and then [ENTER] to select the number of the remote node (one to eight) that is the gateway of this static route.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm or ESC to Cancel:" to save your configuration, or press [ESC] at any time to cancel.	



# CHAPTER 31

## Network Address Translation (NAT)

This chapter discusses how to configure NAT on the Prestige.

### 31.1 Using NAT

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

#### 31.1.1 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. See [Section 31.3 on page 315](#) or a detailed description of the NAT set for SUA. The Prestige also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types.

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

### 31.2 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 162** Menu 4 Applying NAT for Internet Access

```

Menu 4 - Internet Access Setup
  ISP's Name= MyISP
  Encapsulation= RFC 1483
  Multiplexing= LLC-based
  VPI #= 8
  VCI #= 35
  ATM QoS Type= UBR
    Peak Cell Rate (PCR)= 0
    Sustain Cell Rate (SCR)= 0
    Maximum Burst Size (MBS)= 0
  My Login= N/A
  My Password= N/A
  ENET ENCAP Gateway= N/A
  IP Address Assignment= Static
    IP Address= 0.0.0.0
  Network Address Translation= SUA Only
    Address Mapping Set= N/A

Press ENTER to Confirm or ESC to Cancel:

```

The following figure shows how you apply NAT to the remote node in menu 11.1.

- 1 Enter 11 from the main menu.
- 2 When menu 11 appears, as shown in the following figure, type the number of the remote node that you want to configure.
- 3 Move the cursor to the **Edit IP/Bridge** field, press [SPACE BAR] to select **Yes** and then press [ENTER] to bring up **Menu 11.3 - Remote Node Network Layer Options**.

**Figure 163** Applying NAT in Menus 4 & 11.3

```

Menu 11.3 - Remote Node Network Layer Options
IP Options:                               Bridge Options:
  IP Address Assignment = Static           Ethernet Addr Timeout(min)= N/A
  Rem IP Addr = 0.0.0.0
  Rem Subnet Mask= 0.0.0.0
  My WAN Addr= 0.0.0.0
  NAT= SUA Only
    Address Mapping Set= N/A
  Metric= 2
  Private= No
  RIP Direction= Both
    Version= RIP-2B
  Multicast= None
  IP Policies=

Enter here to CONFIRM or ESC to CANCEL:

```

The following table describes the options for Network Address Translation.

**Table 105** 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 (see <a href="#">Figure 165 on page 316</a> ).
	Select <b>None</b> to disable NAT.
	When you select <b>SUA Only</b> , the SMT uses Address Mapping Set 255 (see <a href="#">Figure 166 on page 316</a> ). Choose <b>SUA Only</b> if you have just one public WAN IP address for your Prestige.

## 31.3 NAT Setup

Use the address mapping sets menus and submenus to create the mapping table used to assign global addresses to computers on the LAN. **Set 255** is used for SUA. When you select **Full Feature** in menu 4 or 11.3, the SMT will use **Set 1**. When you select **SUA Only**, the SMT will use the pre-configured **Set 255** (read only).

The server set is a list of LAN servers mapped to external ports. To use this set, a server rule must be set up inside the NAT address mapping set. Please see the section on port forwarding in the chapter on NAT web configurator screens for further information on these menus. To configure NAT, enter 15 from the main menu to bring up the following screen.

**Figure 164** Menu 15 NAT Setup

Menu 15 - NAT Setup
1. Address Mapping Sets 2. NAT Server Sets
Enter Menu Selection Number:

### 31.3.1 Address Mapping Sets

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

**Figure 165** Menu 15.1 Address Mapping Sets

```

Menu 15.1 - Address Mapping Sets
    1.
    2.
    3.
    4.
    5.
    6.
    7.
    8.
    255. SUA (read only)

Enter Menu Selection Number:
    
```

### 31.3.1.1 SUA Address Mapping Set

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

**Figure 166** Menu 15.1.255 SUA Address Mapping Rules

```

Menu 15.1.255 - Address Mapping Rules
Set Name=
Idx  Local Start IP  Local End IP  Global Start IP  Global End IP  Type
----  -
1.   0.0.0.0          255.255.255.255  0.0.0.0          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.

Menu 15.1.255 is read-only.

**Table 106** 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.



**Table 106** SUA Address Mapping Rules (continued)

FIELD	DESCRIPTION
Global Start IP	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the <b>Global Start IP</b> .
Global End IP	This is the ending global IP address (IGA).
Type	These are the mapping types. <b>Server allows us to specify multiple servers of different types behind NAT to this machine. See later for some examples.</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] at any time to cancel.	

### 31.3.1.2 User-Defined Address Mapping Sets

Now let's look at option 1 in menu 15.1. Enter 1 to bring up this menu. We'll just look at the differences from the previous menu. Note the extra **Action** and **Select Rule** fields mean you can configure rules in this screen. Note also that the [?] in the **Set Name** field means that this is a required field and you must enter a name for the set.

**Figure 167** Menu 15.1.1 First Set

```

Menu 15.1.1 - Address Mapping Rules
Set Name= NAT_SET
Idx  Local Start IP   Local End IP   Global Start IP   Global End IP   Type
----  -
1.
2.
3.
4.
5.
6.
7.
8.
9.
10.

Action= Edit          Select Rule=

Press ENTER to Confirm or ESC to Cancel:

```

If the **Set Name** field is left blank, the entire set will be deleted.

The Type, Local and Global Start/End IPs are configured in menu 15.1.1.1 (described later) and the values are displayed here.

### 31.3.1.3 Ordering Your Rules

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

Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so as old rule 5 becomes rule 4, old rule 6 becomes rule 5 and old rule 7 becomes rule 6.

**Table 107** Menu 15.1.1 First Set

FIELD	DESCRIPTION
Set Name	Enter a name for this set of rules. This is a required field. If this field is left blank, the entire set will be deleted.
Action	The default is <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.

You must press **[ENTER]** at the bottom of the screen to save the whole set. You must do this again if you make any changes to the set – including deleting a rule. No changes to the set take place until this action is taken.

Selecting **Edit** in the **Action** field and then selecting a rule brings up the following menu, **Menu 15.1.1.1 - Address Mapping Rule** in which you can edit an individual rule and configure the **Type**, **Local** and **Global Start/End IPs**.

An End IP address must be numerically greater than its corresponding IP Start address.

**Figure 168** Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set

```

Menu 15.1.1.1 Address Mapping Rule
Type= One-to-One
Local IP:
  Start=
  End  = N/A
Global IP:
  Start=
  End  = N/A
Server Mapping Set= N/A

Press ENTER to Confirm or ESC to Cancel:

```

The following table explains the fields in this menu.

**Table 108** 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 allows you to specify multiple servers of different types behind NAT to this computer. See section 27.5.3 for an example.</b>
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 Start IP as 0.0.0.0 and the End IP as 255.255.255.255. This field is <b>N/A</b> for One-to-One and Server types.
Global IP	
Start	This is the starting inside global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the <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</b> types.
Server Mapping Set	Only available when <b>Type</b> is set to <b>Server</b> . Type a number from 1 to 10 to choose a server set from menu 15.2.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm or ESC to Cancel:" to save your configuration, or press [ESC] at any time to cancel.	

## 31.4 Configuring a Server behind NAT

Follow these steps to configure a server behind NAT:

- 1 Enter 15 in the main menu to go to **Menu 15 - NAT Setup**.
- 2 Enter 2 to display **Menu 15.2 - NAT Server Sets** as shown next.

**Figure 169** Menu 15.2 NAT Server Setup

```

Menu 15.2 - NAT Server Sets
  1. Server Set 1 (Used for SUA Only)
  2. Server Set 2
  3. Server Set 3
  4. Server Set 4
  5. Server Set 5
  6. Server Set 6
  7. Server Set 7
  8. Server Set 8
  9. Server Set 9
 10. Server Set 10

Enter Set Number to Edit:
    
```

**3** Enter 1 to go to **Menu 15.2 NAT Server Setup** as follows.

**Figure 170** Menu 15.2 NAT Server Setup

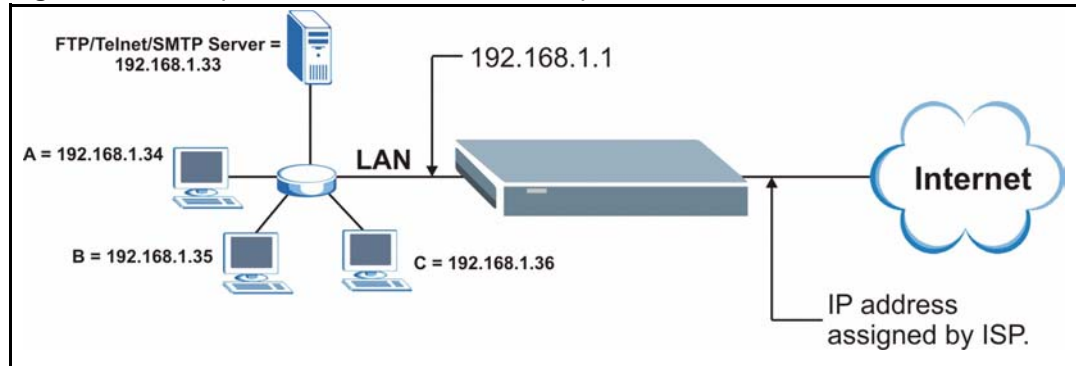
```

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

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

- 4** Enter a port number in an unused **Start Port No** field. To forward only one port, enter it again in the **End Port No** field. To specify a range of ports, enter the last port to be forwarded in the **End Port No** field.
- 5** Enter the inside IP address of the server in the **IP Address** field. In the following figure, you have a computer acting as an FTP, Telnet and SMTP server (ports 21, 23 and 25) at 192.168.1.33.
- 6** Press [ENTER] at the “Press ENTER to confirm ...” prompt to save your configuration after you define all the servers or press [ESC] at any time to cancel.

**Figure 171** Multiple Servers Behind NAT Example



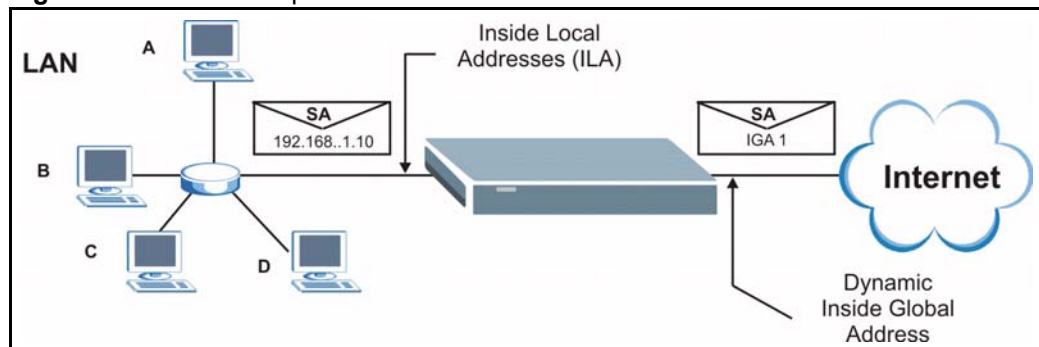
## 31.5 General NAT Examples

The following are some examples of NAT configuration.

### 31.5.1 Example 1: Internet Access Only

In the following Internet access example, you only need one rule where your ILAs (Inside Local addresses) all map to one dynamic IGA (Inside Global Address) assigned by your ISP.

**Figure 172** NAT Example 1



**Figure 173** Menu 4 Internet Access & NAT Example

```

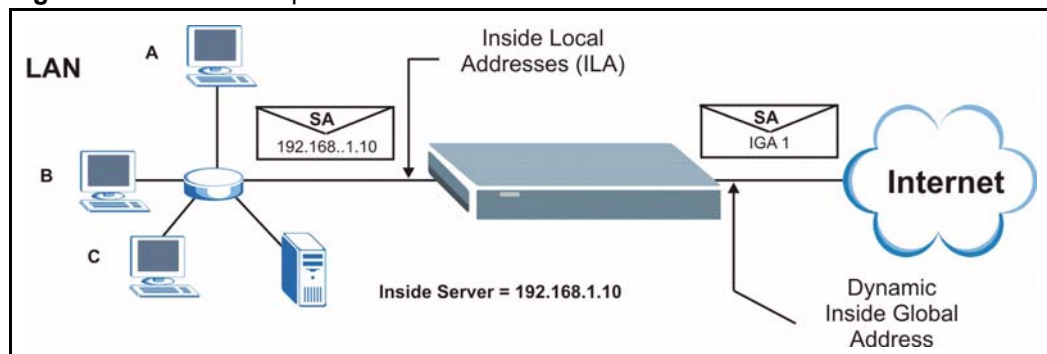
Menu 4 - Internet Access Setup
ISP's Name= MyISP
Encapsulation= RFC 1483
Multiplexing= LLC-based
VPI #= 8
VCI #= 35
ATM QoS Type= UBR
  Peak Cell Rate (PCR)= 0
  Sustain Cell Rate (SCR)= 0
  Maximum Burst Size (MBS)= 0
My Login= N/A
My Password= N/A
ENET ENCAP Gateway= N/A
IP Address Assignment= Static
  IP Address= 0.0.0.0
Network Address Translation= SUA Only
  Address Mapping Set= N/A

Press ENTER to Confirm or ESC to Cancel:

```

From menu 4, choose the **SUA Only** option from the **Network Address Translation** field. This is the **Many-to-One** mapping discussed in [Section 31.5 on page 321](#). 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.

### 31.5.2 Example 2: Internet Access with an Inside Server

**Figure 174** 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 175** Menu 15.2.1 Specifying an Inside Server

Menu 15.2.1 - NAT Server Setup (Used for SUA Only)			
Rule	Start Port No.	End Port No.	IP Address
1.	<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.	0	0	0.0.0.0

Press ENTER to Confirm or ESC to Cancel:

### 31.5.3 Example 3: Multiple Public IP Addresses With Inside Servers

In this example, there are 3 IGAs from our ISP. There are many departments but two have their own FTP server. All departments share the same router. The example will reserve one IGA for each department with an FTP server and all departments use the other IGA. Map the FTP servers to the first two IGAs and the other LAN traffic to the remaining IGA. Map the third IGA to an inside web server and mail server. Four rules need to be configured, two bi-directional and two unidirectional as follows.

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

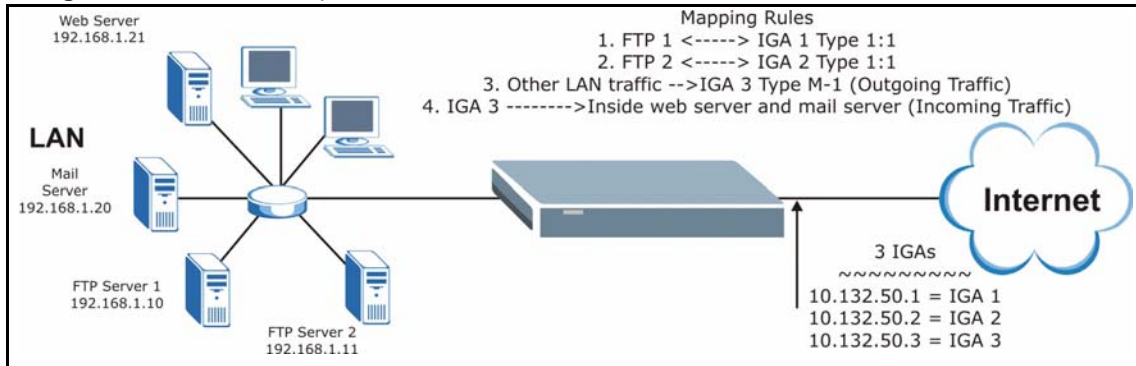
Map the second IGA to our second inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).

Map the other outgoing LAN traffic to IGA3 (**Many : 1** mapping).

You also map your third IGA to the web server and mail server on the LAN. Type **Server** allows you to specify multiple servers, of different types, to other computers behind NAT on the LAN.

The example situation looks somewhat like this:

**Figure 176 NAT Example 3**



In this case you need to configure Address Mapping Set 1 from **Menu 15.1 - Address Mapping Sets**. Therefore you must choose the **Full Feature** option from the **Network Address Translation** field (in menu 4 or menu 11.3) in [Figure 177 on page 324](#).

- 1 Enter 15 from the main menu.
- 2 Enter 1 to configure the Address Mapping Sets.
- 3 Enter 1 to begin configuring this new set. Enter a Set Name, choose the **Edit Action** and then enter 1 for the **Select Rule** field. Press [ENTER] to confirm.
- 4 Select **Type** as **One-to-One** (direct mapping for packets going both ways), and enter the local **Start IP** as 192.168.1.10 (the IP address of FTP Server 1), the global **Start IP** as 10.132.50.1 (our first IGA). (See [Figure 178 on page 325](#)).
- 5 Repeat the previous step for rules 2 to 4 as outlined above.

When finished, menu 15.1.1 should look like as shown in [Figure 179 on page 325](#).

**Figure 177 Example 3: Menu 11.3**

```

Menu 11.3 - Remote Node Network Layer Options
IP Options:                               Bridge Options:
IP Address Assignment= Static              Ethernet Addr Timeout (min)= 0
Rem IP Addr= 0.0.0.0
Rem Subnet Mask= 0.0.0.0
My WAN Addr= 0.0.0.0
NAT= Full Feature
Address Mapping Set= 2
Metric= 2
Private= No
RIP Direction= Both
Version= RIP-2B
Multicast= IGMP-v2
IP Policies=

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

The following figures show how to configure the first rule



**Figure 178** Example 3: Menu 15.1.1.1

```

Menu 15.1.1.1 Address Mapping Rule
  Type= One-to-One
  Local IP:
    Start= 192.168.1.10
    End = N/A
  Global IP:
    Start= 10.132.50.1
    End = N/A
  Server Mapping Set= N/A

Press ENTER to Confirm or ESC to Cancel:

```

**Figure 179** Example 3: Final Menu 15.1.1

```

Menu 15.1.1 - Address Mapping Rules
Set Name= Example3
Idx  Local Start IP   Local End IP   Global Start IP  Global End IP   Type
---  -
1.  192.168.1.10      10.132.50.1   1-1
2.  192.168.1.11      10.132.50.2   1-1
3.  0.0.0.0           255.255.255.255 10.132.50.3   M-1
4.                                     10.132.50.3   Server
5.
6.
7.
8.
9.
10.

Action= Edit      Select Rule=

Press ENTER to Confirm or ESC to Cancel:

```

Now configure the IGA3 to map to our web server and mail server on the LAN.

- 1** Enter 15 from the main menu.
- 2** Enter 2 in **Menu 15 - NAT Setup**.
- 3** Enter 1 in **Menu 15.2 - NAT Server Sets** to see the following menu. Configure it as shown.

**Figure 180** Example 3: Menu 15.2

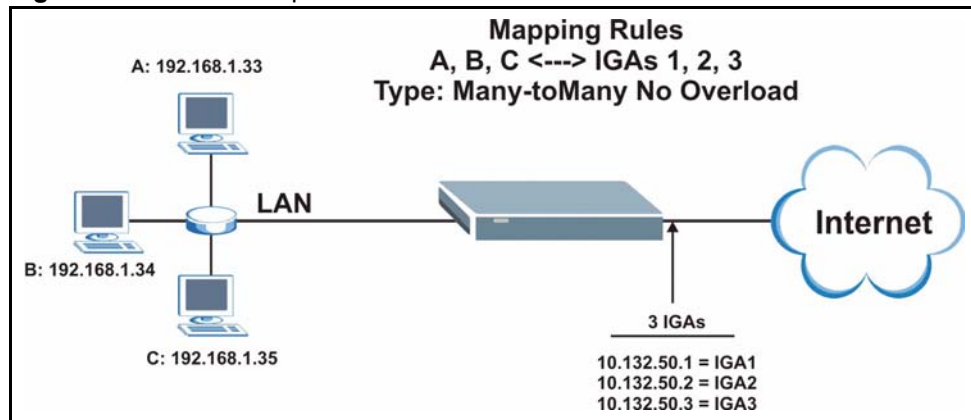
Menu 15.2 - NAT Server Setup			
Rule	Start Port No.	End Port No.	IP Address
1.	Default	Default	0.0.0.0
2.	80	80	192.168.1.21
3.	25	25	192.168.1.20
4.	0	0	0.0.0.0
5.	0	0	0.0.0.0
6.	0	0	0.0.0.0
7.	0	0	0.0.0.0
8.	0	0	0.0.0.0
9.	0	0	0.0.0.0
10.	0	0	0.0.0.0
11.	0	0	0.0.0.0
12.	0	0	0.0.0.0

Press ENTER to Confirm or ESC to Cancel:

### 31.5.4 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 181** NAT Example 4



Other applications such as some gaming programs are NAT unfriendly because they embed addressing information in the data stream. These applications won't work through NAT even when using **One-to-One** and **Many-to-Many No Overload** mapping types.

Follow the steps outlined in example 3 to configure these two menus as follows.

**Figure 182** Example 4: Menu 15.1.1.1 Address Mapping Rule

```

Menu 15.1.1.1 Address Mapping Rule
Type= Many-to-Many No Overload
Local IP:
  Start= 192.168.1.10
  End   = 192.168.1.12
Global IP:
  Start= 10.132.50.1
  End   = 10.132.50.3
Server Mapping Set= N/A

Press ENTER to Confirm or ESC to Cancel:

```

After you've configured your rule, you should be able to check the settings in menu 15.1.1 as shown next.

**Figure 183** Example 4: Menu 15.1.1 Address Mapping Rules

```

Menu 15.1.1 - Address Mapping Rules
Set Name= Example4
Idx  Local Start IP  Local End IP  Global Start IP  Global End IP  Type
---  -
1.   192.168.1.10   192.168.1.12  10.132.50.1     10.132.50.3   M:M NO OV
2.
3.
4.
5.
6.
7.
8.
9.
10.

Action= Edit      Select Rule=

Press ENTER to Confirm or ESC to Cancel:

```



# CHAPTER 32

## Enabling the Firewall

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

### 32.1 Remote Management and the Firewall

When SMT menu 24.11 is configured to allow management (see the *Remote Management* chapter) and the firewall is enabled:

- The firewall blocks remote management from the WAN unless you configure a firewall rule to allow it.
- The firewall allows remote management from the LAN.

### 32.2 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.

### 32.3 Enabling the Firewall

From the main menu enter 21 to go to **Menu 21 - Filter Set and Firewall Configuration** to display the screen shown next.

Enter option 2 in this menu to bring up the following screen. Press [SPACE BAR] and then [ENTER] to select **Yes** in the **Active** field to activate the firewall. The firewall must be active to protect against Denial of Service (DoS) attacks. Additional rules may be configured using the web configurator.

**Figure 184** Menu 21.2 Firewall Setup

```
Menu 21.2 - Firewall Setup
The firewall protects against Denial of Service (DOS) attacks when
it is active. The default Policy sets
  1. allow all sessions originating from the LAN to the WAN and
  2. deny all sessions originating from the WAN to the LAN
You may define additional Policy rules or modify existing ones but
please exercise extreme caution in doing so
Active: Yes
LAN-to-WAN Set Name: ACL Default Set
WAN-to-LAN Set Name: ACL Default Set
Please configure the Firewall function through Web Configurator.

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

Use the web configurator or the command interpreter to configure the firewall rules

# CHAPTER 33

## Filter Configuration

This chapter shows you how to create and apply filters.

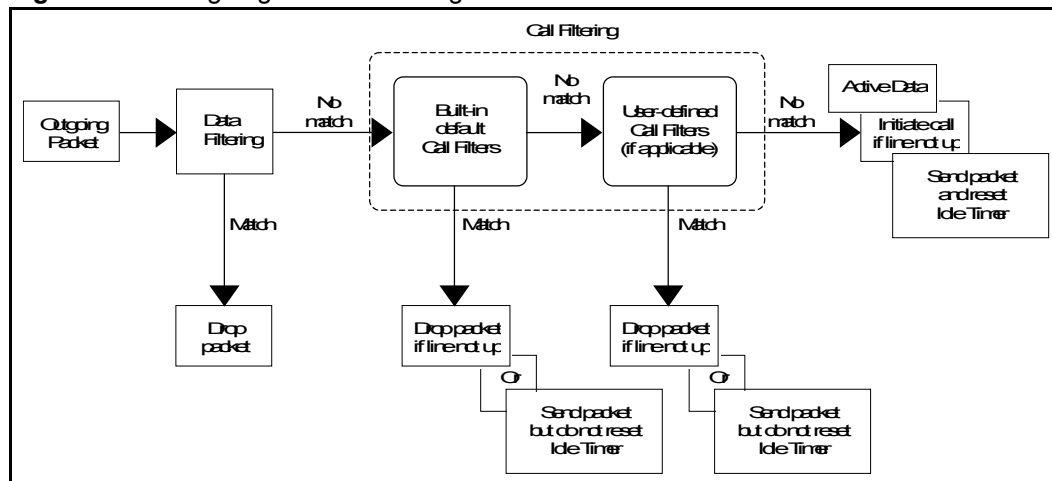
### 33.1 About Filtering

Your Prestige uses filters to decide whether or not to allow passage of a data packet and/or to make a call. There are two types of filter applications: data filtering and call filtering. Filters are subdivided into device and protocol filters, which are discussed later.

Data filtering screens data to determine if the packet should be allowed to pass. Data filters are divided into incoming and outgoing filters, depending on the direction of the packet relative to a port. Data filtering can be applied on either the WAN side or the Ethernet side. Call filtering is used to determine if a packet should be allowed to trigger a call.

Outgoing packets must undergo data filtering before they encounter call filtering. Call filters are divided into two groups, the built-in call filters and user-defined call filters. Your Prestige has built-in call filters that prevent administrative, for example, RIP packets from triggering calls. These filters are always enabled and not accessible to you. Your Prestige applies the built-in filters first and then the user-defined call filters, if applicable, as shown next.

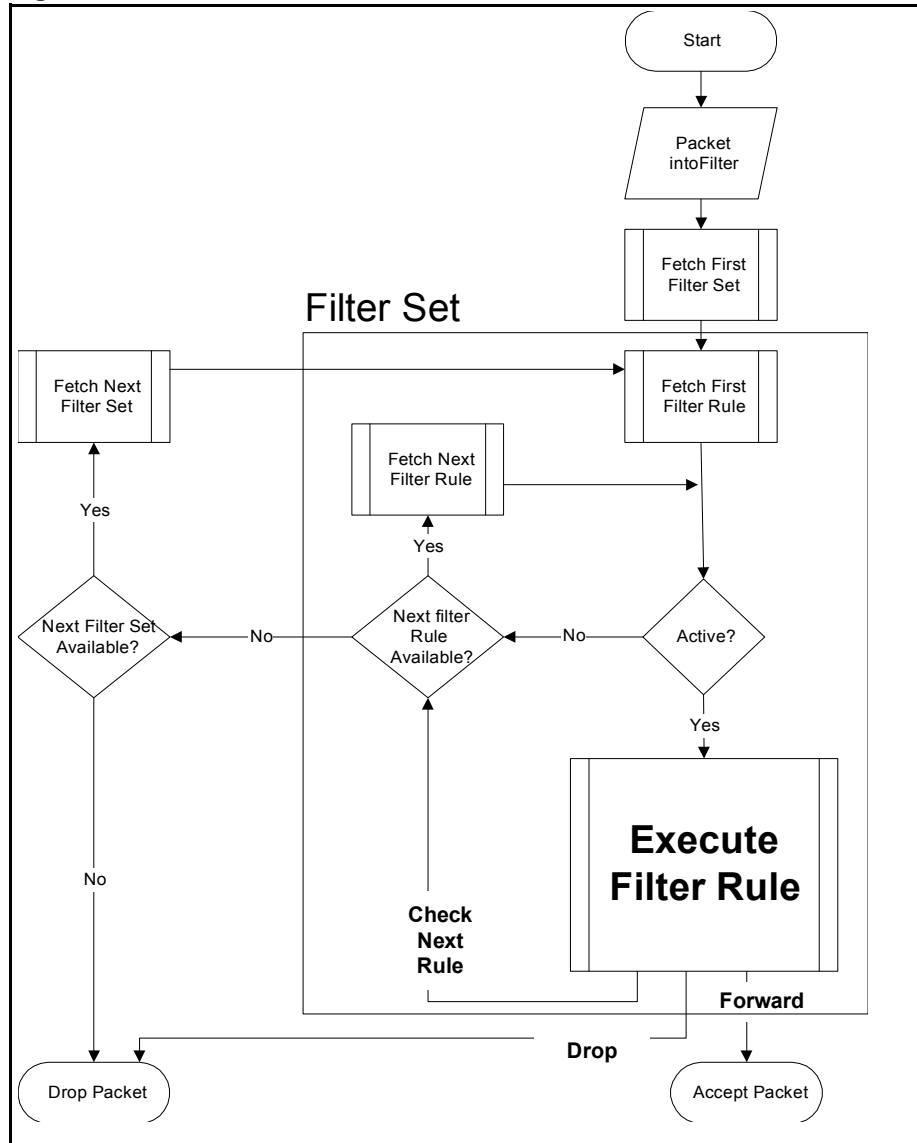
**Figure 185** Outgoing Packet Filtering Process



Two sets of factory filter rules have been configured in menu 21 to prevent NetBIOS traffic from triggering calls. A summary of their filter rules is shown in the figures that follow.

The following figure illustrates the logic flow when executing a filter rule.

**Figure 186** Filter Rule Process



You can apply up to four filter sets to a particular port to block various types of packets. Because each filter set can have up to six rules, you can have a maximum of 24 rules active for a single port.

For incoming packets, your Prestige applies data filters only. Packets are processed depending on whether a match is found. The following sections describe how to configure filter sets.

### 33.1.1 The Filter Structure of the Prestige

A filter set consists of one or more filter rules. Usually, you would group related rules, for example, all the rules for NetBIOS, into a single set and give it a descriptive name. You can configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system.



## 33.2 Configuring a Filter Set for the Prestige

To configure a filter set, follow the steps shown next.

- 1 Enter 21 in the main menu to display **Menu 21 – Filter and Firewall Setup**.
- 2 Enter 1 to display **Menu 21.1 – Filter Set Configuration** as shown next.

**Figure 187** Menu 21 Filter Set Configuration

```

Menu 21.1 - Filter Set Configuration
Filter Set #      Comments                Filter Set #      Comments
-----
 1                _____                7                _____
 2      NetBIOS_WAN                8                _____
 3      NetBIOS_LAN                9                _____
 4      IGMP                        10               _____
 5                _____                11               _____
 6                _____                12               _____

Enter Filter Set Number to Configure= 0

Edit Comments= N/A

Press ENTER to Confirm or ESC to Cancel:

```

- 3 Type the filter set to configure (no. 1 to 12) and press [ENTER].
- 4 Type a descriptive name or comment in the **Edit Comments** field and press [ENTER].
- 5 Press [ENTER] at the message “**Press ENTER to confirm...**” to display **Menu 21.1.1 – Filter Rules Summary** (that is, if you selected filter set 1 in menu 21.1).

**Figure 188** NetBIOS\_WAN Filter Rules Summary

```

Menu 21.1.2 - Filter Rules Summary
# A Type                Filter Rules                M m n
-----
- - - - -
1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=137        N D N
2 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=138        N D N
3 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=139        N D N
4 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=137       N D N
5 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=138       N D N
6 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=139       N D F

Enter Filter Rule Number (1-6) to Configure:

```

**Figure 189** NetBIOS\_LAN Filter Rules Summary

```

Menu 21.1.3 - Filter Rules Summary
# A Type                               Filter Rules                               M m n
-----
1 Y IP   Pr=17, SA=0.0.0.0, SP=137, DA=0.0.0.0, DP=53   N D F
2 N
3 N
4 N
5 N
6 N

Enter Filter Rule Number (1-6) to Configure:
    
```

**Figure 190** IGMP Filter Rules Summary

```

Menu 21.1.4 - Filter Rules Summary
# A Type                               Filter Rules                               M m n
-----
1 Y Gen  Off=0, Len=3, Mask=ffffff, Value=01005e         N D F
2 N
3 N
4 N
5 N
6 N

Enter Filter Rule Number (1-6) to Configure:
    
```

### 33.3 Filter Rules Summary Menus

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

**Table 109** Abbreviations Used in the Filter Rules Summary Menu

FIELD	DESCRIPTION
#	The filter rule number: 1 to 6.
A	Active: "Y" means the rule is active. "N" means the rule is inactive.
Type	The type of filter rule: "GEN" for Generic, "IP" for TCP/IP.
Filter Rules	These parameters are displayed here.
M	More. "Y" means there are more rules to check which form a rule chain with the present rule. An action cannot be taken until the rule chain is complete. "N" means there are no more rules to check. You can specify an action to be taken for instance, forward the packet, drop the packet or check the next rule. For the latter, the next rule is independent of the rule just checked.

**Table 109** Abbreviations Used in the Filter Rules Summary Menu (continued)

FIELD	DESCRIPTION
m	Action Matched. “F” means to forward the packet immediately and skip checking the remaining rules. “D” means to drop the packet. “N” means to check the next rule.
n	Action Not Matched. “F” means to forward the packet immediately and skip checking the remaining rules. “D” means to drop the packet. “N” means to check the next rule.

The protocol dependent filter rules abbreviation are listed as follows:

**Table 110** Rule Abbreviations Used

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

## 33.4 Configuring a Filter Rule

To configure a filter rule, type its number in **Menu 21.1.x – Filter Rules Summary** and press [ENTER] to open menu 21.1.x.1 for the rule.

There are two types of filter rules: **TCP/IP** and **Generic**. Depending on the type of rule, the parameters for each type will be different. Use [SPACE BAR] to select the type of rule that you want to create in the **Filter Type** field and press [ENTER] to open the respective menu.

To speed up filtering, all rules in a filter set must be of the same class, for instance, protocol filters or generic filters. The class of a filter set is determined by the first rule that you create. When applying the filter sets to a port, separate menu fields are provided for protocol and device filter sets. If you include a protocol filter set in a device filters field or vice versa, the Prestige will warn you and will not allow you to save.

### 33.4.1 TCP/IP Filter Rule

This section shows you how to configure a TCP/IP filter rule. TCP/IP rules allow you to base the rule on the fields in the IP and the upper layer protocol, for example, UDP and TCP headers.

To configure TCP/IP rules, select TCP/IP Filter Rule from the **Filter Type** field and press [ENTER] to open **Menu 21.1.x.1 – TCP/IP Filter Rule**, as shown next.

