

Prestige 324

Intelligent Broadband Sharing Gateway

User's Guide

Version V3.61(JF.0)

April 2004



Copyright

Copyright © 2003 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

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.

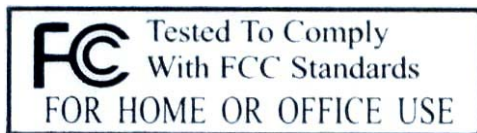
Consult the dealer or an experienced radio/TV technician for help.

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

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



Information for Canadian Users

The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operation, and safety requirements. The Industry Canada does not guarantee that the equipment will operate to a user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly. The customer should be aware that the compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

For their own protection, users should ensure that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution

Users should not attempt to make such connections themselves, but should contact the appropriate electrical inspection authority, or electrician, as appropriate.

Note

This digital apparatus does not exceed the class A limits for radio noise emissions from digital apparatus set out in the radio interference regulations of Industry Canada.

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.



Online Registration

Register online registration at www.zyxel.com for free future product updates and information.

Customer Support

When you contact your customer support representative please have the following information ready:
Please have the following information ready when you contact customer support.

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

METHOD LOCATION	SUPPORT E-MAIL SALES E-MAIL	TELEPHONE ¹ FAX ¹	WEB SITE FTP SITE	REGULAR MAIL
WORLDWIDE	support@zyxel.com.tw sales@zyxel.com.tw	+886-3-578-3942 +886-3-578-2439	www.zyxel.com www.europe.zyxel.com ftp.zyxel.com ftp.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
NORTH AMERICA	support@zyxel.com sales@zyxel.com	+1-800-255-4101 +1-714-632-0882 +1-714-632-0858	www.us.zyxel.com ftp.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
GERMANY	support@zyxel.de sales@zyxel.de	+49-2405-6909-0 +49-2405-6909-99	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
FRANCE	info@zyxel.fr	+33 (0)4 72 52 97 97 +33 (0)4 72 52 19 20	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
SPAIN	support@zyxel.es sales@zyxel.es	+34 902 195 420 +34 913 005 345	www.zyxel.es	ZyXEL Communications Alejandro Villegas 33 1º, 28043 Madrid Spain
DENMARK	support@zyxel.dk sales@zyxel.dk	+45 39 55 07 00 +45 39 55 07 07	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 5 2860 Soeborg Denmark
NORWAY	support@zyxel.no sales@zyxel.no	+47 22 80 61 80 +47 22 80 61 81	www.zyxel.no	ZyXEL Communications A/S Niils Hansens vei 13 0667 Oslo Norway

¹ “+” is the (prefix) number you enter to make an international telephone call.

METHOD LOCATION	SUPPORT E-MAIL SALES E-MAIL	TELEPHONE ¹ FAX ¹	WEB SITE FTP SITE	REGULAR MAIL
SWEDEN	support@zyxel.se sales@zyxel.se	+46 31 744 7700 +46 31 744 7701	www.zyxel.se	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden
FINLAND	support@zyxel.fi	+358-9-4780-8411	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland

Table of Contents

Copyright	ii
Federal Communications Commission (FCC) Interference Statement	iii
Information for Canadian Users	iv
ZyXEL Limited Warranty	v
Customer Support	vi
List of Figures	xvii
List of Tables	xxiii
Preface	xxvii
Getting Started	I
Chapter 1 Getting to Know Your Prestige	1-1
1.1 Prestige Internet Security Gateway Overview	1-1
1.2 Prestige Features	1-1
1.3 Applications for the Prestige	1-4
Chapter 2 Introducing the Web Configurator	2-1
2.1 Web Configurator Overview	2-1
2.2 Accessing the Prestige Web Configurator	2-1
2.3 Resetting the Prestige	2-2
2.4 Navigating the Prestige Web Configurator	2-2
Chapter 3 Wizard Setup	3-1
3.1 Wizard Setup Overview	3-1
3.2 Wizard Setup: General Setup and System Name	3-1
3.3 Wizard Setup: Screen 2	3-2
3.4 Wizard Setup: Screen 3	3-8
3.5 Basic Setup Complete	3-11
System, LAN and WAN	II

Chapter 4 System Screens	4-1
4.1 System Overview	4-1
4.2 Configuring General Setup	4-1
4.3 Dynamic DNS.....	4-2
4.4 Configuring Dynamic DNS	4-3
4.5 Configuring Password.....	4-4
4.6 Configuring Time Setting	4-5
Chapter 5 LAN Screens	5-1
5.1 LAN Overview	5-1
5.2 DHCP Setup.....	5-1
5.3 LAN TCP/IP	5-1
5.4 Configuring IP	5-3
5.5 Configuring IP Alias	5-6
Chapter 6 WAN Screens	6-1
6.1 WAN Overview	6-1
6.2 TCP/IP Priority (Metric).....	6-1
6.3 WAN IP Address Assignment	6-1
6.4 Configuring Route	6-2
6.5 Configuring WAN ISP.....	6-3
6.6 Configuring WAN IP.....	6-9
6.7 Configuring WAN MAC	6-13
6.8 Traffic Redirect.....	6-14
6.9 Configuring Traffic Redirect	6-15
6.10 Configuring Dial Backup.....	6-16
6.11 Advanced Modem Setup.....	6-21
6.12 Configuring Advanced Modem Setup	6-22
NAT and Static Route	III

Chapter 7 Network Address Translation (NAT) Screens.....	7-1
7.1 NAT Overview.....	7-1
7.2 Using NAT.....	7-6
7.3 SUA Server.....	7-6
7.4 Configuring SUA Server.....	7-8
7.5 Configuring Address Mapping.....	7-10
7.6 Trigger Port Forwarding.....	7-13
7.7 Configuring Trigger Port Forwarding.....	7-14
Chapter 8 Static Route Screens	8-1
8.1 Static Route Overview	8-1
8.2 Configuring IP Static Route	8-1
UPnP and Firewall	IV
Chapter 9 UPnP	9-1
9.1 Universal Plug and Play Overview	9-1
9.2 UPnP and ZyXEL	9-2
9.3 Configuring UPnP.....	9-2
9.4 Installing UPnP in Windows Example.....	9-4
9.5 Using UPnP in Windows XP Example	9-6
Chapter 10 Firewall.....	10-1
10.1 Introduction.....	10-1
10.2 Firewall Settings Screen.....	10-3
10.3 The Firewall, NAT and Remote Management	10-5
10.4 Configuring Content Filtering.....	10-6
10.5 Services	10-8
Remote Management	V
Chapter 11 Remote Management Screens	11-1
11.1 Remote Management Overview.....	11-1

11.2	Configuring WWW.....	11-2
11.3	Configuring Telnet.....	11-4
11.4	Configuring TELNET.....	11-4
11.5	Configuring FTP.....	11-5
11.6	SNMP.....	11-6
11.7	Configuring DNS.....	11-10
11.8	Configuring Security.....	11-11
Logs and Maintenance		VI
Chapter 12 Centralized Logs.....		12-1
12.1	View Log.....	12-1
12.2	Log Settings.....	12-2
Chapter 13 Maintenance.....		13-1
13.1	Maintenance Overview.....	13-1
13.2	Status Screen.....	13-1
13.3	DHCP Table Screen.....	13-4
13.4	F/W Upload Screen.....	13-5
13.5	Configuration Screen.....	13-7
13.6	Restart Screen.....	13-10
SMT General Configuration.....		VII
Chapter 14 Introducing the SMT.....		14-1
14.1	SMT Introduction.....	14-1
14.2	Navigating the SMT Interface.....	14-3
14.3	Changing the System Password.....	14-6
Chapter 15 Menu 1 General Setup		15-1
15.1	General Setup.....	15-1
15.2	Procedure To Configure Menu 1	15-1
Chapter 16 WAN and Dial Backup Setup		16-1

16.1	Introduction to WAN	16-1
16.2	Dial Backup.....	16-2
16.3	Configuring Dial Backup in Menu 2.....	16-2
16.4	Advanced WAN Setup.....	16-3
16.5	Remote Node Profile (Backup ISP)	16-5
16.6	Editing PPP Options.....	16-8
16.7	Editing TCP/IP Options	16-9
16.8	Editing Login Script.....	16-11
16.9	Remote Node Filter.....	16-12
Chapter 17 Menu 3 LAN Setup		17-1
17.1	LAN Setup	17-1
17.2	Protocol Dependent Ethernet Setup	17-2
17.3	TCP/IP Ethernet Setup and DHCP	17-2
Chapter 18 Internet Access		18-1
18.1	Introduction to Internet Access Setup	18-1
18.2	Ethernet Encapsulation.....	18-1
18.3	Configuring the PPTP Client.....	18-3
18.4	Configuring the PPPoE Client.....	18-4
18.5	Basic Setup Complete	18-5
Chapter 19 Remote Node Configuration		19-1
19.1	Introduction to Remote Node Setup.....	19-1
19.2	Remote Node Profile Setup.....	19-1
19.3	Edit IP	19-7
19.4	Remote Node Filter	19-9
Chapter 20 Static Route Setup.....		20-1
20.1	IP Static Route Setup.....	20-1
Chapter 21 Network Address Translation (NAT)		21-1

21.1	Using NAT	21-1
21.2	Applying NAT	21-1
21.3	NAT Setup	21-3
21.4	Configuring a Server behind NAT	21-9
21.5	General NAT Examples	21-10
21.6	Configuring Trigger Port Forwarding	21-18
Chapter 22 Enabling the Firewall.....		22-1
22.1	Remote Management and the Firewall	22-1
22.2	Access Methods	22-1
22.3	Enabling the Firewall	22-1
SMT Advanced Management.....		VIII
Chapter 23 Filter Configuration		23-1
23.1	Introduction to Filters	23-1
23.2	Configuring a Filter Set	23-4
23.3	Example Filter.....	23-13
23.4	Filter Types and NAT	23-15
23.5	Firewall Versus Filters	23-16
23.6	Applying a Filter	23-16
Chapter 24 SNMP Configuration.....		24-1
24.1	About SNMP.....	24-1
24.2	Supported MIBs.....	24-2
24.3	SNMP Configuration	24-2
24.4	SNMP Traps	24-4
Chapter 25 System Information and Diagnosis		25-1
25.1	System Status	25-1
25.2	System Information.....	25-3
25.3	Log and Trace	25-5

25.4	Diagnostic	25-9
Chapter 26 Firmware and Configuration File Maintenance		26-1
26.1	Filename Conventions	26-1
26.2	Backup Configuration	26-2
26.3	Restore Configuration	26-6
26.4	Uploading Firmware and Configuration Files.....	26-8
Chapter 27 System Maintenance.....		27-1
27.1	Command Interpreter Mode.....	27-1
27.2	Call Control Support	27-2
27.3	Time and Date Setting.....	27-4
Chapter 28 Remote Management.....		28-1
28.1	Remote Management.....	28-1
Chapter 29 Call Scheduling		29-1
29.1	Introduction to Call Scheduling	29-1
Appendices and Index.....		IX
Appendix A PPPoE		A-1
Appendix B PPTP		B-1
Appendix C NetBIOS Filter Commands		C-1
Appendix D Log Descriptions.....		D-1
Appendix E Setting up Your Computer's IP Address.....		E-1
Appendix F Brute-Force Password Guessing Protection		F-1
Appendix G Triangle Route		G-1
Appendix H Index.....		H-1

List of Figures

Figure 1-1 Secure Internet Access via Cable, DSL or Wireless Modem.....	1-5
Figure 2-1 Change Password Screen.....	2-1
Figure 2-2 The MAIN MENU Screen of the Web Configurator.....	2-3
Figure 3-1 Wizard 1	3-2
Figure 3-2 Wizard 2: Ethernet Encapsulation	3-3
Figure 3-3 Wizard2: PPPoE Encapsulation.....	3-5
Figure 3-4 Wizard 2: PPTP Encapsulation.....	3-6
Figure 3-5 Wizard 3	3-10
Figure 4-1 System General Setup	4-1
Figure 4-2 DDNS.....	4-3
Figure 4-3 Password.....	4-5
Figure 4-4 Time Setting	4-6
Figure 5-1 IP	5-3
Figure 5-2 IP Alias	5-6
Figure 6-1 WAN Setup: Route.....	6-3
Figure 6-2 Ethernet Encapsulation.....	6-4
Figure 6-3 PPPoE Encapsulation.....	6-6
Figure 6-4 PPTP Encapsulation	6-8
Figure 6-5 WAN: IP.....	6-11
Figure 6-6 MAC Setup	6-14
Figure 6-7 Traffic Redirect WAN Setup.....	6-15
Figure 6-8 Traffic Redirect LAN Setup	6-15
Figure 6-9 WAN: Traffic Redirect	6-16
Figure 6-10 Dial Backup Setup	6-18
Figure 6-11 Advanced Setup	6-24

Figure 7-1 How NAT Works	7-3
Figure 7-2 NAT Application With IP Alias	7-4
Figure 7-3 Multiple Servers Behind NAT Example.....	7-8
Figure 7-4 SUA/NAT Setup.....	7-9
Figure 7-5 Address Mapping	7-10
Figure 7-6 Address Mapping Edit.....	7-12
Figure 7-7 Trigger Port Forwarding Process: Example	7-13
Figure 7-8 Trigger Port.....	7-15
Figure 8-1 Example of Static Routing Topology	8-1
Figure 8-2 Static Route.....	8-2
Figure 8-3 Static Route: Edit	8-3
Figure 9-1 Configuring UPnP.....	9-3
Figure 10-1 Firewall: Settings	10-3
Figure 10-2 Firewall Rule Directions	10-5
Figure 10-3 Firewall: Filter.....	10-7
Figure 10-4 Firewall: Service	10-9
Figure 11-1 Remote Management: WWW	11-3
Figure 11-2 Telnet Configuration on a TCP/IP Network	11-4
Figure 11-3 Remote Management: Telnet.....	11-5
Figure 11-4 Remote Management: FTP.....	11-6
Figure 11-5 SNMP Management Model.....	11-7
Figure 11-6 Remote Management: SNMP.....	11-9
Figure 11-7 Remote Management: DNS.....	11-11
Figure 11-8 Security	11-12
Figure 12-1 View Log.....	12-1
Figure 12-2 Log Settings	12-3
Figure 13-1 System Status	13-1

Figure 13-2 System Status: Show Statistics	13-3
Figure 13-3 DHCP Table.....	13-4
Figure 13-4 Firmware Upload.....	13-5
Figure 13-5 Firmware Upload.....	13-6
Figure 13-6 Firmware Upload In Process	13-6
Figure 13-7 Network Temporarily Disconnected.....	13-6
Figure 13-8 Firmware Upload Error	13-7
Figure 13-9 Configuration	13-8
Figure 13-10 Configuration Upload Successful.....	13-9
Figure 13-11 Network Temporarily Disconnected	13-9
Figure 13-12 Restore Configuration Error	13-10
Figure 13-13 Reset Warning Message.....	13-10
Figure 13-14 Restart.....	13-11
Figure 14-1 Login Screen	14-2
Figure 14-2 SMT Menu Overview.....	14-3
Figure 14-3 SMT Main Menu	14-5
Figure 14-4 Menu 23 System Password.....	14-6
Figure 15-1 Menu 1 General Setup.....	15-2
Figure 15-2 Menu 1.1 Configure Dynamic DNS.....	15-4
Figure 16-1 MAC Address Cloning in WAN Setup	16-1
Figure 16-2 Menu 2: Dial Backup Setup	16-2
Figure 16-3 Menu 2.1 Advanced WAN Setup.....	16-4
Figure 16-4 Menu 11.1 Remote Node Profile (Backup ISP).....	16-6
Figure 16-5 Menu 11.2: Remote Node PPP Options.....	16-8
Figure 16-6 Menu 11.2: Remote Node PPP Options.....	16-8
Figure 16-7 Menu 11.3: Remote Node Network Layer Options	16-9
Figure 16-8 Menu 11.4: Remote Node Script	16-12

Figure 16-9 Menu 11.5: Dial Backup Remote Node Filter	16-13
Figure 17-1 Menu 3 LAN Setup	17-1
Figure 17-2 Menu 3.1 LAN Port Filter Setup	17-1
Figure 17-3 Menu 3.2 TCP/IP and DHCP Ethernet Setup	17-2
Figure 17-4 Menu 3.2.1: IP Alias Setup	17-5
Figure 18-1 Menu 4 Internet Access Setup	18-1
Figure 18-2 Internet Access Setup (PPTP)	18-4
Figure 18-3 Internet Access Setup (PPPoE)	18-5
Figure 19-1 Menu 11.1 Remote Node Profile for Ethernet Encapsulation	19-2
Figure 19-2 Menu 11.1 Remote Node Profile for PPPoE Encapsulation	19-4
Figure 19-3 Menu 11.1 Remote Node Profile for PPTP Encapsulation	19-6
Figure 19-4 Menu 11.3 Remote Node Network Layer Options for Ethernet Encapsulation	19-7
Figure 19-5 Menu 11.5: Remote Node Filter (Ethernet Encapsulation)	19-9
Figure 19-6 Menu 11.5: Remote Node Filter (PPPoE or PPTP Encapsulation)	19-10
Figure 19-7 Menu 11.6: Traffic Redirect Setup	19-10
Figure 20-1 Menu 12 IP Static Route Setup	20-1
Figure 20-2 Menu 12.1 Edit IP Static Route	20-2
Figure 21-1 Menu 4 Applying NAT for Internet Access	21-2
Figure 21-2 Menu 11.3 Applying NAT to the Remote Node	21-3
Figure 21-3 Menu 15 NAT Setup	21-4
Figure 21-4 Menu 15.1 Address Mapping Sets	21-4
Figure 21-5 Menu 15.1.255 SUA Address Mapping Rules	21-5
Figure 21-6 Menu 15.1.1 First Set	21-6
Figure 21-7 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set	21-8
Figure 21-8 Menu 15.2.1 NAT Server Setup	21-9
Figure 21-9 Multiple Servers Behind NAT Example	21-10
Figure 21-10 NAT Example 1	21-10