**Figure 191** Menu 21.1.x.1 TCP/IP Filter Rule

```

Menu 21.1.1.1 - TCP/IP Filter Rule

Filter #: 1,1
Filter Type= TCP/IP Filter Rule
Active= No
IP Protocol= 0      IP Source Route= No
Destination: IP Addr=
                IP Mask=
                Port #=
                Port # Comp= None
Source: IP Addr=
        IP Mask=
        Port #=
        Port # Comp= None
TCP Estab= N/A
More= No           Log= None
Action Matched= Check Next Rule
Action Not Matched= Check Next Rule

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

The following table describes how to configure your TCP/IP filter rule.

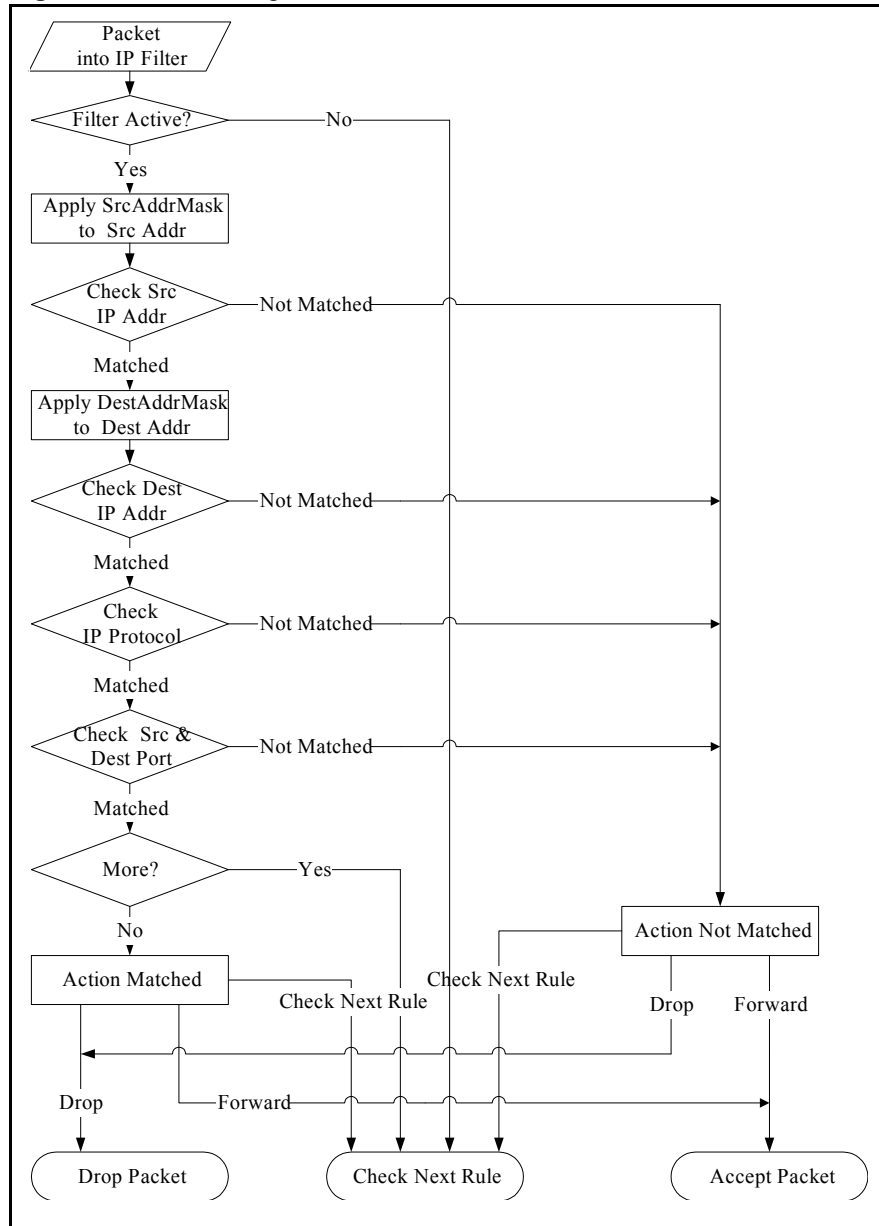
**Table 111** Menu 21.1.x.1 TCP/IP Filter Rule

FIELD	DESCRIPTION
Filter #	This is the filter set, filter rule coordinates, for instance, 2, 3 refers to the second filter set and the third filter rule of that set.
Filter Type	Use [SPACE BAR] and then [ENTER] to choose a rule. Parameters displayed for each type will be different. Choices are <b>TCP/IP Filter Rule</b> or <b>Generic Filter Rule</b> .
Active	Select <b>Yes</b> to activate or <b>No</b> to deactivate the filter rule.
IP Protocol	This is the upper layer protocol, for example, TCP is 6, UDP is 17 and ICMP is 1. The value must be between 0 and 255. A value of 0 matches ANY protocol.
IP Source Route	IP Source Route is an optional header that dictates the route an IP packet takes from its source to its destination. If <b>Yes</b> , the rule applies to any packet with an IP source route. The majority of IP packets do not have source route.
Destination:	
IP Addr	Type the destination IP address of the packet you want to filter. This field is ignored if it is 0.0.0.0.
IP Mask	Type the IP mask to apply to the <b>Destination: IP Addr</b> field.

**Table 111** Menu 21.1.x.1 TCP/IP Filter Rule (continued)

FIELD	DESCRIPTION
Port #	Type the destination port of the packets you want to filter. The field range is 0 to 65535. A 0 field is ignored.
Port # Comp	Select the comparison to apply to the destination port in the packet against the value given in <b>Destination: Port #</b> . Choices are <b>None</b> , <b>Less</b> , <b>Greater</b> , <b>Equal</b> or <b>Not Equal</b> .
Source:	
IP Addr	Type the source IP Address of the packet you want to filter. A 0.0.0.0 field is ignored.
IP Mask	Type the IP mask to apply to the <b>Source: IP Addr</b> field.
Port #	Type the source port of the packets you want to filter. The range of this field is 0 to 65535. A 0 field is ignored.
Port # Comp	Select the comparison to apply to the source port in the packet against the value given in <b>Source: Port #</b> field. Choices are <b>None</b> , <b>Less</b> , <b>Greater</b> , <b>Equal</b> or <b>Not Equal</b> .
TCP Estab	This applies only when the IP Protocol field is 6, TCP. If <b>Yes</b> , the rule matches packets that want to establish TCP connection(s) (SYN=1 and ACK=0); else it is ignored.
More	If <b>Yes</b> , a matching packet is passed to the next filter rule before an action is taken or else the packet is disposed of according to the action fields. If <b>More</b> is <b>Yes</b> , then <b>Action Matched</b> and <b>Action Not Matched</b> will be N/A.
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 matching packet. Choices are <b>Check Next Rule</b> , <b>Forward</b> or <b>Drop</b> .
Action Not Matched	Select the action for a packet not matching the rule. Choices are <b>Check Next Rule</b> , <b>Forward</b> or <b>Drop</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] at any time to cancel.	

The following figure illustrates the logic flow of an IP filter.

**Figure 192** Executing an IP Filter

### 33.4.2 Generic Filter Rule

This section shows you how to configure a generic filter rule. The purpose of generic rules is to allow you to filter non-IP packets. For IP, it is generally easier to use the IP rules directly.

For generic rules, the Prestige treats a packet as a byte stream as opposed to an IP packet. You specify the portion of the packet to check with the **Offset** (from 0) and the **Length** fields, both in bytes. The Prestige applies the Mask (bit-wise ANDing) to the data portion before comparing the result against the Value to determine a match. The **Mask** and **Value** fields are specified in hexadecimal numbers. Note that it takes two hexadecimal digits to represent a byte, so if the length is 4, the value in either field will take 8 digits, for example, FFFFFFFF.

To configure a generic rule select an empty filter set in menu 21, for example 5. Select **Generic Filter Rule** in the **Filter Type** field and press [ENTER] to open **Menu 21.1.5.1 – Generic Filter Rule**, as shown in the following figure.

**Figure 193** Menu 21.1.5.1 Generic Filter Rule

```

Menu 21.1.5.1 - Generic Filter Rule

Filter #: 5,1
Filter Type= Generic Filter Rule
Active= No
Offset= 0
Length= 0
Mask= N/A
Value= N/A
More= No          Log= None
Action Matched= Check Next Rule
Action Not Matched= Check Next Rule

Press ENTER to Confirm or ESC to Cancel:

```

The next table describes the fields in the **Generic Filter Rule** menu.

**Table 112** Menu 21.1.5.1 Generic Filter Rule

FIELD	DESCRIPTION
Filter #	This is the filter set, filter rule coordinates, for instance, 2, 3 refers to the second filter set and the third rule of that set.
Filter Type	Press [SPACE BAR] and then [ENTER] to select a type of rule. Parameters displayed below each type will be different. Choices are <b>Generic Filter Rule</b> or <b>TCP/IP Filter Rule</b> .
Active	Select <b>Yes</b> to turn on or <b>No</b> to turn off the filter rule.
Offset	Type the starting byte of the data portion in the packet that you want to compare. The range for this field is from 0 to 255.
Length	Type the byte count of the data portion in the packet that you want to compare. The range for this field is 0 to 8.
Mask	Type the mask (in Hexadecimal) to apply to the data portion before comparison.
Value	Type the value (in Hexadecimal) to compare with the data portion.
More	If <b>Yes</b> , a matching packet is passed to the next filter rule before an action is taken or else the packet is disposed of according to the action fields. If <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	Select the logging option from the following: <b>None</b> – No packets will be logged. <b>Action Matched</b> – Only matching packets and rules 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 matching packet. Choices are <b>Check Next Rule</b> , <b>Forward</b> or <b>Drop</b> .

**Table 112** Menu 21.1.5.1 Generic Filter Rule (continued)

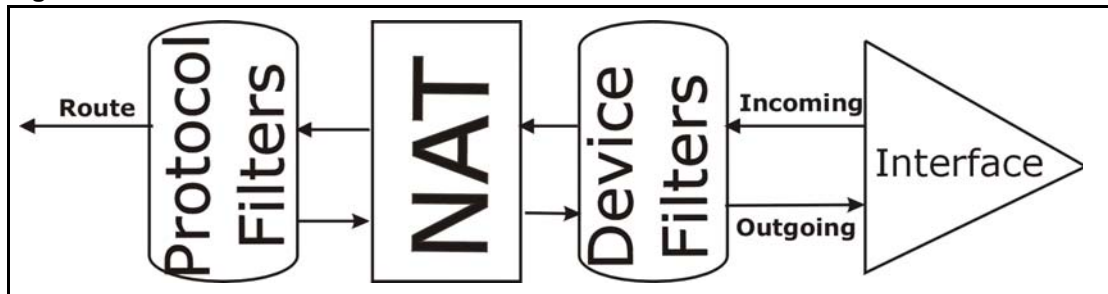
FIELD	DESCRIPTION
Action Not Matched	Select the action for a packet not matching the rule. Choices are <b>Check Next Rule</b> , <b>Forward</b> or <b>Drop</b> .
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm or ESC to Cancel:" to save your configuration, or press [ESC] at any time to cancel.	

### 33.5 Filter Types and NAT

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

When NAT (Network Address Translation) is enabled, the inside IP address and port number are replaced on a connection-by-connection basis, which makes it impossible to know the exact address and port on the wire. Therefore, the Prestige applies the protocol filters to the "native" IP address and port number before NAT for outgoing packets and after NAT for incoming packets. On the other hand, the generic (or device) filters are applied to the raw packets that appear on the wire. They are applied at the point where the Prestige is receiving and sending the packets; for instance, the interface. The interface can be an Ethernet, or any other hardware port. The following figure illustrates this.

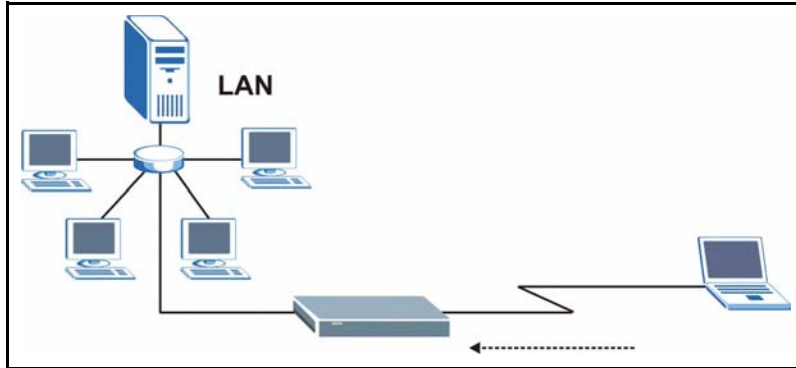
**Figure 194** Protocol and Device Filter Sets



### 33.6 Example Filter

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



**Figure 195** Sample Telnet Filter

- 1 Enter 1 in the menu 21 to display **Menu 21.1 — Filter Set Configuration**.
- 2 Enter the index number of the filter set you want to configure (in this case 6).
- 3 Type a descriptive name or comment in the **Edit Comments** field (for example, TELNET\_WAN) and press [ENTER].
- 4 Press [ENTER] at the message “Press [ENTER] to confirm or [ESC] to cancel ...” to open **Menu 21.1.6 — Filter Rules Summary**.
- 5 Type 1 to configure the first filter rule. Make the entries in this menu as shown next.

When you press [ENTER] to confirm, the following screen appears. Note that there is only one filter rule in this set.

**Figure 196** Menu 21.1.6.1 Sample Filter

```

Menu 21.1.6.1 - TCP/IP Filter Rule

Filter #: 6,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6      IP Source Route= No
Destination: IP Addr= 0.0.0.0
IP Mask= 0.0.0.0
Port #= 23
Port # Comp= Equal
                Source: IP Addr= 0.0.0.0
IP Mask= 0.0.0.0
Port #=
Port # Comp= Equal
TCP Estab= No
More= No          Log= None
Action Matched= Drop
Action Not Matched= Forward

Press ENTER to Confirm or ESC to Cancel:

```

After you have created the filter set, you must apply it.

- 1 Enter 11 in the main menu to display menu 11 and type the remote node number to edit.

**2** Go to the **Edit Filter Sets** field, press [SPACE BAR] to choose **Yes** and press [ENTER].

This brings you to menu 11.5. Apply the example filter set (for example, filter set 3) in this menu as shown in the next section.

This shows you that you have configured and activated (**A = Y**) a TCP/IP filter rule (**Type = IP, Pr = 6**) for destination telnet ports (**DP = 23**).

**M = N** means an action can be taken immediately. The action is to drop the packet (**m = D**) if the action is matched and to forward the packet immediately (**n = F**) if the action is not matched no matter whether there are more rules to be checked (there aren't in this example).

**Figure 197** Menu 21.1.6.1 Sample Filter Rules Summary

Menu 21.1.6 - Filter Rules Summary			
#	A	Type	Filter Rules
1	Y	IP	Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23
2	N		
3	N		
4	N		
5	N		
6	N		

Enter Filter Rule Number (1-6) to Configure: 1

### 33.7 Applying Filters and Factory Defaults

This section shows you where to apply the filter(s) after you design it (them). Sets of factory default filter rules have been configured in menu 21 (but have not been applied) to filter traffic.

**Table 113** Filter Sets Table

FILTER SETS	DESCRIPTION
Input Filter Sets:	Apply filters for incoming traffic. You may apply protocol or device filter rules. See earlier in this chapter for information on filters.
Output Filter Sets:	Apply filters for traffic leaving the Prestige. You may apply filter rules for protocol or device filters. See earlier in this section for information on types of filters.
Call Filter Sets:	Apply filters to decide if a packet should be allowed to trigger a call.

### 33.7.1 Ethernet Traffic

You seldom need to filter Ethernet traffic; however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 3.1 (shown next) and type the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by typing their numbers separated by commas, for example, 3, 4, 6, 11. The factory default filter set, `NetBIOS_LAN`, is inserted in the **protocol filters** field under **Input Filter Sets** in menu 3.1 in order to prevent local NetBIOS messages from triggering calls to the DNS server.

**Figure 198** Filtering Ethernet Traffic

```

Menu 3.1 - LAN Port Filter Setup

Input Filter Sets:
protocol filters= 3
device filters=
Output Filter Sets:
protocol filters=
device filters=

Press ENTER to Confirm or ESC to Cancel:

```

### 33.7.2 Remote Node Filters

Go to menu 11.5 (shown next) and type the number(s) of the filter set(s) as appropriate. You can cascade up to four filter sets by typing their numbers separated by commas. The factory default filter set, `NetBIOS_WAN`, is inserted in the **protocol filters** field under **Call Filter Sets** in menu 11.5 to block local NetBIOS traffic from triggering calls to the ISP.

**Figure 199** Filtering Remote Node Traffic

```

Menu 11.5 - Remote Node Filter

Input Filter Sets:
  protocol filters= 6
  device filters=
Output Filter Sets:
  protocol filters= 2
  device filters=
Call Filter Sets:
  Protocol filters=
  Device filters=

Enter here to CONFIRM or ESC to CANCEL:

```

Note that call filter sets are visible when you select PPPoA or PPPoE encapsulation.



# CHAPTER 34

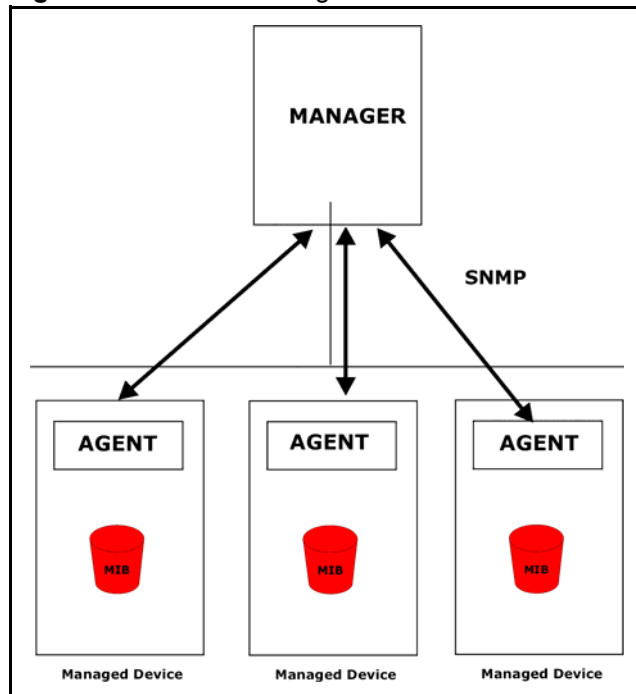
## SNMP Configuration

This chapter explains SNMP Configuration menu 22.

### 34.1 About SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your Prestige supports SNMP agent functionality, which allows a manager station to manage and monitor the Prestige through the network. The Prestige supports SNMP version one (SNMPv1) and version two c (SNMPv2c). The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

**Figure 200** SNMP Management Model



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

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

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

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

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

## 34.2 Supported MIBs

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

## 34.3 SNMP Configuration

To configure SNMP, select option 22 from the main menu to open **Menu 22 — SNMP Configuration** as shown next. The “community” for Get, Set and Trap fields is SNMP terminology for password.

**Figure 201** 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 114** 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.
Trap:	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager.
Destination	Type the IP address of the station to send your SNMP traps to.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm or ESC to Cancel:" to save your configuration, or press [ESC] at any time to cancel.	

## 34.4 SNMP Traps

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

**Table 115** SNMP Traps

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

**Table 115** SNMP Traps (continued)

TRAP #	TRAP NAME	DESCRIPTION
5	authenticationFailure ( <i>defined in RFC-1215</i> )	A trap is sent to the manager when receiving any SNMP gets or sets requirements with wrong community (password).
6	whyReboot (defined in ZYXEL-MIB)	A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start).
6a	For intentional reboot :	A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (for example, download new files, CI command "sys reboot", etc.).

The port number is its interface index under the interface group.

**Table 116** Ports and Permanent Virtual Circuits

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



# CHAPTER 35

## System Security

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

### 35.1 System Security

You can configure the system password..

#### 35.1.1 System Password

Enter 23 in the main menu to display **Menu 23 – System Security**.

You should change the default password. If you forget your password you have to restore the default configuration file. Refer to [Section 22.4 on page 270](#) and [Section 2.1.2 on page 58](#) for information.

**Figure 202** Menu 23 – System Security

```
Menu 23 - System Security

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

Enter Menu Selection Number:
```

#### 35.1.2 Configuring External RADIUS Server

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

**Figure 203** Menu 23 System Security

```
Menu 23 - System Security

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

**Figure 204** Menu 23.2 System Security: RADIUS Server

```

Menu 23.2 - System Security - RADIUS Server

Authentication Server:
Active= No
Server Address= 10.11.12.13
Port #= 1812
Shared Secret= *****
Accounting Server:
Active= No
Server Address= 10.11.12.13
Port #= 1813
Shared Secret= *****

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

The following table describes the fields in this menu.

**Table 117** Menu 23.2 System Security: RADIUS Server

FIELD	DESCRIPTION
Authentication Server	
Active	Press [SPACE BAR] to select <b>Yes</b> and press [ENTER] to enable user authentication through an external authentication server.
Server Address	Enter the IP address of the external authentication server in dotted decimal notation.
Port	The default port of the RADIUS server for authentication is <b>1812</b> . You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Specify a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the access points. The key is not sent over the network. This key must be the same on the external authentication server and Prestige.
Accounting Server	
Active	Press [SPACE BAR] to select <b>Yes</b> and press [ENTER] to enable user authentication through an external accounting server.
Server Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port	The default port of the RADIUS server for accounting is <b>1813</b> . You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret	Specify a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the access points. The key is not sent over the network. This key must be the same on the external accounting server and Prestige.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm or ESC to Cancel:" to save your configuration, or press [ESC] at any time to cancel.	

### 35.1.3 IEEE802.1x

The IEEE802.1x standards outline enhanced security methods for both the authentication of wireless stations and encryption key management.

Follow the steps below to enable EAP authentication on your Prestige.

- 1 From the main menu, enter 23 to display **Menu23 – System Security**.

**Figure 205** Menu 23 System Security

```

Menu 23 - System Security

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

Enter Menu Selection Number:

```

- 2 Enter 4 to display **Menu 23.4 – System Security – IEEE802.1x**.

**Figure 206** Menu 23.4 System Security: IEEE802.1x

```

Menu 23.4 - System Security - IEEE802.1x

Wireless Port Control= No Authentication Required
ReAuthentication Timer (in second)= N/A
Idle Timeout (in second)= N/A

Key Management Protocol= N/A
Dynamic WEP Key Exchange= N/A
PSK= N/A
WPA Mixed Mode= N/A
Data Privacy for Broadcast/Multicast packets= N/A
WPA Broadcast/Multicast Key Update Timer= N/A

Authentication Databases= N/A

Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the fields in this menu.

**Table 118** Menu 23.4 System Security: IEEE802.1x

FIELD	DESCRIPTION
Wireless Port Control	<p>Press [SPACE BAR] and select a security mode for the wireless LAN access. Select <b>No Authentication Required</b> to allow any wireless stations access to your wired network without entering usernames and passwords. This is the default setting.</p> <p>Selecting <b>Authentication Required</b> means wireless stations have to enter usernames and passwords before access to the wired network is allowed.</p> <p>Select <b>No Access Allowed</b> to block all wireless stations access to the wired network.</p> <p>The following fields are not available when you select <b>No Authentication Required</b> or <b>No Access Allowed</b>.</p>
ReAuthentication Timer (in second)	<p>Specify how often a client has to re-enter username and password to stay connected to the wired network.</p> <p>This field is activated only when you select <b>Authentication Required</b> in the <b>Wireless Port Control</b> field. Enter a time interval between 10 and 9999 (in seconds). The default time interval is <b>1800</b> seconds (or 30 minutes).</p>
Idle Timeout (in second)	<p>The Prestige automatically disconnects a client from the wired network after a period of inactivity. The client needs to enter the username and password again before access to the wired network is allowed.</p> <p>This field is activated only when you select <b>Authentication Required</b> in the <b>Wireless Port Control</b> field. The default time interval is <b>3600</b> seconds (or 1 hour).</p>
Key Management Protocol	<p>Press [SPACE BAR] to select <b>802.1x</b>, <b>WPA</b> or <b>WPA-PSK</b> and press [ENTER].</p>
Dynamic WEP Key Exchange	<p>This field is activated only when you select <b>Authentication Required</b> in the <b>Wireless Port Control</b> field. Also set the <b>Authentication Databases</b> field to <b>RADIUS Only</b>. Local user database may not be used.</p> <p>Select <b>Disable</b> to allow wireless stations to communicate with the access points without using Dynamic WEP Key Exchange.</p> <p>Select <b>64-bit WEP</b> or <b>128-bit WEP</b> to enable data encryption.</p> <p>Up to 32 stations can access the Prestige when you configure Dynamic WEP Key Exchange. This field is not available when you set <b>Key Management Protocol</b> to <b>WPA</b> or <b>WPA-PSK</b>.</p>
PSK	<p>Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols) when you select <b>WPA-PSK</b> in the <b>Key Management Protocol</b> field.</p>
WPA Mixed Mode	<p>Select <b>Enable</b> to activate WPA mixed mode. Otherwise, select <b>Disable</b> and configure <b>Group Data Privacy</b> field.</p>
Data Privacy for Broadcast/Multicast packets	<p>This field allows you to choose <b>TKIP</b> (recommended) or <b>WEP</b> for broadcast and multicast ("group") traffic if the <b>Key Management Protocol</b> is <b>WPA</b> and <b>WPA Mixed Mode</b> is disabled. <b>WEP</b> is used automatically if you have enabled <b>WPA Mixed Mode</b>.</p> <p>All unicast traffic is automatically encrypted by <b>TKIP</b> when <b>WPA</b> or <b>WPA-PSK Key Management Protocol</b> is selected.</p>
WPA Broadcast/Multicast Key Update Timer	<p>The <b>WPA Broadcast/Multicast Key Update Timer</b> is the rate at which the AP (if using <b>WPA-PSK</b> key management) or RADIUS server (if using <b>WPA</b> key management) sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the WEP key for an AP and all stations in a WLAN on a periodic basis. Setting of the <b>WPA Broadcast/Multicast Key Update Timer</b> is also supported in WPA-PSK mode. The Prestige default is 1800 seconds (30 minutes).</p>

**Table 118** Menu 23.4 System Security: IEEE802.1x (continued)

FIELD	DESCRIPTION
Authentication Databases	<p>The authentication database contains wireless station login information. The local user database is the built-in database on the Prestige. The RADIUS is an external server. Use this field to decide which database the Prestige should use (first) to authenticate a wireless station.</p> <p>Before you specify the priority, make sure you have set up the corresponding database correctly first.</p> <p>When you configure <b>Key Management Protocol</b> to <b>WPA</b>, the <b>Authentication Databases</b> must be <b>RADIUS Only</b>. You can only use the <b>Local User Database</b> with <b>802.1x Key Management Protocol</b>.</p> <p>Select <b>Local User Database Only</b> to have the Prestige just check the built-in user database on the Prestige for a wireless station's username and password.</p> <p>Select <b>RADIUS Only</b> to have the Prestige just check the user database on the specified RADIUS server for a wireless station's username and password.</p> <p>Select <b>Local first, then RADIUS</b> to have the Prestige first check the user database on the Prestige for a wireless station's username and password. If the user name is not found, the Prestige then checks the user database on the specified RADIUS server.</p> <p>Select <b>RADIUS first, then Local</b> to have the Prestige first check the user database on the specified RADIUS server for a wireless station's username and password. If the Prestige cannot reach the RADIUS server, the Prestige then checks the local user database on the Prestige. When the user name is not found or password does not match in the RADIUS server, the Prestige will not check the local user database and the authentication fails.</p>
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm or ESC to Cancel:" to save your configuration, or press [ESC] at any time to cancel.	

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

## 35.2 Creating User Accounts on the Prestige

By storing user profiles locally, your Prestige is able to authenticate wireless users without interacting with a network RADIUS server.

Follow the steps below to set up user profiles on your Prestige.

- 1 From the main menu, enter 14 to display **Menu 14 - Dial-in User Setup**.

**Figure 207** Menu 14 Dial-in User Setup

```

Menu 14 - Dial-in User Setup

1. _____      9. _____      17. _____      25. _____
2. _____      10. _____     18. _____     26. _____
3. _____      11. _____     19. _____     27. _____
4. _____      12. _____     20. _____     28. _____
5. _____      13. _____     21. _____     29. _____
6. _____      14. _____     22. _____     30. _____
7. _____      15. _____     23. _____     31. _____
8. _____      16. _____     24. _____     32. _____

Enter Menu Selection Number:
    
```

**2** Type a number and press [ENTER] to edit the user profile.

**Figure 208** Menu 14.1 Edit Dial-in User

```

Menu 14.1 - Edit Dial-in User

User Name= test
Active= Yes
Password= *****

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

The following table describes the fields in this menu.

**Table 119** Menu 14.1 Edit Dial-in User

FIELD	DESCRIPTION
User Name	Enter a username up to 31 alphanumeric characters long for this user profile. This field is case sensitive.
Active	Press [SPACE BAR] to select <b>Yes</b> and press [ENTER] to enable the user profile.
Password	Enter a password up to 31 characters long for this user profile.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm or ESC to Cancel:" to save your configuration, or press [ESC] at any time to cancel.	

# CHAPTER 36

## System Information and Diagnosis

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

### 36.1 Overview

These tools include updates on system status, port status, log and trace capabilities and upgrades for the system software. This chapter describes how to use these tools in detail.

Type 24 in the main menu to open **Menu 24 – System Maintenance**, as shown in the following figure.

**Figure 209** Menu 24 System Maintenance

```
Menu 24 - System Maintenance

1. System Status
2. System Information and Console Port Speed
3. Log and Trace
4. Diagnostic
5. Backup Configuration
6. Restore Configuration
7. Upload Firmware
8. Command Interpreter Mode
9. Call Control
10. Time and Date Setting
11. Remote Management

Enter Menu Selection Number:
```

### 36.2 System Status

The first selection, System Status gives you information on the status and statistics of the ports, as shown next. System Status is a tool that can be used to monitor your Prestige. Specifically, it gives you information on your DSL telephone line status, number of packets sent and received.

To get to System Status, type 24 to go to **Menu 24 — System Maintenance**. From this menu, type 1. **System Status**. There are two commands in **Menu 24.1 — System Maintenance — Status**. Entering 1 resets the counters; [ESC] takes you back to the previous screen.

The following table describes the fields present in **Menu 24.1 — System Maintenance — Status** which are read-only and meant for diagnostic purposes.

**Figure 210** Menu 24.1 System Maintenance : Status

```

Menu 24.1 - System Maintenance - Status                                00:36:37
                                                                    Sat. Jan. 01, 2000
Node-Lnk Status      TxPkts      RxPkts      Errors  Tx B/s  Rx B/s      Up
Time
1-PPPoA N/A          0          0          0       0       0       0:00:00
2      N/A           0          0          0       0       0       0:00:00
3      N/A           0          0          0       0       0       0:00:00
4      N/A           0          0          0       0       0       0:00:00
5      N/A           0          0          0       0       0       0:00:00
6      N/A           0          0          0       0       0       0:00:00
7      N/A           0          0          0       0       0       0:00:00
My WAN IP (from ISP): 0.0.0.0
  Ethernet:
    Status:                Tx Pkts: 528          WAN:
                          Rx Pkts: 505          Line Status: Down
    Collisions: 0          Upstream Speed:    0 kbps
    CPU Load =   2.12%    Downstream Speed:  0 kbps

                          Press Command:
                          COMMANDS: 1-Reset Counters  ESC-Exit
    
```

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

**Table 120** Menu 24.1 System Maintenance: Status

FIELD	DESCRIPTION
Node-Lnk	This is the node index number and link type. Link types are: PPP, ENET, 1483.
Status	This shows the status of the remote node.
TxPkts	The number of transmitted packets to this remote node.
RxPkts	The number of received packets from this remote node.
Errors	The number of error packets on this connection.
Tx B/s	This shows the transmission rate in bytes per second.
Rx B/s	This shows the receiving rate in bytes per second.
Up Time	This is the time this channel has been connected to the current remote node.
My WAN IP (from ISP)	This is the IP address of the ISP remote node.
Ethernet	This shows statistics for the LAN.
Status	This shows the current status of the LAN.
Tx Pkts	This is the number of transmitted packets to the LAN.
Rx Pkts	This is the number of received packets from the LAN.
Collision	This is the number of collisions.
WAN	This shows statistics for the WAN.



**Table 120** Menu 24.1 System Maintenance: Status (continued)

FIELD	DESCRIPTION
Line Status	This shows the current status of the xDSL line, which can be Up or Down.
Upstream Speed	This shows the upstream transfer rate in kbps.
Downstream Speed	This shows the downstream transfer rate in kbps.
CPU Load	This specifies the percentage of CPU utilization.

## 36.3 System Information

To get to the System Information:

- 1** Enter 24 to display **Menu 24 — System Maintenance**.
- 2** Enter 2 to display Menu 24.2 — System Information and Console Port Speed.

From this menu you have two choices as shown in the next figure:

**Figure 211** 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>
--

### 36.3.1 System Information

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

**Figure 212** Menu 24.2.1 System Maintenance: Information

```

Menu 24.2.1 - System Maintenance - Information

Name:
Routing: IP
ZyNOS F/W Version: V3.40(MF.2) | 07/16/2004
ADSL Chipset Vendor: TI AR7 01.01.00.00
Standard: Multi-Mode
LAN
Ethernet Address: 00:a0:c5:78:de:8d
IP Address: 192.168.1.1
IP Mask: 255.255.255.0
DHCP: Server

Press ESC or RETURN to Exit:
    
```

The following table describes the fields in this menu.

**Table 121** 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.
ADSL Chipset Vendor	Displays the vendor of the ADSL chipset and DSL version.
Standard	This refers to the operational protocol the Prestige and the DSLAM (Digital Subscriber Line Access Multiplexer) are using.
LAN	
Ethernet Address	Refers to the Ethernet MAC (Media Access Control) of your Prestige.
IP Address	This is the IP address of the Prestige in dotted decimal notation.
IP Mask	This shows the subnet mask of the Prestige.
DHCP	This field shows the DHCP setting (None, Relay or Server) of the Prestige.

### 36.3.2 Console Port Speed

You can set up different port speeds for the console port through **Menu 24.2.2 – System Maintenance – Console Port Speed**. Your Prestige supports 9600 (default), 19200, 38400, 57600 and 115200 bps. Press [SPACE BAR] and then [ENTER] to select the desired speed in menu 24.2.2, as shown in the following figure.

**Figure 213** Menu 24.2.2 System Maintenance : Change Console Port Speed

```
Menu 24.2.2 - System Maintenance - Change Console Port Speed

Console Port Speed: 9600

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

Once you change the Prestige console port speed, you must also set the speed parameter for the communication software you are using to connect to the Prestige.

## 36.4 Log and Trace

There are two logging facilities in the Prestige. The first is the error logs and trace records that are stored locally. The second is the syslog facility for message logging.

### 36.4.1 Viewing Error Log

The first place you should look for clues when something goes wrong is the error log. Follow the procedures to view the local error/trace log:

- 1 Type 24 in the main menu to display **Menu 24 – System Maintenance**.
- 2 From menu 24, type 3 to display **Menu 24.3 – System Maintenance – Log and Trace**.

**Figure 214** Menu 24.3 System Maintenance: Log and Trace

```
Menu 24.3 - System Maintenance - Log and Trace

1. View Error Log
2. UNIX Syslog

Please enter selection
```

- 3 Enter 1 from **Menu 24.3 — System Maintenance — Log and Trace** to display the error log in the system.

After the Prestige finishes displaying the error log, you will have the option to clear it. Samples of typical error and information messages are presented in the next figure.

**Figure 215** Sample Error and Information Messages

```

53 Sat Jan 01 00:00:03 2000 PP01 -WARN  SNMP TRAP 0: cold start
54 Sat Jan 01 00:00:03 2000 PP01  INFO  main: init completed
55 Sat Jan 01 00:00:03 2000 PP01  INFO  Starting Connectivity Monitor
56 Sat Jan 01 00:00:03 2000 PP20  INFO  adjtime task pause 1 day
57 Sat Jan 01 00:00:03 2000 PP21  INFO  monitoring WAN connectivity
58 Sat Jan 01 00:03:06 2000 PP19  INFO  SMT Password pass
59 Sat Jan 01 00:03:06 2000 PP01  INFO  SMT Session Begin
60 Sat Jan 01 00:23:21 2000 PP01  INFO  SMT Session End
62 Sat Jan 01 00:23:38 2000 PP19  INFO  SMT Password pass
63 Sat Jan 01 00:23:38 2000 PP01  INFO  SMT Session Begin
Clear Error Log (y/n):
    
```

### 36.4.2 Syslog and Accounting

The Prestige uses the syslog facility to log the CDR (Call Detail Record) and system messages to a syslog server. Syslog and accounting can be configured in **Menu 24.3.2 — System Maintenance — UNIX Syslog**, as shown next.

**Figure 216** Menu 24.3.2 System Maintenance: Syslog and Accounting

```

Menu 24.3.2 - System Maintenance - UNIX Syslog

UNIX Syslog:
Active= No
Syslog IP Address= ?
Log Facility= Local 1

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

You need to configure the UNIX syslog parameters described in the following table to activate syslog then choose what you want to log.

**Table 122** Menu 24.3.2 System Maintenance : Syslog and Accounting

PARAMETER	DESCRIPTION
UNIX Syslog:	
Active	Use [SPACE BAR] and then [ENTER] to turn syslog on or off.
Syslog IP Address	Type the IP address of your syslog server.
Log Facility	Use [SPACE BAR] and then [ENTER] to select one of seven different local options. The log facility lets you log the message in different server files. Refer to your UNIX manual.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm or ESC to Cancel:" to save your configuration, or press [ESC] at any time to cancel.	

The following are examples of the four types of syslog messages sent by the Prestige:

**Figure 217 Syslog Example**

```

1 - CDR
SdcmdSyslogSend ( SYSLOG_CDR, SYSLOG_INFO, String);
String = board xx line xx channel xx, call xx, str
board = the hardware board ID
line = the WAN ID in a board
Channel = channel ID within the WAN
call = the call reference number which starts from 1 and increments by 1 for each new
call
str = C01 Outgoing Call dev xx ch xx (dev:device No. ch:channel No.)
C01 Incoming Call xxxxBps xxxxxx (L2TP, xxxxxx = Remote Call ID)
C01 Incoming Call xxxx (= connected speed) xxxxxx (= Remote Call ID)
L02 Tunnel Connected (L2TP)
C02 OutCall Connected xxxx (= connected speed) xxxxxx (= Remote Call ID)
C02 CLID call refused
L02 Call Terminated
C02 Call Terminated

Jul 19 11:19:27 192.168.102.2 ZYXEL: board 0 line 0 channel 0, call 1, C01 Outgoing
Call dev=2 ch=0 40002
Jul 19 11:19:32 192.168.102.2 ZYXEL: board 0 line 0 channel 0, call 1, C02 OutCall
Connected 64000 40002
Jul 19 11:20:06 192.168.102.2 ZYXEL: board 0 line 0 channel 0, call 1, C02 Call
Terminated

2 - Packet Triggered
SdcmdSyslogSend (SYSLOG_PKTTRI, SYSLOG_NOTICE, String);
String = Packet trigger: Protocol=xx Data=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=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e0000000600220008cd40000
020405b4
Jul 19 11:29:06 192.168.102.2 ZYXEL: Packet Trigger: Protocol=1,
Data=45000028240140001f06ac12c0a86614ca849a7b0427001700195b451d1430135004000077600000

3 - Filter Log
SdcmdSyslogSend (SYSLOG_FILLOG, SYSLOG_NOTICE, String);
String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx] S04>R01mD
IP[...] is the packet header and S04>R01mD means filter set 4 (S) and rule 1 (R), match
(m), drop (D).
Src: Source Address
Dst: Destination Address

```

**Figure 217** Syslog Example (continued)

```

prot: Protocol ("TCP", "UDP", "ICMP")
spo: Source port
dpo: Destination port
Jul 19 14:43:55 192.168.102.2 ZYXEL: IP [Src=202.132.154.123 Dst=255.255.255.255 UDP
spo=0208 dpo=0208]} S03>R01mF
Jul 19 14:44:00 192.168.102.2 ZYXEL: IP [Src=192.168.102.20 Dst=202.132.154.1 UDP
spo=05d4 dpo=0035]} S03>R01mF
Jul 19 14:44:04 192.168.102.2 ZYXEL: IP [Src=192.168.102.20 Dst=202.132.154.1 UDP
spo=05d4 dpo=0035]} S03>R01mF
4 - PPP Log
SdcmdSyslogSend (SYSLOG_PPPLOG, SYSLOG_NOTICE, String);
String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto
Shutdown
Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP / IPXCP
Jul 19 11:42:44 192.168.102.2 ZYXEL: ppp:LCP Closing
Jul 19 11:42:49 192.168.102.2 ZYXEL: ppp:IPCP Closing
Jul 19 11:42:54 192.168.102.2 ZYXEL: ppp:CCP Closing

```

## 36.5 Diagnostic

The diagnostic facility allows you to test the different aspects of your Prestige to determine if it is working properly. Menu 24.4 allows you to choose among various types of diagnostic tests to evaluate your system, as shown in the following figure.

Follow the procedure next to get to **Diagnostic**:

- 1** From the main menu, type 24 to open **Menu 24 – System Maintenance**.
- 2** From this menu, type 4. Diagnostic to open **Menu 24.4 – System Maintenance – Diagnostic**.

**Figure 218** Menu 24.4 System Maintenance : Diagnostic

```

Menu 24.4 - System Maintenance - Diagnostic

xDSL                               System
  1. Reset xDSL                     21. Reboot System
                                     22. Command Mode

TCP/IP
  12. Ping Host

Enter Menu Selection Number:

Host IP Address= N/A

```

The following table describes the diagnostic tests available in menu 24.4 for and the connections.

**Table 123** Menu 24.4 System Maintenance Menu: Diagnostic

<b>FIELD</b>	<b>DESCRIPTION</b>
Reset xDSL	Re-initialize the xDSL link to the telephone company.
Ping Host	Ping the host to see if the links and TCP/IP protocol on both systems are working.
Reboot System	Reboot the Prestige.
Command Mode	Type the mode to test and diagnose your Prestige using specified commands.
Host IP Address	If you typed 12 to Ping Host, now type the address of the computer you want to ping.





# CHAPTER 37

## 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.

### 37.1 Filename Conventions

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

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

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

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

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

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

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

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

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

**Table 124** 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

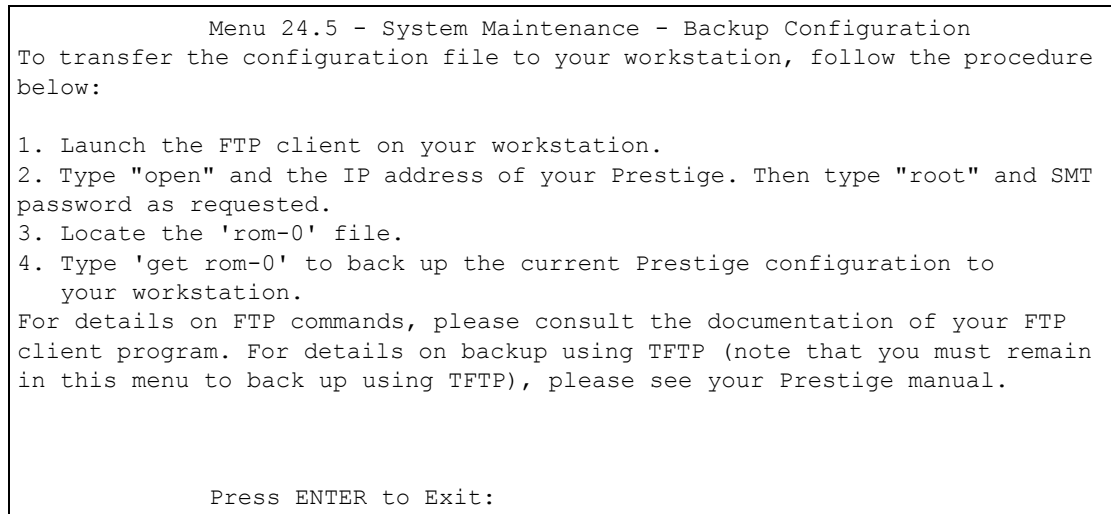
## 37.2 Backup Configuration

Option 5 from **Menu 24 – System Maintenance** allows you to backup the current Prestige configuration to your computer. Backup is highly recommended once your Prestige is functioning properly. FTP is the preferred methods for backing up your current configuration to your computer since they are faster. Any serial communications program should work fine; however, you must use Xmodem protocol to perform the download/upload and you don't have to rename the files.

Please note that terms “download” and “upload” are relative to the computer. Download means to transfer from the Prestige to the computer, while upload means from your computer to the Prestige.

### 37.2.1 Backup Configuration

Follow the instructions as shown in the next screen.

**Figure 219** Telnet in Menu 24.5

### 37.2.2 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.

### 37.2.3 Example of FTP Commands from the Command Line

**Figure 220** 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

```

### 37.2.4 GUI-based FTP Clients

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

**Table 125** General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

### 37.2.5 TFTP and FTP over WAN Management Limitations

TFTP, FTP and Telnet over WAN will not work when:

- You have disabled Telnet service in menu 24.11.
- You have applied a filter in menu 3.1 (LAN) or in menu 11.5 (WAN) to block Telnet service.
- The IP address in the **Secured Client IP** field in menu 24.11 does not match the client IP. If it does not match, the Prestige will disconnect the Telnet session immediately.
- You have an SMT console session running.

## 37.2.6 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.

## 37.2.7 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`.

## 37.2.8 GUI-based TFTP Clients

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

**Table 126** General Commands for GUI-based TFTP Clients

COMMAND	DESCRIPTION
Host	Enter the IP address of the Prestige. 192.168.1.1 is the Prestige's default IP address when shipped.
Send/Fetch	Use "Send" to upload the file to the Prestige and "Fetch" to back up the file on your computer.
Local File	Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer.
Remote File	This is the filename on the Prestige. The filename for the firmware is "ras" and for the configuration file, is "rom-0".
Binary	Transfer the file in binary mode.
Abort	Stop transfer of the file.

Refer to [Section 37.2.5 on page 368](#) to read about configurations that disallow TFTP and FTP over WAN.

### 37.2.9 Backup Via Console Port

Back up configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

- 1 Display menu 24.5 and enter "y" at the following screen.

**Figure 221** System Maintenance: Backup Configuration

```
Ready to backup Configuration via Xmodem.
Do you want to continue (y/n):
```

- 2 The following screen indicates that the Xmodem download has started.

**Figure 222** System Maintenance: Starting Xmodem Download Screen

```
You can enter ctrl-x to terminate operation any
time.
Starting XMODEM download...
```

- 3 Run the HyperTerminal program by clicking **Transfer**, then **Receive File** as shown in the following screen.

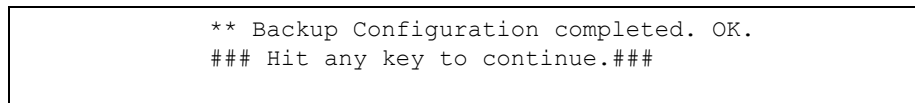
**Figure 223** Backup Configuration Example

Type a location for storing the configuration file or click **Browse** to look for one.

Choose the **Xmodem** protocol.

Then click **Receive**.

- 4 After a successful backup you will see the following screen. Press any key to return to the SMT menu.

**Figure 224** Successful Backup Confirmation Screen

## 37.3 Restore Configuration

This section shows you how to restore a previously saved configuration. Note that this function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

FTP is the preferred method for restoring your current computer configuration to your Prestige since FTP is faster. Please note that you must wait for the system to automatically restart after the file transfer is complete.

**Note:** Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR Prestige.

### 37.3.1 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 225** 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.

### 37.3.2 Restore Using FTP Session Example

**Figure 226** Restore Using FTP Session Example

```
ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
ftp>quit
```

Refer to [Section 37.2.5 on page 368](#) to read about configurations that disallow TFTP and FTP over WAN.



### 37.3.3 Restore Via Console Port

Restore configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

- 1 Display menu 24.6 and enter “y” at the following screen.

**Figure 227** System Maintenance: Restore Configuration

```
Ready to restore Configuration via Xmodem.
Do you want to continue (y/n):
```

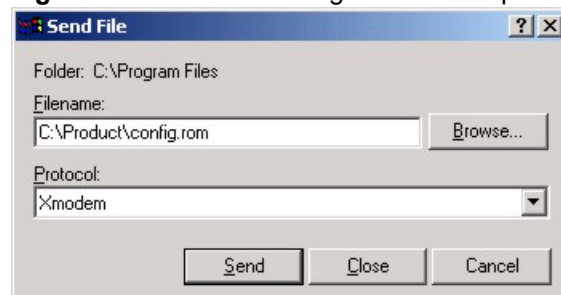
- 2 The following screen indicates that the Xmodem download has started.

**Figure 228** System Maintenance: Starting Xmodem Download Screen

```
Starting XMODEM download (CRC mode) ...CCCCCCCC
```

- 3 Run the HyperTerminal program by clicking **Transfer**, then **Send File** as shown in the following screen.

**Figure 229** Restore Configuration Example



Type the configuration file's location, or click **Browse** to search for it.

Choose the **Xmodem** protocol.

Then click **Send**.

- 4 After a successful restoration you will see the following screen. Press any key to restart the Prestige and return to the SMT menu.

**Figure 230** Successful Restoration Confirmation Screen

```
Save to ROM
Hit any key to start system reboot.
```

## 37.4 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 37.2 on page 366](#) or by following the instructions in **Menu 24.7.2 – System Maintenance – Upload System Configuration File**.

**Note:** Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR Prestige.

### 37.4.1 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 231** Telnet Into Menu 24.7.1 Upload System Firmware

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

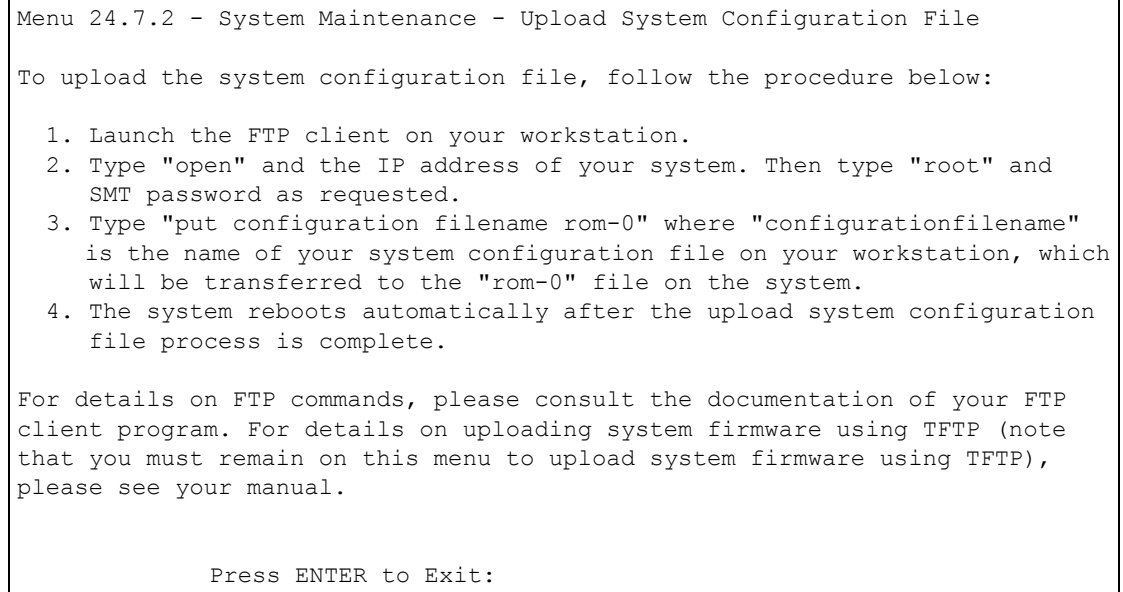
To upload the system firmware, follow the procedure below:
1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your workstation. Then type "root" and
   SMT password as requested.
3. Type "put firmware filename ras" where "firmwarefilename" is the name
   of your firmware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

### 37.4.2 Configuration File Upload

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

**Figure 232** Telnet Into Menu 24.7.2 System Maintenance

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

### 37.4.3 FTP File Upload Command from the DOS Prompt Example

- 1 Launch the FTP client on your computer.
- 2 Enter “open”, followed by a space and the IP address of your Prestige.
- 3 Press [ENTER] when prompted for a username.
- 4 Enter your password as requested (the default is “1234”).
- 5 Enter “bin” to set transfer mode to binary.
- 6 Use “put” to transfer files from the computer to the Prestige, for example, “put firmware.bin ras” transfers the firmware on your computer (firmware.bin) to the Prestige and renames it “ras”. Similarly, “put config.rom rom-0” transfers the configuration file on your computer (config.rom) to the Prestige and renames it “rom-0”. Likewise “get rom-0 config.rom” transfers the configuration file on the Prestige to your computer and renames it “config.rom.” See earlier in this chapter for more information on filename conventions.
- 7 Enter “quit” to exit the ftp prompt.

The Prestige automatically restarts after a successful file upload.

## 37.4.4 FTP Session Example of Firmware File Upload

**Figure 233** FTP Session Example of Firmware File Upload

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

More commands (found in GUI-based FTP clients) are listed earlier in this chapter.

Refer to [Section 37.2.5 on page 368](#) to read about configurations that disallow TFTP and FTP over WAN.

## 37.4.5 TFTP File Upload

The Prestige also supports the uploading of firmware files using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To transfer the firmware and the configuration file, follow the procedure shown next.

- 1 Use telnet from your computer to connect to the Prestige and log in. Because TFTP does not have any security checks, the Prestige records the IP address of the telnet client and accepts TFTP requests only from this address.
- 2 Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
- 3 Enter the command “`sys stdio 0`” to disable the console timeout, so the TFTP transfer will not be interrupted. Enter “`sys stdio 5`” to restore the five-minute console timeout (default) when the file transfer is complete.
- 4 Launch the TFTP client on your computer and connect to the Prestige. Set the transfer mode to binary before starting data transfer.
- 5 Use the TFTP client (see the example below) to transfer files between the Prestige and the computer. The file name for the firmware is “`ras`”.

Note that the telnet connection must be active and the Prestige in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use “`get`” to transfer from the Prestige to the computer, “`put`” the other way around, and “`binary`” to set binary transfer mode.

### 37.4.6 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.

### 37.4.7 Uploading Via Console Port

FTP or TFTP are the preferred methods for uploading firmware to your Prestige. However, in the event of your network being down, uploading files is only possible with a direct connection to your Prestige via the console port. Uploading files via the console port under normal conditions is not recommended since FTP or TFTP is faster. Any serial communications program should work fine; however, you must use the Xmodem protocol to perform the download/upload.

### 37.4.8 Uploading Firmware File Via Console Port

- 1 Select 1 from Menu 24.7 – System Maintenance – Upload Firmware to display Menu 24.7.1 - System Maintenance - Upload System Firmware, and then follow the instructions as shown in the following screen.

**Figure 234** Menu 24.7.1 As Seen Using the Console Port

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

To upload system firmware:
1. Enter "y" at the prompt below to go into debug mode.
2. Enter "atur" after "Enter Debug Mode" message.
3. Wait for "Starting XMODEM upload" message before activating
Xmodem upload on your terminal.
4. After successful firmware upload, enter "atgo" to restart
the router.

Warning: Proceeding with the upload will erase the current
system      firmware.

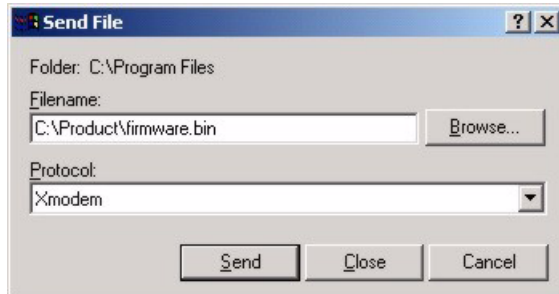
Do You Wish To Proceed: (Y/N)
```

- 2 After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

### 37.4.9 Example Xmodem Firmware Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

**Figure 235** Example Xmodem Upload



After the firmware upload process has completed, the Prestige will automatically restart.

### 37.4.10 Uploading Configuration File Via Console Port

- 1 Select 2 from Menu 24.7 – System Maintenance – Upload Firmware to display Menu 24.7.2 - System Maintenance - Upload System Configuration File. Follow the instructions as shown in the next screen.

**Figure 236** Menu 24.7.2 As Seen Using the Console Port

```

Menu 24.7.2 - System Maintenance - Upload System Configuration
File

To upload system configuration file:
1. Enter "y" at the prompt below to go into debug mode.
2. Enter "atlc" after "Enter Debug Mode" message.
3. Wait for "Starting XMODEM upload" message before activating
   Xmodem upload on your terminal.
4. After successful firmware upload, enter "atgo" to restart
   the system.

Warning:
1. Proceeding with the upload will erase the current
   configuration file.
2. The system's console port speed (Menu 24.2.2) may change
   when it is restarted; please adjust your terminal's speed
   accordingly. The password may change (menu 23), also.
3. When uploading the DEFAULT configuration file, the console
   port speed will be reset to 9600 bps and the password to
   "1234".

Do You Wish To Proceed: (Y/N)
  
```

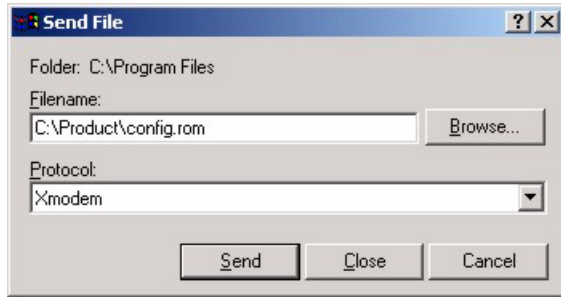
- 2 After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

3 Enter “atgo” to restart the Prestige.

### 37.4.11 Example Xmodem Configuration Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

**Figure 237** Example Xmodem Upload



After the configuration upload process has completed, restart the Prestige by entering “atgo”.





# CHAPTER 38

## System Maintenance

This chapter leads you through SMT menus 24.8 to 24.10.

### 38.1 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**. A list of valid commands can be found by typing `help` or `?` at the command prompt. Type “`exit`” to return to the SMT main menu when finished.

**Figure 238** Command Mode in Menu 24

```

Menu 24 - System Maintenance

1. System Status
2. System Information and Console Port Speed
3. Log and Trace
4. Diagnostic
5. Backup Configuration
6. Restore Configuration
7. Upload Firmware
8. Command Interpreter Mode
9. Call Control
10. Time and Date Setting
11. Remote Management

Enter Menu Selection Number:

```

**Figure 239** Valid Commands

```

Copyright (c) 1994 - 2005 ZyXEL Communications Corp.
ras> ?

Valid commands are:
sys          exit          device          ether
wan          poe           config         wlan
ip           ipsec          ppp           bridge
hdap        lan            radius         8021x
dsp         voice

```

## 38.2 Call Control Support

Call Control Support is only applicable when **Encapsulation** is set to **PPPoE** in menu 4 or menu 11.1.

The budget management function allows you to set a limit on the total outgoing call time of the Prestige within certain times. When the total outgoing call time exceeds the limit, the current call will be dropped and any future outgoing calls will be blocked.

To access the call control menu, select option 9 in menu 24 to go to **Menu 24.9 — System Maintenance — Call Control**, as shown in the next table.

**Figure 240** Menu 24.9 System Maintenance: Call Control

```

Menu 24.9 - System Maintenance - Call Control

1. Budget Management

Enter Menu Selection Number:
    
```

### 38.2.1 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 241** Menu 24.9.1 System Maintenance: Budget Management

```

Menu 24.9.1 - System Maintenance - Budget Management

Remote Node      Connection Time/Total Budget  Elapsed Time/Total Period
1.MyIsp          No Budget                     No Budget
2.-----
3.-----
4.-----
5.-----
6.-----
7.-----
8.-----

Reset Node (0 to update screen):
    
```

The total budget is the time limit on the accumulated time for outgoing calls to a remote node. When this limit is reached, the call will be dropped and further outgoing calls to that remote node will be blocked. After each period, the total budget is reset. The default for the total budget is 0 minutes and the period is 0 hours, meaning no budget control. You can reset the accumulated connection time in this menu by entering the index of a remote node. Enter 0 to update the screen. The budget and the reset period can be configured in menu 11.1 for the remote node when PPPoE encapsulation is selected.

**Table 127** Menu 24.9.1 System Maintenance: Budget Management

FIELD	DESCRIPTION
Remote Node	Enter the index number of the remote node you want to reset (just one in this case)
Connection Time/Total Budget	This is the total connection time that has gone by (within the allocated budget that you set in menu 11.1.
Elapsed Time/Total Period	The period is the time cycle in hours that the allocation budget is reset (see menu 11.1.) The elapsed time is the time used up within this period.
Enter "0" to update the screen or press [ESC] to return to the previous screen.	

### 38.3 Time and Date Setting

The Prestige keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server when you turn on your Prestige. Menu 24.10 allows you to update the time and date settings of your Prestige. The real time is then displayed in the Prestige error logs and firewall logs.

Select menu 24 in the main menu to open **Menu 24 System Maintenance**, as shown next.

**Figure 242** Menu 24 System Maintenance

Menu 24 - System Maintenance
<ol style="list-style-type: none"> <li>1. System Status</li> <li>2. System Information and Console Port Speed</li> <li>3. Log and Trace</li> <li>4. Diagnostic</li> <li>5. Backup Configuration</li> <li>6. Restore Configuration</li> <li>7. Upload Firmware</li> <li>8. Command Interpreter Mode</li> <li>9. Call Control</li> <li>10. Time and Date Setting</li> <li>11. Remote Management</li> </ol>
Enter Menu Selection Number:

Then enter 10 to go to **Menu 24.10 System Maintenance Time and Date Setting** to update the time and date settings of your Prestige as shown in the following screen.

**Figure 243** Menu 24.10 System Maintenance: Time and Date Setting

```

Menu 24.10 - System Maintenance - Time and Date Setting
Use Time Server when Bootup= None
Time Server Address= N/A
Current Time:                00 : 51 : 24
New Time (hh:mm:ss):        00 : 51 : 19
Current Date:                2000 - 01 - 01
New Date (yyyy-mm-dd):      2000 - 01 - 01
Time Zone= GMT
Daylight Saving= No
Start Date (mm-dd):         01 - 00
End Date (mm-dd):           01 - 00

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

**Table 128** Menu 24.10 System Maintenance: Time and Date Setting

FIELD	DESCRIPTION
Use Time Server when Bootup	Enter the time service protocol that your time server sends when you turn on the Prestige. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main differences between them are the format. <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. <b>NTP (RFC-1305)</b> is similar to <b>Time (RFC-868)</b> . <b>None.</b> The default, enter the time manually.
Time Server Address	Enter the IP address or domain name of your time server. Check with your ISP/network administrator if you are unsure of this information.
Current Time	This field displays an updated time only when you reenter this menu.
New Time	Enter the new time in hour, minute and second format.
Current Date	This field displays an updated date only when you re-enter this menu.
New Date	Enter the new date in year, month and day format.
Time Zone	Press [SPACE BAR] and then [ENTER] to set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Saving	If you use daylight savings time, then choose <b>Yes</b> .
Start Date	If using daylight savings time, enter the month and day that it starts on.
End Date	If using daylight savings time, enter the month and day that it ends on
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm or ESC to Cancel:" to save your configuration, or press [ESC] at any time to cancel.	

### 38.3.1 Resetting the Time

- The Prestige resets the time in three instances:
- On leaving menu 24.10 after making changes.
- When the Prestige starts up, if there is a timeserver configured in menu 24.10.

- 24-hour intervals after starting.



# CHAPTER 39

## Remote Management

This chapter covers remote management (SMT menu 24.11).

### 39.1 Remote Management Overview

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

When you configure remote management to allow management from the WAN, you still need to configure a firewall rule to allow access. See the firewall chapters for details on configuring firewall rules.

### 39.2 Remote Management

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

Enter 11 from menu 24 to display **Menu 24.11 — Remote Management Control**.

#### 39.2.1 Remote Management Setup

You may manage your Prestige from a remote location via:

the Internet (**WAN only**), the **LAN only**, **All** (LAN and WAN) or **Disable** (neither).

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

If you enable remote management of a service, but have applied a filter to block the service, then you will not be able to remotely manage the Prestige using the service.

Enter 11, from menu 24, to display **Menu 24.11 — Remote Management Control** (shown next).

**Figure 244** Menu 24.11 Remote Management Control

```

Menu 24.11 - Remote Management Control

TELNET Server:
  Server Port = 23                Server Access = LAN only
  Secured Client IP = 0.0.0.0
FTP Server:
  Server Port = 21                Server Access = LAN only
  Secured Client IP = 0.0.0.0
Web Server:
  Server Port = 80                Server Access = LAN only
  Secured Client IP = 0.0.0.0

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

The following table describes the fields in this menu.

**Table 129** Menu 24.11 Remote Management Control

FIELD	DESCRIPTION
Telnet Server FTP Server Web Server	Each of these read-only labels denotes a service or protocol.
Port	This field shows the port number for the service or protocol. You may change the port number if needed, but you must use the same port number to access the Prestige.
Access	Select the access interface (if any) by pressing the [SPACE BAR]. Choices are: <b>LAN only</b> , <b>WAN only</b> , <b>All</b> or <b>Disable</b> . The default is <b>LAN only</b> .
Secured Client IP	The default 0.0.0.0 allows any client to use this service or protocol to access the Prestige. Enter an IP address to restrict access to a client with a matching IP address.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm or ESC to Cancel:" to save your configuration, or press [ESC] at any time to cancel.	

### 39.2.2 Remote Management Limitations

Remote management over LAN or WAN will not work when:

- A filter in menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
- You have disabled that service in menu 24.11.
- The IP address in the **Secured Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the Prestige will disconnect the session immediately.
- There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.
- There is a firewall rule that blocks it.



## 39.3 Remote Management and NAT

When NAT is enabled:

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

## 39.4 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The Prestige automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when it is continuously updating the status in menu 24.1 or when `sys stdio` has been changed on the command line.



# CHAPTER 40

## IP Policy Routing

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

### 40.1 IP Policy Routing Overview

Traditionally, routing is based on the destination address only and the IAD takes the shortest path to forward a packet. IP Routing Policy (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing.

### 40.2 Benefits of IP Policy Routing

**Source-Based Routing** – Network administrators can use policy-based routing to direct traffic from different users through different connections.

**Quality of Service (QoS)** – Organizations can differentiate traffic by setting the precedence or TOS (Type of Service) values in the IP header at the periphery of the network to enable the backbone to prioritize traffic.

**Cost Savings** – IPPR allows organizations to distribute interactive traffic on high-bandwidth, high-cost paths while using low-cost paths for batch traffic.

**Load Sharing** – Network administrators can use IPPR to distribute traffic among multiple paths.

### 40.3 Routing Policy

Individual routing policies are used as part of the overall IPPR process. A policy defines the matching criteria and the action to take when a packet meets the criteria. The action is taken only when all the criteria are met. The criteria includes the source address and port, IP protocol (ICMP, UDP, TCP, etc.), destination address and port, TOS and precedence (fields in the IP header) and length. The inclusion of length criterion is to differentiate between interactive and bulk traffic. Interactive applications, for example, telnet, tend to have short packets, while bulk traffic, for example, file transfer, tends to have large packets.

The actions that can be taken include:

- routing the packet to a different gateway (and hence the outgoing interface).
- setting the TOS and precedence fields in the IP header.

IPPR follows the existing packet filtering facility of RAS in style and in implementation. The policies are divided into sets, where related policies are grouped together. A user defines the policies before applying them to an interface or a remote node, in the same fashion as the filters. There are 12 policy sets with six policies in each set.

## 40.4 IP Routing Policy Setup

Menu 25 shows all the policies defined.

**Figure 245** Menu 25 IP Routing Policy Setup

```

Menu 25 - IP Routing Policy Setup

Policy          Policy
Set #          Name          Set #          Name
-----
 1      _____      7      _____
 2      _____      8      _____
 3      _____      9      _____
 4      _____     10     _____
 5      _____     11     _____
 6      _____     12     _____

Enter Policy Set Number to Configure= 0

Edit Name= N/A

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

To setup a routing policy, perform the following procedures:

- 1** Type 25 in the main menu to open **Menu 25 – IP Routing Policy Setup**.
- 2** Type the index of the policy set you want to configure to open **Menu 25.1 – IP Routing Policy Setup**.

Menu 25.1 shows the summary of a policy set, including the criteria and the action of a single policy, and whether a policy is active or not. Each policy contains two lines. The former part is the criteria of the incoming packet and the latter is the action. Between these two parts, separator “|” means the action is taken on criteria matched and separator “=” means the action is taken on criteria not matched.

**Figure 246** Menu 25.1 IP Routing Policy Setup

```

Menu 25.1 - IP Routing Policy Setup

# A                Criteria/Action
- - - - -
1 Y SA=1.1.1.1-1.1.1.1,DA=2.2.2.2-2.2.2.5
   SP=20-25,DP=20-25,P=6,T=NM,PR=0          |GW=192.168.1.1,T=MT,PR=0
2 N _____
3 N _____
4 N _____
5 N _____
6 N _____

Enter Policy Rule Number (1-6) to Configure:
    
```

**Table 130** Menu 25.1 IP Routing Policy Setup

ABBREVIATION		MEANING
<b>Criterion</b>	SA	Source IP Address
	SP	Source Port
	DA	Destination IP Address
	DP	Destination Port
	P	IP layer 4 protocol number (TCP=6, UDP=17...)
	T	Type of service of incoming packet
	PR	Precedence of incoming packet
<b>Action</b>	GW	Gateway IP address
	T	Outgoing Type of service
	P	Outgoing Precedence
<b>Service</b>	NM	Normal
	MD	Minimum Delay
	MT	Maximum Throughput
	MR	Maximum Reliability
	MC	Minimum Cost

Type a number from 1 to 6 to display **Menu 25.1.1 – IP Routing Policy** (see the next figure). This menu allows you to configure a policy rule.

**Figure 247** Menu 25.1.1 IP Routing Policy

```

Menu 25.1.1 - IP Routing Policy

Policy Set Name= test
Active= No
Criteria:
  IP Protocol      = 0
  Type of Service= Don't Care      Packet length= 0
  Precedence      = Don't Care      Len Comp= N/A
Source:
  addr start= 0.0.0.0              end= N/A
  port start= N/A                  end= N/A
Destination:
  addr start= 0.0.0.0              end= N/A
  port start= N/A                  end= N/A
Action= Matched
Gateway addr      = 0.0.0.0        Log= No
Type of Service= No Change
Precedence       = No Change

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

The following table describes the fields in this menu.

**Table 131** Menu 25.1.1 IP Routing Policy

FIELD	DESCRIPTION
Policy Set Name	This is the policy set name assigned in <b>Menu 25 – IP Routing Policy Setup</b> .
Active	Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> to activate or <b>No</b> to deactivate the policy. Inactive policies are displayed with a minus sign “-“ in SMT menu 25.
Criteria	
IP Protocol	IP layer 4 protocol, for example, <b>UDP, TCP, ICMP</b> , etc.
Type of Service	Prioritize incoming network traffic by choosing from <b>Don't Care, Normal, Min Delay, Max Thruput, Min Cost</b> or <b>Max Reliable</b> .
Precedence	Precedence value of the incoming packet. Press [SPACE BAR] and then [ENTER] to select a value from <b>0 to 7</b> or <b>Don't Care</b> .
Packet Length	Type the length of incoming packets (in bytes). The operators in the <b>Len Comp</b> (next field) apply to packets of this length.
Len Comp	Press [SPACE BAR] and then [ENTER] to choose from <b>Equal, Not Equal, Less, Greater, Less or Equal</b> or <b>Greater or Equal</b> .
Source:	
addr start / end	Source IP address range from start to end.
port start / end	Source port number range from start to end; applicable only for TCP/UDP.
Destination:	
addr start / end	Destination IP address range from start to end.
port start / end	Destination port number range from start to end; applicable only for TCP/UDP.
Action	Specifies whether action should be taken on criteria <b>Matched</b> or <b>Not Matched</b> .

**Table 131** Menu 25.1.1 IP Routing Policy (continued)

FIELD	DESCRIPTION
Gateway addr	Defines the outgoing gateway address. The gateway must be on the same subnet as the Prestige if it is on the LAN, otherwise, the gateway must be the IP address of a remote node. The default gateway is specified as 0.0.0.0.
Type of Service	Set the new TOS value of the outgoing packet. Prioritize incoming network traffic by choosing <b>No Change</b> , <b>Normal</b> , <b>Min Delay</b> , <b>Max Thruput</b> , <b>Max Reliable</b> or <b>Min Cost</b> .
Precedence	Set the new outgoing packet precedence value. Values are <b>0</b> to <b>7</b> or <b>No Change</b> .
Log	Press [SPACE BAR] and then [ENTER] to select <b>Yes</b> to make an entry in the system log when a policy is executed.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm or ESC to Cancel:" to save your configuration, or press [ESC] at any time to cancel.	

## 40.5 Applying an IP Policy

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

### 40.5.1 Ethernet IP Policies

From **Menu 3 — Ethernet Setup**, type 2 to go to **Menu 3.2 — TCP/IP and DHCP Ethernet Setup**.

You can choose up to four IP policy sets (from 12) by typing their numbers separated by commas, for example, 2, 4, 7, 9.

**Figure 248** Menu 3.2 TCP/IP and DHCP Ethernet Setup

```

Menu 3.2 - TCP/IP and DHCP Setup
  DHCP Setup
    DHCP= Server
    Client IP Pool Starting Address= 192.168.1.33
    Size of Client IP Pool= 32
    Primary DNS Server= 0.0.0.0
    Secondary DNS Server= 0.0.0.0
    Remote DHCP Server= N/A
  TCP/IP Setup:
    IP Address= 192.168.1.1
    IP Subnet Mask= 255.255.255.0
    RIP Direction= Both
      Version= RIP-1
    Multicast= None
    IP Policies=
    Edit IP Alias= No
  Press ENTER to Confirm or ESC to Cancel:

```

Go to menu 11.3 (shown next) and type the number(s) of the IP Routing Policy set(s) as appropriate. You can cascade up to four policy sets by typing their numbers separated by commas.

**Figure 249** Menu 11.3 Remote Node Network Layer Options

```

Menu 11.3 - Remote Node Network Layer Options

IP Options:
  IP Address Assignment= Static
  Rem IP Addr: 0.0.0.0
  Rem Subnet Mask= 0.0.0.0
  My WAN Addr= 0.0.0.0
  NAT= Full Feature
    Address Mapping Set= 2
  Metric= 2
  Private= No
  RIP Direction= Both
    Version= RIP-2B
  Multicast= IGMP-v2
  IP Policies=

Bridge Options:
  Ethernet Addr Timeout (min)= 0

Press ENTER to Confirm or ESC to Cancel:

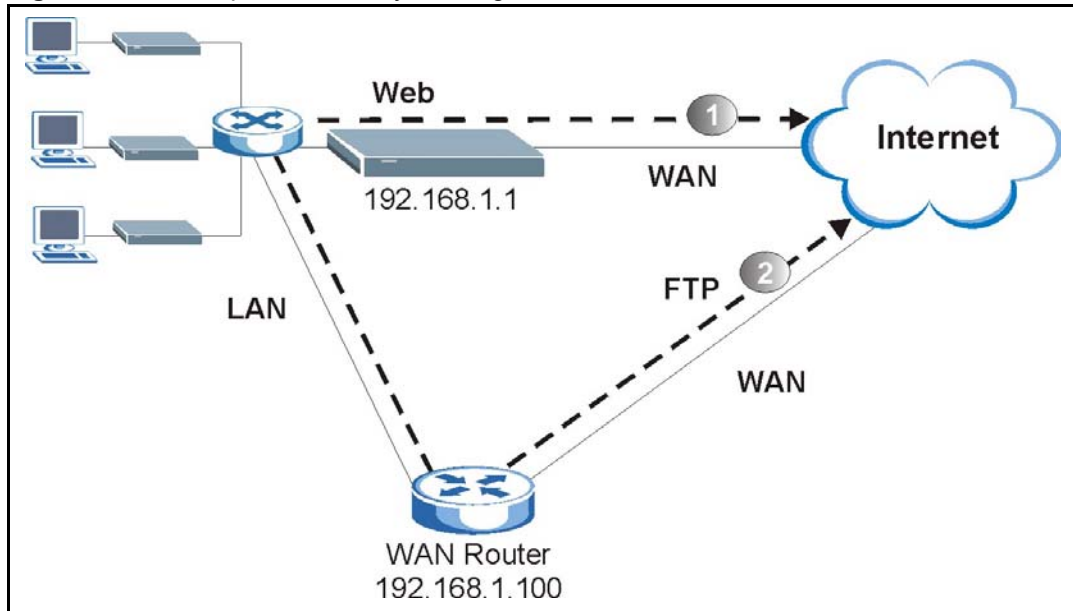
```

## 40.6 IP Policy Routing Example

If a network has both Internet and remote node connections, you can route Web packets to the Internet using one policy and route FTP packets to a remote network using another policy. See the next figure.

Route 1 represents the default IP route and route 2 represents the configured IP route.



**Figure 250** Example of IP Policy Routing

To force packets coming from clients with IP addresses of 192.168.1.33 to 192.168.1.64 to be routed to the Internet via the WAN port of the Prestige, follow the steps as shown next.

- 1 Create a routing policy set in menu 25.
- 2 Create a rule for this set in **Menu 25.1.1 — IP Routing Policy** as shown next.

**Figure 251** IP Routing Policy Example

```

Menu 25.1.1 - IP Routing Policy

Policy Set Name= set1                Packet length= 10
Active= Yes                          Len Comp= N/A
Criteria:
  IP Protocol      = 6                end= 192.168.1.64
  Type of Service = Don't Care        end= N/A
  Precedence      = Don't Care        end= N/A
  Source:
    addr start= 192.168.1.2          end= 80
    port start= 0                    Log= No
  Destination:
    addr start= 0.0.0.0
    port start= 80
Action= Matched
Gateway addr  = 192.168.1.1
  Type of Service= No Change
  Precedence   = No Change

Press ENTER to Confirm or ESC to Cancel:

```

- 1 Check **Menu 25.1 — IP Routing Policy Setup** to see if the rule is added correctly.
- 2 Create another policy set in menu 25.

- 3 Create a rule in menu 25.1 for this set to route packets from any host (IP=0.0.0.0 means any host) with protocol TCP and port FTP access through another gateway (192.168.1.100).

**Figure 252** IP Routing Policy Example

```

Menu 25.1.1 - IP Routing Policy

Policy Set Name= set2                Packet length= 10
Active= Yes                          Len Comp= N/A
Criteria:
  IP Protocol      = 6                end= N/A
  Type of Service= Don't Care         end= N/A
  Precedence      = Don't Care         end= N/A
  Source:
    addr start= 0.0.0.0              Log= No
  port start= 0
  Destination:
    addr start= 0.0.0.0
    port start= 20
  Action= Matched
Gateway addr =192.168.1.100
  Type of Service= No Change
  Precedence    = No Change

Press ENTER to Confirm or ESC to Cancel:

```

- 4 Check **Menu 25.1 — IP Routing Policy Setup** to see if the rule is added correctly.

- 5 Apply both policy sets in menu 3.2 as shown next.

**Figure 253** Applying IP Policies Example

```

Menu 3.2 - TCP/IP and DHCP Ethernet Setup

DHCP Setup
  DHCP= Server
  Client IP Pool Starting Address= 192.168.1.33
  Size of Client IP Pool= 64
  Primary DNS Server= 0.0.0.0
  Secondary DNS Server= 0.0.0.0
  Remote DHCP Server= N/A
TCP/IP Setup:
  IP Address= 192.168.1.1
  IP Subnet Mask= 255.255.255.0
  RIP Direction= Both
    Version= RIP-1
  Multicast= None
  IP Policies= 1,2
  Edit IP Alias= No

Press ENTER to Confirm or ESC to Cancel:

```

# CHAPTER 41

## Call Scheduling

Call scheduling (applicable for PPPoA or PPPoE encapsulation only) allows you to dictate when a remote node should be called and for how long.

### 41.1 Introduction

The call scheduling feature allows the Prestige to manage a remote node and dictate when a remote node should be called and for how long. This feature is similar to the scheduler in a videocassette recorder (you can specify a time period for the VCR to record). You can apply up to 4 schedule sets in **Menu 11.1 — Remote Node Profile**. From the main menu, enter 26 to access **Menu 26 — Schedule Setup** as shown next.

**Figure 254** 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 are applied in the remote node then set 1 will take precedence over set 2, 3 and 4 as the Prestige, by default, applies the lowest numbered set first. Set 2 will take precedence over set 3 and 4, and so on.

You can design up to 12 schedule sets but you can only apply up to four schedule sets for a remote node.

To delete a schedule set, enter the set number and press **[SPACE BAR]** and then **[ENTER]** (or delete) in the **Edit Name** field.

To setup a schedule set, select the schedule set you want to setup from menu 26 (1-12) and press [ENTER] to see **Menu 26.1 — Schedule Set Setup** as shown next.

**Figure 255** 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 132** 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.

**Table 132** Menu 26.1 Schedule Set Setup (continued)

FIELD	DESCRIPTION
Action	<p><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.</p> <p><b>Forced Down</b> means that the connection is blocked whether or not there is a demand call on the line.</p> <p><b>Enable Dial-On-Demand</b> means that this schedule permits a demand call on the line.</p> <p><b>Disable Dial-On-Demand</b> means that this schedule prevents a demand call on the line.</p>
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm or ESC to Cancel:" to save your configuration, or press [ESC] at any time to cancel.	

Once your schedule sets are configured, you must then apply them to the desired remote node(s). Enter 11 from the **Main Menu** and then enter the target remote node index. Using [SPACE BAR], select **PPPoE** or **PPPoA** in the **Encapsulation** field and then press [ENTER] to make the schedule sets field available as shown next.

**Figure 256** Applying Schedule Set(s) to a Remote Node (PPPoE)