Figure 21-11 Menu 4 Internet Access & NAT Example.....	21-11
Figure 21-12 NAT Example 2	21-11
Figure 21-13 Menu 15.2.1 Specifying an Inside Server.....	21-12
Figure 21-14 NAT Example 3	21-13
Figure 21-15 Example 3: Menu 11.3.....	21-14
Figure 21-16 Example 3: Menu 15.1.1.1	21-14
Figure 21-17 Example 3: Final Menu 15.1.1	21-15
Figure 21-18 NAT Example 4	21-16
Figure 21-19 Example 4: Menu 15.1.1.1 Address Mapping Rule.....	21-17
Figure 21-20 Example 4: Menu 15.1.1 Address Mapping Rules	21-17
Figure 21-21 Menu 15.3 Trigger Port Setup	21-18
Figure 22-1 Menu 21.2 Firewall Setup	22-2
Figure 23-1 Outgoing Packet Filtering Process	23-2
Figure 23-2 Filter Rule Process.....	23-3
Figure 23-4 Menu 21: Filter and Firewall Setup.....	23-4
Figure 23-5 Menu 21.1: Filter Set Configuration.....	23-4
Figure 23-6 Menu 21.1.1.1 TCP/IP Filter Rule.....	23-7
Figure 23-7 Executing an IP Filter	23-10
Figure 23-8 Menu 21.1.4.1 Generic Filter Rule	23-11
Figure 23-9 Telnet Filter Example	23-13
Figure 23-10 Example Filter: Menu 21.1.3.1	23-14
Figure 23-11 Example Filter Rules Summary: Menu 21.1.3.....	23-15
Figure 23-12 Protocol and Device Filter Sets	23-16
Figure 23-13 Filtering LAN Traffic	23-17
Figure 23-14 Filtering Remote Node Traffic	23-18
Figure 24-1 SNMP Management Model.....	24-1
Figure 24-2 Menu 22 SNMP Configuration.....	24-3

Figure 25-1 Menu 24 System Maintenance	25-1
Figure 25-2 Menu 24.1 System Maintenance : Status	25-2
Figure 25-3 Menu 24.2 System Information and Console Port Speed.....	25-3
Figure 25-4 Menu 24.2.1 System Maintenance : Information	25-4
Figure 25-5 Menu 24.2.2 System Maintenance : Change Console Port Speed.....	25-5
Figure 25-6 Menu 24.3.2 System Maintenance : Syslog Logging.....	25-5
Figure 25-7 Call-Trigging Packet Example	25-9
Figure 25-8 Menu 24.4 System Maintenance : Diagnostic	25-10
Figure 25-9 LAN & WAN DHCP	25-10
Figure 26-1 Telnet in Menu 24.5	26-3
Figure 26-2 FTP Session Example.....	26-4
Figure 26-3 Telnet into Menu 24.6	26-7
Figure 26-4 Restore Using FTP Session Example	26-8
Figure 26-5 Telnet Into Menu 24.7.1 Upload System Firmware	26-9
Figure 26-6 Telnet Into Menu 24.7.2 System Maintenance	26-9
Figure 26-7 FTP Session Example of Firmware File Upload	26-10
Figure 27-1 Command Mode in Menu 24	27-1
Figure 27-2 Valid Commands	27-2
Figure 27-3 Menu 24.9 System Maintenance : Call Control	27-2
Figure 27-4 Budget Management	27-3
Figure 27-5 Call History	27-4
Figure 27-6 Menu 24: System Maintenance.....	27-5
Figure 27-7 Menu 24.10 System Maintenance: Time and Date Setting	27-5
Figure 28-1 Menu 24.11 – Remote Management Control	28-1
Figure 29-1 Menu 26 Schedule Setup.....	29-1
Figure 29-2 Menu 26.1 Schedule Set Setup.....	29-2
Figure 29-3 Applying Schedule Set(s) to a Remote Node (PPPoE).....	29-4

List of Tables

Table 2-1 Screens Summary.....	2-3
Table 3-1 Ethernet Encapsulation	3-3
Table 3-2 PPPoE Encapsulation.....	3-5
Table 3-3 PPTP Encapsulation.....	3-7
Table 3-4 Private IP Address Ranges	3-8
Table 3-5 Example of Network Properties for LAN Servers with Fixed IP Addresses.....	3-9
Table 3-6 WAN Setup	3-10
Table 4-1 System General Setup.....	4-1
Table 4-2 DDNS.....	4-4
Table 4-3 Password	4-5
Table 4-4 Time Setting.....	4-6
Table 5-1 IP.....	5-3
Table 5-2 IP Alias	5-6
Table 6-1 Private IP Address Ranges	6-2
Table 6-2 Example of Network Properties for LAN Servers with Fixed IP Addresses.....	6-2
Table 6-3 WAN Setup: Route	6-3
Table 6-4 Ethernet Encapsulation	6-4
Table 6-5 PPPoE Encapsulation	6-6
Table 6-6 PPTP Encapsulation	6-8
Table 6-7 WAN: IP	6-11
Table 6-8 WAN: Traffic Redirect.....	6-16
Table 6-9 Dial Backup Setup.....	6-19
Table 6-10 Advanced Setup	6-24
Table 7-1 NAT Definitions.....	7-1
Table 7-2 NAT Mapping Types	7-5

Table 7-3 Services and Port Numbers.....	7-7
Table 7-4 SUA/NAT Setup	7-9
Table 7-5 Address Mapping.....	7-11
Table 7-6 Address Mapping Edit	7-12
Table 7-7 Trigger Port.....	7-15
Table 8-1 Static Route.....	8-2
Table 8-2 Static Route: Edit.....	8-3
Table 9-1 Configuring UPnP	9-3
Table 10-1 Firewall: Settings.....	10-4
Table 10-2 Firewall: Filter	10-7
Table 10-3 Firewall: Service.....	10-9
Table 11-1 Remote Management: WWW	11-3
Table 11-2 Remote Management: Telnet	11-5
Table 11-3 Remote Management: FTP	11-6
Table 11-4 SNMP Traps.....	11-8
Table 11-5 Remote Management: SNMP	11-10
Table 11-6 Remote Management: DNS	11-11
Table 11-7 Security.....	11-12
Table 12-1 View Log	12-2
Table 12-2 Log Settings.....	12-3
Table 13-1 System Status.....	13-2
Table 13-2 System Status: Show Statistics	13-3
Table 13-3 DHCP Table.....	13-4
Table 13-4 Restore Configuration.....	13-9
Table 14-1 Main Menu Commands	14-4
Table 14-2 Main Menu Summary	14-5
Table 15-1 Menu 1 General Setup	15-2

Table 15-2 Menu 1.1 Configure Dynamic DNS.....	15-4
Table 16-1 MAC Address Cloning in WAN Setup.....	16-1
Table 16-2 Menu 2: Dial Backup Setup	16-3
Table 16-3 Advanced WAN Port Setup: AT Commands Fields	16-4
Table 16-4 Advanced WAN Port Setup: Call Control Parameters	16-5
Table 16-5 Menu 11.1 Remote Node Profile (Backup ISP).....	16-6
Table 16-6 Menu 11.3: Remote Node Network Layer Options.....	16-9
Table 16-7 Menu 11.4: Remote Node Script.....	16-12
Table 17-1 Menu 3.2: DHCP Ethernet Setup Fields	17-2
Table 17-2 Menu 3.2: LAN TCP/IP Setup Fields	17-4
Table 17-3 Menu 3.2.1: IP Alias Setup.....	17-5
Table 18-1 Menu 4: Internet Access Setup (Ethernet).....	18-2
Table 18-2 New Fields in Menu 4 (PPTP) Screen	18-4
Table 18-3 New Fields in Menu 4 (PPPoE) screen.....	18-5
Table 19-1 Menu 11.1 Remote Node Profile for Ethernet Encapsulation	19-2
Table 19-2 Fields in Menu 11.1 (PPPoE Encapsulation Specific)	19-5
Table 19-3 Menu 11.1 Remote Node Profile for PPTP Encapsulation.....	19-6
Table 19-4 Remote Node Network Layer Options.....	19-7
Table 19-5 Menu 11.6: Traffic Redirect Setup	19-10
Table 20-1 Menu 12.1 Edit IP Static Route.....	20-2
Table 21-1 Applying NAT in Menus 4 & 11.3	21-3
Table 21-2 SUA Address Mapping Rules	21-5
Table 21-3 Menu 15.1.1 First Set.....	21-7
Table 21-4 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set.....	21-8
Table 21-5 Menu 15.3 Trigger Port Setup.....	21-18
Table 23-1 Abbreviations Used in the Filter Rules Summary Menu.....	23-5
Table 23-2 Rule Abbreviations Used	23-6