```

Menu 11.1 - Remote Node Profile
Rem Node Name= MyISP           Route= IP
Active= Yes                    Bridge= No
Encapsulation= PPPoA          Edit IP/Bridge= No
Multiplexing= LLC-based       Edit ATM Options= No
Service Name= N/A            Edit Advance Options= N/A
Incoming:                     Telco Option:
  Rem Login=                  Allocated Budget(min)= 0
  Rem Password= *****      Period(hr)= 0
Outgoing:                     Schedule Sets=
  My Login= ChangeMe         Nailed-Up Connection= No
  My Password= *****      Session Options:
  Authen= CHAP/PAP           Edit Filter Sets= No
                              Idle Timeout(sec)= 0
                              Press ENTER to Confirm or ESC to Cancel:

```

You can apply up to four schedule sets, separated by commas, for one remote node. Change the schedule set numbers to your preference(s).



# CHAPTER 42

## VPN/IPSec Setup

This chapter introduces the VPN SMT menus.

### 42.1 VPN/IPSec Overview

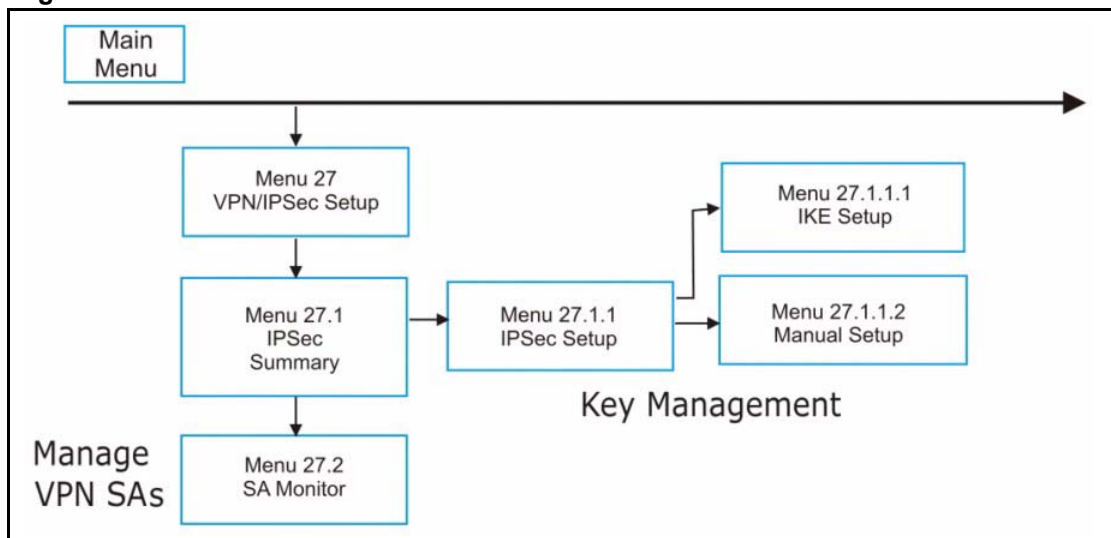
The VPN/IPSec main SMT menu has these main submenus:

Define VPN policies in menu 27.1 submenus, including security policies, endpoint IP addresses, peer IPSec router IP address and key management.

**Menu 27.2 - SA Monitor** allows you to manage (refresh or disconnect) your SA connections.

This is an overview of the VPN menu tree.

**Figure 257** VPN SMT Menu Tree



From the main menu, enter 27 to display the first VPN menu (shown next).

**Figure 258** Menu 27 VPN/IPSec Setup

```

Menu 27 - VPN/IPSec Setup

      1. IPSec Summary
      2. SA Monitor

Enter Menu Selection Number:
    
```

## 42.2 IPSec Summary Screen

Type 1 in menu 27 and then press [ENTER] to display **Menu 27.1 IPSec Summary**. This is a summary read-only menu of your IPSec rules (tunnels). Edit or create an IPSec rule by selecting an index number and then configuring the associated submenus.

**Figure 259** Menu 27.1 IPSec Summary

```

Menu 27.1 - IPSec Summary

#   Name      A   Local Addr Start   -   Addr End / Mask   Encap   IPSec Algorithm
   Key Mgt    Remote Addr Start -   Addr End / Mask   Secure GW Addr
-----
001 Taiwan     Y   192.168.1.35       192.168.1.38      Tunnel  ESP AES MD5
    IKE       172.16.2.40       172.16.2.46       193.81.13.2
002 zw50       N   1.1.1.1            1.1.1.1           Tunnel  AH SHA1
    IKE       4.4.4.4           255.255.0.0       zw50test.zyxel.
003 China     N   192.168.1.40       192.168.1.42      Tunnel  ESP DES MD5
    IKE       N/A               N/A               0.0.0.0
004
005

Select Command= None           Select Rule= N/A
Press ENTER to Confirm or ESC to Cancel:
    
```

**Table 133** Menu 27.1 IPSec Summary

FIELD	DESCRIPTION
#	This is the VPN policy index number.
Name	This field displays the unique identification name for this VPN rule. The name may be up to 32 characters long but only 10 characters will be displayed here.



**Table 133** Menu 27.1 IPSec Summary (continued)

FIELD	DESCRIPTION
A	Y signifies that this VPN rule is active.
Local Addr Start	When the <b>Addr Type</b> field in <b>Menu 27.1.1 IPSec Setup</b> is configured to <b>Single</b> , this is a static IP address on the LAN behind your Prestige. When the <b>Addr Type</b> field in <b>Menu 27.1.1 IPSec Setup</b> is configured to <b>Range</b> , this is the beginning (static) IP address, in a range of computers on the LAN behind your Prestige. When the <b>Addr Type</b> field in <b>Menu 27.1.1 IPSec Setup</b> is configured to <b>SUBNET</b> , this is a static IP address on the LAN behind your Prestige.
Addr End / Mask	When the <b>Addr Type</b> field in <b>Menu 27.1.1 IPSec Setup</b> is configured to <b>Single</b> , this is the same (static) IP address as in the <b>Local Addr Start</b> field. When the <b>Addr Type</b> field in <b>Menu 27.1.1 IPSec Setup</b> is configured to <b>Range</b> , this is the end (static) IP address, in a range of computers on the LAN behind your Prestige. When the <b>Addr Type</b> field in <b>Menu 27.1.1 IPSec Setup</b> is configured to <b>SUBNET</b> , this is a subnet mask on the LAN behind your Prestige.
Encap	This field displays <b>Tunnel</b> mode or <b>Transport</b> mode. See earlier for a discussion of these. You need to finish configuring the VPN policy in menu 27.1.1.1 or 27.1.1.2 if <b>???</b> is displayed.
IPSec Algorithm	This field displays the security protocols used for an SA. <b>ESP</b> provides confidentiality and integrity of data by encrypting the data and encapsulating it into IP packets. Encryption methods include 56-bit <b>DES</b> and 168-bit <b>3DES</b> . <b>NULL</b> denotes a tunnel without encryption. 168-bit <b>3DES</b> and 128-bit <b>AES</b> . <b>NULL</b> denotes a tunnel without encryption. <b>AH</b> (Authentication Header) provides strong integrity and authentication by adding authentication information to IP packets. This authentication information is calculated using header and payload data in the IP packet. This provides an additional level of security. <b>AH</b> choices are <b>MD5</b> (default - 128 bits) and <b>SHA -1</b> (160 bits). Both <b>AH</b> and <b>ESP</b> increase the Prestige's processing requirements and communications latency (delay). You need to finish configuring the VPN policy in menu 27.1.1.1 or 27.1.1.2 if <b>???</b> is displayed.
Key Mgt	This field displays the SA's type of key management, ( <b>IKE</b> or <b>Manual</b> ).
Remote Addr Start	When the <b>Addr Type</b> field in <b>Menu 27.1.1 IPSec Setup</b> is configured to <b>Single</b> , this is a static IP address on the network behind the remote IPSec router. When the <b>Addr Type</b> field in <b>Menu 27.1.1 IPSec Setup</b> is configured to <b>Range</b> , this is the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router. When the <b>Addr Type</b> field in <b>Menu 27.1.1 IPSec Setup</b> is configured to <b>SUBNET</b> , this is a static IP address on the network behind the remote IPSec router. This field displays <b>N/A</b> when you configure the <b>Secure Gateway Address</b> field in SMT 27.1.1 to 0.0.0.0.
Addr End / Mask	When the <b>Addr Type</b> field in <b>Menu 27.1.1 IPSec Setup</b> is configured to <b>Single</b> , this is the same (static) IP address as in the <b>Remote Addr Start</b> field. When the <b>Addr Type</b> field in <b>Menu 27.1.1 IPSec Setup</b> is configured to <b>Range</b> , this is the end (static) IP address, in a range of computers on the network behind the remote IPSec router. When the <b>Addr Type</b> field in <b>Menu 27.1.1 IPSec Setup</b> is configured to <b>SUBNET</b> , this is a subnet mask on the network behind the remote IPSec router. This field displays <b>N/A</b> when you configure the <b>Secure Gateway Address</b> field in SMT 27.1.1 to 0.0.0.0.

**Table 133** Menu 27.1 IPSec Summary (continued)

FIELD	DESCRIPTION
Secure GW Addr	This is the WAN IP address or the domain name (up to the first 15 characters are displayed) of the IPSec router with which you are making the VPN connection. This field displays <b>0.0.0.0</b> when you configure the <b>Secure Gateway Address</b> field in SMT 27.1.1 to 0.0.0.0.
Select Command	Press [SPACE BAR] to choose from <b>None</b> , <b>Edit</b> , <b>Delete</b> , <b>Go To Rule</b> , <b>Next Page</b> or <b>Previous Page</b> and then press [ENTER]. You must select a rule in the next field when you choose the <b>Edit</b> , <b>Delete</b> or <b>Go To</b> commands. Select <b>None</b> and then press [ENTER] to go to the "Press ENTER to Confirm..." prompt. Use <b>Edit</b> to create or edit a rule. Use <b>Delete</b> to remove a rule. To edit or delete a rule, first make sure you are on the correct page. When a VPN rule is deleted, subsequent rules do <u>not</u> move up in the page list. Use <b>Go To Rule</b> to view the page where your desired rule is listed. Select <b>Next Page</b> or <b>Previous Page</b> to view the next or previous page of rules (respectively).
Select Rule	Type the VPN rule index number you wish to edit or delete and then press [ENTER].
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm or ESC to Cancel:" to save your configuration, or press [ESC] at any time to cancel.	

## 42.3 IPSec Setup

Select **Edit** in the **Select Command** field; type the index number of a rule in the **Select Rule** field and press [ENTER] to edit the VPN using the menu shown next.

**Note:** You must also configure menu 27.1.1.1 or menu 27.1.1.2 to fully configure and use a VPN.

**Figure 260** Menu 27.1.1 IPSec Setup

```

Menu 27.1.1 - IPSec Setup

Index= 1          Name= Taiwan
Active= Yes      Keep Alive= No    Nat Traversal= No
Local ID type= IP          Content:
My IP Addr= 0.0.0.0
Peer ID type= IP          Content:
Secure Gateway Address= zw50test.zyxel.com.tw
Protocol= 0        DNS Server= 0.0.0.0
Local:            Addr Type= SINGLE
                  IP Addr Start= 1.1.1.1          End/Subnet Mask= N/A
                  Port Start= 0                   End= N/A
Remote:          Addr Type= SUBNET
                  IP Addr Start= 4.4.4.4          End/Subnet Mask= 255.255.0.0
                  Port Start= 0                   End= N/A
Enable Replay Detection = No
Key Management= IKE
Edit Key Management Setup= No

Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the fields in this menu.

**Table 134** Menu 27.1.1 IPSec Setup

FIELD	DESCRIPTION
Index	This is the VPN rule index number you selected in the previous menu.
Name	Enter a unique identification name for this VPN rule. The name may be up to 32 characters long but only 10 characters will be displayed in <b>Menu 27.1 - IPSec Summary</b> .
Active	Press [SPACE BAR] to choose either <b>Yes</b> or <b>No</b> . Choose <b>Yes</b> and press [ENTER] to activate the VPN tunnel. This field determines whether a VPN rule is applied before a packet leaves the firewall.
Keep Alive	Press [SPACE BAR] to choose either <b>Yes</b> or <b>No</b> . Choose <b>Yes</b> and press [ENTER] to have the Prestige automatically re-initiate the SA after the SA lifetime times out, even if there is no traffic. The remote IPSec router must also have keep alive enabled in order for this feature to work.

**Table 134** Menu 27.1.1 IPSec Setup (continued)

FIELD	DESCRIPTION
Nat Traversal	<p>Press [SPACE BAR] to choose either <b>Yes</b> or <b>No</b>. Choose <b>Yes</b> and press [ENTER] to enable NAT traversal. NAT traversal allows you to set up a VPN connection when there are NAT routers between the two IPSec routers.</p> <p>The remote IPSec router must also have NAT traversal enabled. You can use NAT traversal with <b>ESP</b> protocol using <b>Transport</b> or <b>Tunnel</b> mode, but not with <b>AH</b> protocol nor with <b>Manual</b> key management.</p> <p>In order for an IPSec router behind a NAT router to receive an initiating IPSec packet, set the NAT router to forward UDP port 500 to the IPSec router behind the NAT router.</p>
Local ID type	<p>Press [SPACE BAR] to choose <b>IP</b>, <b>DNS</b>, or <b>E-mail</b> and press [ENTER].</p> <p>Select <b>IP</b> to identify this Prestige by its IP address.</p> <p>Select <b>DNS</b> to identify this Prestige by a domain name.</p> <p>Select <b>E-mail</b> to identify this Prestige by an e-mail address.</p>
Content	<p>When you select <b>IP</b> in the <b>Local ID Type</b> field, type the IP address of your computer or leave the field blank to have the Prestige automatically use its own IP address.</p> <p>When you select <b>DNS</b> in the <b>Local ID Type</b> field, type a domain name (up to 31 characters) by which to identify this Prestige.</p> <p>When you select <b>E-mail</b> in the <b>Local ID Type</b> field, type an e-mail address (up to 31 characters) by which to identify this Prestige.</p> <p>The domain name or e-mail address that you use in the <b>Content</b> field is used for identification purposes only and does not need to be a real domain name or e-mail address.</p>
My IP Addr	<p>Enter the IP address of your Prestige. The Prestige uses its current WAN IP address (static or dynamic) in setting up the VPN tunnel if you leave this field as 0.0.0.0.</p> <p>The VPN tunnel has to be rebuilt if this IP address changes.</p>
Peer ID type	<p>Press [SPACE BAR] to choose <b>IP</b>, <b>DNS</b>, or <b>E-mail</b> and press [ENTER].</p> <p>Select <b>IP</b> to identify the remote IPSec router by its IP address.</p> <p>Select <b>DNS</b> to identify the remote IPSec router by a domain name.</p> <p>Select <b>E-mail</b> to identify the remote IPSec router by an e-mail address.</p>
Content	<p>When you select <b>IP</b> in the <b>Peer ID Type</b> field, type the IP address of the computer with which you will make the VPN connection or leave the field blank to have the Prestige automatically use the address in the <b>Secure Gateway Address</b> field.</p> <p>When you select <b>DNS</b> in the <b>Peer ID Type</b> field, type a domain name (up to 31 characters) by which to identify the remote IPSec router.</p> <p>When you select <b>E-mail</b> in the <b>Peer ID Type</b> field, type an e-mail address (up to 31 characters) by which to identify the remote IPSec router.</p> <p>The domain name or e-mail address that you use in the <b>Content</b> field is used for identification purposes only and does not need to be a real domain name or e-mail address. The domain name also does not have to match the remote router's IP address or what you configure in the <b>Secure Gateway Address</b> field below.</p>
Secure Gateway Address	<p>Type the IP address or the domain name (up to 31 characters) of the IPSec router with which you're making the VPN connection.</p> <p>Set this field to 0.0.0.0 if the remote IPSec router has a dynamic WAN IP address (the <b>Key Management</b> field must be set to <b>IKE</b>, see later).</p>
Protocol	<p>Enter 1 for ICMP, 6 for TCP, 17 for UDP, etc. 0 is the default and signifies any protocol.</p>

**Table 134** Menu 27.1.1 IPsec Setup (continued)

FIELD	DESCRIPTION
DNS Server	<p>If there is a private DNS server that services the VPN, type its IP address here. The Prestige assigns this additional DNS server to the Prestige's DHCP clients that have IP addresses in this IPsec rule's range of local addresses.</p> <p>A DNS server allows clients on the VPN to find other computers and servers on the VPN by their (private) domain names.</p>
Local	<p>Local IP addresses must be static and correspond to the remote IPsec router's configured remote IP addresses.</p> <p>Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.</p>
Addr Type	<p>Press [SPACE BAR] to choose <b>SINGLE</b>, <b>RANGE</b>, or <b>SUBNET</b> and press [ENTER]. Select <b>SINGLE</b> with a single IP address. Select <b>RANGE</b> for a specific range of IP addresses. Select <b>SUBNET</b> to specify IP addresses on a network by their subnet mask.</p>
IP Addr Start	<p>When the <b>Addr Type</b> field is configured to <b>Single</b>, enter a static IP address on the LAN behind your Prestige.</p> <p>When the <b>Addr Type</b> field is configured to <b>Range</b>, enter the beginning (static) IP address, in a range of computers on your LAN behind your Prestige.</p> <p>When the <b>Addr Type</b> is configured to <b>SUBNET</b>, this is a (static) IP address on the LAN behind your Prestige.</p>
End/Subnet Mask	<p>When the <b>Addr Type</b> field is configured to <b>Single</b>, this field is <b>N/A</b>.</p> <p>When the <b>Addr Type</b> field is configured to <b>Range</b>, enter the end (static) IP address, in a range of computers on the LAN behind your Prestige.</p> <p>When the <b>Addr Type</b> field is configured to <b>SUBNET</b>, this is a subnet mask on the LAN behind your Prestige.</p>
Port Start	<p>0 is the default and signifies any port. Type a port number from 0 to 65535. You cannot create a VPN tunnel if you try to connect using a port number that does not match this port number or range of port numbers.</p> <p>Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3</p>
End	<p>Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. This field is <b>N/A</b> when 0 is configured in the <b>Port Start</b> field.</p>
Remote	<p>Remote IP addresses must be static and correspond to the remote IPsec router's configured local IP addresses. The remote fields are <b>N/A</b> when the <b>Secure Gateway Address</b> field is configured to 0.0.0.0.</p> <p>Two active SAs cannot have the local and remote IP address(es) both the same. Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.</p>
Addr Type	<p>Press [SPACE BAR] to choose <b>SINGLE</b>, <b>RANGE</b>, or <b>SUBNET</b> and press [ENTER]. Select <b>SINGLE</b> with a single IP address. Use <b>RANGE</b> for a specific range of IP addresses. Use <b>SUBNET</b> to specify IP addresses on a network by their subnet mask.</p>

**Table 134** Menu 27.1.1 IPSec Setup (continued)

FIELD	DESCRIPTION
IP Addr Start	<p>When the <b>Addr Type</b> field is configured to <b>Single</b>, enter a static IP address on the network behind the remote IPSec router.</p> <p>When the <b>Addr Type</b> field is configured to <b>Range</b>, enter the beginning (static) IP address, in a range of computers on the network behind the remote IPSec router.</p> <p>When the <b>Addr Type</b> field is configured to <b>SUBNET</b>, enter a static IP address on the network behind the remote IPSec router.</p> <p>This field displays <b>N/A</b> when you configure the <b>Secure Gateway Address</b> field to 0.0.0.0.</p>
End/Subnet Mask	<p>When the <b>Addr Type</b> field is configured to <b>Single</b>, this field is <b>N/A</b>.</p> <p>When the <b>Addr Type</b> field is configured to <b>Range</b>, enter the end (static) IP address, in a range of computers on the network behind the remote IPSec router.</p> <p>When the <b>Addr Type</b> field is configured to <b>SUBNET</b>, enter a subnet mask on the network behind the remote IPSec router.</p> <p>This field displays <b>N/A</b> when you configure the <b>Secure Gateway Address</b> field to 0.0.0.0.</p>
Port Start	<p>0 is the default and signifies any port. Type a port number from 0 to 65535. Someone behind the remote IPSec router cannot create a VPN tunnel when attempting to connect using a port number that does not match this port number or range of port numbers.</p> <p>Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.</p>
End	<p>Enter a port number in this field to define a port range. This port number must be greater than that specified in the previous field. This field is <b>N/A</b> when 0 is configured in the <b>Port Start</b> field.</p>
Enable Replay Detection	<p>As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DoS) attacks. The IPSec receiver can detect and reject old or duplicate packets to protect against replay attacks. Enable replay detection by setting this field to <b>Yes</b>. Press [SPACE BAR] to select <b>Yes</b> or <b>No</b>. Choose <b>Yes</b> and press [ENTER] to enable replay detection.</p>
Key Management	<p>Press [SPACE BAR] to choose either <b>IKE</b> or <b>Manual</b> and then press [ENTER]. <b>Manual</b> is useful for troubleshooting if you have problems using <b>IKE</b> key management.</p>
Edit Key Management Setup	<p>Press [SPACE BAR] to change the default <b>No</b> to <b>Yes</b> and then press [ENTER] to go to a key management menu for configuring your key management setup (described later). If you set the <b>Key Management</b> field to <b>IKE</b>, this will take you to <b>Menu 27.1.1.1 – IKE Setup</b>. If you set the <b>Key Management</b> field to <b>Manual</b>, this will take you to <b>Menu 27.1.1.2 – Manual Setup</b>.</p>
<p>When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm or ESC to Cancel:" to save your configuration, or press [ESC] at any time to cancel.</p>	

## 42.4 IKE Setup

To edit this menu, the **Key Management** field in **Menu 27.1.1 – IPSec Setup** must be set to **IKE**. Move the cursor to the **Edit Key Management Setup** field in **Menu 27.1.1 – IPSec Setup**; press [SPACE BAR] to select **Yes** and then press [ENTER] to display **Menu 27.1.1.1 – IKE Setup**.

**Figure 261** Menu 27.1.1.1 IKE Setup

```

Menu 27.1.1.1 - IKE Setup
Phase 1
Negotiation Mode= Main
PSK=
Encryption Algorithm = AES
Authentication Algorithm = SHA1
SA Life Time (Seconds)= 28800
Key Group= DH1
Phase 2
Active Protocol = ESP
Encryption Algorithm = AES
Authentication Algorithm = MD5
SA Life Time (Seconds)= 28800
Encapsulation = Tunnel
Perfect Forward Secrecy (PFS)= None
Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the fields in this menu.

**Table 135** Menu 27.1.1.1 IKE Setup

FIELD	DESCRIPTION
Phase 1	
Negotiation Mode	Press [SPACE BAR] to choose from <b>Main</b> or <b>Aggressive</b> and then press [ENTER]. See earlier for a discussion of these modes. Multiple SAs connecting through a secure gateway must have the same negotiation mode.
PSK	Prestige gateways authenticate an IKE VPN session by matching pre-shared keys. Pre-shared keys are best for small networks with fewer than ten nodes. Enter your pre-shared key here. Enter up to 31 characters. Any character may be used, including spaces, but trailing spaces are truncated.  Both ends of the VPN tunnel must use the same pre-shared key. You will receive a "PYLD_MALFORMED" (payload malformed) packet if the same pre-shared key is not used on both ends.
Encryption Algorithm	The Prestige and the remote IPsec router generate an encryption key from the Diffie-Hellman key exchange. Prestige <b>DES</b> encryption algorithm uses a 56-bit key. Triple DES ( <b>3DES</b> ), is a variation on DES that uses a 168-bit key. As a result, <b>3DES</b> is more secure than <b>DES</b> . It also requires more processing power, resulting in slightly increased latency and decreased throughput.  This implementation of <b>AES</b> uses a 128-bit key. <b>AES</b> is faster than <b>3DES</b> . Press [SPACE BAR] to choose from <b>DES</b> , <b>3DES</b> or <b>AES</b> and then press [ENTER].
Authentication Algorithm	<b>MD5</b> (Message Digest 5) and <b>SHA1</b> (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The <b>SHA1</b> algorithm is generally considered stronger than <b>MD5</b> , but is slightly slower.  Press [SPACE BAR] to choose from <b>SHA1</b> or <b>MD5</b> and then press [ENTER].
SA Life Time (Seconds)	Define the length of time before an IKE Security Association automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days).  A short <b>SA Life Time</b> increases security by forcing the two VPN gateways to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.

**Table 135** Menu 27.1.1.1 IKE Setup (continued)

FIELD	DESCRIPTION
Key Group	You must choose a key group for phase 1 IKE setup. <b>DH1</b> (default) refers to Diffie-Hellman Group 1 a 768 bit random number. <b>DH2</b> refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number.
Phase 2	
Active Protocol	Press [SPACE BAR] to choose from <b>ESP</b> or <b>AH</b> and then press [ENTER]. See earlier for a discussion of these protocols.
Encryption Algorithm	Press [SPACE BAR] to choose from <b>NULL</b> , <b>DES</b> , <b>3DES</b> or <b>AES</b> and then press [ENTER]. Select <b>NULL</b> to set up a tunnel without encryption.
Authentication Algorithm	Press [SPACE BAR] to choose from <b>SHA1</b> or <b>MD5</b> and then press [ENTER].
SA Life Time (Seconds)	Define the length of time before an IPSec Security Association automatically renegotiates in this field. It may range from 60 to 3,000,000 seconds (almost 35 days).
Encapsulation	Press [SPACE BAR] to choose from <b>Tunnel</b> mode or <b>Transport</b> mode and then press [ENTER]. See earlier for a discussion of these.
Perfect Forward Secrecy (PFS)	Perfect Forward Secrecy (PFS) is disabled ( <b>None</b> ) by default in phase 2 IPSec SA setup. This allows faster IPSec setup, but is not so secure. Press [SPACE BAR] and choose from <b>DH1</b> or <b>DH2</b> to enable PFS. <b>DH1</b> refers to Diffie-Hellman Group 1 a 768 bit random number. <b>DH2</b> refers to Diffie-Hellman Group 2 a 1024 bit (1Kb) random number (more secure, yet slower).
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm or ESC to Cancel:" to save your configuration, or press [ESC] at any time to cancel.	

## 42.5 Manual Setup

You only configure **Menu 27.1.1.2 – Manual Setup** when you select **Manual** in the **Key Management** field in **Menu 27.1.1 – IPSec Setup**. Manual key management is useful if you have problems with **IKE** key management.

### 42.5.1 Active Protocol

This field is a combination of mode and security protocols used for the VPN. See the Web Configurator part on VPN for more information on these parameters.

**Table 136** Active Protocol: Encapsulation and Security Protocol

MODE	SECURITY PROTOCOL
Tunnel	ESP
Transport	AH

### 42.5.2 Security Parameter Index (SPI)

To edit this menu, move the cursor to the **Edit Manual Setup** field in **Menu 27.1.1 – IPSec Setup** press [SPACE BAR] to select **Yes** and then press [ENTER] to go to **Menu 27.1.1.2 – Manual Setup**.



**Figure 262** Menu 27.1.1.2 Manual Setup

```

Menu 27.1.1.2 - Manual Setup

Active Protocol= ESP Tunnel
ESP Setup
  SPI (Decimal)= 0
  Encryption Algorithm= DES
  Key1= ?
  Key2= N/A
  Key3= N/A
  Authentication Algorithm= MD5
  Key= ?

AH Setup
  SPI (Decimal)= N/A
  Authentication Algorithm= N/A
  Key= N/A

Press ENTER to Confirm or ESC to Cancel:

```

The following table describes the fields in this menu.

**Table 137** Menu 27.1.1.2 Manual Setup

FIELD	DESCRIPTION
Active Protocol	Press [SPACE BAR] to choose from <b>ESP Tunnel</b> , <b>ESP Transport</b> , <b>AH Tunnel</b> or <b>AH Transport</b> and then press [ENTER]. Choosing an <b>ESP</b> combination causes the <b>AH Setup</b> fields to be non-applicable ( <b>N/A</b> )
ESP Setup	The <b>ESP Setup</b> fields are <b>N/A</b> if you chose an <b>AH Active Protocol</b> .
SPI (Decimal)	The <b>SPI</b> must be unique and from one to four integers ("0" to "9").
Encryption Algorithm	Press [SPACE BAR] to choose from <b>NULL</b> , <b>DES</b> , <b>3DES</b> or <b>AES</b> and then press [ENTER]. Fill in the <b>Key1</b> field below when you choose <b>DES</b> and fill in fields <b>Key1</b> to <b>Key3</b> when you choose <b>3DES</b> . Select <b>NULL</b> to set up a tunnel without encryption. When you select <b>NULL</b> , you do not enter any encryption keys.
Key1	Enter a unique eight-character key. Any character may be used, including spaces, but trailing spaces are truncated. Fill in the <b>Key1</b> field when you choose <b>DES</b> and fill in fields <b>Key1</b> to <b>Key3</b> when you choose <b>3DES</b> .
Key2	Enter a unique eight-character key. It can be comprised of any character including spaces (but trailing spaces are truncated).
Key3	Enter a unique eight-character key. It can be comprised of any character including spaces (but trailing spaces are truncated).
Authentication Algorithm	Press [SPACE BAR] to choose from <b>MD5</b> or <b>SHA1</b> and then press [ENTER].
Key	Enter the authentication key to be used by IPSec if applicable. The key must be unique. Enter 16 characters for <b>MD5</b> authentication and 20 characters for <b>SHA-1</b> authentication. Any character may be used, including spaces, but trailing spaces are truncated.
AH Setup	The <b>AH Setup</b> fields are <b>N/A</b> if you chose an <b>ESP Active Protocol</b> .
SPI (Decimal)	The <b>SPI</b> must be from one to four unique decimal characters ("0" to "9") long.

**Table 137** Menu 27.1.1.2 Manual Setup (continued)

FIELD	DESCRIPTION
Authentication Algorithm	Press [SPACE BAR] to choose from <b>MD5</b> or <b>SHA1</b> and then press [ENTER].
Key	Enter the authentication key to be used by IPsec if applicable. The key must be unique. Enter 16 characters for <b>MD5</b> authentication and 20 characters for <b>SHA-1</b> authentication. Any character may be used, including spaces, but trailing spaces are truncated.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm or ESC to Cancel:" to save your configuration, or press [ESC] at any time to cancel.	

# CHAPTER 43

## SA Monitor

This chapter teaches you how to manage your SAs by using the SA Monitor in SMT menu 27.2.

### 43.1 SA Monitor Overview

A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This menu (shown next) displays active VPN connections.

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

### 43.2 Using SA Monitor

Use the **Refresh** function to display active VPN connections.

Use the **Disconnect** function to cut off active connections.

Type 2 in **Menu 27 - VPN/IPSec Setup**, and then press [ENTER] to go to **Menu 27.2 - SA Monitor**.

**Figure 263** Menu 27.2 SA Monitor

```

Menu 27.2 - SA Monitor

#      Name                               Encap.      IPSec ALgorithm
---      -----
001    Taiwan : 3.3.3.1 - 3.3.3.3.100      Tunnel      ESP DES MD5
002
003
004
005
006
007
008
009
010

Select Command= Refresh
Select Connection= N/A
Press ENTER to Confirm or ESC to Cancel:
    
```

The following table describes the fields in this menu.

**Table 138** Menu 27.2 SA Monitor

FIELD	DESCRIPTION
#	This is the security association index number.
Name	This field displays the identification name for this VPN policy. This name is unique for each connection where the secure gateway IP address is a public static IP address. When the secure gateway IP address is 0.0.0.0 (as discussed in the last chapter), there may be different connections using this same VPN rule. In this case, the name is followed by the remote IP address as configured in <b>Menu 27.1.1. – IPSec Setup</b> . Individual connections using the same VPN rule may be terminated without affecting other connections using the same rule.
Encap.	This field displays <b>Tunnel</b> mode or <b>Transport</b> mode. See previous for discussion.
IPSec Algorithm	This field displays the security protocols used for an SA. <b>ESP</b> provides confidentiality and integrity of data by encrypting the data and encapsulating it into IP packets. Encryption methods include 56-bit <b>DES</b> and 168-bit <b>3DES</b> . <b>NULL</b> denotes a tunnel without encryption.  An incoming SA may have an <b>AH</b> in addition to <b>ESP</b> . The Authentication Header provides strong integrity and authentication by adding authentication information to IP packets. This authentication information is calculated using header and payload data in the IP packet. This provides an additional level of security. <b>AH</b> choices are <b>MD5</b> (default - 128 bits) and <b>SHA -1</b> (160 bits).  Both <b>AH</b> and <b>ESP</b> increase Prestige processing requirements and communications latency (delay).

**Table 138** Menu 27.2 SA Monitor (continued)

FIELD	DESCRIPTION
Select Command	Press [SPACE BAR] to choose from <b>Refresh</b> , <b>Disconnect</b> , <b>None</b> , <b>Next Page</b> , or <b>Previous Page</b> and then press [ENTER]. You must select a connection in the next field when you choose the <b>Disconnect</b> command. <b>Refresh</b> displays current active VPN connections. <b>None</b> allows you to jump to the "Press ENTER to Confirm..." prompt. Select <b>Next Page</b> or <b>Previous Page</b> to view the next or previous page of rules (respectively).
Select Connection	Type the VPN connection index number that you want to disconnect and then press [ENTER].
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm or ESC to Cancel:" to save your configuration, or press [ESC] at any time to cancel.	



# CHAPTER 44

## Troubleshooting

This chapter covers potential problems and the corresponding remedies.

### 44.1 Problems Starting Up the Prestige

**Table 139** Troubleshooting the Start-Up of Your Prestige

PROBLEM	CORRECTIVE ACTION
None of the LEDs turn on when I turn on the Prestige.	<p>Make sure that the Prestige's power adaptor is connected to the Prestige and plugged in to an appropriate power source. Check that the Prestige and the power source are both turned on.</p> <p>Turn the Prestige off and on.</p> <p>If the error persists, you may have a hardware problem. In this case, you should contact your vendor.</p>

### 44.2 Problems with the LAN LED

**Table 140** Troubleshooting the LAN LED

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

## 44.3 Problems with the DSL LED

**Table 141** Troubleshooting the DSL LED

PROBLEM	CORRECTIVE ACTION
The DSL LED is off.	Check the telephone wire and connections between the Prestige DSL port and the wall jack.
	Make sure that the telephone company has checked your phone line and set it up for DSL service.
	Reset your ADSL line to reinitialize your link to the DSLAM. For details, refer to <a href="#">Chapter 21 on page 253</a> (web configurator) or <a href="#">Chapter 36 on page 355</a> (SMT).

## 44.4 Problems with the LAN Interface

**Table 142** Troubleshooting the LAN Interface

PROBLEM	CORRECTIVE ACTION
I cannot access the Prestige from the LAN.	If the 10M/100M LEDs on the front panel are both off, refer to . Make sure that the IP address and the subnet mask of the Prestige and your computer(s) are on the same subnet.
I cannot ping any computer on the LAN.	If the 10M/100M LEDs on the front panel are both off, refer to . Make sure that the IP address and the subnet mask of the Prestige and the computers are on the same subnet.

## 44.5 Problems with the WAN Interface

**Table 143** Troubleshooting the WAN Interface

PROBLEM	CORRECTIVE ACTION
I cannot get a WAN IP address from the ISP.	The ISP provides the WAN IP address after authenticating you. Authentication may be through the user name and password, the MAC address or the host name.  The username and password apply to PPPoE and PPPoA encapsulation only. Make sure that you have entered the correct <b>Service Type</b> , <b>User Name</b> and <b>Password</b> (be sure to use the correct casing). Refer to <a href="#">Chapter 7 on page 109</a> (web configurator) or <a href="#">Chapter 27 on page 289</a> (SMT).



## 44.6 Problems with Internet Access

**Table 144** Troubleshooting Internet Access

PROBLEM	CORRECTIVE ACTION
I cannot access the Internet.	<p>Make sure the Prestige is turned on and connected to the network.</p> <p>If the DSL LED is off, refer to .</p> <p>Verify your WAN settings. Refer to the chapter on WAN setup (web configurator) or the section on Internet Access (SMT).</p> <p>Make sure you entered the correct user name and password.</p> <p>If you use PPPoE pass through, make sure that bridge is turned on. See <a href="#">Chapter 23 on page 273</a> for details.</p> <p>For wireless stations, check that both the Prestige and wireless station(s) are using the same ESSID, channel, WEP keys (if WEP encryption is activated) and authentication method.</p>
Internet connection disconnects.	<p>Check the schedule rules. Refer to <a href="#">Chapter 41 on page 399</a> (SMT).</p> <p>If you use PPPoA or PPPoE encapsulation, check the idle time-out setting. Refer to <a href="#">Chapter 7 on page 109</a> (web configurator) or <a href="#">Chapter 28 on page 295</a> (SMT).</p> <p>Contact your ISP.</p>

## 44.7 Problems with the Password

**Table 145** Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
I cannot access the Prestige.	<p>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.</p> <p>If you have changed the password and have now forgotten it, you will need to upload the default configuration file (Refer to <a href="#">Section 2.1.2 on page 58</a>). This restores all of the factory defaults including the password.</p>

## 44.8 Problems with the Web Configurator

**Table 146** Troubleshooting the Web Configurator

PROBLEM	CORRECTIVE ACTION
I cannot access the web configurator.	<p>Refer to .</p> <p>Make sure that there is not an SMT console session running.</p> <p>Check that you have enabled web service access. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on remote management for details.</p> <p>For WAN access, you must configure remote management to allow server access from the Wan (or all). You must also configure a firewall rule to allow access from the WAN. Refer to the chapters on remote management and firewall for details.</p> <p>Your computer's and the Prestige's IP addresses must be on the same subnet for LAN access.</p> <p>If you changed the Prestige's LAN IP address, then enter the new one as the URL.</p> <p>Remove any filters in SMT menu 3.1 (LAN) or menu 11.5 (WAN) that block web service.</p> <p>See also <a href="#">Section 44.9 on page 422</a>.</p>

## 44.9 Problems with Remote Management

**Table 147** Troubleshooting Remote Management

PROBLEM	CORRECTIVE ACTION
I cannot remotely manage the Prestige from the LAN or WAN.	Refer to <a href="#">Section 18.1.1 on page 229</a> for scenarios when remote management may not be possible.
	Use the Prestige's WAN IP address when configuring from the WAN. Use the Prestige's LAN IP address when configuring from the LAN.
	Refer to for instructions on checking your LAN connection.
	Refer to <a href="#">Section 44.4 on page 420</a> for instructions on checking your WAN connection.
	See also <a href="#">Section 44.8 on page 422</a> .

## 44.10 Telephone Problems

**Table 148** Troubleshooting Telephone

PROBLEM	CORRECTIVE ACTION
The telephone port won't work or the telephone lacks a dial tone.	Check the telephone connections and telephone wire. Make sure you have the <b>Voice SIP Settings</b> screen properly configured.
I cannot call from one of the Prestige's phone ports to the other phone port.	You cannot call the SIP number of the SIP account that you are using to make a call. The Prestige generates a busy tone and does not attempt to establish a call if the SIP number you dial matches the outgoing SIP number of the phone port you are using. For example, if you set <b>Phone 1</b> to use SIP account 1 and set <b>Phone 2</b> to use SIP account 2, then you can use <b>Phone 1</b> to call to SIP account 2's SIP number or <b>Phone 2</b> to call to SIP account 1's SIP number.

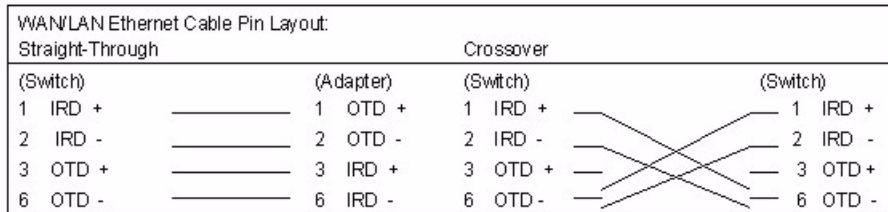


# APPENDIX A

## Hardware Specifications

### Ethernet Cable Pin Assignments

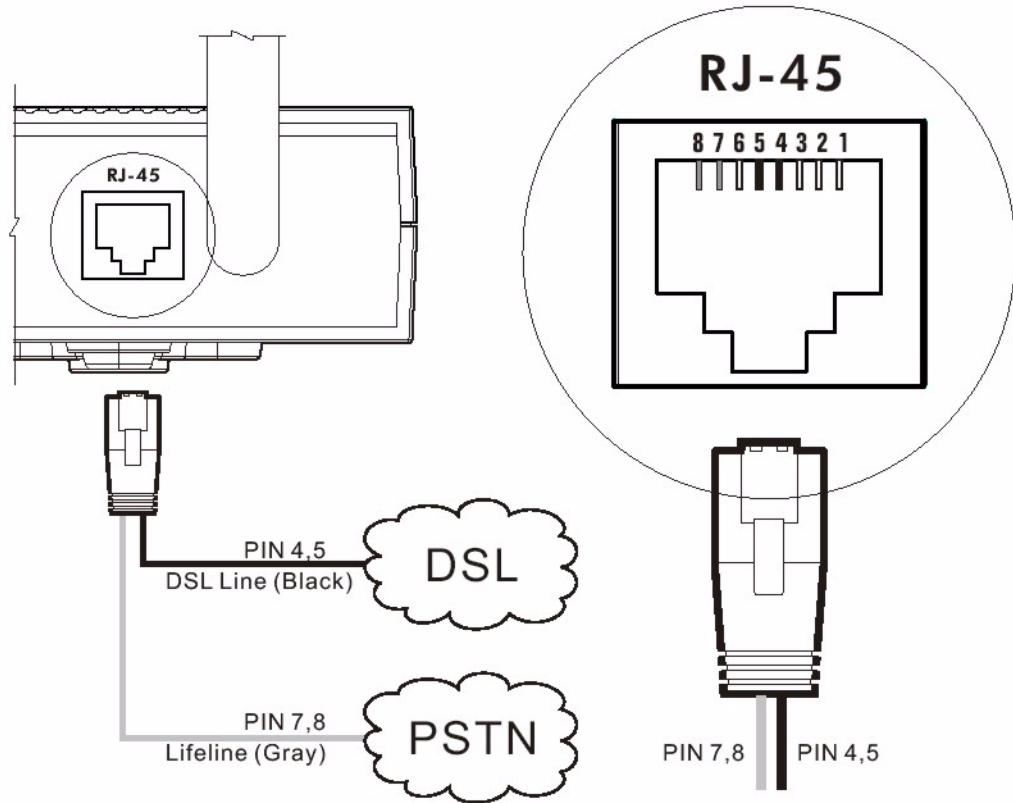
**Figure 264** Ethernet Cable Pin Assignments



### Prestige 2602HW-L DSL Port Pin Assignments

The following figure describes the pin assignments for the **DSL** port on the Prestige 2602HW-L

**Figure 265** Prestige 2602HW-L DSL Port Pin Assignments



## Prestige 2602HW Series Power Adaptor Specifications

**Table 149** Prestige 2602HW Series Power Adaptor Specifications

<b>NORTH AMERICAN PLUG STANDARDS</b>	
AC Power Adapter Model	ADS6818-1818-W 1810
Input Power	AC 100~240Volts/50/60Hz/0.5A
Output Power	DC 18Volts/1A
Power Consumption	15W
Safety Standards	UL, CUL(UL 1950)
<b>EUROPEAN PLUG STANDARDS</b>	
AC Power Adapter Model	ADS6818-1818-B 1810
Input Power	AC 100~240Volts/50/60Hz/0.5A
Output Power	DC 18Volts/1A
Power Consumption	15W
Safety Standards	TUV, CE(EN 60950)
<b>UNITED KINGDOM PLUG STANDARDS</b>	
AC Power Adapter Model	ADS6818-1818-D 1810
Input Power	AC 100~240Volts/50/60Hz/0.5A
Output Power	DC 18Volts/1A
Power Consumption	15W
Safety Standards	TUV, CE(EN 60950)





# APPENDIX B

## Setting up Your Computer's IP Address

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

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

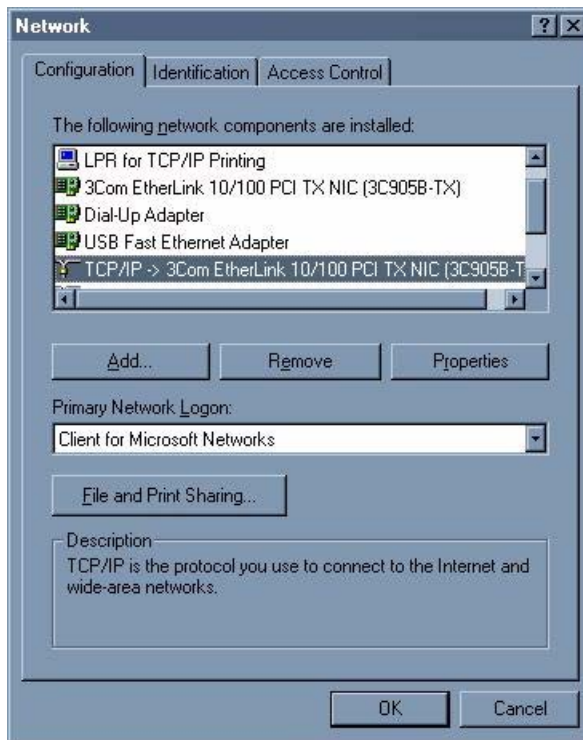
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

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

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

### Windows 95/98/Me

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

**Figure 266** 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:

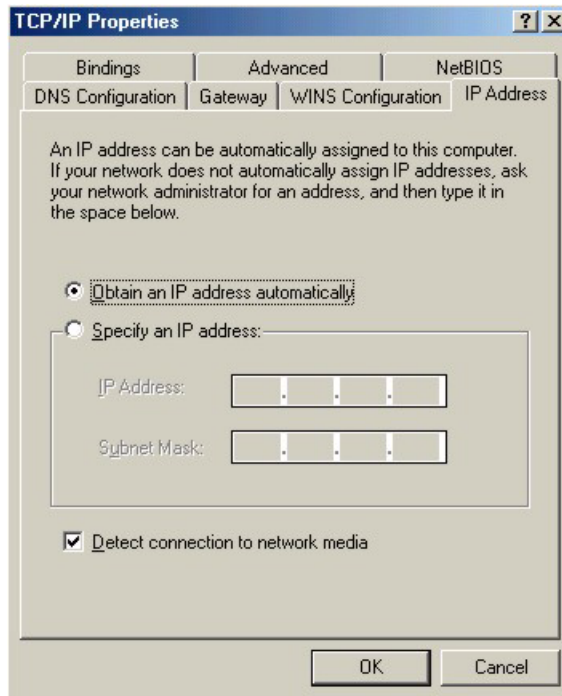
- 1 Click **Add**.
- 2 Select **Client** and then click **Add**.

- 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

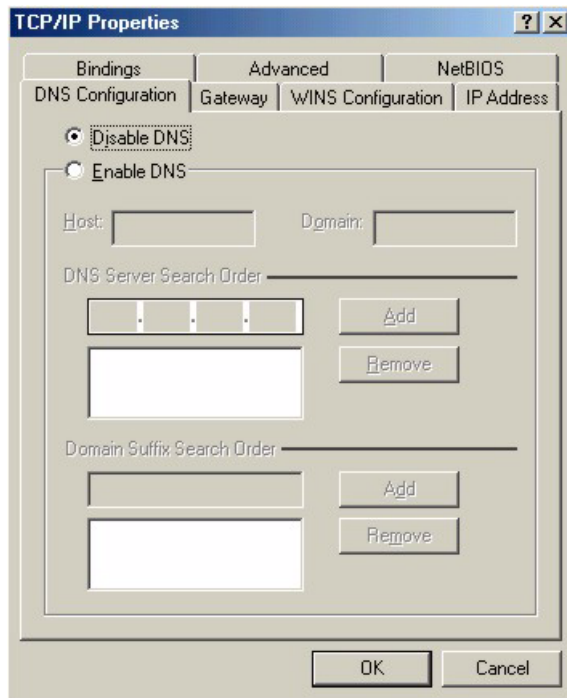
- 1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**
- 2 Click the **IP Address** tab.
  - If your IP address is dynamic, select **Obtain an IP address automatically**.
  - If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

**Figure 267** 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 268** Windows 95/98/Me: TCP/IP Properties: DNS Configuration



**4** Click the **Gateway** tab.

- If you do not know your gateway's IP address, remove previously installed gateways.
- If you have a gateway IP address, type it in the **New gateway field** and click **Add**.

**5** Click **OK** to save and close the **TCP/IP Properties** window.

**6** Click **OK** to close the **Network** window. Insert the Windows CD if prompted.

**7** Turn on your Prestige and restart your computer when prompted.

## Verifying Settings

**1** Click **Start** and then **Run**.

**2** In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.

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

## Windows 2000/NT/XP

**1** For Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.

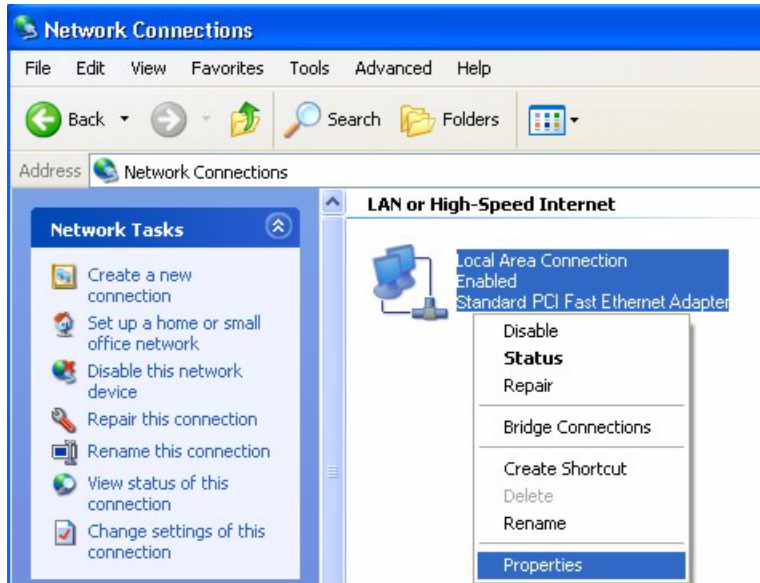
**Figure 269** Windows XP: Start Menu

**2** For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.

**Figure 270** Windows XP: Control Panel

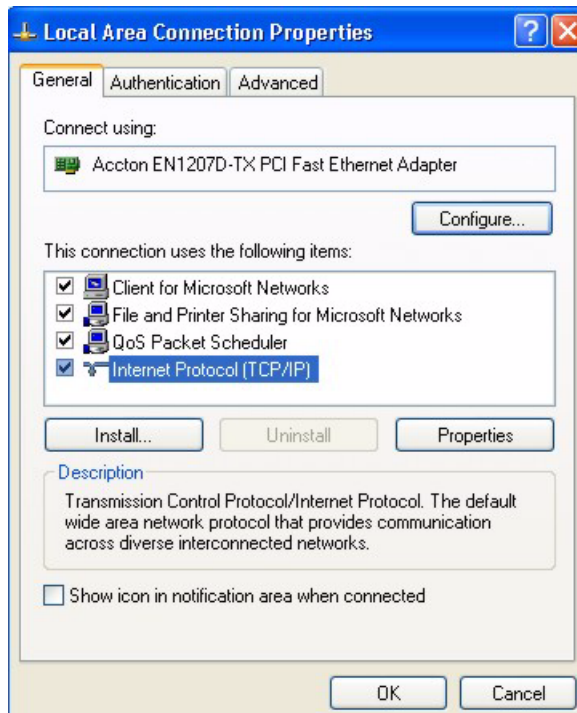
**3** Right-click **Local Area Connection** and then click **Properties**.

**Figure 271** Windows XP: Control Panel: Network Connections: Properties



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

**Figure 272** Windows XP: Local Area Connection Properties

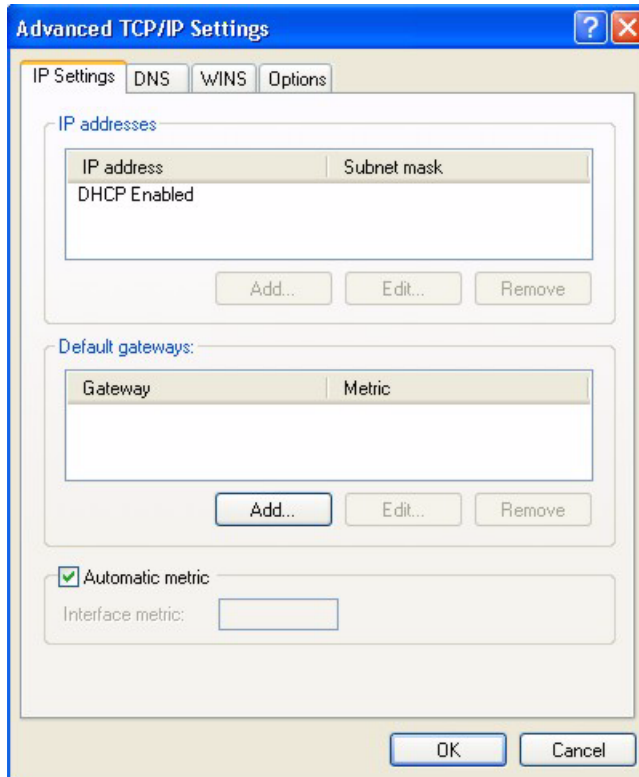


**5** The **Internet Protocol TCP/IP Properties** window opens (the **General** tab in Windows XP).

- 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 273** Windows XP: Advanced TCP/IP Settings



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

Do one or more of the following if you want to configure additional IP addresses:

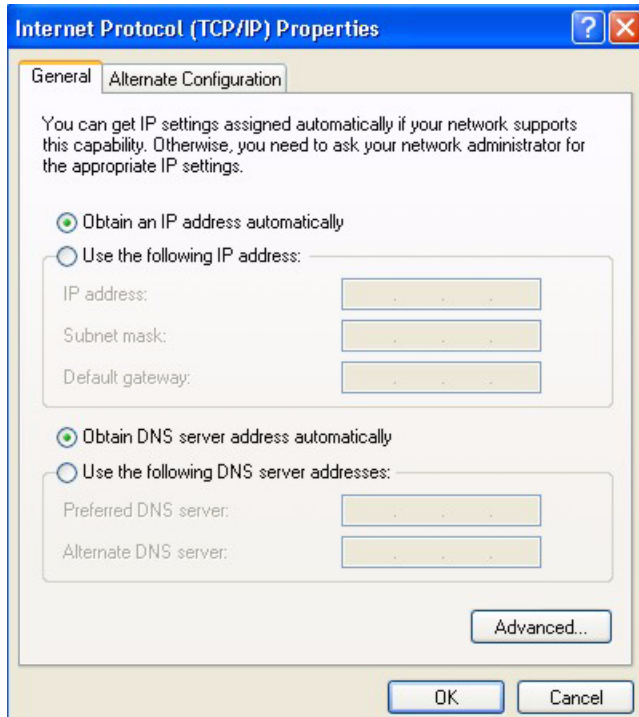
- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP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

**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 274** Windows XP: Internet Protocol (TCP/IP) Properties



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

**9** Click **OK** to close the **Local Area Connection Properties** window.

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

## Verifying Settings

**1** Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

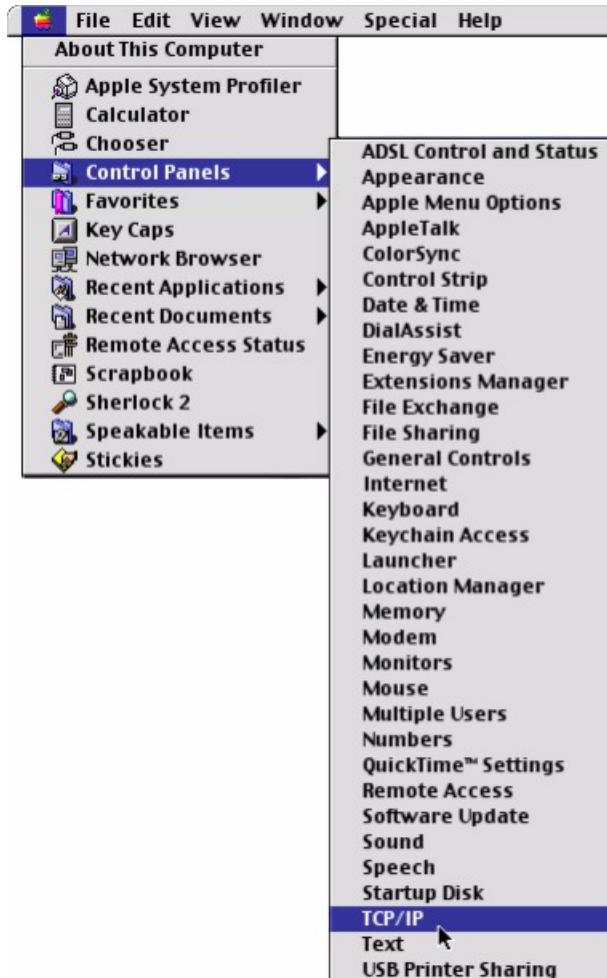
**2** In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.



## Macintosh OS 8/9

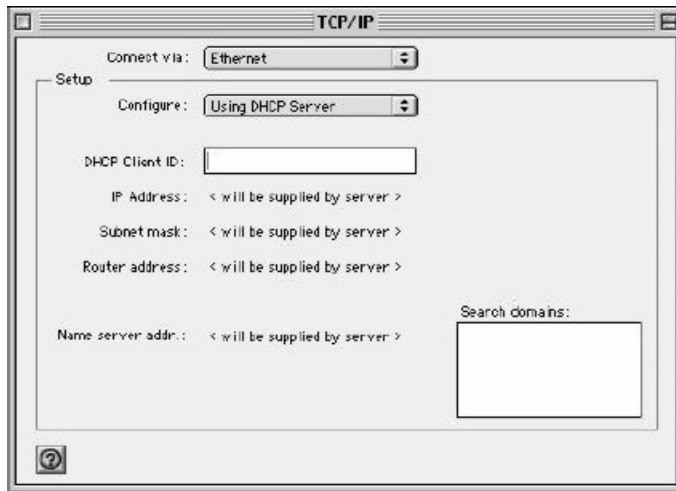
- 1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 275 Macintosh OS 8/9: Apple Menu



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

**Figure 276** Macintosh OS 8/9: TCP/IP



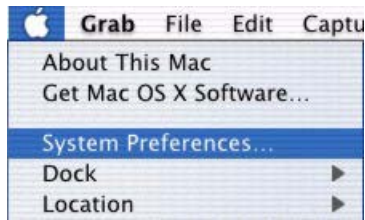
- 3** For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.
- 4** For statically assigned settings, do the following:
  - From the **Configure** box, select **Manually**.
  - Type your IP address in the **IP Address** box.
  - Type your subnet mask in the **Subnet 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

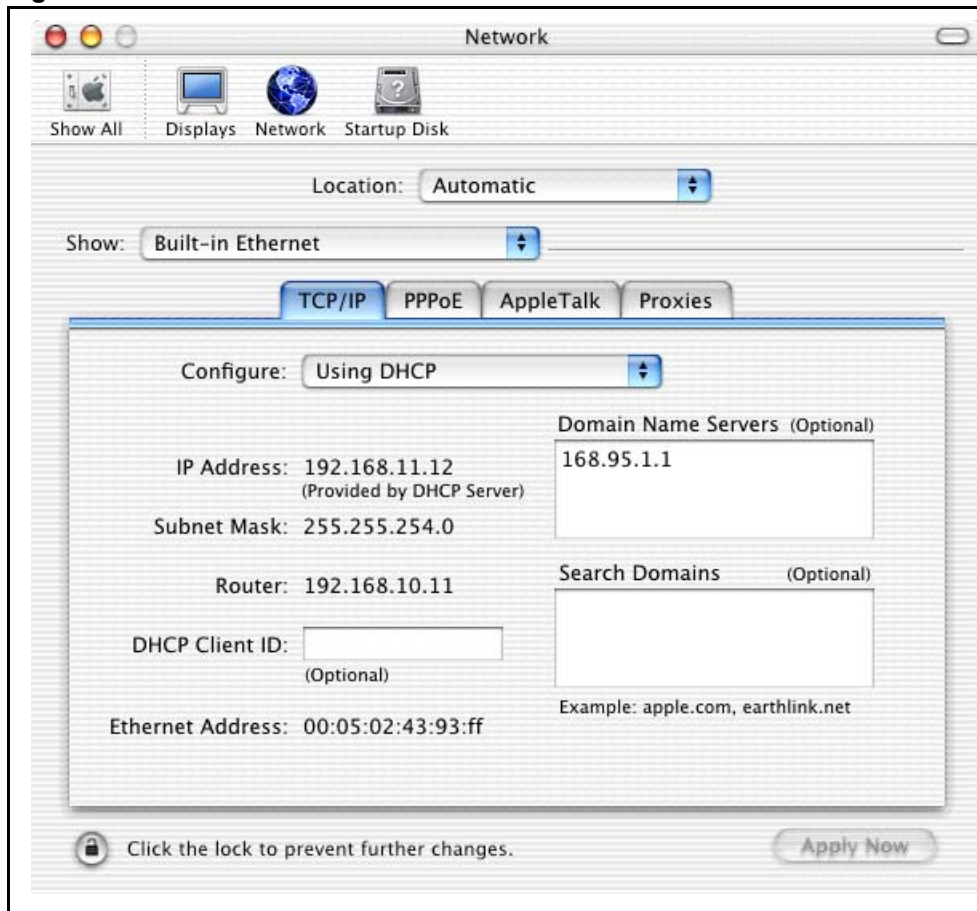
- 1** Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

**Figure 277** 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 278** Macintosh OS X: Network

**4** For statically assigned settings, do the following:

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

- 5 Click **Apply Now** and close the window.
- 6 Turn on your Prestige and restart your computer (if prompted).

## Verifying Settings

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

# APPENDIX C

## IP Subnetting

### IP Addressing

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

### IP Classes

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

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

**Table 150** 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 151** 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 152** “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 153** 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 154** Two Subnets Example

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

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

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

**Note:** In the following charts, shaded/bold last octet bit values indicate host ID bits “borrowed” to form network ID bits. The number of “borrowed” host ID bits determines the number of subnets you can have. The remaining number of host ID bits (after “borrowing”) determines the number of hosts you can have on each subnet.

**Table 155** 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 156** 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 157** 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 158** 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 159** 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 160** 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 161** 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 162** 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 ([Table 150 on page 441](#)) available for subnetting.

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

**Table 163** Class B Subnet Planning

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



# APPENDIX D

## PPPoE

### PPPoE in Action

An ADSL modem bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your computer to an ATM PVC (Permanent Virtual Circuit) which connects to a DSL Access Concentrator where the PPP session terminates ([Figure 279 on page 450](#)). 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.

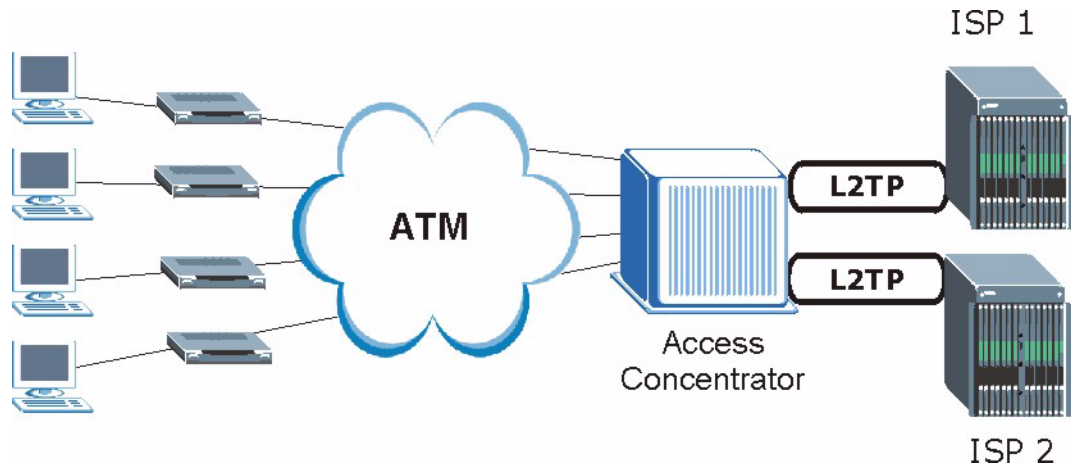
It lessens the burden on the carriers of provisioning virtual circuits all the way to the ISP on multiple switches for thousands of users. For GSTN (PSTN and ISDN), the switching fabric is already in place.

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 279** Single-Computer per Router Hardware Configuration



## How PPPoE Works

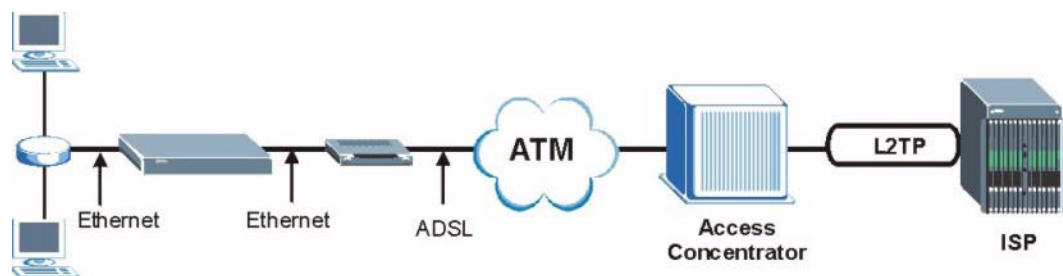
The PPPoE driver makes the Ethernet appear as a serial link to the computer and the computer runs PPP over it, while the modem bridges the Ethernet frames to the Access Concentrator (AC). Between the AC and an ISP, the AC is acting as a L2TP (Layer 2 Tunneling Protocol) LAC (L2TP Access Concentrator) 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 280** Prestige as a PPPoE Client



# APPENDIX E

## Wireless LAN and IEEE 802.11

A wireless LAN (WLAN) provides a flexible data communications system that you can use to access various services (navigating the Internet, E-mail, printer services, etc.) without the use of a cabled connection. In effect a wireless LAN environment provides you the freedom to stay connected to the network while roaming around in the coverage area.

### Benefits of a Wireless LAN

Wireless LAN offers the following benefits:

It provides you with access to network services in areas otherwise hard or expensive to wire, such as historical buildings, buildings with asbestos materials and classrooms.

It provides healthcare workers like doctors and nurses access to a complete patient's profile on a handheld or notebook computer upon entering a patient's room.

It allows flexible workgroups a lower total cost of ownership for workspaces that are frequently reconfigured.

It allows conference room users access to the network as they move from meeting to meeting, getting up-to-date access to information and the ability to communicate decisions while "on the go".

It provides campus-wide networking mobility, allowing enterprises the roaming capability to set up easy-to-use wireless networks that cover the entire campus transparently.

### IEEE 802.11

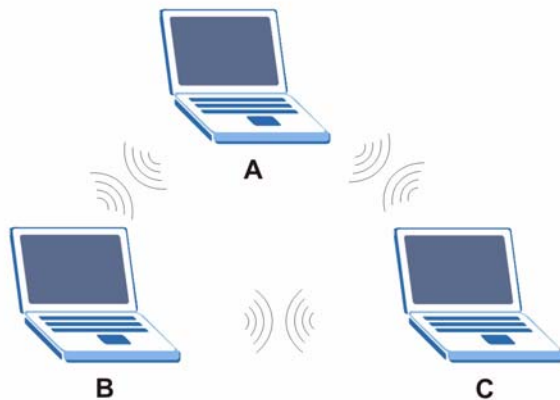
The 1997 completion of the IEEE 802.11 standard for wireless LANs (WLANs) was a first important step in the evolutionary development of wireless networking technologies. The standard was developed to maximize interoperability between differing brands of wireless LANs as well as to introduce a variety of performance improvements and benefits.

The IEEE 802.11 specifies three different transmission methods for the PHY, the layer responsible for transferring data between nodes. Two of the methods use spread spectrum RF signals, Direct Sequence Spread Spectrum (DSSS) and Frequency-Hopping Spread Spectrum (FHSS), in the 2.4 to 2.4825 GHz unlicensed ISM (Industrial, Scientific and Medical) band. The third method is infrared technology, using very high frequencies, just below visible light in the electromagnetic spectrum to carry data.

## Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless nodes or stations (STA), which is called a Basic Service Set (BSS). In the most basic form, a wireless LAN connects a set of computers with wireless adapters. Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an Ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an Ad-hoc wireless LAN.

**Figure 281** Peer-to-Peer Communication in an Ad-hoc Network



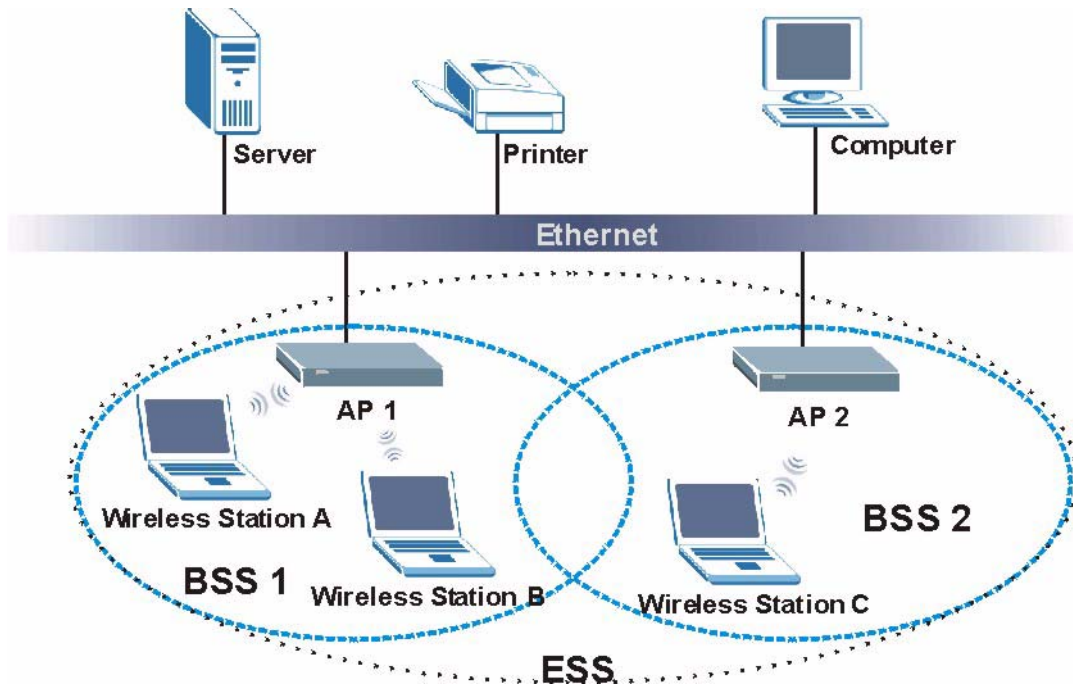
## Infrastructure Wireless LAN Configuration

For Infrastructure WLANs, multiple Access Points (APs) link the WLAN to the wired network and allow users to efficiently share network resources. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood. Multiple Access Points can provide wireless coverage for an entire building or campus. All communications between stations or between a station and a wired network client go through the Access Point.

The Extended Service Set (ESS) shown in the next figure consists of a series of overlapping BSSs (each containing an Access Point) connected together by means of a Distribution System (DS). Although the DS could be any type of network, it is almost invariably an Ethernet LAN. Mobile nodes can roam between Access Points and seamless campus-wide coverage is possible.



Figure 282 ESS Provides Campus-Wide Coverage





# APPENDIX F

## Wireless LAN With IEEE 802.1x

As wireless networks become popular for both portable computing and corporate networks, security is now a priority.

### Security Flaws with IEEE 802.11

Wireless networks based on the original IEEE 802.11 have a poor reputation for safety. The IEEE 802.11b wireless access standard, first published in 1999, was based on the MAC address. As the MAC address is sent across the wireless link in clear text, it is easy to spoof and fake. Even the WEP (Wire Equivalent Privacy) data encryption is unreliable as it can be easily decrypted with current computer speed

### Deployment Issues with IEEE 802.11

User account management has become a network administrator's nightmare in a corporate environment, as the IEEE 802.11b standard does not provide any central user account management. User access control is done through manual modification of the MAC address table on the access point. Although WEP data encryption offers a form of data security, you have to reset the WEP key on the clients each time you change your WEP key on the access point.

### IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices.

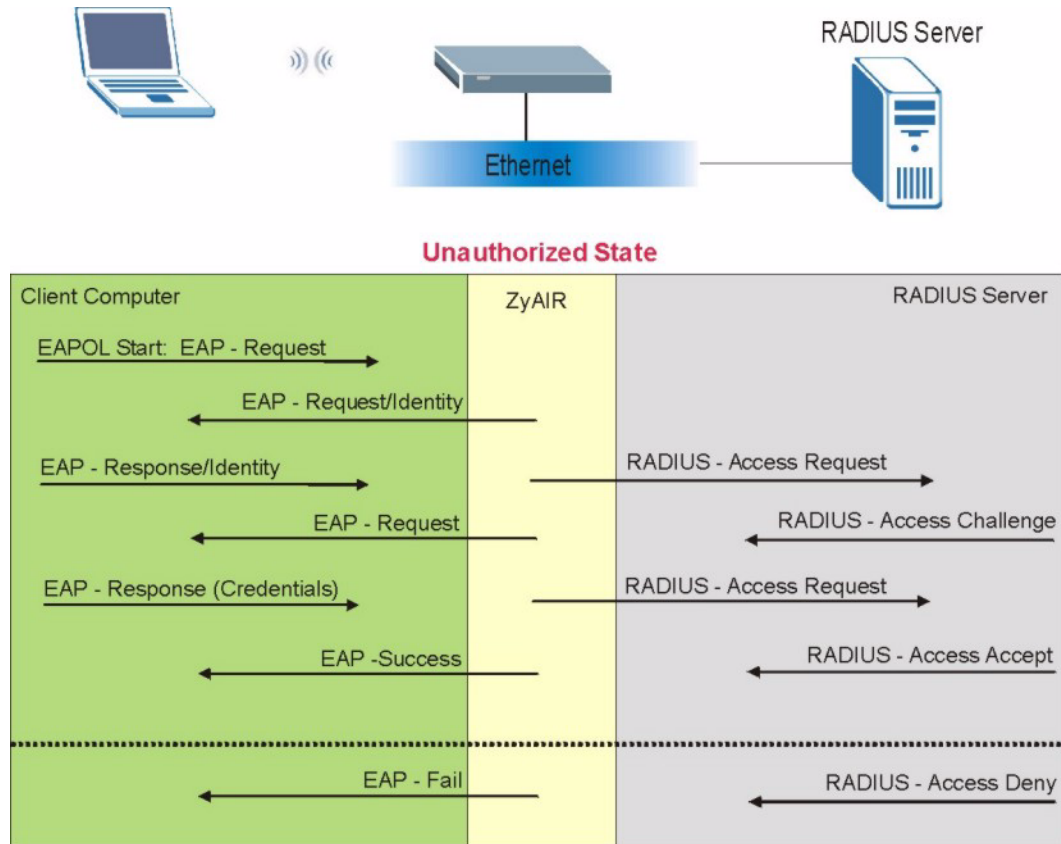
### Advantages of the IEEE 802.1x

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

## RADIUS Server Authentication Sequence

The following figure depicts a typical wireless network with a remote RADIUS server for user authentication using EAPOL (EAP Over LAN).

**Figure 283** Sequences for EAP MD5–Challenge Authentication



# APPENDIX G

## Types of EAP Authentication

This appendix discusses three popular EAP authentication types: **EAP-MD5**, **EAP-TLS** and **EAP-TTLS**. The type of authentication you use depends on the RADIUS server or the AP. Consult your network administrator for more information.

### **EAP-MD5 (Message-Digest Algorithm 5)**

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless station. The wireless station 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

### **EAP-TLS (Transport Layer Security)**

With EAP-TLS, digital certifications are needed by both the server and the wireless stations for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

### **EAP-TTLS (Tunneled Transport Layer Service)**

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

## LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE802.1x.

**Table 164** Comparison of EAP Authentication Types

	<b>EAP-MD5</b>	<b>EAP-TLS</b>	<b>EAP-TTLS</b>	<b>PEAP</b>	<b>LEAP</b>
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

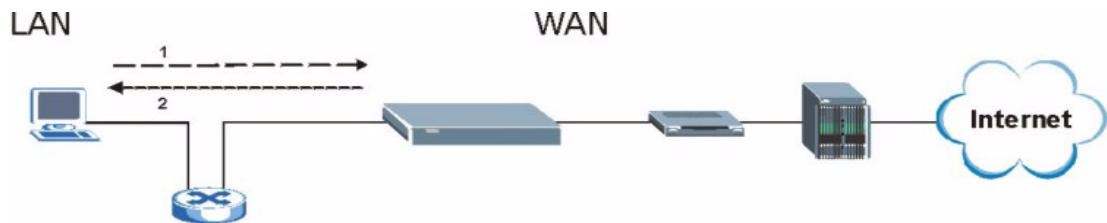
# APPENDIX H

## Triangle Route

### The Ideal Setup

When the firewall is on, your Prestige acts as a secure gateway between your LAN and the Internet. In an ideal network topology, all incoming and outgoing network traffic passes through the Prestige to protect your LAN against attacks.

**Figure 284** Ideal Setup



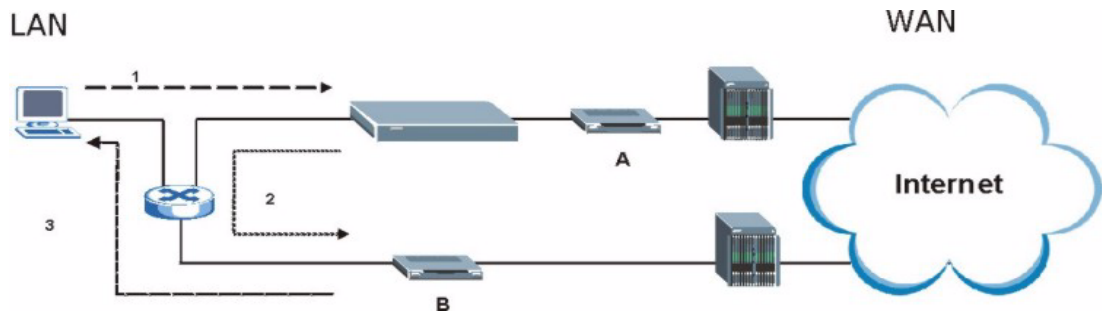
### The “Triangle Route” Problem

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 285** “Triangle Route” Problem



## The “Triangle Route” Solutions

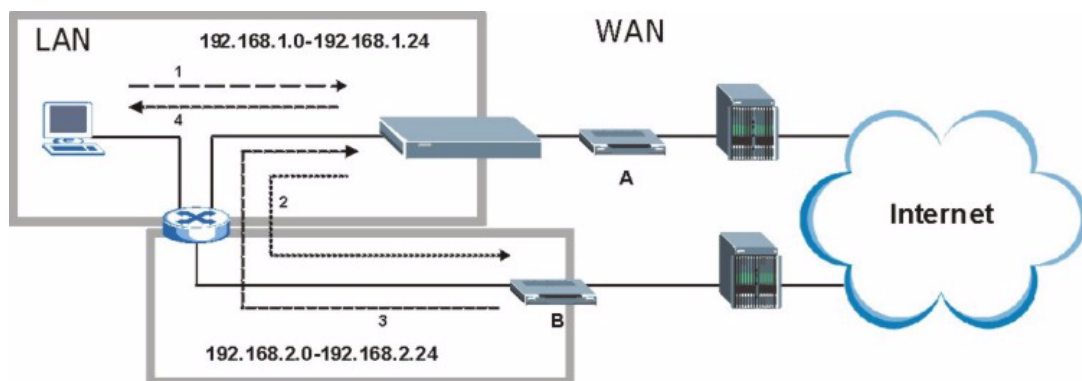
This section presents you two solutions to the “triangle route” problem.

### IP Aliasing

IP alias allows you to partition your network into logical sections over the same Ethernet interface. Your Prestige supports up to three logical LAN interfaces with the Prestige being the gateway for each logical network. By putting your LAN and Gateway B in different subnets, all returning network traffic must pass through the Prestige to your LAN. The following steps describe such a scenario.

- 1 A computer on the LAN initiates a connection by sending a SYN packet to a receiving server on the WAN.
- 2 The Prestige reroutes the packet to Gateway B, which is in Subnet 2.
- 3 The reply from WAN goes through the Prestige to the computer on the LAN in Subnet 1.

**Figure 286** IP Alias

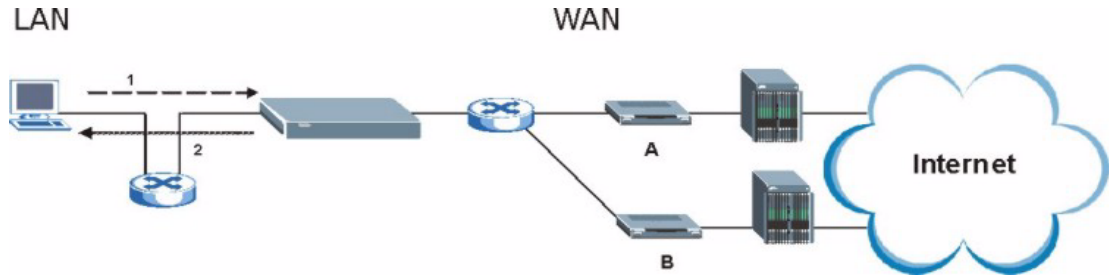




## Gateways on the WAN Side

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 287** Gateways on the WAN Side  
LAN





# APPENDIX I

## Internal SPTGEN

### Internal SPTGEN Overview

Internal SPTGEN (System Parameter Table Generator) is a configuration text file useful for efficient configuration of multiple Prestiges. Internal SPTGEN lets you configure, save and upload multiple menus at the same time using just one configuration text file – eliminating the need to navigate and configure individual SMT menus for each Prestige.

### The Configuration Text File Format

All Internal SPTGEN text files conform to the following format:

```
<field identification number = field name = parameter values
allowed = input>,
```

where <input> is your input conforming to <parameter values allowed>.

The figure shown next is an example of an Internal SPTGEN text file.

**Figure 288** Configuration Text File Format: Column Descriptions

```
/ Menu 1 General Setup
10000000 = Configured           <0 (No) | 1 (Yes)>      = 1
10000001 = System Name         <Str>                 = Prestige
10000002 = Location            <Str>                 =
10000003 = Contact Person's Name <Str>                 =
10000004 = Route IP            <0 (No) | 1 (Yes)>      = 1
10000005 = Route IPX          <0 (No) | 1 (Yes)>      = 0
10000006 = Bridge              <0 (No) | 1 (Yes)>      = 0
```

**Note:** DO NOT alter or delete any field except parameters in the Input column.

For more text file examples, refer to the *Example Internal SPTGEN Screens Appendix*.

### Internal SPTGEN File Modification - Important Points to Remember

Each parameter you enter must be preceded by one “=” sign and one space.

Some parameters are dependent on others. For example, if you disable the **Configured** field in menu 1 (see [Figure 288 on page 463](#)), then you disable every field in this menu.

If you enter a parameter that is invalid in the **Input** column, the Prestige will not save the configuration and the command line will display the **Field Identification Number**. [Figure 289 on page 464](#), shown next, is an example of what the Prestige displays if you enter a value other than “0” or “1” in the **Input** column of **Field Identification Number** 1000000 (refer to [Figure 288 on page 463](#)).

**Figure 289** Invalid Parameter Entered: Command Line Example

```
field value is not legal error:-1
ROM-t is not saved, error Line ID:10000000
reboot to get the original configuration
Bootbase Version: V2.02 | 2/22/2001 13:33:11
RAM: Size = 8192 Kbytes
FLASH: Intel 8M *2
```

The Prestige will display the following if you enter parameter(s) that *are* valid.

**Figure 290** Valid Parameter Entered: Command Line Example

```
Please wait for the system to write SPT text file(ROM-t)...
Bootbase Version: V2.02 | 2/22/2001 13:33:11
RAM: Size = 8192 Kbytes
FLASH: Intel 8M *2
```

## Internal SPTGEN FTP Download Example

- 1 Launch your FTP application.
- 2 Enter "bin". The command “bin” sets the transfer mode to binary.
- 3 Get "rom-t" file. The command “get” transfers files from the Prestige to your computer. The name “rom-t” is the configuration filename on the Prestige.
- 4 Edit the "rom-t" file using a text editor (do not use a word processor). You must leave this FTP screen to edit.

**Figure 291** Internal SPTGEN FTP Download Example

```

c:\ftp 192.168.1.1
220 PPP FTP version 1.0 ready at Sat Jan 1 03:22:12 2000
User (192.168.1.1:(none)):
331 Enter PASS command
Password:
230 Logged in
ftp>bin
200 Type I OK
ftp> get rom-t
ftp>bye
c:\edit rom-t
(edit the rom-t text file by a text editor and save it)

```

**Note:** You can rename your “rom-t” file when you save it to your computer but it must be named “rom-t” when you upload it to your Prestige.

## Internal SPTGEN FTP Upload Example

- 1 Launch your FTP application.
- 2 Enter "bin". The command “bin” sets the transfer mode to binary.
- 3 Upload your “rom-t” file from your computer to the Prestige using the “put” command.  
computer to the Prestige.
- 4 Exit this FTP application.

**Figure 292** Internal SPTGEN FTP Upload Example

```

c:\ftp 192.168.1.1
220 PPP FTP version 1.0 ready at Sat Jan 1 03:22:12 2000
User (192.168.1.1:(none)):
331 Enter PASS command
Password:
230 Logged in
ftp>bin
200 Type I OK
ftp> put rom-t
ftp>bye

```

## Example Internal SPTGEN Screens

This section covers Prestige Internal SPTGEN screens.

**Table 165** Abbreviations Used in the Example Internal SPTGEN Screens Table

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

**Table 165** Abbreviations Used in the Example Internal SPTGEN Screens Table

ABBREVIATION	MEANING
PVA	Parameter Values Allowed
INPUT	An example of what you may enter
*	Applies to the Prestige.

The following are Internal SPTGEN screens associated with the SMT screens of your Prestige.

**Table 166** Menu 1 General Setup (SMT Menu 1)

/ Menu 1 General Setup (SMT Menu 1)			
FIN	FN	PVA	INPUT
10000000 =	Configured	<0 (No)   1 (Yes)>	= 0
10000001 =	System Name	<Str>	= Prestige
10000002 =	Location	<Str>	=
10000003 =	Contact Person's Name	<Str>	=
10000004 =	Route IP	<0 (No)   1 (Yes)>	= 1
10000006 =	Bridge	<0 (No)   1 (Yes)>	= 0

**Table 167** Menu 3 (SMT Menu 3 )

/ Menu 3.1 General Ethernet Setup (SMT menu 3.1)			
FIN	FN	PVA	INPUT
30100001 =	Input Protocol filters Set 1		= 2
30100002 =	Input Protocol filters Set 2		= 256
30100003 =	Input Protocol filters Set 3		= 256
30100004 =	Input Protocol filters Set 4		= 256
30100005 =	Input device filters Set 1		= 256
30100006 =	Input device filters Set 2		= 256
30100007 =	Input device filters Set 3		= 256
30100008 =	Input device filters Set 4		= 256
30100009 =	Output protocol filters Set 1		= 256
30100010 =	Output protocol filters Set 2		= 256
30100011 =	Output protocol filters Set 3		= 256
30100012 =	Output protocol filters Set 4		= 256
30100013 =	Output device filters Set 1		= 256
30100014 =	Output device filters Set 2		= 256
30100015 =	Output device filters Set 3		= 256
30100016 =	Output device filters Set 4		= 256
/ Menu 3.2 TCP/IP and DHCP Ethernet Setup (SMT Menu 3.2)			

**Table 167** Menu 3 (SMT Menu 3 (continued))

FIN	FN	PVA	INPUT
30200001 =	DHCP	<0 (None)   1 (Server)   2 (Relay)>	= 0
30200002 =	Client IP Pool Starting Address		= 192.168.1.33
30200003 =	Size of Client IP Pool		= 32
30200004 =	Primary DNS Server		= 0.0.0.0
30200005 =	Secondary DNS Server		= 0.0.0.0
30200006 =	Remote DHCP Server		= 0.0.0.0
30200008 =	IP Address		= 172.21.2.200
30200009 =	IP Subnet Mask		= 16
30200010 =	RIP Direction	<0 (None)   1 (Both)   2 (In Only)   3 (Out Only)>	= 0
30200011 =	Version	<0 (Rip-1)   1 (Rip-2B)  2 (Rip-2M)>	= 0
30200012 =	Multicast	<0 (IGMP-v2)   1 (IGMP-v1)   2 (None)>	= 2
30200013 =	IP Policies Set 1 (1~12)		= 256
30200014 =	IP Policies Set 2 (1~12)		= 256
30200015 =	IP Policies Set 3 (1~12)		= 256
30200016 =	IP Policies Set 4 (1~12)		= 256
/ Menu 3.2.1 IP Alias Setup (SMT Menu 3.2.1)			
FIN	FN	PVA	INPUT
30201001 =	IP Alias 1	<0 (No)   1 (Yes)>	= 0
30201002 =	IP Address		= 0.0.0.0
30201003 =	IP Subnet Mask		= 0
30201004 =	RIP Direction	<0 (None)   1 (Both)   2 (In Only)   3 (Out Only)>	= 0
30201005 =	Version	<0 (Rip-1)   1 (Rip-2B)  2 (Rip-2M)>	= 0
30201006 =	IP Alias #1 Incoming protocol filters Set 1		= 256
30201007 =	IP Alias #1 Incoming protocol filters Set 2		= 256

**Table 167** Menu 3 (SMT Menu 3 (continued))

30201008 =	IP Alias #1 Incoming protocol filters Set 3		= 256	
30201009 =	IP Alias #1 Incoming protocol filters Set 4		= 256	
30201010 =	IP Alias #1 Outgoing protocol filters Set 1		= 256	
30201011 =	IP Alias #1 Outgoing protocol filters Set 2		= 256	
30201012 =	IP Alias #1 Outgoing protocol filters Set 3		= 256	
30201013 =	IP Alias #1 Outgoing protocol filters Set 4		= 256	
30201014 =	IP Alias 2 <0 (No)   1 (Yes)>		= 0	
30201015 =	IP Address		= 0.0.0.0	
30201016 =	IP Subnet Mask		= 0	
30201017 =	RIP Direction	<0 (None)   1 (Both)   2 (In Only)   3 (Out Only)>	= 0	
30201018 =	Version	<0 (Rip-1)   1 (Rip-2B)   2 (Rip-2M)>	= 0	
30201019 =	IP Alias #2 Incoming protocol filters Set 1		= 256	
30201020 =	IP Alias #2 Incoming protocol filters Set 2		= 256	
30201021 =	IP Alias #2 Incoming protocol filters Set 3		= 256	
30201022 =	IP Alias #2 Incoming protocol filters Set 4		= 256	
30201023 =	IP Alias #2 Outgoing protocol filters Set 1		= 256	
30201024 =	IP Alias #2 Outgoing protocol filters Set 2		= 256	
30201025 =	IP Alias #2 Outgoing protocol filters Set 3		= 256	
30201026 =	IP Alias #2 Outgoing protocol filters Set 4		= 256	
*/ Menu 3.5 Wireless LAN Setup (SMT Menu 3.5)				
	FIN	FN	PVA	INPUT
30500001 =	ESSID			Wireless
30500002 =	Hide ESSID		<0 (No)   1 (Yes)>	= 0
30500003 =	Channel ID		<1 2 3 4 5 6 7 8 9 10 11 12 13>	= 1



**Table 167** Menu 3 (SMT Menu 3 (continued))

30500004 =	RTS Threshold	<0 ~ 2432>	= 2432
30500005 =	FRAG. Threshold	<256 ~ 2432>	= 2432
30500006 =	WEP	<0 (DISABLE)   1 (64-bit WEP)   2 (128-bit WEP)>	= 0
30500007 =	Default Key	<1 2 3 4>	= 0
30500008 =	WEP Key1		=
30500009 =	WEP Key2		=
30500010 =	WEP Key3		=
30500011 =	WEP Key4		=
30500012 =	Wlan Active	<0 (Disable)   1 (Enable)>	= 0
*/ MENU 3.5.1 WLAN MAC ADDRESS FILTER (SMT MENU 3.5.1)			
FIN	FN	PVA	INPUT
30501001 =	Mac Filter Active	<0 (No)   1 (Yes)>	= 0
30501002 =	Filter Action	<0 (Allow)   1 (Deny)>	= 0
30501003 =	Address 1		= 00:00:00:00:0 0:00
30501004 =	Address 2		= 00:00:00:00:0 0:00
30501005 =	Address 3		= 00:00:00:00:0 0:00
Continued	...		...
30501034 =	Address 32		= 00:00:00:00:0 0:00

**Table 168** Menu 4 Internet Access Setup (SMT Menu 4)

/ Menu 4 Internet Access Setup (SMT Menu 4)			
FIN	FN	PVA	INPUT
40000000 =	Configured	<0 (No)   1 (Yes)>	= 1
40000001 =	ISP	<0 (No)   1 (Yes)>	= 1

**Table 168** Menu 4 Internet Access Setup (SMT Menu 4) (continued)

40000002 =	Active	<0 (No)   1 (Yes)>	= 1
40000003 =	ISP's Name		= ChangeMe
40000004 =	Encapsulation	<2 (PPPOE)   3 (RFC 1483)   4 (PPPoA )   5 (ENET ENCAP)>	= 2
40000005 =	Multiplexing	<1 (LLC-based)   2 (VC-based)>	= 1
40000006 =	VPI #		= 0
40000007 =	VCI #		= 35
40000008 =	Service Name	<Str>	= any
40000009 =	My Login	<Str>	= test@pqa
40000010 =	My Password	<Str>	= 1234
40000011 =	Single User Account	<0 (No)   1 (Yes)>	= 1
40000012 =	IP Address Assignment	<0 (Static)   1 (Dynamic)>	= 1
40000013 =	IP Address		= 0.0.0.0
40000014 =	Remote IP address		= 0.0.0.0
40000015 =	Remote IP subnet mask		= 0
40000016 =	ISP incoming protocol filter set 1		= 6
40000017 =	ISP incoming protocol filter set 2		= 256
40000018 =	ISP incoming protocol filter set 3		= 256
40000019 =	ISP incoming protocol filter set 4		= 256
40000020 =	ISP outgoing protocol filter set 1		= 256
40000021 =	ISP outgoing protocol filter set 2		= 256
40000022 =	ISP outgoing protocol filter set 3		= 256
40000023 =	ISP outgoing protocol filter set 4		= 256
40000024 =	ISP PPPoE idle timeout		= 0
40000025 =	Route IP	<0 (No)   1 (Yes)>	= 1
40000026 =	Bridge	<0 (No)   1 (Yes)>	= 0
40000027 =	ATM QoS Type	<0 (CBR)   1 (UBR)>	= 1
40000028 =	Peak Cell Rate (PCR)		= 0
40000029 =	Sustain Cell Rate (SCR)		= 0
40000030 =	Maximum Burst Size (MBS)		= 0
40000031 =	RIP Direction	<0 (None)   1 (Both)   2 (In Only)   3 (Out Only)>	= 0

**Table 168** Menu 4 Internet Access Setup (SMT Menu 4) (continued)

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

**Table 169** Menu 12 (SMT Menu 12)

/ Menu 12.1.1 IP Static Route Setup (SMT Menu 12.1.1)			
FIN	FN	PVA	INPUT
120101001 =	IP Static Route set #1, Name	<Str>	=
120101002 =	IP Static Route set #1, Active	<0 (No)  1 (Yes)>	= 0
120101003 =	IP Static Route set #1, Destination IP address		= 0.0.0.0
120101004 =	IP Static Route set #1, Destination IP subnetmask		= 0
120101005 =	IP Static Route set #1, Gateway		= 0.0.0.0
120101006 =	IP Static Route set #1, Metric		= 0
120101007 =	IP Static Route set #1, Private	<0 (No)  1 (Yes)>	= 0
/ Menu 12.1.2 IP Static Route Setup (SMT Menu 12.1.2)			
FIN	FN	PVA	INPUT
120102001 =	IP Static Route set #2, Name		=
120102002 =	IP Static Route set #2, Active	<0 (No)  1 (Yes)>	= 0
120102003 =	IP Static Route set #2, Destination IP address		= 0.0.0.0
120102004 =	IP Static Route set #2, Destination IP subnetmask		= 0
120102005 =	IP Static Route set #2, Gateway		= 0.0.0.0
120102006 =	IP Static Route set #2, Metric		= 0
120102007 =	IP Static Route set #2, Private	<0 (No)  1 (Yes)>	= 0
/ Menu 12.1.3 IP Static Route Setup (SMT Menu 12.1.3)			
FIN	FN	PVA	INPUT
120103001 =	IP Static Route set #3, Name	<Str>	=
120103002 =	IP Static Route set #3, Active	<0 (No)  1 (Yes)>	= 0
120103003 =	IP Static Route set #3, Destination IP address		= 0.0.0.0
120103004 =	IP Static Route set #3, Destination IP subnetmask		= 0
120103005 =	IP Static Route set #3, Gateway		= 0.0.0.0
120103006 =	IP Static Route set #3, Metric		= 0
120103007 =	IP Static Route set #3, Private	<0 (No)  1 (Yes)>	= 0

**Table 169** Menu 12 (SMT Menu 12) (continued)

/ Menu 12.1.4 IP Static Route Setup (SMT Menu 12.1.4)			
FIN	FN	PVA	INPUT
120104001 =	IP Static Route set #4, Name	<Str>	=
120104002 =	IP Static Route set #4, Active	<0 (No)  1 (Yes)>	= 0
120104003 =	IP Static Route set #4, Destination IP address		= 0.0.0.0
120104004 =	IP Static Route set #4, Destination IP subnetmask		= 0
120104005 =	IP Static Route set #4, Gateway		= 0.0.0.0
120104006 =	IP Static Route set #4, Metric		= 0
120104007 =	IP Static Route set #4, Private	<0 (No)  1 (Yes)>	= 0
/ Menu 12.1.5 IP Static Route Setup (SMT Menu 12.1.5)			
FIN	FN	PVA	INPUT
120105001 =	IP Static Route set #5, Name	<Str>	=
120105002 =	IP Static Route set #5, Active	<0 (No)  1 (Yes)>	= 0
120105003 =	IP Static Route set #5, Destination IP address		= 0.0.0.0
120105004 =	IP Static Route set #5, Destination IP subnetmask		= 0
120105005 =	IP Static Route set #5, Gateway		= 0.0.0.0
120105006 =	IP Static Route set #5, Metric		= 0
120105007 =	IP Static Route set #5, Private	<0 (No)  1 (Yes)>	= 0
/ Menu 12.1.6 IP Static Route Setup (SMT Menu 12.1.6)			
FIN	FN	PVA	INPUT
120106001 =	IP Static Route set #6, Name	<Str>	=
120106002 =	IP Static Route set #6, Active	<0 (No)  1 (Yes)>	= 0
120106003 =	IP Static Route set #6, Destination IP address		= 0.0.0.0
120106004 =	IP Static Route set #6, Destination IP subnetmask		= 0
120106005 =	IP Static Route set #6, Gateway		= 0.0.0.0
120106006 =	IP Static Route set #6, Metric		= 0
120106007 =	IP Static Route set #6, Private	<0 (No)  1 (Yes)>	= 0
/ Menu 12.1.7 IP Static Route Setup (SMT Menu 12.1.7)			
FIN	FN	PVA	INPUT
120107001 =	IP Static Route set #7, Name	<Str>	=
120107002 =	IP Static Route set #7, Active	<0 (No)  1 (Yes)>	= 0
120107003 =	IP Static Route set #7, Destination IP address		= 0.0.0.0
120107004 =	IP Static Route set #7, Destination IP subnetmask		= 0
120107005 =	IP Static Route set #7, Gateway		= 0.0.0.0

**Table 169** Menu 12 (SMT Menu 12) (continued)

120107006 =	IP Static Route set #7, Metric		= 0
120107007 =	IP Static Route set #7, Private	<0(No)  1(Yes)>	= 0
/ Menu 12.1.8 IP Static Route Setup (SMT Menu 12.1.8)			
FIN	FN	PVA	INPUT
120108001 =	IP Static Route set #8, Name	<Str>	=
120108002 =	IP Static Route set #8, Active	<0(No)  1(Yes)>	= 0
120108003 =	IP Static Route set #8, Destination IP address		= 0.0.0.0
120108004 =	IP Static Route set #8, Destination IP subnetmask		= 0
120108005 =	IP Static Route set #8, Gateway		= 0.0.0.0
120108006 =	IP Static Route set #8, Metric		= 0
120108007 =	IP Static Route set #8, Private	<0(No)  1(Yes)>	= 0
*/ Menu 12.1.9 IP Static Route Setup (SMT Menu 12.1.9)			
FIN	FN	PVA	INPUT
120109001 =	IP Static Route set #9, Name	<Str>	=
120109002 =	IP Static Route set #9, Active	<0(No)  1(Yes)>	= 0
120109003 =	IP Static Route set #9, Destination IP address		= 0.0.0.0
120109004 =	IP Static Route set #9, Destination IP subnetmask		= 0
120109005 =	IP Static Route set #9, Gateway		= 0.0.0.0
120109006 =	IP Static Route set #9, Metric		= 0
120109007 =	IP Static Route set #9, Private	<0(No)  1(Yes)>	= 0
*/ Menu 12.1.10 IP Static Route Setup (SMT Menu 12.1.10)			
FIN	FN	PVA	INPUT
120110001 =	IP Static Route set #10, Name		=
120110002 =	IP Static Route set #10, Active	<0(No)  1(Yes)>	= 0
120110003 =	IP Static Route set #10, Destination IP address		= 0.0.0.0
120110004 =	IP Static Route set #10, Destination IP subnetmask		= 0
120110005 =	IP Static Route set #10, Gateway		= 0.0.0.0
120110006 =	IP Static Route set #10, Metric		= 0
120110007 =	IP Static Route set #10, Private	<0(No)  1(Yes)>	= 0
*/ Menu 12.1.11 IP Static Route Setup (SMT Menu 12.1.11)			
FIN	FN	PVA	INPUT
120111001 =	IP Static Route set #11, Name	<Str>	=
120111002 =	IP Static Route set #11, Active	<0(No)  1(Yes)>	= 0
120111003 =	IP Static Route set #11, Destination IP address		= 0.0.0.0

**Table 169** Menu 12 (SMT Menu 12) (continued)

120111004 =	IP Static Route set #11, Destination IP subnetmask		= 0
120111005 =	IP Static Route set #11, Gateway		= 0.0.0.0
120111006 =	IP Static Route set #11, Metric		= 0
120111007 =	IP Static Route set #11, Private	<0 (No)  1 (Yes)>	= 0
*/ Menu 12.1.12 IP Static Route Setup (SMT Menu 12.1.12)			
FIN	FN	PVA	INPUT
120112001 =	IP Static Route set #12, Name	<Str>	=
120112002 =	IP Static Route set #12, Active	<0 (No)  1 (Yes)>	= 0
120112003 =	IP Static Route set #12, Destination IP address		= 0.0.0.0
120112004 =	IP Static Route set #12, Destination IP subnetmask		= 0
120112005 =	IP Static Route set #12, Gateway		= 0.0.0.0
120112006 =	IP Static Route set #12, Metric		= 0
120112007 =	IP Static Route set #12, Private	<0 (No)  1 (Yes)>	= 0
*/ Menu 12.1.13 IP Static Route Setup (SMT Menu 12.1.13)			
FIN	FN	PVA	INPUT
120113001 =	IP Static Route set #13, Name	<Str>	=
120113002 =	IP Static Route set #13, Active	<0 (No)  1 (Yes)>	= 0
120113003 =	IP Static Route set #13, Destination IP address		= 0.0.0.0
120113004 =	IP Static Route set #13, Destination IP subnetmask		= 0
120113005 =	IP Static Route set #13, Gateway		= 0.0.0.0
120113006 =	IP Static Route set #13, Metric		= 0
120113007 =	IP Static Route set #13, Private	<0 (No)  1 (Yes)>	= 0
*/ Menu 12.1.14 IP Static Route Setup (SMT Menu 12.1. 14)			
FIN	FN	PVA	INPUT
120114001 =	IP Static Route set #14, Name	<Str>	=
120114002 =	IP Static Route set #14, Active	<0 (No)  1 (Yes)>	= 0
120114003 =	IP Static Route set #14, Destination IP address		= 0.0.0.0
120114004 =	IP Static Route set #14, Destination IP subnetmask		= 0
120114005 =	IP Static Route set #14, Gateway		= 0.0.0.0
120114006 =	IP Static Route set #14, Metric		= 0
120114007 =	IP Static Route set #14, Private	<0 (No)  1 (Yes)>	= 0
*/ Menu 12.1.15 IP Static Route Setup (SMT Menu 12.1. 15)			
FIN	FN	PVA	INPUT
120115001 =	IP Static Route set #15, Name	<Str>	=

**Table 169** Menu 12 (SMT Menu 12) (continued)

120115002 =	IP Static Route set #15, Active	<0 (No)   1 (Yes)>	= 0
120115003 =	IP Static Route set #15, Destination IP address		= 0.0.0.0
120115004 =	IP Static Route set #15, Destination IP subnetmask		= 0
120115005 =	IP Static Route set #15, Gateway		= 0.0.0.0
120115006 =	IP Static Route set #15, Metric		= 0
120115007 =	IP Static Route set #15, Private	<0 (No)   1 (Yes)>	= 0
*/ Menu 12.1.16 IP Static Route Setup (SMT Menu 12.1. 16)			
FIN	FN	PVA	INPUT
120116001 =	IP Static Route set #16, Name	<Str>	=
120116002 =	IP Static Route set #16, Active	<0 (No)   1 (Yes)>	= 0
120116003 =	IP Static Route set #16, Destination IP address		= 0.0.0.0
120116004 =	IP Static Route set #16, Destination IP subnetmask		= 0
120116005 =	IP Static Route set #16, Gateway		= 0.0.0.0
120116006 =	IP Static Route set #16, Metric		= 0
120116007 =	IP Static Route set #16, Private	<0 (No)   1 (Yes)>	= 0

**Table 170** Menu 15 SUA Server Setup (SMT Menu 15)

/ Menu 15 SUA Server Setup (SMT Menu 15)			
FIN	FN	PVA	INPUT
150000001 =	SUA Server IP address for default port		= 0.0.0.0
150000002 =	SUA Server #2 Active	<0 (No)   1 (Yes)>	= 0
150000003 =	SUA Server #2 Protocol	<0 (All)   6 (TCP)   17 (UDP)>	= 0
150000004 =	SUA Server #2 Port Start		= 0
150000005 =	SUA Server #2 Port End		= 0
150000006 =	SUA Server #2 Local IP address		= 0.0.0.0
150000007 =	SUA Server #3 Active	<0 (No)   1 (Yes)>	= 0
150000008 =	SUA Server #3 Protocol	<0 (All)   6 (TCP)   17 (UDP)>	= 0
150000009 =	SUA Server #3 Port Start		= 0
150000010 =	SUA Server #3 Port End		= 0
150000011 =	SUA Server #3 Local IP address		= 0.0.0.0
150000012 =	SUA Server #4 Active	<0 (No)   1 (Yes)>	= 0
150000013 =	SUA Server #4 Protocol	<0 (All)   6 (TCP)   17 (UDP)>	= 0

**Table 170** Menu 15 SUA Server Setup (SMT Menu 15) (continued)

150000014 =	SUA Server #4 Port Start		= 0
150000015 =	SUA Server #4 Port End		= 0
150000016 =	SUA Server #4 Local IP address		= 0.0.0.0
150000017 =	SUA Server #5 Active	<0 (No)   1 (Yes)>	= 0
150000018 =	SUA Server #5 Protocol	<0 (All)   6 (TCP)   17 (UDP)>	= 0
150000019 =	SUA Server #5 Port Start		= 0
150000020 =	SUA Server #5 Port End		= 0
150000021 =	SUA Server #5 Local IP address		= 0.0.0.0
150000022 =	SUA Server #6 Active	<0 (No)   1 (Yes)> = 0	= 0
150000023 =	SUA Server #6 Protocol	<0 (All)   6 (TCP)   17 (UDP)>	= 0
150000024 =	SUA Server #6 Port Start		= 0
150000025 =	SUA Server #6 Port End		= 0
150000026 =	SUA Server #6 Local IP address		= 0.0.0.0
150000027 =	SUA Server #7 Active	<0 (No)   1 (Yes)>	= 0
150000028 =	SUA Server #7 Protocol	<0 (All)   6 (TCP)   17 (UDP)>	= 0.0.0.0
150000029 =	SUA Server #7 Port Start		= 0
150000030 =	SUA Server #7 Port End		= 0
150000031 =	SUA Server #7 Local IP address		= 0.0.0.0
150000032 =	SUA Server #8 Active	<0 (No)   1 (Yes)>	= 0
150000033 =	SUA Server #8 Protocol	<0 (All)   6 (TCP)   17 (UDP)>	= 0
150000034 =	SUA Server #8 Port Start		= 0
150000035 =	SUA Server #8 Port End		= 0
150000036 =	SUA Server #8 Local IP address		= 0.0.0.0
150000037 =	SUA Server #9 Active	<0 (No)   1 (Yes)>	= 0
150000038 =	SUA Server #9 Protocol	<0 (All)   6 (TCP)   17 (UDP)>	= 0
150000039 =	SUA Server #9 Port Start		= 0
150000040 =	SUA Server #9 Port End		= 0
150000041 =	SUA Server #9 Local IP address		= 0.0.0.0
150000042 =	SUA Server #10 Active	<0 (No)   1 (Yes)>	= 0
150000043 =	SUA Server #10 Protocol	<0 (All)   6 (TCP)   17 (UDP)>	= 0
150000044 =	SUA Server #10 Port Start		= 0
150000045 =	SUA Server #10 Port End		= 0
150000046 =	SUA Server #10 Local IP address		= 0.0.0.0
150000047 =	SUA Server #11 Active	<0 (No)   1 (Yes)>	= 0



**Table 170** Menu 15 SUA Server Setup (SMT Menu 15) (continued)

150000048 =	SUA Server #11 Protocol	<0 (All)   6 (TCP)   17 (UDP) >	= 0
150000049 =	SUA Server #11 Port Start		= 0
150000050 =	SUA Server #11 Port End		= 0
150000051 =	SUA Server #11 Local IP address		= 0.0.0.0
150000052 =	SUA Server #12 Active	<0 (No)   1 (Yes) >	= 0
150000053 =	SUA Server #12 Protocol	<0 (All)   6 (TCP)   17 (UDP) >	= 0
150000054 =	SUA Server #12 Port Start		= 0
150000055 =	SUA Server #12 Port End		= 0
150000056 =	SUA Server #12 Local IP address		= 0.0.0.0

**Table 171** Menu 21.1 Filter Set #1 (SMT Menu 21.1)

/ Menu 21 Filter set #1 (SMT Menu 21)			
FIN	FN	PVA	INPUT
210100001 =	Filter Set 1, Name	<Str>	=
/ Menu 21.1.1.1 set #1, rule #1 (SMT Menu 21.1.1.1)			
FIN	FN	PVA	INPUT
210101001 =	IP Filter Set 1, Rule 1 Type	<2 (TCP/IP) >	= 2
210101002 =	IP Filter Set 1, Rule 1 Active	<0 (No)   1 (Yes) >	= 1
210101003 =	IP Filter Set 1, Rule 1 Protocol		= 6
210101004 =	IP Filter Set 1, Rule 1 Dest IP address		= 0.0.0.0
210101005 =	IP Filter Set 1, Rule 1 Dest Subnet Mask		= 0
210101006 =	IP Filter Set 1, Rule 1 Dest Port		= 137
210101007 =	IP Filter Set 1, Rule 1 Dest Port Comp	<0 (none)   1 (equal)   2 (not equal)   3 (less)   4 (greater) >	= 1
210101008 =	IP Filter Set 1, Rule 1 Src IP address		= 0.0.0.0
210101009 =	IP Filter Set 1, Rule 1 Src Subnet Mask		= 0
210101010 =	IP Filter Set 1, Rule 1 Src Port		= 0
210101011 =	IP Filter Set 1, Rule 1 Src Port Comp	<0 (none)   1 (equal)   2 (not equal)   3 (less)   4 (greater) >	= 0
210101013 =	IP Filter Set 1, Rule 1 Act Match	<1 (check next)   2 (forward)   3 (drop) >	= 3
210101014 =	IP Filter Set 1, Rule 1 Act Not Match	<1 (check next)   2 (forward)   3 (drop) >	= 1

**Table 171** Menu 21.1 Filter Set #1 (SMT Menu 21.1) (continued)

/ Menu 21.1.1.2 set #1, rule #2 (SMT Menu 21.1.1.2)			
FIN	FN	PVA	INPUT
210102001 =	IP Filter Set 1,Rule 2 Type	<2 (TCP/IP)>	= 2
210102002 =	IP Filter Set 1,Rule 2 Active	<0 (No)  1 (Yes)>	= 1
210102003 =	IP Filter Set 1,Rule 2 Protocol		= 6
210102004 =	IP Filter Set 1,Rule 2 Dest IP address		= 0.0.0.0
210102005 =	IP Filter Set 1,Rule 2 Dest Subnet Mask		= 0
210102006 =	IP Filter Set 1,Rule 2 Dest Port		= 138
210102007 =	IP Filter Set 1,Rule 2 Dest Port Comp	<0 (none)  1 (equal)  2 (not equal)  3 (less)  4 (greater)>	= 1
210102008 =	IP Filter Set 1,Rule 2 Src IP address		= 0.0.0.0
210102009 =	IP Filter Set 1,Rule 2 Src Subnet Mask		= 0
210102010 =	IP Filter Set 1,Rule 2 Src Port		= 0
210102011 =	IP Filter Set 1,Rule 2 Src Port Comp	<0 (none)  1 (equal)  2 (not equal)  3 (less)  4 (greater)>	= 0
210102013 =	IP Filter Set 1,Rule 2 Act Match	<1 (check next)  2 (forward)  3 (drop)>	= 3
210102014 =	IP Filter Set 1,Rule 2 Act Not Match	<1 (check next)  2 (forward)  3 (drop)>	= 1
/ Menu 21.1.1.3 set #1, rule #3 (SMT Menu 21.1.1.3)			
FIN	FN	PVA	INPUT
210103001 =	IP Filter Set 1,Rule 3 Type	<2 (TCP/IP)>	= 2
210103002 =	IP Filter Set 1,Rule 3 Active	<0 (No)  1 (Yes)>	= 1
210103003 =	IP Filter Set 1,Rule 3 Protocol		= 6
210103004 =	IP Filter Set 1,Rule 3 Dest IP address		= 0.0.0.0
210103005 =	IP Filter Set 1,Rule 3 Dest Subnet Mask		= 0
210103006 =	IP Filter Set 1,Rule 3 Dest Port		= 139
210103007 =	IP Filter Set 1,Rule 3 Dest Port Comp	<0 (none)  1 (equal)  2 (not equal)  3 (less)  4 (greater)>	= 1
210103008 =	IP Filter Set 1,Rule 3 Src IP address		= 0.0.0.0
210103009 =	IP Filter Set 1,Rule 3 Src Subnet Mask		= 0
210103010 =	IP Filter Set 1,Rule 3 Src Port		= 0
210103011 =	IP Filter Set 1,Rule 3 Src Port Comp	<0 (none)  1 (equal)  2 (not equal)  3 (less)  4 (greater)>	= 0

**Table 171** Menu 21.1 Filter Set #1 (SMT Menu 21.1) (continued)

210103013 =	IP Filter Set 1,Rule 3 Act Match	<1 (check next)  2 (forward)   3 (drop)	= 3
210103014 =	IP Filter Set 1,Rule 3 Act Not Match	<1 (check next)  2 (forward)   3 (drop)	= 1
/ Menu 21.1.1.4 set #1, rule #4 (SMT Menu 21.1.1.4)			
FIN	FN	PVA	INPUT
210104001 =	IP Filter Set 1,Rule 4 Type	<2 (TCP/IP)>	= 2
210104002 =	IP Filter Set 1,Rule 4 Active	<0 (No)  1 (Yes)>	= 1
210104003 =	IP Filter Set 1,Rule 4 Protocol		= 17
210104004 =	IP Filter Set 1,Rule 4 Dest IP address		= 0.0.0.0
210104005 =	IP Filter Set 1,Rule 4 Dest Subnet Mask		= 0
210104006 =	IP Filter Set 1,Rule 4 Dest Port		= 137
210104007 =	IP Filter Set 1,Rule 4 Dest Port Comp	<0 (none)  1 (equal)  2 (not equal)  3 (less)  4 (greater)>	= 1
210104008 =	IP Filter Set 1,Rule 4 Src IP address		= 0.0.0.0
210104009 =	IP Filter Set 1,Rule 4 Src Subnet Mask		= 0
210104010 =	IP Filter Set 1,Rule 4 Src Port		= 0
210104011 =	IP Filter Set 1,Rule 4 Src Port Comp	<0 (none)  1 (equal)  2 (not equal)  3 (less)  4 (greater)>	= 0
210104013 =	IP Filter Set 1,Rule 4 Act Match	<1 (check next)  2 ( forward)   3 (drop)	= 3
210104014 =	IP Filter Set 1,Rule 4 Act Not Match	<1 (check next)  2 (forward)   3 (drop)	= 1
/ Menu 21.1.1.5 set #1, rule #5 (SMT Menu 21.1.1.5)			
FIN	FN	PVA	INPUT
210105001 =	IP Filter Set 1,Rule 5 Type	<2 (TCP/IP)>	= 2
210105002 =	IP Filter Set 1,Rule 5 Active	<0 (No)  1 (Yes)>	= 1
210105003 =	IP Filter Set 1,Rule 5 Protocol		= 17
210105004 =	IP Filter Set 1,Rule 5 Dest IP address		= 0.0.0.0
210105005 =	IP Filter Set 1,Rule 5 Dest Subnet Mask		= 0
210105006 =	IP Filter Set 1,Rule 5 Dest Port		= 138
210105007 =	IP Filter Set 1,Rule 5 Dest Port Comp	<0 (none)  1 (equal)  2 (not equal)  3 (less)  4 (greater)>	= 1
210105008 =	IP Filter Set 1,Rule 5 Src IP Address		= 0.0.0.0

**Table 171** Menu 21.1 Filter Set #1 (SMT Menu 21.1) (continued)

210105009 =	IP Filter Set 1,Rule 5 Src Subnet Mask		= 0
210105010 =	IP Filter Set 1,Rule 5 Src Port		= 0
210105011 =	IP Filter Set 1,Rule 5 Src Port Comp	<0 (none)  1 (equal)  2 (not equal)  3 (less)  4 (greater)>	= 0
210105013 =	IP Filter Set 1,Rule 5 Act Match	<1 (check next)  2 (forward)  3 (drop)>	= 3
210105014 =	IP Filter Set 1,Rule 5 Act Not Match	<1 (Check Next)  2 (Forward)  3 (Drop)>	= 1
/ Menu 21.1.1.6 set #1, rule #6 (SMT Menu 21.1.1.6)			
FIN	FN	PVA	INPUT
210106001 =	IP Filter Set 1,Rule 6 Type	<2 (TCP/IP)>	= 2
210106002 =	IP Filter Set 1,Rule 6 Active	<0 (No)  1 (Yes)>	= 1
210106003 =	IP Filter Set 1,Rule 6 Protocol		= 17
210106004 =	IP Filter Set 1,Rule 6 Dest IP address		= 0.0.0.0
210106005 =	IP Filter Set 1,Rule 6 Dest Subnet Mask		= 0
210106006 =	IP Filter Set 1,Rule 6 Dest Port		= 139
210106007 =	IP Filter Set 1,Rule 6 Dest Port Comp	<0 (none)  1 (equal)  2 (not equal)  3 (less)  4 (greater)>	= 1
210106008 =	IP Filter Set 1,Rule 6 Src IP address		= 0.0.0.0
210106009 =	IP Filter Set 1,Rule 6 Src Subnet Mask		= 0
210106010 =	IP Filter Set 1,Rule 6 Src Port		= 0
210106011 =	IP Filter Set 1,Rule 6 Src Port Comp	<0 (none)  1 (equal)  2 (not equal)  3 (less)  4 (greater)>	= 0
210106013 =	IP Filter Set 1,Rule 6 Act Match	<1 (check next)  2 (forward)  3 (drop)>	= 3
210106014 =	IP Filter Set 1,Rule 6 Act Not Match	<1 (check next)  2 (forward)  3 (drop)>	= 2

**Table 172** Menu 21.1 Filer Set #2, (SMT Menu 21.1)

/ Menu 21.1 filter set #2, (SMT Menu 21.1)			
FIN	FN	PVA	INPUT
210200001 =	Filter Set 2, Nam	<Str>	= NetBIOS_WAN

**Table 172** Menu 21.1 Filer Set #2, (SMT Menu 21.1) (continued)

/ Menu 21.1.2.1 Filter set #2, rule #1 (SMT Menu 21.1.2.1)			
FIN	FN	PVA	INPUT
210201001 =	IP Filter Set 2, Rule 1 Type	<0 (none)   2 (TCP/IP)>	= 2
210201002 =	IP Filter Set 2, Rule 1 Active	<0 (No)   1 (Yes)>	= 1
210201003 =	IP Filter Set 2, Rule 1 Protocol		= 6
210201004 =	IP Filter Set 2, Rule 1 Dest IP address		= 0.0.0.0
210201005 =	IP Filter Set 2, Rule 1 Dest Subnet Mask		= 0
210201006 =	IP Filter Set 2, Rule 1 Dest Port		= 137
210201007 =	IP Filter Set 2, Rule 1 Dest Port Comp	<0 (none)   1 (equal)   2 (not equal)   3 (less)   4 (greater)>	= 1
210201008 =	IP Filter Set 2, Rule 1 Src IP address		= 0.0.0.0
210201009 =	IP Filter Set 2, Rule 1 Src Subnet Mask		= 0
210201010 =	IP Filter Set 2, Rule 1 Src Port		= 0
210201011 =	IP Filter Set 2, Rule 1 Src Port Comp	<0 (none)   1 (equal)   2 (not equal)   3 (less)   4 (greater)>	= 0
210201013 =	IP Filter Set 2, Rule 1 Act Match	<1 (check next)   2 (forward)   3 (drop)>	= 3
210201014 =	IP Filter Set 2, Rule 1 Act Not Match	<1 (check next)   2 (forward)   3 (drop)>	= 1
/ Menu 21.1.2.2 Filter set #2, rule #2 (SMT Menu 21.1.2.2)			
FIN	FN	PVA	INPUT
210202001 =	IP Filter Set 2, Rule 2 Type	<0 (none)   2 (TCP/IP)>	= 2
210202002 =	IP Filter Set 2, Rule 2 Active	<0 (No)   1 (Yes)>	= 1
210202003 =	IP Filter Set 2, Rule 2 Protocol		= 6
210202004 =	IP Filter Set 2, Rule 2 Dest IP address		= 0.0.0.0
210202005 =	IP Filter Set 2, Rule 2 Dest Subnet Mask		= 0
210202006 =	IP Filter Set 2, Rule 2 Dest Port		= 138
210202007 =	IP Filter Set 2, Rule 2 Dest Port Comp	<0 (none)   1 (equal)   2 (not equal)   3 (less)   4 (greater)>	= 1
210202008 =	IP Filter Set 2, Rule 2 Src IP address		= 0.0.0.0

**Table 172** Menu 21.1 Filer Set #2, (SMT Menu 21.1) (continued)

210202009 =	IP Filter Set 2, Rule 2 Src Subnet Mask		= 0
210202010 =	IP Filter Set 2, Rule 2 Src Port		= 0
210202011 =	IP Filter Set 2, Rule 2 Src Port Comp	<0 (none)  1 (equal)  2 (not equal)  3 (less)  4 (greater)>	= 0
210202013 =	IP Filter Set 2, Rule 2 Act Match	<1 (check next)  2 (forward)  3 (drop)>	= 3
210202014 =	IP Filter Set 2, Rule 2 Act Not Match	<1 (check next)  2 (forward)  3 (drop)>	= 1
/ Menu 21.1.2.3 Filter set #2, rule #3 (SMT Menu 21.1.2.3)			
FIN	FN	PVA	INPUT
210203001 =	IP Filter Set 2, Rule 3 Type	<0 (none)  2 (TCP/IP)>	= 2
210203002 =	IP Filter Set 2, Rule 3 Active	<0 (No)  1 (Yes)>	= 1
210203003 =	IP Filter Set 2, Rule 3 Protocol		= 6
210203004 =	IP Filter Set 2, Rule 3 Dest IP address		= 0.0.0.0
210203005 =	IP Filter Set 2, Rule 3 Dest Subnet Mask		= 0
210203006 =	IP Filter Set 2, Rule 3 Dest Port		= 139
210203007 =	IP Filter Set 2, Rule 3 Dest Port Comp	<0 (none)  1 (equal)  2 (not equal)  3 (less)  4 (greater)>	= 1
210203008 =	IP Filter Set 2, Rule 3 Src IP address		= 0.0.0.0
210203009 =	IP Filter Set 2, Rule 3 Src Subnet Mask		= 0
210203010 =	IP Filter Set 2, Rule 3 Src Port		= 0
210203011 =	IP Filter Set 2, Rule 3 Src Port Comp	<0 (none)  1 (equal)  2 (not equal)  3 (less)  4 (greater)>	= 0
210203013 =	IP Filter Set 2, Rule 3 Act Match	<1 (check next)  2 (forward)  3 (drop)>	= 3
210203014 =	IP Filter Set 2, Rule 3 Act Not Match	<1 (check next)  2 (forward)  3 (drop)>	= 1
/ Menu 21.1.2.4 Filter set #2, rule #4 (SMT Menu 21.1.2.4)			
FIN	FN	PVA	INPUT
210204001 =	IP Filter Set 2, Rule 4 Type	<0 (none)  2 (TCP/IP)>	= 2

**Table 172** Menu 21.1 Filer Set #2, (SMT Menu 21.1) (continued)

210204002 =	IP Filter Set 2, Rule 4 Active		<0 (No)   1 (Yes) > = 1
210204003 =	IP Filter Set 2, Rule 4 Protocol		= 17
210204004 =	IP Filter Set 2, Rule 4 Dest IP address		= 0.0.0.0
210204005 =	IP Filter Set 2, Rule 4 Dest Subnet Mask		= 0
210204006 =	IP Filter Set 2, Rule 4 Dest Port		= 137
210204007 =	IP Filter Set 2, Rule 4 Dest Port Comp	<0 (none)   1 (equal)   2 (not equal)   3 (less)   4 (greater) >	= 1
210204008 =	IP Filter Set 2, Rule 4 Src IP address		= 0.0.0.0
210204009 =	IP Filter Set 2, Rule 4 Src Subnet Mask		= 0
210204010 =	IP Filter Set 2, Rule 4 Src Port		= 0
210204011 =	IP Filter Set 2, Rule 4 Src Port Comp	<0 (none)   1 (equal)   2 (not equal)   3 (less)   4 (greater) >	= 0
210204013 =	IP Filter Set 2, Rule 4 Act Match	<1 (check next)   2 (forward)   3 (drop) >	= 3
210204014 =	IP Filter Set 2, Rule 4 Act Not Match	<1 (check next)   2 (forward)   3 (drop) >	= 1
/ Menu 21.1.2.5 Filter set #2, rule #5 (SMT Menu 21.1.2.5)			
FIN	FN	PVA	INPUT
210205001 =	IP Filter Set 2, Rule 5 Type	<0 (none)   2 (TCP/IP) >	= 2
210205002 =	IP Filter Set 2, Rule 5 Active	<0 (No)   1 (Yes) >	= 1
210205003 =	IP Filter Set 2, Rule 5 Protocol		= 17
210205004 =	IP Filter Set 2, Rule 5 Dest IP address		= 0.0.0.0
210205005 =	IP Filter Set 2, Rule 5 Dest Subnet Mask		= 0
210205006 =	IP Filter Set 2, Rule 5 Dest Port		= 138
210205007 =	IP Filter Set 2, Rule 5 Dest Port Comp	<0 (none)   1 (equal)   2 (not equal)   3 (less)   4 (greater) >	= 1
210205008 =	IP Filter Set 2, Rule 5 Src IP address		= 0.0.0.0
210205009 =	IP Filter Set 2, Rule 5 Src Subnet Mask		= 0
210205010 =	IP Filter Set 2, Rule 5 Src Port		= 0

**Table 172** Menu 21.1 Filer Set #2, (SMT Menu 21.1) (continued)

210205011 =	IP Filter Set 2, Rule 5 Src Port Comp	<0 (none)  1 (equal)  2 (not equal)  3 (less)  4 (greater)>	= 0
210205013 =	IP Filter Set 2, Rule 5 Act Match	<1 (check next)  2 (forward)  3 (drop)>	= 3
210205014 =	IP Filter Set 2, Rule 5 Act Not Match	<1 (check next)  2 (forward)  3 (drop)>	= 1
/ Menu 21.1.2.6 Filter set #2, rule #6 (SMT Menu 21.1.2.5)			
FIN	FN	PVA	INPUT
210206001 =	IP Filter Set 2, Rule 6 Type	<0 (none)  2 (TCP/IP)>	= 2
210206002 =	IP Filter Set 2, Rule 6 Active	<0 (No)  1 (Yes)>	= 1
210206003 =	IP Filter Set 2, Rule 6 Protocol		= 17
210206004 =	IP Filter Set 2, Rule 6 Dest IP address		= 0.0.0.0
210206005 =	IP Filter Set 2, Rule 6 Dest Subnet Mask		= 0
210206006 =	IP Filter Set 2, Rule 6 Dest Port		= 139
210206007 =	IP Filter Set 2, Rule 6 Dest Port Comp	<0 (none)  1 (equal)  2 (not equal)  3 (less)  4 (greater)>	= 1
210206008 =	IP Filter Set 2, Rule 6 Src IP address		= 0.0.0.0
210206009 =	IP Filter Set 2, Rule 6 Src Subnet Mask		= 0
210206010 =	IP Filter Set 2, Rule 6 Src Port		= 0
210206011 =	IP Filter Set 2, Rule 6 Src Port Comp	<0 (none)  1 (equal)  2 (not equal)  3 (less)  4 (greater)>	= 0
210206013 =	IP Filter Set 2, Rule 6 Act Match	<1 (check next)  2 (forward)  3 (drop)>	= 3
210206014 =	IP Filter Set 2, Rule 6 Act Not Match	<1 (check next)  2 (forward)  3 (drop)>	= 2
241100005 =	FTP Server Access	<0 (all)  1 (none)  2 (LAN)  3 (Wan)>	= 0
241100006 =	FTP Server Secured IP address		= 0.0.0.0
241100007 =	WEB Server Port		= 80
241100008 =	WEB Server Access	<0 (all)  1 (none)  2 (LAN)  3 (Wan)>	= 0
241100009 =	WEB Server Secured IP address		= 0.0.0.0



**Table 173** Menu 23 System Menus (SMT Menu 23)

*/ Menu 23.1 System Password Setup (SMT Menu 23.1)			
FIN	FN	PVA	INPUT
230000000 =	System Password		= 1234
*/ Menu 23.2 System security: radius server (SMT Menu 23.2)			
FIN	FN	PVA	INPUT
230200001 =	Authentication Server Configured	<0 (No)   1 (Yes)>	= 1
230200002 =	Authentication Server Active	<0 (No)   1 (Yes)>	= 1
230200003 =	Authentication Server IP Address		= 192.168.1.32
230200004 =	Authentication Server Port		= 1822
230200005 =	Authentication Server Shared Secret		= 111111111111 111 111111111111 1111
230200006 =	Accounting Server Configured	<0 (No)   1 (Yes)>	= 1
230200007 =	Accounting Server Active	<0 (No)   1 (Yes)>	= 1
230200008 =	Accounting Server IP Address		= 192.168.1.44
230200009 =	Accounting Server Port		= 1823
230200010 =	Accounting Server Shared Secret		= 1234
*/ Menu 23.4 System security: IEEE802.1x (SMT Menu 23.4)			
FIN	FN	PVA	INPUT
230400001 =	Wireless Port Control	<0 (Authentication Required)   1 (No Access Allowed)   2 (No Authentication Required)>	= 2
230400002 =	ReAuthentication Timer (in second)		= 555
230400003 =	Idle Timeout (in second)		= 999
230400004 =	Authentication Databases	<0 (Local User Database Only)   1 (RADIUS Only)   2 (Local, RADIUS)   3 (RADIUS, Local)>	= 1
230400005 =	Key Management Protocol	<0 (8021x)   1 (WPA)   2 (WPAPSK)>	= 0
230400006 =	Dynamic WEP Key Exchange	<0 (Disable)   1 (64-bit WEP)   2 (128-bit WEP)>	= 0
230400007 =	PSK =		=

**Table 173** Menu 23 System Menus (SMT Menu 23) (continued)

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

**Table 174** Menu 24.11 Remote Management Control (SMT Menu 24.11)

/ Menu 24.11 Remote Management Control (SMT Menu 24.11)			
FIN	FN	PVA	INPUT
241100001 =	TELNET Server Port		= 23
241100002 =	TELNET Server Access	<0 (all)   1 (none)   2 (LAN)   3 (Wan)>	= 0
241100003 =	TELNET Server Secured IP address		= 0.0.0.0
241100004 =	FTP Server Port		= 21
241100005 =	FTP Server Access	<0 (all)   1 (none)   2 (LAN)   3 (Wan)>	= 0
241100006 =	FTP Server Secured IP address		= 0.0.0.0
241100007 =	WEB Server Port		= 80
241100008 =	WEB Server Access	<0 (all)   1 (none)   2 (LAN)   3 (Wan)>	= 0
241100009 =	WEB Server Secured IP address		= 0.0.0.0

## Command Examples

The following are example Internal SPTGEN screens associated with the Prestige's command interpreter commands.

**Table 175** Command Examples

FIN	FN	PVA	INPUT
/ci command (for annex a): wan adsl opencmd			
990000001 =	ADSL OPMD	<0 (glite)   1 (t1.413)   2 (gdm)   3 (multimode)>	= 3
/ci command (for annex B): wan adsl opencmd			

**Table 175** Command Examples (continued)

	<b>FIN</b>	<b>FN</b>	<b>PVA</b>	<b>INPUT</b>
	FIN	FN	PVA	INPUT
	990000001 =	ADSL OPMD	<0(etsi) 1(normal)  2(gdmt) 3(multimo de)>	= 3



# APPENDIX J

## Command Interpreter

The following describes how to use the command interpreter. Enter 24 in the main menu to bring up the system maintenance menu. Enter 8 to go to **Menu 24.8 - Command Interpreter Mode**. See the included disk or [zyxel.com](http://zyxel.com) for more detailed information on these commands.

**Note:** Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.

### Command Syntax

- The command keywords are in `courier new` font.
- Enter the command keywords exactly as shown, do not abbreviate.
- The required fields in a command are enclosed in angle brackets `<>`.
- The optional fields in a command are enclosed in square brackets `[]`.
- The `|` symbol means or.

For example,