Table 23-3 TCP/IP Filter Rule	23-7
Table 23-4 Generic Filter Rule Menu Fields	23-11
Table 24-1 Menu 22 SNMP Configuration	24-3
Table 24-2 SNMP Traps.....	24-4
Table 24-3 Ports and Permanent Virtual Circuits.....	24-4
Table 25-1 System Maintenance: Status Menu Fields	25-2
Table 25-2 Menu 24.2.1 System Maintenance : Information.....	25-4
Table 25-3 Menu 24.3.2 System Maintenance : Syslog and Accounting.....	25-5
Table 25-4 System Maintenance Menu Diagnostic	25-11
Table 26-1 Filename Conventions	26-2
Table 26-2 General Commands for GUI-based FTP Clients	26-4
Table 26-3 General Commands for GUI-based TFTP Clients	26-6
Table 27-1 Budget Management.....	27-3
Table 27-2 Call History Fields.....	27-4
Table 27-3 Time and Date Setting Fields.....	27-6
Table 28-1 Menu 24.11 – Remote Management Control.....	28-2
Table 29-1 Menu 26.1 Schedule Set Setup	29-2
Table C-1 NetBIOS Filter Default Settings	C-2

Preface

About This User's Manual

Congratulations on your purchase of the Prestige 324 Intelligent Broadband Sharing Gateway. This manual is designed to guide you through the configuration of your Prestige for its various applications.

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.

The web configurator parts of this guide contain background information on features configurable by the web configurator and the SMT. The SMT parts of this guide contain background information solely on features not configurable by the web configurator.

This manual may refer to the Prestige 324 Broadband Security Gateway with 4 Port Switch as the Prestige.

Related Documentation

- Support Disk
Refer to the included CD for support documents.
- Quick Start Guide
The Quick Start Guide is designed to help you get up and running right away. It contains a detailed easy-to-follow connection diagram, default settings, handy checklists and information on setting up your network and configuring for Internet access.
- Web Configurator Online Help
Embedded web help for descriptions of individual screens and supplementary information.
- Packing List Card
The Packing List Card lists all items that should have come in the package.
- Certifications
Refer to the product page at www.zyxel.com for information on product certifications.
- ZyXEL Glossary and Web Site
Please refer to www.zyxel.com for an online glossary of networking terms and additional support documentation.

User's Guide Feedback

Help us help you. E-mail all User's Guide-related comments, questions or suggestions for improvement to techwriters@zyxel.com.tw or send regular mail to The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Thank you.

Syntax Conventions

- The version number on the title page is the latest firmware version that is documented in this *User's Guide*. Earlier versions may also be included.
- “Enter” means for you to type one or more characters and press the carriage return. “Select” or “Choose” means for you to use one of the predefined choices.
- The SMT menu titles and labels are in **Bold Times New Roman** 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.
- The choices of a menu item are in **Bold Arial** font.
- 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.

Part I:

Getting Started

This part helps you get to know your Prestige, introduces the web configurator and covers how to configure the Wizard Setup screens.

Chapter 1

Getting to Know Your Prestige

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

1.1 Prestige Internet Security Gateway Overview

The Prestige is the ideal secure gateway for all data passing between the Internet and LAN's. By integrating NAT, and firewall, ZyXEL's Prestige is a complete security solution that protects your Intranet and efficiently manages data traffic on your network. The embedded web configurator is easy to operate.

1.2 Prestige Features

The following sections describe Prestige features.

1.2.1 Physical Features

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 10/100 Mbps Ethernet Interface(s)

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

4-Port Switch

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

All-in-one Console and Auxiliary Port

Set the CON/AUX switch to the "CON" side when using the CON/AUX port as a regular console port for local device configuration and management. Set this switch to the "AUX" side when using the CON/AUX port as an auxiliary dial-up WAN connection.

Time and Date

The Prestige allows you to get the current time and date from an external server when you turn on your Prestige. You can also set the time manually.

Reset Button

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

1.2.2 Non-Physical Features

Firewall

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

Content Filtering

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

Packet Filtering

Packet filtering blocks unwanted traffic from entering/leaving your network.

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.

Call Scheduling

Configure call time periods to restrict and allow access for users on remote nodes.

PPPoE

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

PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server.

PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet. The Prestige supports one PPTP server connection at any given time.

Dynamic DNS Support

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

IP Multicast

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

IP Alias

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

SNMP

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

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).

Traffic Redirect

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

Port Forwarding

Use this feature to forward incoming service requests to a server on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server.

DHCP (Dynamic Host Configuration Protocol)

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

Full Network Management

The embedded web configurator is an all-platform web-based utility that allows you to easily access the Prestige's management settings and configure the firewall. Most functions of the Prestige are also software configurable via the SMT (System Management Terminal) interface. The SMT is a menu-driven interface that you can access over a telnet connection.

RoadRunner Support

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

Logging and Tracing

- ◆ Built-in message logging and packet tracing.
- ◆ Unix syslog facility support.
- ◆ Firewall logs.
- ◆ Content filtering logs.

Upgrade Prestige Firmware via LAN

The firmware of the Prestige can be upgraded via the LAN (*refer to Maintenance- F/W Upload Screen*).

Embedded FTP and TFTP Servers

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

1.3 Applications for the Prestige

Here are some examples of what you can do with your Prestige.

1.3.1 Secure Broadband Internet Access via Cable or DSL Modem

You can connect a cable modem, DSL or wireless modem to the Prestige for broadband Internet access via an Ethernet or a wireless port on the modem. The Prestige guarantees not only high speed Internet access, but secure internal network protection and traffic management as well.

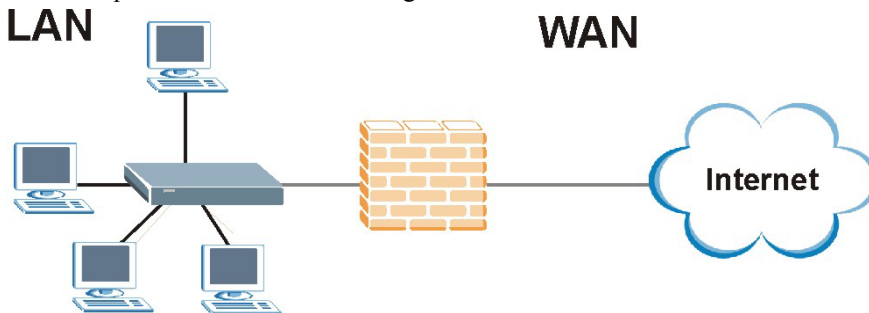


Figure 1-1 Secure Internet Access via Cable, DSL or Wireless Modem

Chapter 2

Introducing the Web Configurator

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

2.1 Web Configurator Overview

The 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. The screens you see in the web configurator may vary somewhat from the ones shown in this document due to differences between individual Prestige models or firmware versions.

2.2 Accessing the Prestige Web Configurator

- Step 1.** Make sure your Prestige hardware is properly connected and prepare your computer/computer network to connect to the Prestige (refer to the *Quick Start Guide*).
- Step 2.** Launch your web browser.
- Step 3.** Type "192.168.1.1" as the URL.
- Step 4.** Type "1234" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.
- Step 5.** You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) and click **Apply** or click **Ignore**.

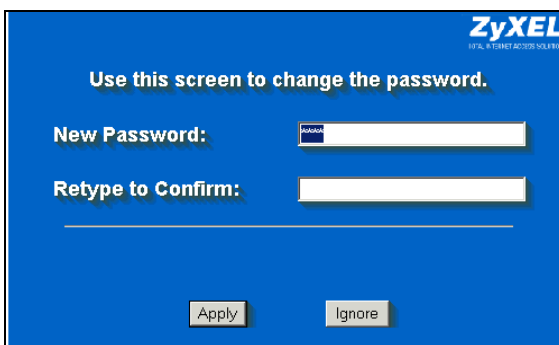


Figure 2-1 Change Password Screen

Step 6. You should now see the **MAIN MENU** screen (see *Figure 2-2*).

The management session automatically times out when the time period set in the Administrator Inactivity Timer field expires (default five minutes). Simply log back into the Prestige if this happens to you.

2.3 Resetting the Prestige

If you forget your password or cannot access the web configurator, you will need to 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”.

2.3.1 Procedure To Use The Reset Button

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

Step 1. Make sure the **PWR** LED is on (not blinking).

Step 2. Press the **RESET** button for ten seconds or until the **PWR** LED begins to blink and then release it. When the **PWR** LED begins to blink, the defaults have been restored and the Prestige restarts.

2.4 Navigating the Prestige Web Configurator

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

Follow the instructions you see in the MAIN MENU screen or click the  icon (located in the top right corner of most screens) to view online help.

The  icon does not appear in the MAIN MENU screen.

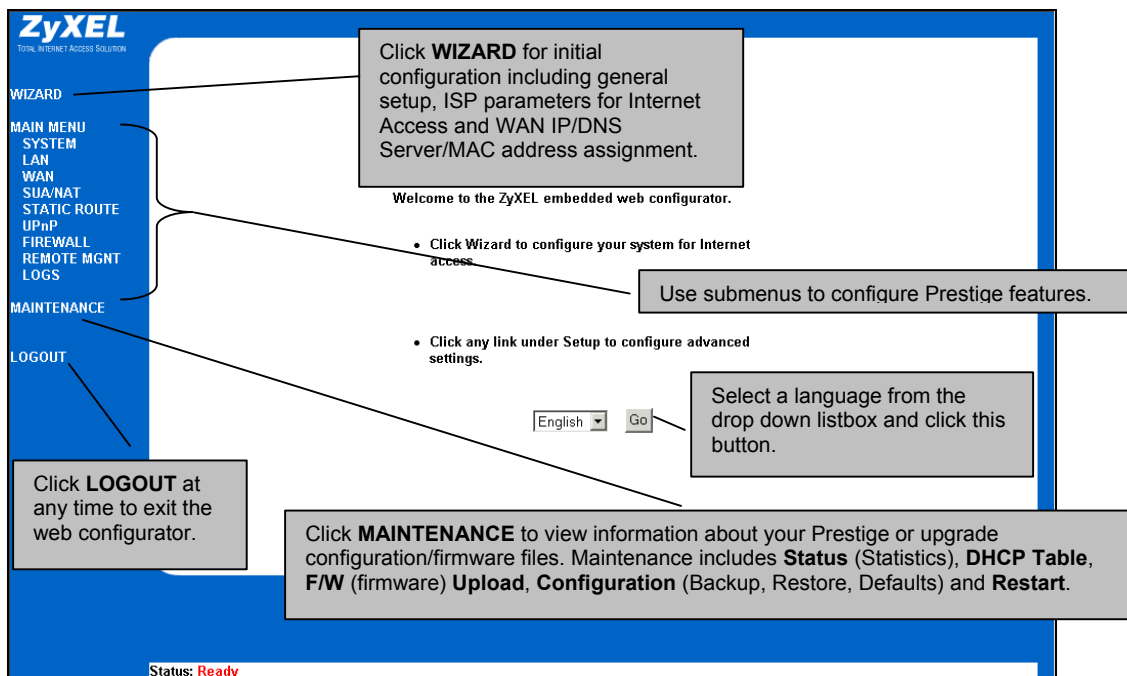


Figure 2-2 The MAIN MENU Screen of the Web Configurator

2.4.1 Navigation Panel

After you enter the password, use the sub-menus on the navigation panel to configure Prestige features. The following table describes the sub-menus.

Table 2-1 Screens Summary

LINK	TAB	FUNCTION
WIZARD		Use these screens for initial configuration including general setup, ISP parameters for Internet Access and WAN IP/DNS Server/MAC address assignment.
SYSTEM	General	This screen contains administrative and system-related information.
	DDNS	Use this screen to set up dynamic DNS.
	Password	Use this screen to change your password.
	Time Setting	Use this screen to change your Prestige's time and date.

Table 2-1 Screens Summary

LINK	TAB	FUNCTION
LAN	IP	Use this screen to configure LAN DHCP and TCP/IP settings.
	IP Alias	Use this screen to partition your LAN interface into subnets.
WAN	Route	This screen allows you to configure route priority.
	WAN ISP	Use this screen to change your Prestige's WAN ISP settings.
	WAN IP	Use this screen to change your Prestige's WAN IP settings.
	WAN MAC	Use this screen to change your Prestige's WAN MAC settings.
	Traffic Redirect	Use this screen to configure your traffic redirect properties and parameters.
	Dial Backup	Use this screen to configure a backup WAN connection.
SUA/NAT	SUA Server	Use this screen to configure servers behind the Prestige.
	Address Mapping	Use this screen to configure network address translation mapping rules.
	Trigger Port	Use this screen to change your Prestige's trigger port settings.
STATIC ROUTE	IP Static Route	Use this screen to configure IP static routes.
UPnP	UPnP	Use this screen to enable UPnP on the Prestige.
FIREWALL	Settings	Use this screen to activate/deactivate the firewall and log packets related to firewall rules.
	Filter	This screen allows you to block sites containing certain keywords in the URL and set the days and times for the Prestige to perform content filtering.
	Services	Use this screen to enable service blocking.
REMOTE MGMT	WWW	Use this screen to configure through which interface(s) and from which IP address(es) users can use HTTP to manage the Prestige.
	TELNET	Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet to manage the Prestige.
	FTP	Use this screen to configure through which interface(s) and from which IP address(es) users can use FTP to access the Prestige.
	SNMP	Use this screen to configure your Prestige's settings for Simple Network Management Protocol management.

Table 2-1 Screens Summary

LINK	TAB	FUNCTION
	DNS	Use this screen to configure through which interface(s) and from which IP address(es) users can send DNS queries to the Prestige.
	Security	Use this screen to change your anti-probing settings.
LOGS	View Log	Use this screen to view the logs for the categories that you selected.
	Log Settings	Use this screen to change your Prestige's log settings.
MAINTENANCE	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.
	F/W Upload	Use this screen to upload firmware to your Prestige.
	Configuration	Use this screen to backup and restore the configuration or reset the factory defaults to your Prestige.
	Restart	This screen allows you to reboot the Prestige without turning the power off.
LOGOUT		Click this label to exit the web configurator.

Chapter 3

Wizard Setup

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

3.1 Wizard Setup Overview

The web configurator's setup wizard helps you configure your device to access the Internet. The second screen has three variations depending on what encapsulation type you use. Refer to your ISP checklist in the *Quick Start Guide* to know what to enter in each field. Leave a field blank if you don't have that information.

3.2 Wizard Setup: General Setup and System Name

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

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

3.2.1 Domain Name

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

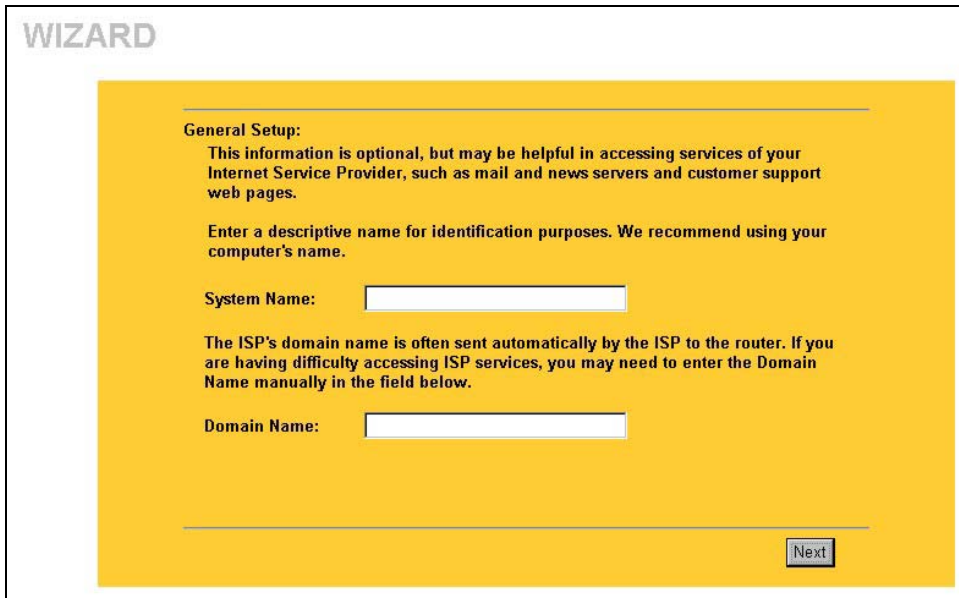


Figure 3-1 Wizard 1

3.3 Wizard Setup: Screen 2

The Prestige offers three choices of encapsulation. They are **Ethernet**, **PPP over Ethernet** or **PPTP**.