```
sys filter netbios config <type> <on|off>
```

means that you must specify the type of netbios filter and whether to turn it on or off.

### Command Usage

A list of valid commands can be found by typing `help` or `?` at the command prompt. Always type the full command. Type `exit` to return to the SMT main menu when finished.



# APPENDIX K

## Firewall Commands

### Sys Firewall Commands

The following describes the firewall commands. See the Command Interpreter appendix for information on the command structure. Each of these commands must be preceded by `sys firewall` when you use them. For example, type `sys firewall active yes` to turn on the firewall.

**Table 176** Sys Firewall Commands

Command		Description
acl		
	disp	Displays ACLs or a specific ACL set # and rule #.
active	<yes no>	Active firewall or deactivate firewall Enables/disables the firewall.
cnt		
	disp	Displays the firewall log type and count.
	clear	Clears the firewall log count.
pktdump		Dumps the last 64 bytes of packets that the firewall has dropped.
dynamicrule	display	Displays the firewall's dynamic rules.
tcprst		
	rst	Turns TCP reset sending on/off.
	rst113	Turns TCP reset sending for port 113 on/off.
	display	Displays the TCP reset sending settings.
icmp		This rule is not in use.
dos		
	smtp	Enables/disables the SMTP DoS defender.
	display	Displays the SMTP DoS defender setting.
	ignore	Sets if the firewall will ignore DoS attacks on the lan/wan.
ignore		
	dos	Sets if the firewall will ignore DoS attacks on the lan/wan.
	triangle	Sets if the firewall will ignore triangle route packets on the lan/wan.





# APPENDIX L

## Boot Commands

The BootModule AT commands execute from within the router's bootup software, when debug mode is selected before the main router firmware is started. When you start up your Prestige, you are given a choice to go into debug mode by pressing a key at the prompt shown in the following screen. In debug mode you have access to a series of boot module commands, for example ATUR (for uploading firmware) and ATLC (for uploading the configuration file). These are already discussed in the **Firmware and Configuration File Maintenance** chapter.

**Figure 293** Option to Enter Debug Mode

```
Bootbase Version: V1.02 | 08/08/2001 15:40:50
RAM: Size = 16384 Kbytes
DRAM Post: Testing: 16384K OK
FLASH: Intel 16M
RAS Version: V3.50(WB.0)b3 | 08/08/2001 16:21:27
Press any key to enter debug mode within 3
seconds.
.....
```

Enter ATHE to view all available Prestige boot module commands as shown in the next screen. ATBAx allows you to change the console port speed. The x denotes the number preceding the colon to give the console port speed following the colon in the list of numbers that follows; for example ATBA3 will give a console port speed of 9.6 Kbps. ATSE displays the seed that is used to generate a password to turn on the debug flag in the firmware. The ATSH command shows product related information such as boot module version, vendor name, product model, RAS code revision, etc. ATGO allows you to continue booting the system. Most other commands aid in advanced troubleshooting and should only be used by qualified engineers.

**Figure 294** Boot Module Commands

AT	just answer OK
ATHE	print help
ATBAx	change baudrate. 1:38.4k, 2:19.2k, 3:9.6k 4:57.6k 5:115.2k
ATENx, (y)	set BootExtension Debug Flag (y=password)
ATSE	show the seed of password generator
ATTI(h,m,s)	change system time to hour:min:sec or show current time
ATDA(y,m,d)	change system date to year/month/day or show current date
ATDS	dump RAS stack
ATDT	dump Boot Module Common Area
ATDUx,y	dump memory contents from address x for length y
ATRBx	display the 8-bit value of address x
ATRWx	display the 16-bit value of address x
ATRLx	display the 32-bit value of address x
ATGO(x)	run program at addr x or boot router
ATGR	boot router
ATGT	run Hardware Test Program
ATRTw,x,y(,z)	RAM test level w, from address x to y (z iterations)
ATSH	dump manufacturer related data in ROM
ATDOx,y	download from address x for length y to PC via XMODEM
ATTD	download router configuration to PC via XMODEM
ATUR	upload router firmware to flash ROM
ATLC	upload router configuration file to flash ROM
ATXSx	xmodem select: x=0: CRC mode(default); x=1: checksum mode
ATSR	system reboot

# APPENDIX M

## Log Descriptions

This appendix provides descriptions of example log messages.

**Table 177** System Maintenance Logs

LOG MESSAGE	DESCRIPTION
Time calibration is successful	The router has adjusted its time based on information from the time server.
Time calibration failed	The router failed to get information from the time server.
WAN interface gets IP: %s	A WAN interface got a new IP address from the DHCP, PPPoE, PPTP or dial-up server.
DHCP client IP expired	A DHCP client's IP address has expired.
DHCP server assigns %s	The DHCP server assigned an IP address to a client.
Successful SMT login	Someone has logged on to the router's SMT interface.
SMT login failed	Someone has failed to log on to the router's SMT interface.
Successful WEB login	Someone has logged on to the router's web configurator interface.
WEB login failed	Someone has failed to log on to the router's web configurator interface.
Successful TELNET login	Someone has logged on to the router via telnet.
TELNET login failed	Someone has failed to log on to the router via telnet.
Successful FTP login	Someone has logged on to the router via ftp.
FTP login failed	Someone has failed to log on to the router via ftp.
NAT Session Table is Full!	The maximum number of NAT session table entries has been exceeded and the table is full.
Starting Connectivity Monitor	Starting Connectivity Monitor.
Time initialized by Daytime Server	The router got the time and date from the Daytime server.
Time initialized by Time server	The router got the time and date from the time server.
Time initialized by NTP server	The router got the time and date from the NTP server.
Connect to Daytime server fail	The router was not able to connect to the Daytime server.
Connect to Time server fail	The router was not able to connect to the Time server.
Connect to NTP server fail	The router was not able to connect to the NTP server.
Too large ICMP packet has been dropped	The router dropped an ICMP packet that was too large.
SMT Session Begin	An SMT management session has started.
SMT Session End	An SMT management session has ended.

**Table 177** System Maintenance Logs (continued)

LOG MESSAGE	DESCRIPTION
Configuration Change: PC = 0x%x, Task ID = 0x%x	The router is saving configuration changes.
Successful SSH login	Someone has logged on to the router's SSH server.
SSH login failed	Someone has failed to log on to the router's SSH server.
Successful HTTPS login	Someone has logged on to the router's web configurator interface using HTTPS protocol.
HTTPS login failed	Someone has failed to log on to the router's web configurator interface using HTTPS protocol.

**Table 178** System Error Logs

LOG MESSAGE	DESCRIPTION
%s exceeds the max. number of session per host!	This attempt to create a NAT session exceeds the maximum number of NAT session table entries allowed to be created per host.
setNetBIOSFilter: calloc error	The router failed to allocate memory for the NetBIOS filter settings.
readNetBIOSFilter: calloc error	The router failed to allocate memory for the NetBIOS filter settings.
WAN connection is down.	A WAN connection is down. You cannot access the network through this interface.

**Table 179** 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 180** TCP Reset Logs

LOG MESSAGE	DESCRIPTION
Under SYN flood attack, sent TCP RST	The router sent a TCP reset packet when a host was under a SYN flood attack (the TCP incomplete count is per destination host.)
Exceed TCP MAX incomplete, sent TCP RST	The router sent a TCP reset packet when the number of TCP incomplete connections exceeded the user configured threshold. (the TCP incomplete count is per destination host.) Note: Refer to <b>TCP Maximum Incomplete</b> in the <b>Firewall Attack Alerts</b> screen.
Peer TCP state out of order, sent TCP RST	The router sent a TCP reset packet when a TCP connection state was out of order. Note: The firewall refers to RFC793 Figure 6 to check the TCP state.
Firewall session time out, sent TCP RST	The router sent a TCP reset packet when a dynamic firewall session timed out. Default timeout values: ICMP idle timeout (s): 60 UDP idle timeout (s): 60 TCP connection (three way handshaking) timeout (s): 30 TCP FIN-wait timeout (s): 60 TCP idle (established) timeout (s): 3600
Exceed MAX incomplete, sent TCP RST	The router sent a TCP reset packet when the number of incomplete connections (TCP and UDP) exceeded the user-configured threshold. (Incomplete count is for all TCP and UDP connections through the firewall.) Note: When the number of incomplete connections (TCP + UDP) > "Maximum Incomplete High", the router sends TCP RST packets for TCP connections and destroys TOS (firewall dynamic sessions) until incomplete connections < "Maximum Incomplete Low".
Access block, sent TCP RST	The router sends a TCP RST packet and generates this log if you turn on the firewall TCP reset mechanism (via CLI command: "sys firewall tcprst").

**Table 181** 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 190 on page 501](#).

**Table 182** 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.

**Table 182** ICMP Logs (continued)

LOG MESSAGE	DESCRIPTION
Triangle route packet forwarded: ICMP	The firewall allowed a triangle route session to pass through.
Packet without a NAT table entry blocked: ICMP	The router blocked a packet that didn't have a corresponding NAT table entry.
Unsupported/out-of-order ICMP: ICMP	The firewall does not support this kind of ICMP packets or the ICMP packets are out of order.
Router reply ICMP packet: ICMP	The router sent an ICMP reply packet to the sender.

**Table 183** CDR Logs

LOG MESSAGE	DESCRIPTION
board %d line %d channel %d, call %d, %s C01 Outgoing Call dev=%x ch=%x %s	The router received the setup requirements for a call. "call" is the reference (count) number of the call. "dev" is the device type (3 is for dial-up, 6 is for PPPoE, 10 is for PPTP). "channel" or "ch" is the call channel ID. For example, "board 0 line 0 channel 0, call 3, C01 Outgoing Call dev=6 ch=0" Means the router has dialed to the PPPoE server 3 times.
board %d line %d channel %d, call %d, %s C02 OutCall Connected %d %s	The PPPoE, PPTP or dial-up call is connected.
board %d line %d channel %d, call %d, %s C02 Call Terminated	The PPPoE, PPTP or dial-up call was disconnected.

**Table 184** PPP Logs

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

**Table 185** UPnP Logs

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

**Table 186** Content Filtering Logs

LOG MESSAGE	DESCRIPTION
%s: block keyword	The content of a requested web page matched a user defined keyword.
%s	The system forwarded web content.

For type and code details, see [Table 190 on page 501](#).

**Table 187** 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.

**Table 187** Attack Logs (continued)

LOG MESSAGE	DESCRIPTION
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.

**Table 188** 802.1X Logs

LOG MESSAGE	DESCRIPTION
Local User Database accepts user.	A user was authenticated by the local user database.
Local User Database reports user credential error.	A user was not authenticated by the local user database because of an incorrect user password.
Local User Database does not find user`s credential.	A user was not authenticated by the local user database because the user is not listed in the local user database.
RADIUS accepts user.	A user was authenticated by the RADIUS Server.
RADIUS rejects user. Pls check RADIUS Server.	A user was not authenticated by the RADIUS Server. Please check the RADIUS Server.
Local User Database does not support authentication method.	The local user database only supports the EAP-MD5 method. A user tried to use another authentication method and was not authenticated.
User logout because of session timeout expired.	The router logged out a user whose session expired.
User logout because of user deassociation.	The router logged out a user who ended the session.
User logout because of no authentication response from user.	The router logged out a user from which there was no authentication response.
User logout because of idle timeout expired.	The router logged out a user whose idle timeout period expired.
User logout because of user request.	A user logged out.
Local User Database does not support authentication method.	A user tried to use an authentication method that the local user database does not support (it only supports EAP-MD5).
No response from RADIUS. Pls check RADIUS Server.	There is no response message from the RADIUS server, please check the RADIUS server.
Use Local User Database to authenticate user.	The local user database is operating as the authentication server.
Use RADIUS to authenticate user.	The RADIUS server is operating as the authentication server.



**Table 188** 802.1X Logs (continued)

LOG MESSAGE	DESCRIPTION
No Server to authenticate user.	There is no authentication server to authenticate a user.
Local User Database does not find user's credential.	A user was not authenticated by the local user database because the user is not listed in the local user database.

**Table 189** ACL Setting Notes

PACKET DIRECTION	DIRECTION	DESCRIPTION
(L to W)	LAN to WAN	ACL set for packets traveling from the LAN to the WAN.
(W to L)	WAN to LAN	ACL set for packets traveling from the WAN to the LAN.
(L to L/Prestige)	LAN to LAN/ Prestige	ACL set for packets traveling from the LAN to the LAN or the Prestige.
(W to W/Prestige)	WAN to WAN/ Prestige	ACL set for packets traveling from the WAN to the WAN or the Prestige.

**Table 190** ICMP Notes

TYPE	CODE	DESCRIPTION
0		Echo Reply
	0	Echo reply message
3		Destination Unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)
	5	Source route failed
4		Source Quench
	0	A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host
8		Echo
	0	Echo message

**Table 190** ICMP Notes (continued)

TYPE	CODE	DESCRIPTION
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp Reply
	0	Timestamp reply message
15		Information Request
	0	Information request message
16		Information Reply
	0	Information reply message

**Table 191** Syslog Logs

LOG MESSAGE	DESCRIPTION
<pre>&lt;Facility*8 + Severity&gt;Mon dd hr:mm:ss hostname src="&lt;srcIP:srcPort&gt;" dst="&lt;dstIP:dstPort&gt;" msg="&lt;msg&gt;" note="&lt;note&gt;" devID="&lt;mac address last three numbers&gt;" cat="&lt;category&gt;"</pre>	<p>"This message is sent by the system ("RAS" displays as the system name if you haven't configured one) when the router generates a syslog. The facility is defined in the web MAIN MENU-&gt;LOGS-&gt;Log Settings page. The severity is the log's syslog class. The definition of messages and notes are defined in the various log charts throughout this appendix. The "devID" is the last three characters of the MAC address of the router's LAN port. The "cat" is the same as the category in the router's logs.</p>

**Table 192** 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 193** 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 194** 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 195** 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 196** 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.

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 197** 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
DEL	Delete
VID	Vendor ID

## Log Commands

Go to the command interpreter interface ([Appendix J on page 489](#) explains how to access and use the commands).

### Configuring What You Want the Prestige to Log

- 1 Use the `sys logs load` command to load the log setting buffer that allows you to configure which logs the Prestige is to record.
- 2 Use `sys logs category` to view a list of the log categories.

**Figure 295** Displaying Log Categories Example

```

Copyright (c) 1994 - 2004 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys          exit          ether          wan
wlan         ip            bridge        lan
radius       8021x         dsp           voiceradius   8021x
ras>
    
```

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

**Figure 296** Displaying Log Parameters Example

```
ras> sys logs category access
Usage: [0:none/1:log/2:alert/3:both]
ras>
```

- 4 Use `sys logs category` followed by a log category and a parameter to decide what to record.

Use 0 to not record logs for that category, 1 to record only logs for that category, 2 to record only alerts for that category, and 3 to record both logs and alerts for that category. Not every parameter is available with every category.

- 5 Use the `sys logs save` command to store the settings in the Prestige (you must do this in order to record logs).

## Displaying Logs

- Use the `sys logs display` command to show all of the logs in the Prestige's log.
- Use the `sys logs category display` command to show the log settings for all of the log categories.
- Use the `sys logs display [log category]` command to show the logs in an individual Prestige log category.
- Use the `sys logs clear` command to erase all of the Prestige's logs.

## Log Command Example

This example shows how to set the Prestige to record the access logs and alerts and then view the results.

**Figure 297** Log Command Example