3.3.1 Ethernet

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

WIZARD SETUP

ISP Parameters for Internet Access

Encapsulation	Ethernet
Service Type	Standard
User Name	N/A
Password	N/A
Login Server IP Address	N/A

Back Next

Figure 3-2 Wizard 2: Ethernet Encapsulation

The following table describes the fields in this screen.

Table 3-1 Ethernet Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	You must choose the Ethernet option when the WAN port is used as a regular Ethernet. Otherwise, choose PPP over Ethernet or PPTP for a dial-up connection.
Service Type	Choose from Standard , Telstra (RoadRunner Telstra authentication method), RR-Manager (Roadrunner Manager authentication method), RR-Toshiba (Roadrunner Toshiba authentication method) or Telia Login . The following fields are not applicable (N/A) for the Standard service type.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Login Server IP Address	Type the authentication server IP address here if your ISP gave you one.
Login Server	This field only applies when you select Telia Login in the Service Type field. Type the domain name of the Telia login server, for example "login1.telia.com".

Table 3-1 Ethernet Encapsulation

LABEL	DESCRIPTION
Relogin Every(min)	This field only applies when you select Telia Login in the Service Type field. The Telia server logs the Prestige out if the Prestige does not log in periodically. Type the number of minutes from 1 to 59 (30 default) for the Prestige to wait between logins.
Next	Click Next to continue.
Back	Click Back to return to the previous screen.

3.3.2 PPPoE Encapsulation

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

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for instance, Radius). For the user, 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 end users 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 specific users.

Operationally, PPPoE saves significant effort for both the subscriber and the ISP/carrier, as it requires no specific configuration of the broadband modem at the subscriber's 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 LAN's computers will have Internet access.

Refer to the appendix for more information on PPPoE.

Figure 3-3 Wizard2: PPPoE Encapsulation

The following table describes the fields in this screen.

Table 3-2 PPPoE Encapsulation

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

Table 3-2 PPPoE Encapsulation

LABEL	DESCRIPTION
Back	Click Back to return to the previous screen.

3.3.3 PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables transfers of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet.

Refer to the appendix for more information on PPTP.

The PRESTIGE supports one PPTP server connection at any given time.

Figure 3-4 Wizard 2: PPTP Encapsulation

The following table describes the fields in this screen.

Table 3-3 PPTP Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Select PPTP from the drop-down list box.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
Nailed-Up Connection	Select Nailed-Up Connection if you do not want the connection to time out.
Idle Timeout	Type the time in seconds that elapses before the router automatically disconnects from the PPTP server. The default is 100 seconds.
PPTP Configuration	
Get Automatically from ISP	Select this option if your ISP did not assign you a fixed IP address.
Use fixed IP address	Select this option if your ISP already assigned you an IP address. This is the default selection.
My IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your Prestige automatically assigns a subnet mask based on the IP address typed in the previous field.
Server IP Address	Select this option if your ISP gave you an IP address. Otherwise select Server Domain Name . Type the IP address of the PPTP server as given by your ISP.
Server Domain Name	Select this option if your ISP gave you a domain name for your PPTP server. Otherwise select Server IP Address . Type the domain name of your PPTP server, for example "server.PPTP.com". Note that if Use fixed IP address is selected, this option is not available.
Connection ID/Name	Enter the connection ID or connection name in this field. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your DSL modem.
Next	Click Next to continue.

Table 3-3 PPTP Encapsulation

LABEL	DESCRIPTION
Back	Click Back to return to the previous screen.

3.4 Wizard Setup: Screen 3

The third wizard screen allows you to configure WAN IP address assignment, DNS server address assignment and the WAN MAC address.

3.4.1 WAN IP Address Assignment

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

Table 3-4 Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

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

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.

3.4.2 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. 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.

3.4.3 DNS Server Address Assignment

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

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

1. The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the DNS Server fields in DHCP Setup.
2. If the ISP did not give you DNS server information, leave the DNS Server fields in DHCP Setup set to 0.0.0.0 for the ISP to dynamically assign the DNS server IP addresses.

3.4.4 WAN MAC Address

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 can configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Once it is successfully configured, the address will be copied to the "rom" file (ZyNOS configuration file). It will not change unless you change the setting or upload a different "rom" file.

ZyXEL recommends you clone the MAC address from a computer on your LAN even if your ISP does not require MAC address authentication.

Table 3-5 Example of Network Properties for LAN Servers with Fixed IP Addresses

Choose an IP address	192.168.1.2-192.168.1.32; 192.168.1.65-192.168.1.254.
Subnet mask	255.255.255.0
Gateway (or default route)	192.168.1.1(Prestige LAN IP)

The third wizard screen varies according to the type of encapsulation that you select in the second wizard screen.

Figure 3-5 Wizard 3

The following table describes the fields in this screen.

Table 3-6 WAN Setup

LABEL	DESCRIPTION
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use fixed IP address	Select this option If the ISP assigned a fixed IP address.
IP Address	Enter your WAN IP address in this field if you selected Use Fixed IP Address .

Table 3-6 WAN Setup

LABEL	DESCRIPTION
IP Subnet Mask	Enter the IP subnet mask in this field if you selected Use Fixed IP Address . This field is not available when you select PPPoE encapsulation in the previous wizard screen.
Gateway IP Address	Enter the gateway IP address in this field if you selected Use Fixed IP Address . This field is not available when you select PPPoE encapsulation in the previous wizard screen.
<p>System DNS Servers (if applicable)</p> <p>DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The Prestige uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.</p>	
First DNS Server	<p>Select From ISP if your ISP dynamically assigns DNS server information (and the Prestige's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.</p> <p>Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right.</p> <p>Select None if you do not want to configure DNS servers. If you do not configure a system DNS server, you must use IP addresses when configuring VPN, DDNS and the time server.</p>
Second DNS Server	
Third DNS Server	
WAN MAC Address	The MAC address field allows you to configure the WAN port's MAC Address by either using the factory default or cloning the MAC address from a computer on your LAN.
Factory Default	Select this option to use the factory assigned default MAC Address.
Spoof this Computer's MAC address - IP Address	Select this option and enter the IP address of the computer on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different rom file. It is advisable to clone the MAC address from a computer on your LAN even if your ISP does not presently require MAC address authentication.
Back	Click Back to return to the previous screen.
Finish	Click Finish to complete and save the wizard setup.

3.5 Basic Setup Complete

Well done! You have successfully set up your Prestige to operate on your network and access the Internet.

Part II:

System, LAN and WAN

This part covers configuration of the system, LAN, and WAN screens.

Chapter 4

System Screens

This chapter provides information on the System screens.

4.1 System Overview

See the *Wizard Setup* chapter for more information on the next few screens.

4.2 Configuring General Setup

Click **SYSTEM** to open the **General** screen.

Figure 4-1 System General Setup

The following table describes the labels in this screen.

Table 4-1 System General Setup

LABEL	DESCRIPTION
System Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field (see the <i>Wizard Setup</i> chapter for how to find your computer's name). This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.

Table 4-1 System General Setup

LABEL	DESCRIPTION
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. The domain name entered by you is given priority over the ISP assigned domain name.
Administrator Inactivity Timer	Type how many minutes a management session (either via the web configurator or SMT) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
System DNS Servers (if applicable) DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The Prestige uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.	
First DNS Server Second DNS Server Third DNS Server	Select From ISP if your ISP dynamically assigns DNS server information (and the Prestige's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose User-Defined , but leave the IP address set to 0.0.0.0, User-Defined changes to None after you click Apply . If you set a second choice to User-Defined , and enter the same IP address, the second User-Defined changes to None after you click Apply . Select None if you do not want to configure DNS servers. If you do not configure a system DNS server, you must use IP addresses when configuring VPN, DDNS and the time server.
Apply	Click Apply to save your changes back to the Prestige.
Reset	Click Reset to begin configuring this screen afresh.

4.3 Dynamic DNS

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

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

4.3.1 DYNDNS Wildcard

Enabling the wildcard feature for your host causes `*.yourhost.dyndns.org` to be aliased to the same IP address as `yourhost.dyndns.org`. This feature is useful if you want to be able to use, for example, `www.yourhost.dyndns.org` and still reach your hostname.

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

4.4 Configuring Dynamic DNS

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

Figure 4-2 DDNS

The following table describes the labels in this screen.

Table 4-2 DDNS

LABEL	DESCRIPTION
Active	Select this check box to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
DDNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider.
Host Names 1~3	Enter the host names in the three fields provided. You can specify up to two host names in each field separated by a comma (",").
User	Enter your user name.
Password	Enter the password assigned to you.
Enable Wildcard	Select the check box to enable DYNDNS Wildcard.
Off Line	This option is available when CustomDNS is selected in the DDNS Type field. Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
Edit Update IP Address:	
Server Auto Detect	Select this option to update the IP address of the host name(s) automatically by the DDNS server. It is recommended that you select this option.
User Specify	Select this option to update the IP address of the host name(s) to the IP address specified below. Use this option if you have a static IP address.
IP Address	Enter the IP address if you select the User Specify option.
Apply	Click Apply to save your changes back to the Prestige.
Reset	Click Reset to begin configuring this screen afresh.

4.5 Configuring Password

To change your Prestige's password (recommended), click **SYSTEM**, then the **Password** tab. The screen appears as shown. This screen allows you to change the Prestige's password.

The screenshot shows a web interface for password management. At the top, the word 'PASSWORD' is displayed. Below it are four tabs: 'General', 'DDNS', 'Password', and 'Time Setting'. The 'Password' tab is highlighted. The main area contains three text input fields with labels 'Old Password', 'New Password', and 'Retype to Confirm'. At the bottom of the form are two buttons labeled 'Apply' and 'Reset'.

Figure 4-3 Password

The following table describes the labels in this screen.

Table 4-3 Password

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

4.6 Configuring Time Setting

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

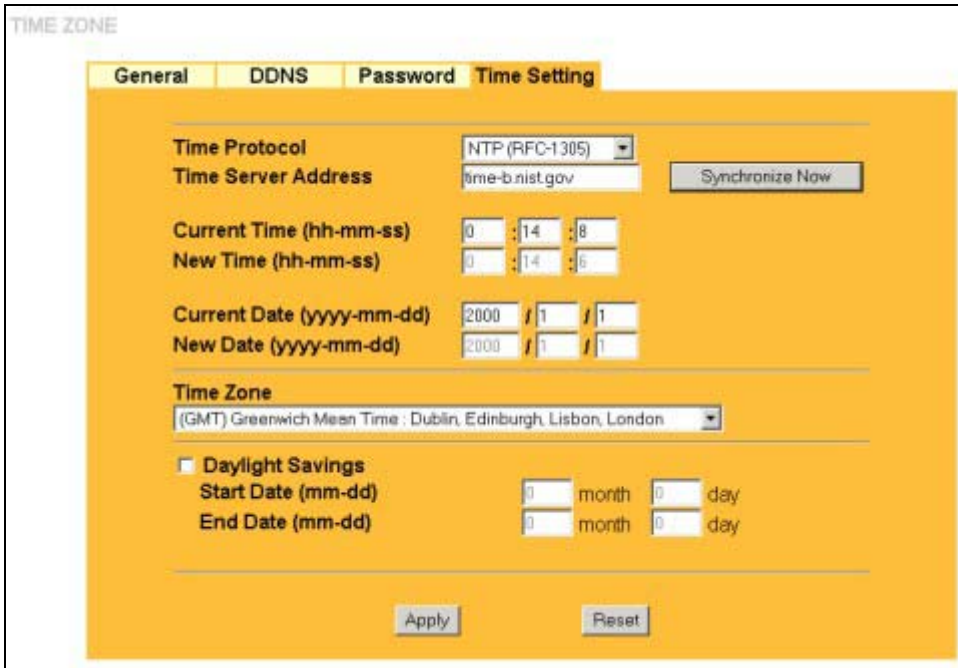


Figure 4-4 Time Setting

The following table describes the labels in this screen.

Table 4-4 Time Setting

LABEL	DESCRIPTION
Time Protocol	<p>Select the time service protocol that your time server sends when you turn on the Prestige. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works.</p> <p>The main difference between them is the format.</p> <p>Daytime (RFC 867) format is day/month/year/time zone of the server.</p> <p>Time (RFC 868) format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.</p> <p>The default, NTP (RFC 1305), is similar to Time (RFC 868).</p> <p>Select None to enter the time and date manually.</p>
Time Server Address	<p>Enter the IP address or URL of your time server. Check with your ISP/network administrator if you are unsure of this information (the default is tick.stdtime.gov.tw).</p>

Table 4-4 Time Setting

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

Chapter 5

LAN Screens

This chapter describes how to configure LAN settings.

5.1 LAN Overview

Local Area Network (LAN) is a shared communication system to which many computers are attached. The LAN screens can help you configure a LAN DHCP server, manage IP addresses, and partition your physical network into logical networks.

5.2 DHCP Setup

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

5.2.1 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. This configuration leaves 31 IP addresses (excluding the Prestige itself) in the lower range for other server computers, for instance, servers for mail, FTP, TFTP, web, etc., that you may have.

5.2.2 System DNS Servers

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

5.3 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.

5.3.1 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.

5.3.2 IP Address and Subnet Mask

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

5.3.3 RIP Setup

RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. **RIP Direction** controls the sending and receiving of RIP packets. When set to **Both** or **Out Only**, the Prestige will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received.

RIP Version 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** send routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.

By default, **RIP Direction** is set to **Both** and **RIP Version** to **RIP-1**.

5.3.4 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.

5.4 Configuring IP

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

Figure 5-1 IP

The following table describes the fields in this screen.

Table 5-1 IP

LABEL	DESCRIPTION
DHCP Server	DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (computers) to obtain TCP/IP configuration at startup from a server. Leave the DHCP Server check box selected unless your ISP instructs you to do otherwise. Clear it to disable the Prestige acting as a DHCP server. When configured as a server, the Prestige provides TCP/IP configuration for the clients. If not, DHCP service is disabled and you must have another DHCP server on your LAN, or else the computers must be manually configured. When set as a server, fill in the following four fields.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.

Table 5-1 IP

LABEL	DESCRIPTION
Pool Size	This field specifies the size, or count of the IP address pool.
<p>DNS Servers Assigned by DHCP Server</p> <p>The Prestige passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. The Prestige only passes this information to the LAN DHCP clients when you select the DHCP Server check box. When you clear the DHCP Server check box, DHCP service is disabled and you must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured.</p>	
<p>First DNS Server Second DNS Server Third DNS Server</p>	<p>Select From ISP if your ISP dynamically assigns DNS server information (and the Prestige's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.</p> <p>Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. If you chose User-Defined, but leave the IP address set to 0.0.0.0, User-Defined changes to None after you click Apply. If you set a second choice to User-Defined, and enter the same IP address, the second User-Defined changes to None after you click Apply.</p> <p>Select DNS Relay to have the Prestige act as a DNS proxy. The Prestige's LAN IP address displays in the field to the right (read-only). The Prestige tells the DHCP clients on the LAN that the Prestige itself is the DNS server. When a computer on the LAN sends a DNS query to the Prestige, the Prestige forwards the query to the Prestige's system DNS server (configured in the SYSTEM General screen) and relays the response back to the computer. You can only select DNS Relay for one of the three servers; if you select DNS Relay for a second or third DNS server, that choice changes to None after you click Apply.</p> <p>Select None if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a computer in order to access it.</p>
LAN TCP/IP	
IP Address	Type the IP address of your Prestige in dotted decimal notation 192.168.1.1 (factory default).
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. 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 255.255.255.0.

Table 5-1 IP

LABEL	DESCRIPTION
RIP Direction	RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The RIP Direction field controls the sending and receiving of RIP packets. Select the RIP direction from Both/In Only/Out Only/None . When set to Both or Out Only , the Prestige will broadcast its routing table periodically. When set to Both or In Only , it will incorporate the RIP information that it receives; when set to None , it will not send any RIP packets and will ignore any RIP packets received. Both is the default.
RIP Version	The RIP 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. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to Both and the Version set to RIP-1 .
Multicast	Select IGMP V-1 or IGMP V-2 or None . 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.
Windows Networking (NetBIOS over TCP/IP): NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN.	
Allow between LAN and WAN	Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.
Apply	Click Apply to save your changes back to the Prestige.
Reset	Click Reset to begin configuring this screen afresh.

5.5 Configuring IP Alias

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

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

Figure 5-2 IP Alias

The following table describes the labels in this screen.

Table 5-2 IP Alias

LABEL	DESCRIPTION
IP Alias 1,2	Select the check box to configure another LAN network for the Prestige.
IP Address	Enter the IP address of your Prestige 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.