```
ras> sys logs load
ras> sys logs category access 3
ras> sys logs save
ras> sys logs display access
# .time                source                destination           notes
message
7|01/01/2000 09:40:13 |192.168.1.1:3        |192.168.1.33:1      |ACCESS FO
RWARD
Router reply ICMP packet: ICMP(type:3, code:1)
8|01/01/2000 09:40:07 |192.168.1.1:3        |192.168.1.33:1      |ACCESS FO
RWARD
Router reply ICMP packet: ICMP(type:3, code:1)
9|01/01/2000 09:40:04 |192.168.1.1:3        |192.168.1.33:1      |ACCESS FO
RWARD
Router reply ICMP packet: ICMP(type:3, code:1)
10|01/01/2000 09:40:04 |192.168.1.33:1199   |207.69.188.186:110  |ACCESS FO
RWARD
Firewall default policy: TCP (L to W)
11|01/01/2000 09:40:04 |192.168.1.1:53      |192.168.1.33:1200   |ACCESS FO
RWARD
none: UDP
```

# Index

## Numerics

110V AC [5](#)  
 230V AC [5](#)  
 64kbps [140](#)  
 8kbps [140](#)

## A

Abnormal Working Conditions [6](#)  
 AbS [136](#)  
 AC [5](#)  
 Access methods [329](#)  
 Accessories [5](#)  
 ACK Message [132](#)  
 Acts of God [6](#)  
 Address mapping [127](#)  
 Address Resolution Protocol (ARP) [83](#)  
 Ad-hoc Configuration [452](#)  
 ADSL Standards [45](#), [51](#)  
 ADSL, what is it? [44](#)  
 AH [197](#)  
 AH (Authentication Header) [405](#)  
 AH Protocol [201](#)  
 Airflow [5](#)  
 ALG [47](#), [135](#)  
 Allow Asymmetrical Route [173](#)  
 Alternative Subnet Mask Notation [443](#)  
 American Wire Gauge [5](#)  
 Analysis-by-Synthesis [136](#)  
 antenna [49](#)  
 Any IP [48](#), [82](#)  
   How it works [83](#)  
   note [83](#)  
 Any IP Setup [85](#)  
 Any IP Table [258](#)  
 AP (access point) [87](#)  
 Application Layer Gateway [47](#), [135](#)  
 Application-level Firewalls [155](#)  
 Applications  
   Internet access [53](#)  
 Association List [259](#)  
 AT command [366](#)  
 ATM layer options [302](#)  
 ATM Loopback Test [261](#)  
 ATM QoS Type [293](#)  
 ATM Status [261](#)  
 Attack Alert [189](#)  
 Attack Types [160](#)  
 Authentication [297](#), [298](#)  
 Authentication databases [101](#)  
 authentication databases [353](#)  
 Authentication Header [201](#)  
 Authentication Password [73](#), [138](#)  
 Authentication protocol [298](#)  
 Authentication User ID [72](#), [138](#)  
 Authority [4](#)  
 auto-Crossover [50](#)  
 auto-negotiation [50](#)  
 Auto-provisioning [47](#)  
 AWG [5](#)

## B

Backup [366](#)  
 Backup Type [116](#)  
 Basement [5](#)  
 Basic Service Set [452](#)  
 Blocking Time [188](#), [189](#)  
 Bridging [298](#), [309](#)  
   Ether Address [311](#)  
   Ethernet [309](#)  
   Ethernet Addr Timeout [310](#)  
   Remote Node [309](#)  
   Static Route Setup [311](#)  
 Brute-force Attack, [159](#)  
 BSS [452](#)  
 Budget Management [382](#), [383](#)  
 BYE Request [132](#)

## C

CA [457](#)  
 Cables, Connecting [5](#)

Call filtering [331](#)  
Call filters  
  Built-in [331](#)  
  User-defined [331](#)  
Call Scheduling [399](#)  
  Maximum Number of Schedule Sets [399](#)  
  PPPoE [401](#)  
  Precedence [399](#)  
  Precedence Example [399](#)  
Caller ID [73](#), [138](#)  
CBR [293](#)  
CBR (Continuous Bit Rate) [113](#)  
CCK [49](#)  
CDR [361](#)  
CDR (Call Detail Record) [360](#)  
CE regulations [49](#)  
Certificate Authority [457](#)  
Certifications [4](#)  
change password at login [58](#)  
Changes or Modifications [4](#)  
Channel [87](#)  
  Interference [87](#)  
Channel ID [286](#)  
CHAP [297](#)  
Charge [6](#)  
Circuit [4](#)  
Class B [4](#)  
Class of Service [141](#)  
Class of Service (CoS) [141](#)  
Client-server Protocol [132](#)  
Codec [136](#), [140](#)  
Codecs [47](#)  
Coder/Decoder [136](#), [140](#)  
Collision [356](#)  
Collisions [257](#)  
Comfort Noise Generation [143](#)  
Command Interpreter Mode [381](#)  
Communications [4](#)  
Community [346](#)  
Complementary Code Keying Modulation [49](#)  
Compliance, FCC [4](#)  
Components [6](#)  
Computer [43](#)  
Computer Name [273](#)  
Condition [6](#)  
Conditions that prevent TFTP and FTP from working over WAN [368](#)  
Configuration [73](#), [257](#)  
configuration file [365](#)  
Connecting Cables [5](#)  
Consequential Damages [6](#)

Console Port [265](#)  
  Configuration File Upload [378](#)  
  File Backup [370](#)  
  File Upload [377](#)  
  Restoring Files [373](#)  
Contact Information [7](#)  
Contacting Customer Support [7](#)  
Content Filtering [191](#)  
  Categories [191](#)  
  Schedule [192](#)  
  Trusted computers [193](#)  
  URL keyword blocking [191](#)  
Content filtering [191](#)  
content filtering [48](#)  
Continuous Bit Rate [293](#)  
Copyright [3](#)  
Correcting Interference [4](#)  
Corrosive Liquids [5](#)  
CoS [141](#)  
Cost Of Transmission [300](#), [307](#)  
Country Code [358](#)  
Covers [5](#)  
CPU Load [357](#)  
CTS (Clear to Send) [88](#)  
Custom Ports  
  Creating/Editing [179](#)  
Customer Support [7](#)  
Customized Services [179](#)  
Customized services [179](#)

## D

Damage [5](#)  
Dampness [5](#)  
Danger [5](#)  
Data Confidentiality [196](#)  
Data encryption [90](#)  
Data Filtering [331](#)  
Data Integrity [196](#)  
Data Origin Authentication [196](#)  
data privacy [352](#)  
Daylight Savings [152](#)  
DBPSK [49](#)  
Dealer [4](#)  
default LAN IP address [57](#)  
default user name and password [57](#)  
Defective [6](#)  
Denial of Service [156](#), [157](#), [188](#), [329](#)  
Denmark, Contact Information [7](#)



Destination Address [171](#)  
Device Filter rules [340](#)  
Device rule [340](#)  
DH [216](#)  
DHCP [51](#), [73](#), [80](#), [81](#), [149](#), [257](#), [358](#)  
DHCP client [51](#)  
DHCP relay [51](#)  
DHCP server [51](#)  
DHCP Table [257](#)  
Diagnostic Screens [260](#)  
Diagnostic Tools [355](#)  
Dialing Interval [144](#)  
Differential Binary Phase Shift Keyed Modulation [49](#)  
Differential Quadrature Phase Shift Keying Modulation [49](#)  
Differentiated Services [141](#)  
Diffie-Hellman Key Groups [216](#)  
DiffServ [141](#)  
DiffServ Code Point (DSCP) [141](#)  
DiffServ Code Points [141](#)  
DiffServ marking rule [141](#)  
Digital Subscriber Line Access Multiplexer [52](#)  
Direct Sequence Spread Spectrum [451](#)  
Disclaimer [3](#)  
Discretion [6](#)  
Distribution System [452](#)  
Distribution System (DS) [97](#)  
DNS [283](#)  
DNS Server  
    For VPN Host [205](#)  
DNS server [409](#)  
DNS Server Address [80](#)  
DNS Server Address Assignment [80](#)  
Domain Name [80](#), [123](#)  
Domain Name System [80](#)  
DoS [157](#)  
    Basics [157](#)  
    Types [158](#)  
DoS (Denial of Service) [48](#)  
DoS attacks, types of [158](#)  
Downstream Noise Margin [261](#)  
DQPSK [49](#)  
DS [452](#)  
DS Field [141](#)  
DS field [141](#)  
DSCPs [141](#)  
DSL (Digital Subscriber Line) [43](#)  
DSL, What Is It? [43](#)  
DSLAM [52](#)  
DSLAM (Digital Subscriber Line Access Multiplexer) [53](#)

DSSS [451](#)  
DTMF [136](#)  
DTMF Mode [140](#)  
Dual-Tone MultiFrequency [136](#)  
Dust [5](#)  
Dynamic DNS [50](#), [149](#), [274](#)  
dynamic DNS [50](#)  
Dynamic Host Configuration Protocol [51](#)  
Dynamic Jitter Buffer [46](#)  
Dynamic Secure Gateway Address [203](#)  
Dynamic WEP key exchange [101](#)  
dynamic WEP key exchange [352](#)  
DYNDNS Wildcard [149](#)

## E

EAP [89](#), [94](#), [95](#)  
EAP Authentication [457](#)  
    MD5 [457](#)  
    TLS [457](#)  
    TTLS [457](#)  
EAP authentication [351](#)  
EAP Authentication Sequence [95](#)  
ECHO [123](#)  
Echo Cancellation [47](#), [143](#)  
Electric Shock [5](#)  
Electrical Pipes [5](#)  
Electrocution [5](#)  
E-mail  
    Log Example [251](#)  
embedded help [59](#)  
Emergency Numbers [146](#)  
Encapsulated Routing Link Protocol (ENET ENCAP) [63](#)  
Encapsulation [52](#), [63](#), [65](#), [197](#), [293](#), [296](#)  
    ENET ENCAP [63](#)  
    PPP over Ethernet [63](#)  
    PPPoA [63](#)  
    RFC 1483 [64](#)  
encapsulation [52](#)  
Encapsulation Security Payload [202](#)  
Encryption [96](#), [195](#)  
Equal Value [6](#)  
Error Log [359](#)  
Errors [257](#)  
ESP [197](#)  
ESP Protocol [202](#)  
ESS [87](#), [452](#)  
ESS ID [87](#)  
ESSID (Extended Service Set Identification) [91](#)

Europe [5](#)  
 Exiting the SMT [268](#)  
 Expiration Duration [139](#)  
 Exposure [5](#)  
 Extended Service Set [452](#)  
 Extended Service Set (ESS) [87](#)  
 Extensible Authentication Protocol [89](#)  
 External Antenna [49](#)

## F

Factory LAN Defaults [81](#)  
 Failure [6](#)  
 FCC [4](#)  
     Compliance [4](#)  
     Rules, Part 15 [4](#)  
 FCC Rules [4](#)  
 Federal Communications Commission [4](#)  
 FHSS [451](#)  
 Filename Conventions [365](#)  
 filename conventions [366](#)  
 Filter [281](#), [331](#)  
     Applying Filters [342](#)  
     Ethernet Traffic [343](#)  
     Ethernet traffic [343](#)  
     Filter Rules [334](#)  
     Filter structure [332](#)  
     Generic Filter Rule [338](#)  
     Remote Node [301](#)  
     Remote Node Filter [301](#)  
     Remote Node Filters [343](#)  
     Sample [341](#)  
     SUA [340](#)  
     TCP/IP Filter Rule [336](#)  
 Filter Log [361](#)  
 Filter Rule Process [332](#)  
 Filter Rule Setup [335](#)  
 Filter Set  
     Class [335](#)  
 Filtering [331](#), [335](#)  
 Filtering Process  
     Outgoing Packets [331](#)  
 Finger [123](#)  
 Finland, Contact Information [7](#)  
 Firewall [155](#)  
     Access Methods [169](#), [329](#)  
     Address Type [178](#)  
     Alerts [173](#)  
     Anti-Probing [186](#)  
     Connection Direction [171](#)  
     Creating/Editing Rules [176](#)

Custom Ports [179](#)  
 Enabling [173](#)  
 Firewall Vs Filters [166](#)  
 Guidelines For Enhancing Security [164](#)  
 Introduction [156](#)  
 LAN to WAN Rules [172](#)  
 Policies [169](#)  
 Remote Management [329](#)  
 Rule Checklist [170](#)  
 Rule Logic [170](#)  
 Rule Security Ramifications [170](#)  
 Services [184](#)  
 SMT menus [329](#)  
 Types [155](#)  
 When To Use [166](#)  
 firmware [365](#)  
 Firmware Upgrade [262](#)  
 Fitness [6](#)  
 Flow Control [265](#)  
 Fragment Threshold [286](#)  
 Fragmentation Threshold [89](#)  
 Fragmentation threshold [89](#)  
 Frame Relay [53](#)  
 France, Contact Information [7](#)  
 Frequency-Hopping Spread Spectrum [451](#)  
 FTP [123](#), [229](#), [388](#)  
     Restrictions [388](#)  
 FTP File Transfer [374](#)  
 FTP Restrictions [229](#), [368](#)  
 FTP Server [324](#)  
 Functionally Equivalent [6](#)

## G

G.168 [47](#), [143](#)  
 G.168 Active [144](#)  
 G.711 [47](#), [136](#), [140](#)  
 G.729 [47](#), [136](#), [140](#)  
 Gas Pipes [5](#)  
 Gateway [307](#)  
 Gateway Node [311](#)  
 General Ethernet Setup [281](#)  
 General Setup [273](#)  
 Generic filter [340](#)  
 Germany, Contact Information [7](#)  
 God, act of [6](#)  
 Graphical User Interface (GUI) [46](#)

**H**

Half-Open Sessions **188**  
 Harmful Interference **4**  
 Hidden Menus **267**  
 Hidden node **88**  
 High Voltage Points **5**  
 Hop Count **300, 307**  
 Host **77**  
 Host IDs **441**  
 HTTP **123, 155, 157, 158, 409, 410**  
 HyperTerminal **378, 379**  
 HyperTerminal program **370, 373**

**I**

IANA **66, 67**  
 IANA (Internet Assigned Number Authority) **179**  
 IBSS **452**  
 ICMP echo **160**  
 ID Type and Content **207**  
 Idle timeout **298**  
 IEEE 802.11 **451**  
   Deployment Issues **455**  
   Security Flaws **455**  
 IEEE 802.11g **49**  
 IEEE 802.11g Data Rates **49**  
 IEEE 802.11g Modulation **49**  
 IEEE 802.11g Wireless LAN **49**  
 IEEE 802.11i **49**  
 IEEE 802.1Q VLAN **141**  
 IEEE 802.1x **455**  
   Additional requirements **87**  
   Advantages **455**  
 IEEE802.1x **351**  
 IGMP **82**  
 IGMP support **300**  
 IKE Phases **214**  
 Immediate Dial **148**  
 Independent Basic Service Set **452**  
 Indirect Damages **6**  
 Infrastructure Configuration **452**  
 Initial Screen **265**  
 initialization vector (IV) **96**  
 Inside Header **198**  
 Install UPnP **235**  
   Windows Me **235**  
   Windows XP **237**  
 Insurance **6**  
 Interactive Applications **391**  
 Interference **4**  
 Interference Correction Measures **4**  
 Interference Statement **4**  
 Internal SPTGEN **463**  
   FTP Upload Example **465**  
   Points to Remember **463**  
   Text File **463**  
 Internet Access **48, 54, 289, 292, 293**  
 Internet access **63, 289**  
 Internet Access Setup **313, 420**  
 Internet access wizard setup **64**  
 Internet Assigned Number Authority **66**  
 Internet Assigned Numbers AuthoritySee IANA **67**  
 Internet Control Message Protocol (ICMP) **159, 186**  
 Internet Key Exchange **214**  
 Internet Protocol Security **195**  
 Internet Telephony Service Provider **54**  
 IP Address **65, 81, 123, 257, 283, 307, 311, 337, 358, 363, 393**  
 IP Address Assignment **66**  
   ENET ENCAP **66**  
   PPPoA or PPPoE **66**  
   RFC 1483 **66**  
 IP Addressing **441**  
 IP alias **51, 289**  
 IP Alias Setup **290**  
 IP Classes **441**  
 IP Filter **338**  
   Logic Flow **337**  
 IP mask **336**  
 IP Packet **338**  
 IP Policies **289, 395**  
 IP policy **289**  
 IP policy routing **391**  
 IP Policy Routing (IPPR) **52, 289**  
   Applying an IP Policy **395**  
   Ethernet IP Policies **395**  
   Gateway **395**  
 IP Pool Setup **73**  
 IP Ports **409, 410**  
 IP Protocol **394**  
 IP protocol **391**  
 IP protocol type **184**  
 IP Routing Policy (IPPR) **391**  
   Benefits **391**  
   Cost Savings **391**  
   Criteria **391**  
   Load Sharing **391**  
   Setup **392**  
 IP Spoofing **158, 161**

IP Static Route [305](#)  
IP Static Route Setup [306](#)  
IPSec [195](#)  
IPSec Algorithm [405](#)  
IPSec algorithm [416](#)  
IPSec Algorithms [197](#), [201](#)  
IPSec and NAT [198](#)  
IPSec Architecture [197](#)  
IPSec rule [404](#)  
IPSec standard [48](#)  
IPSec VPN Capability [48](#)  
ISDN (Integrated Synchronous Digital System) [46](#)  
ITSP [54](#)  
ITU-T [143](#)

## J

Jitter Buffer [46](#)

## K

Keep Alive [205](#)  
Key Fields For Configuring Rules [171](#)  
Key management protocol [352](#)

## L

Labor [6](#)  
LAN [356](#)  
LAN Information [255](#)  
LAN Setup [79](#), [109](#), [281](#)  
LAN TCP/IP [81](#)  
LAN to WAN Rules [172](#)  
LAND [158](#), [159](#)  
Legal Rights [6](#)  
Liability [3](#)  
License [3](#)  
Lifeline [46](#), [146](#)  
Lifeline Screen [147](#)  
Lightning [5](#)  
Link type [356](#)  
Liquids, Corrosive [5](#)  
Listening Port [72](#), [138](#)  
Listening Volume [144](#)

LLC-based Multiplexing [303](#)  
Local Network  
    Rule Summary [174](#)  
Local User Authentication [105](#)  
Local User Database [105](#), [353](#)  
Local user database [105](#)  
Locations, Customer Support [7](#)  
Log and Trace [359](#)  
Log Facility [360](#)  
Logging Option [337](#), [339](#)  
Logical networks [289](#)  
Login [297](#)  
Login Screen [266](#)  
Logs [247](#)

## M

MAC (Media Access Control) address. [92](#)  
MAC address [311](#)  
MAC Address Filter [286](#)  
MAC address filter [286](#)  
    Filter action [287](#)  
MAC Address Filter Action [93](#), [287](#)  
MAC Address Filtering [92](#)  
MAC filter [92](#)  
Main Menu [268](#)  
Maintenance [253](#)  
management idle timeout period [58](#)  
Management Information Base (MIB) [346](#)  
Materials [6](#)  
Maximum Burst Size [293](#)  
Maximum Burst Size (MBS) [110](#), [113](#)  
Max-incomplete High [188](#)  
Max-incomplete Low [188](#)  
MBS [293](#)  
MBSSee Maximum Burst Size [293](#)  
MD5 [457](#)  
MD5 (Message Digest 5) [411](#)  
MDI/MDI-X [50](#)  
Media Access Control [309](#)  
Merchantability [6](#)  
Message Digest Algorithm 5 [457](#)  
Message Integrity Check [96](#)  
Message Integrity Check (MIC) [96](#)  
Message Logging [359](#)  
Metric [109](#), [279](#), [300](#), [307](#)  
MIC [96](#)  
Min-SE [140](#)

Modem [43](#)  
 Modifications [4](#)  
 Moving the Cursor [267](#)  
 MSDU (MAC Service Data Unit) [286](#)  
 Multicast [82](#), [300](#)  
 Multimedia [131](#)  
 Multiple SIP Accounts [47](#)  
 Multiple Voice Channels [47](#)  
 Multiplexing [52](#), [64](#), [65](#), [293](#), [296](#)  
 multiplexing [52](#), [64](#)  
   LLC-based [64](#)  
   VC-based [64](#)  
 Multiprotocol Encapsulation [64](#)  
 My IP Address [202](#)  
 My WAN Address [299](#)

## N

N/A Fields [267](#)  
 Nailed-Up Connection [67](#)  
 NAT [66](#), [123](#), [124](#), [340](#)  
   Address mapping rule [128](#)  
   Application [121](#)  
   Applying NAT in the SMT Menus [313](#)  
   Configuring [315](#)  
   Definitions [119](#)  
   Examples [321](#)  
   How it works [120](#)  
   Mapping Types [121](#)  
   Non NAT Friendly Application Programs [326](#)  
   Ordering Rules [318](#)  
   What it does [120](#)  
   What NAT does [120](#)  
 NAT (Network Address Translation) [119](#)  
 NAT mode [125](#)  
 NAT Traversal [233](#)  
 NAT traversal [206](#), [408](#)  
 navigating the web configurator [58](#)  
 Negotiation Mode [216](#), [411](#)  
 NetBIOS commands [160](#)  
 Network Address Translation [293](#)  
 Network Address Translation (NAT) [50](#), [313](#)  
 Network Authentication [94](#)  
 Network Management [52](#), [123](#)  
 Network Topology With RADIUS Server Example [456](#)  
 New [6](#)  
 NNTP [123](#)  
 Non-Proxy [145](#)  
 North America [5](#)  
 North America Contact Information [7](#)

Norway, Contact Information [7](#)  
 Notebook Computer [43](#)  
 NTP Time Servers [151](#)

## O

OFDM [49](#)  
 OK Response [132](#)  
 One-Minute High [188](#)  
 Opening [5](#)  
 Operating Condition [6](#)  
 Operating frequency [286](#)  
 Orthogonal Frequency Division Multiplexing Modulation [49](#)  
 Out-dated Warranty [6](#)  
 Outgoing Call use [144](#)  
 Outlet [4](#)  
 Outside Header [198](#)

## P

Packet  
   Error [356](#)  
   Received [356](#)  
   Transmitted [356](#)  
 Packet Filtering [166](#)  
 Packet filtering  
   When to use [166](#)  
 Packet Filtering Firewalls [155](#)  
 Packet Triggered [361](#)  
 Packets [356](#)  
 Pairwise Master Key (PMK) [96](#)  
 PAP [298](#)  
 Parts [6](#)  
 Password [77](#), [266](#), [267](#), [270](#), [297](#), [346](#)  
 Patent [3](#)  
 PCM [136](#)  
 PCR [293](#)  
 Peak Cell Rate [293](#)  
 Peak Cell Rate (PCR) [110](#), [113](#)  
 Perfect Forward Secrecy [216](#)  
 Perfect Forward Secrecy (PFS) [412](#)  
 Per-Hop Behavior [141](#)  
 Permission [3](#)  
 PFS [216](#)  
 PHB (Per-Hop Behavior) [141](#)  
 Phone [142](#)

PHONE 1 and 2 Ports [138](#)  
 Phone Port Screen [143](#), [148](#)  
 Phone Port Settings [144](#), [148](#)  
 Photocopying [3](#)  
 Ping [260](#), [363](#)  
 Ping of Death [158](#)  
 Pipes [5](#)  
 Point to Point Protocol over ATM Adaptation Layer 5 (AAL5) [63](#)  
 Point-to-Point [44](#)  
 Point-to-Point Tunneling Protocol [124](#)  
 policy-based routing [391](#)  
 Pool [5](#)  
 POP3 [123](#), [157](#), [158](#)  
 Port Numbers [123](#)  
 Postage Prepaid. [6](#)  
 Power Adaptor [5](#)  
 Power Cord [5](#)  
 Power Outlet [5](#)  
 Power Supply [5](#)  
 Power Supply, repair [5](#)  
 PPP (Point-to-Point Protocol) [94](#)  
 PPP Encapsulation [303](#)  
 PPP Log [362](#)  
 PPP session over Ethernet (PPP over Ethernet, RFC 2516) [63](#)  
 PPPoA [296](#)  
 PPPoE [110](#), [449](#)  
     Benefits [110](#)  
 PPPoE (Point-to-Point Protocol over Ethernet) [50](#), [110](#)  
 PPPoE pass-through [304](#)  
 PPTP [124](#)  
 Precedence [391](#), [394](#)  
 Pre-defined NTP Time Servers List [151](#)  
 Preferred Codec [140](#)  
 Pre-Shared Key [209](#), [352](#), [411](#)  
     Format [97](#)  
 Prestige [43](#)  
 Prestige 2602HW-L [46](#)  
 Prestige model [365](#)  
 Prestige models [45](#)  
 Prestige Wireless Security Levels [89](#)  
 Private [300](#), [307](#)  
 Private IP Addresses [67](#)  
 Product Model [7](#)  
 Product Page [4](#)  
 Product Serial Number [7](#)  
 Products [6](#)  
 Proof of Purchase [6](#)  
 Proper Operating Condition [6](#)

Protocol [336](#)  
 Protocol filter [340](#)  
 Protocol Filter Rules [340](#)  
 Protocol Support [51](#)  
 PSK [352](#)  
 PSTN [46](#)  
 PSTN Call Setup Signaling [136](#)  
 PSTN Pre-fix Number [147](#)  
 Public Switched Telephone Network [46](#)  
 Pulse Code Modulation [136](#)  
 Pulse Dialing [136](#)  
 Purchase, Proof of [6](#)  
 Purchaser [6](#)  
 PVC (Permanent Virtual Circuit) [63](#)

## Q

QoS [47](#), [140](#), [142](#)  
 Qualified Service Personnel [5](#)  
 Quality of Service [47](#), [140](#), [391](#)  
 Quality of Service (QoS) [47](#)  
 Quick Start Guide [57](#)

## R

Radio Communications [4](#)  
 Radio frequency [91](#)  
 Radio Frequency Energy [4](#)  
 Radio Interference [4](#)  
 Radio Reception [4](#)  
 Radio Technician [4](#)  
 RADIUS [89](#), [94](#)  
     Configuring [106](#)  
     Shared Secret Key [95](#)  
 RADIUS Message Types [94](#)  
 RADIUS Messages [94](#)  
 RADIUS server [349](#)  
 RAS [358](#), [392](#)  
 Rate  
     Receiving [356](#)  
     Transmission [356](#)  
 Read Me First [41](#)  
 Real time Transport Protocol [135](#), [140](#)  
 Receiving Antenna [4](#)  
 Register [255](#)  
 Register Resend Timer [139](#)  
 REGISTER Server Address [72](#), [138](#)

- REGISTER Server Port [72](#), [138](#)
  - Registered [3](#)
  - Registered Trademark [3](#)
  - Regular Mail [7](#)
  - Related Documentation [41](#)
  - Relay to PSTN [147](#)
  - Relocate [4](#)
  - Re-manufactured [6](#)
  - Remote Authentication Dial-In User Service [89](#)
  - Remote DHCP Server [283](#)
  - Remote Management [229](#)
    - Firewall [329](#)
  - Remote Management and NAT [230](#)
  - Remote Management Limitations [229](#), [388](#)
  - Remote Management Setup [387](#)
  - Remote Node [295](#), [356](#)
    - Remote Node Profile [297](#)
    - Remote Node Setup [295](#)
  - Remote Node Index Number [356](#)
  - Remote Node Network Layer Options [299](#)
  - Removing [5](#)
  - REN [46](#)
  - Reorient [4](#)
  - Repair [5](#), [6](#)
  - Replace [6](#)
  - Replacement [6](#)
  - Reproduction [3](#)
  - Required fields [267](#)
  - Reset ADSL Line [261](#)
  - Reset button, the [58](#)
  - resetting the Prestige [58](#)
  - Restore [6](#)
  - Restore Configuration [371](#)
  - Return Material Authorization (RMA) Number [6](#)
  - Returned Products [6](#)
  - Returns [6](#)
  - RF (Radio Frequency) [49](#)
  - RF signals [451](#)
  - RFC 1483 [64](#)
  - RFC 1631 [119](#)
  - RFC 1889 [46](#), [135](#)
  - RFC 189 [46](#)
  - RFC 2327 [46](#)
  - RFC 3261 [46](#)
  - RFC-1483 [296](#)
  - RFC-2364 [296](#), [297](#)
  - RFC2516 [50](#)
  - Rights [3](#)
  - Rights, Legal [6](#)
  - Ringer Equivalence Number [46](#)
  - RIP [283](#), [300](#)
  - RIPSee Routing Information Protocol [81](#)
  - Risk [5](#)
  - Risks [5](#)
  - RMA [6](#)
  - Romfile [365](#)
  - Router [43](#)
  - Routing [289](#)
  - Routing Information Protocol [81](#)
    - Direction [81](#)
    - Version [81](#)
  - Routing Policy [391](#)
  - RTCP [46](#)
  - RTP [46](#), [135](#)
  - RTP Port Range [140](#)
  - RTS (Request To Send) [88](#), [286](#)
  - RTS (Request To Send) threshold [91](#)
  - RTS Threshold [88](#), [286](#)
  - Rule Summary [174](#)
  - Rules [172](#)
    - Checklist [170](#)
    - Key Fields [171](#)
    - LAN to WAN [172](#)
    - Logic [170](#)
    - Predefined Services [184](#)
    - Summary [174](#)
  - Rx B/s [257](#)
  - RxPkts [257](#)
- ## S
- SA [195](#), [409](#)
  - SA life time [411](#)
  - SA lifetime [415](#)
  - SA Monitor [415](#)
  - SA monitor [415](#)
  - Safety Warnings [5](#)
  - Sample IP Addresses [300](#)
  - Saving SMT Configuration [268](#)
  - Saving the State [161](#)
  - Schedule Sets
    - Duration [400](#)
  - SCR [293](#)
  - SCRSee Sustain Cell Rate [293](#)
  - SDP [46](#)
  - Secure Gateway Address [203](#), [408](#)
  - Security Association [195](#), [415](#)
  - Security In General [165](#)
  - Security Parameter Index [219](#)

- Security Parameter Index (SPI) [412](#)
- Security Parameters [98](#)
- security protocols [405](#)
- Security Ramifications [170](#)
- Separation Between Equipment and Receiver [4](#)
- Serial Number [7](#)
- Server [43](#), [122](#), [315](#), [317](#), [319](#), [320](#), [322](#), [323](#), [384](#)
- Server behind NAT [319](#)
- Service [5](#), [6](#), [171](#)
- Service Personnel [5](#)
- Service Type [180](#), [420](#)
- Services [123](#)
- Session Expires [139](#)
- Session Initiation Protocol [131](#)
- setup a schedule [400](#)
- Shared secret [107](#), [350](#)
- Shipping [6](#)
- Shock, Electric [5](#)
- Silence Suppression [47](#), [143](#)
- Single User Account (SUA) [54](#)
- SIP [131](#)
- SIP Account [131](#), [138](#)
- SIP ALG [47](#), [135](#)
- SIP Application Layer Gateway [47](#), [135](#)
- SIP Call Progression [132](#)
- SIP Client [132](#)
- SIP Identities [131](#)
- SIP INVITE Request [132](#)
- SIP Local Port [72](#), [138](#)
- SIP Number [72](#), [131](#), [138](#), [145](#)
- SIP Proxy Server [133](#)
- SIP Redirect Server [134](#)
- SIP Register Server [135](#)
- SIP Registration Status [255](#)
- SIP Server Address [72](#), [138](#)
- SIP Server Port [72](#), [138](#)
- SIP Servers [132](#)
- SIP Service Domain [72](#), [132](#), [138](#)
- SIP URI [131](#), [145](#)
- SIP User Agent Server [133](#)
- SIP Version 2 [46](#)
- SMT [265](#)
- SMT Main Menu [268](#)
- SMT Menu Overview [269](#)
- SMTP [123](#)
- SMTP Error Messages [250](#)
- Smurf [159](#), [160](#)
- SNMP [123](#), [124](#)
  - Community [347](#)
  - Configuration [346](#)
  - Get [346](#)
  - GetNext [346](#)
  - Manager [345](#)
  - MIBs [346](#)
  - Set [346](#)
  - Trap [346](#)
  - Trusted Host [347](#)
- SOHO (Small Office/Home Office) [54](#)
- Source Address [171](#), [178](#)
- Source-Based Routing [391](#)
- Spain, Contact Information [7](#)
- Speaking Volume [144](#)
- Speed Dial [144](#), [145](#)
- Speed Dial Phone Book [146](#)
- Speed Dial Screen [145](#)
- SPI [219](#), [412](#), [413](#)
- Stateful Inspection [48](#), [155](#), [156](#), [161](#), [162](#)
  - Prestige [163](#)
  - Process [162](#)
- Static DHCP [85](#)
- Static Route [305](#)
- Static route [305](#)
- Static Routing Topology [305](#)
- SUA [122](#), [124](#)
- SUA (Single User Account) [122](#), [313](#)
- SUA server [123](#), [125](#)
  - Default server set [123](#)
- SUA vs NAT [122](#)
- SUA/NAT Server Set [126](#)
- Subnet Mask [65](#), [81](#), [178](#), [283](#), [299](#), [307](#), [358](#)
- Subnet Masks [442](#)
- Subnetting [442](#)
- Supply Voltage [5](#)
- Support E-mail [7](#)
- Supporting Disk [41](#)
- Sustain Cell Rate [293](#)
- Sustain Cell Rate (SCR) [113](#)
- Sustained Cell Rate (SCR) [110](#)
- Sweden, Contact Information [7](#)
- Swimming Pool [5](#)
- Switch [43](#)
- SYN Flood [158](#), [159](#)
- SYN-ACK [159](#)
- Syntax Conventions [42](#)
- Syslog [183](#), [360](#)
- Syslog IP Address [360](#)
- Syslog Server [360](#)
- System
  - Console Port Speed [358](#)
  - Diagnostic [362](#)
  - Log and Trace [359](#)
  - Syslog and Accounting [360](#)



System Information [357](#)  
 System Status [355](#)  
 System Information [357](#)  
 System Information & Diagnosis [355](#)  
 System Maintenance [250, 355, 357, 366, 369, 376, 377, 381, 382, 384](#)  
 System Management Terminal [265, 267](#)  
 System Parameter Table Generator [463](#)  
 System password [349](#)  
 System Security [349](#)  
 System Statistics [256](#)  
 System Status [253, 255, 356](#)  
 System Timeout [230, 389](#)

## T

Talk Time [257](#)  
 Tampering [6](#)  
 TCP Maximum Incomplete [188, 189](#)  
 TCP Security [163](#)  
 TCP/IP [157, 158, 230, 340, 363](#)  
 Teardrop [158](#)  
 Telecommunication Line Cord. [5](#)  
 Telephone [7, 43](#)  
 Television Interference [4](#)  
 Television Reception [4](#)  
 Telnet [230](#)  
 Telnet Configuration [230](#)  
 Temporal Key Integrity Protocol (TKIP) [96](#)  
 Terminal Emulation [265](#)  
 Test Your Internet Connection [76](#)  
 Text File Format [463](#)  
 TFTP  
   Restrictions [388](#)  
 TFTP File Transfer [376](#)  
 TFTP Restrictions [229, 368](#)  
 Three-Way Handshake [159](#)  
 Threshold Values [188](#)  
 Thunderstorm [5](#)  
 Time and Date Setting [383](#)  
 Time Zone [384](#)  
 Timeout [278](#)  
 TKIP [96](#)  
 TLS [457](#)  
 ToS [140](#)  
 TOS (Type of Service) [391](#)  
 Trace Records [359](#)  
 Traceroute [161](#)

Trademark [3](#)  
 Trademark Owners [3](#)  
 Trademarks [3](#)  
 Traffic Redirect [114, 115](#)  
   Setup [278](#)  
 Traffic redirect [114](#)  
 traffic redirect [50](#)  
 Traffic shaping [110](#)  
 Translation [3](#)  
 Transmission Rates [48](#)  
 Transport Layer Security [457](#)  
 Transport Mode [198](#)  
 Triangle [459](#)  
 Triangle Route Solutions [460](#)  
 Triple DES (3DES) [411](#)  
 TTLS [457](#)  
 Tunnel Mode [198](#)  
 Tunneled Transport Layer Service [457](#)  
 TV Technician [4](#)  
 Tx B/s [257](#)  
 TxPkts [257](#)  
 Type Of Service [140](#)  
 Type of Service [142, 391, 393, 394, 395](#)

## U

UBR [293](#)  
 UBR (Unspecified Bit Rate) [113](#)  
 UDP/ICMP Security [164](#)  
 Undesired Operations [4](#)  
 Uniform Resource Identifier [131](#)  
 Universal Plug and Play [233](#)  
   Application [233](#)  
   Security issues [233](#)  
 Universal Plug and Play (UPnP) [50](#)  
 Universal Plug and Play Forum [234](#)  
 UNIX Syslog [359, 360](#)  
 UNIX syslog parameters [360](#)  
 Unregister [255](#)  
 Unspecified Bit Rate [293](#)  
 Up Time [257](#)  
 Upload Firmware [262, 374](#)  
 UPnP [233](#)  
 Upper Layer Protocols [163, 164](#)  
 Upstream Noise Margin [261](#)  
 URL Type [139](#)  
 Use Proxy [145](#)  
 Used Port [255](#)

User Authentication [96](#)

User Name [150](#)

User Profiles [105](#)

user profiles [353](#)

## V

VAD [47, 143](#)

VAD Support [144](#)

Value [6](#)

Variable Bit Rate [293](#)

VBR [293](#)

VBR (Variable Bit Rate) [113](#)

VC-based Multiplexing [296](#)

VCI [65](#)

Vendor [5](#)

Ventilation Slots [5](#)

VID [142](#)

Viewing Certifications [4](#)

Virtual Channel Identifier [65](#)

Virtual Channel Identifier (VCI) [64](#)

Virtual Circuit ID [65](#)

Virtual Local Area Network [141](#)

Virtual Path Identifier [65](#)

Virtual Path Identifier (VPI) [64](#)

Virtual Private Network [48, 195](#)

VLAN [141](#)

VLAN Group [141](#)

VLAN ID [141](#)

VLAN ID Tags [141](#)

VLAN Tag [142](#)

Voice Activity Detection [47, 143](#)

Voice Coding [47, 136](#)

Voice Information [255](#)

Voice Priority [142](#)

Voice Statistics [257](#)

VoIP [131](#)

VoIP Screen [137](#)

VoIP Standards Compliance [46](#)

Voltage Supply [5](#)

Voltage, High [5](#)

VPI [65](#)

VPI & VCI [64](#)

VPN [195](#)

VPN Applications [196](#)

VPN/IPSec [403](#)

VT100 [265](#)

## W

Wall Mount [5](#)

WAN (Wide Area Network) [109](#)

WAN backup [115](#)

WAN Information [255](#)

WAN Setup [277](#)

WAN to LAN Rules [172](#)

Warnings [5](#)

Warranty [6](#)

Warranty Information [7](#)

Warranty Period [6](#)

Water [5](#)

Water Pipes [5](#)

Web Configurator [57, 58, 59, 156, 164, 171, 330](#)

web configurator screen summary [59](#)

Web Site [7](#)

WEP

    Default Key [286](#)

WEP (Wired Equivalent Privacy) [49, 92, 286](#)

WEP Encryption [286](#)

WEP encryption [90](#)

Wet Basement [5](#)

Wi-Fi Protected Access [96](#)

Wi-Fi Protected Access (WPA) [49](#)

Wireless Client WPA Supplicants [99](#)

Wireless LAN [87, 285, 451](#)

    Benefits [451](#)

    Configuring [90](#)

Wireless LAN Association List [259](#)

Wireless LAN MAC Address Filtering [49](#)

Wireless LAN Setup [285](#)

Wireless port control [100, 352](#)

Wireless security [89](#)

WLAN [451](#)

    Interference [87](#)

    Security parameters [98](#)

WLAN Information [255](#)

Workmanship [6](#)

Worldwide Contact Information [7](#)

WPA [96, 352](#)

    Supplicants [99](#)

    with RADIUS Application Example [97](#)

WPA Mixed Mode [352](#)

WPA -Pre-Shared Key [96](#)

WPA with RADIUS Application [97](#)

WPA-PSK [96](#)

WPA-PSK Application [97](#)

Written Permission [3](#)

## **X**

Xmodem

File Upload [378](#)

XMODEM protocol [366](#)

## **Z**

Zero Configuration [114](#)

Zero Configuration Internet Access [48](#)

Zero configuration Internet access [111](#)

ZyNOS [3](#), [366](#)

ZyNOS (ZyXEL Network Operating System) [365](#)

ZyNOS F/W Version [366](#)

ZyXEL Communications Corporation [3](#)

ZyXEL Home Page [4](#)

ZyXEL Limited Warranty

Note [6](#)

ZyXEL Network Operating System [3](#)

ZyXEL\_s Firewall

Introduction [156](#)