Table 5-2 IP Alias

LABEL	DESCRIPTION
RIP Direction	RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The RIP Direction field controls the sending and receiving of RIP packets. Select the RIP direction from Both/In Only/Out Only/None . When set to Both or Out Only , the Prestige will broadcast its routing table periodically. When set to Both or In Only , it will incorporate the RIP information that it receives; when set to None , it will not send any RIP packets and will ignore any RIP packets received.
RIP Version	The RIP 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. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to Both and the Version set to RIP-1 .
Apply	Click Apply to save your changes back to the Prestige.
Reset	Click Reset to begin configuring this screen afresh.

Chapter 6

WAN Screens

This chapter describes how to configure WAN settings.

6.1 WAN Overview

See the *LAN* chapter for information about *Primary and Secondary DNS Server*, *DNS Server Address Assignment* and *IP Address and Subnet Mask*.

6.2 TCP/IP Priority (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

1. **WAN**: designated by the ISP (see *section 6.6*) or a static route (see the *IP Static Route Setup* chapter)
2. **Traffic Redirect** (see *section 6.9*)
3. **Dial Backup** (see *section 6.10*)

For example, if **WAN** has a metric of "1" and **Traffic Redirect** has a metric of "2" and **Dial Backup** has a metric of "3", the **WAN** connection acts as the primary default route. If the **WAN** route fails to connect to the Internet, the Prestige tries **Traffic Redirect** next. In the same manner, the Prestige uses **Dial Backup** if **Traffic Redirect** also fails.

If you want **Dial Backup** to take first priority over **Traffic Redirect** or even **WAN**, all you need to do is set **Dial Backup**'s metric to "1" and the others to "2" (or greater).

6.3 WAN IP Address Assignment

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

Table 6-1 Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

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

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

6.3.1 WAN MAC Address

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 can configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a computer on your LAN. Once it is successfully configured, the address will be copied to the "rom" file (configuration file). It will not change unless you change the setting or upload a different "rom" file.

Nortel Networks recommends you clone the MAC address from a computer on your LAN even if your ISP does not require MAC address authentication.

Your Prestige's WAN Port is set at half-duplex mode as most cable/DSL modems only support half-duplex mode. Make sure your modem is in half-duplex mode. Your Prestige supports full duplex mode on the LAN side.

Table 6-2 Example of Network Properties for LAN Servers with Fixed IP Addresses

Choose an IP address	192.168.1.2-192.168.132; 192.168.1.65-192.168.1.254.
Subnet mask	255.255.255.0
Gateway (or default route)	192.168.1.1(Prestige LAN IP)

6.4 Configuring Route

Click **WAN** to open the **Route** screen.

WAN

Route WAN ISP WAN IP WAN MAC Traffic Redirect Dial Backup

Route Selection

WAN Priority (metric) 1 Priority = 1(highest)-15(lowest)

Traffic Redirect Priority (metric) 14 Priority = 1(highest)-15(lowest)

Dial Backup Priority (metric) 2 Priority = 1(highest)-15(lowest)

Apply Reset

Figure 6-1 WAN Setup: Route

The following table describes the fields in this screen.

Table 6-3 WAN Setup: Route

LABEL	DESCRIPTION
WAN	The default WAN connection is "1" as your broadband connection via the WAN port should always be your preferred method of accessing the WAN. The default priority of the routes is WAN , Traffic Redirect and then Dial Backup :
Traffic Redirect	You have two choices for an auxiliary connection (Traffic Redirect and Dial Backup) in the event that your regular WAN connection goes down. If Dial Backup is preferred to Traffic Redirect , then type "14" in the Dial Backup Priority (metric) field (and leave the Traffic Redirect Priority (metric) at the default of "15").
Dial Backup	
Apply	Click Apply to save your changes back to the Prestige.
Reset	Click Reset to begin configuring this screen afresh.

6.5 Configuring WAN ISP

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

6.5.1 Ethernet Encapsulation

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

The screenshot shows a configuration interface for WAN settings. At the top, there are several tabs: 'Route', 'WAN ISP' (which is selected), 'WAN IP', 'WAN MAC', 'Traffic Redirect', and 'Dial Backup'. Below the tabs, the section is titled 'ISP Parameters for Internet Access'. It contains the following fields:

- Encapsulation:** A dropdown menu with 'Ethernet' selected.
- Service Type:** A dropdown menu with 'RR-Toshiba' selected.
- User Name:** A text input field.
- Password:** A text input field with masked characters.
- Retype to Confirm:** A text input field with masked characters.
- Login Server IP Address:** A text input field with '0.0.0.0' entered.

At the bottom of the form, there are two buttons: 'Apply' and 'Reset'.

Figure 6-2 Ethernet Encapsulation

The following table describes the labels in this screen.

Table 6-4 Ethernet Encapsulation

LABEL	DESCRIPTION
Encapsulation	You must choose the Ethernet option when the WAN port is used as a regular Ethernet.
Service Type	Choose from Standard , Telstra (RoadRunner Telstra authentication method), RR-Manager (Roadrunner Manager authentication method), RR-Toshiba (Roadrunner Toshiba authentication method) or Telia Login . The following fields do not appear with the Standard service type.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Retype to Confirm	Type the password again to make sure that you have entered it correctly.
Login Server IP Address	Type the authentication server IP address here if your ISP gave you one.
Login Server	This field only applies when you select Telia Login in the Service Type field. Type the domain name of the Telia login server, for example "login1.telia.com".

Table 6-4 Ethernet Encapsulation

LABEL	DESCRIPTION
Relogin Every(min)	This field only applies when you select Telia Login in the Service Type field. The Telia server logs the Prestige out if the Prestige does not log in periodically. Type the number of minutes from 1 to 59 (30 default) for the Prestige to wait between logins.
Apply	Click Apply to save your changes back to the Prestige.
Reset	Click Reset to begin configuring this screen afresh.

6.5.2 PPPoE Encapsulation

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

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example Radius). 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.

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

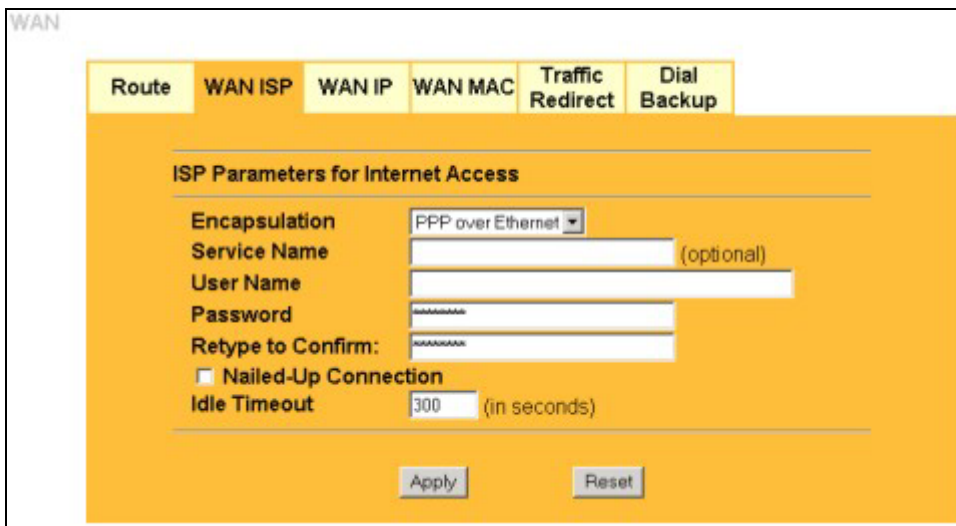


Figure 6-3 PPPoE Encapsulation

The following table describes the labels in this screen.

Table 6-5 PPPoE Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	The PPP over Ethernet choice is for a dial-up connection using PPPoE. 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 (i.e. xDSL, cable, wireless, etc.) connection. Operationally, PPPoE saves significant effort for both the end user and ISP/carrier, as it requires no specific configuration of the broadband modem at the customer site. By implementing PPPoE directly on the router rather than individual computers, the computers on the LAN do not need PPPoE software installed, since the router does that part of the task. Further, with NAT, all of the LAN's computers will have access.
Service Name	Type the PPPoE service name provided to you. PPPoE uses a service name to identify and reach the PPPoE server.
User Name	Type the User Name given to you by your ISP.
Password	Type the password associated with the User Name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.

Table 6-5 PPPoE Encapsulation

LABEL	DESCRIPTION
Nailed-Up Connection	Select Nailed-Up Connection if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the router automatically disconnects from the PPPoE server.
Apply	Click Apply to save your changes back to the Prestige.
Reset	Click Reset to begin configuring this screen afresh.

6.5.3 PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks. PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet.

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

Figure 6-4 PPTP Encapsulation

The following table describes the labels in this screen.

Table 6-6 PPTP Encapsulation

LABEL	DESCRIPTION
ISP Parameters for Internet Access	
Encapsulation	Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks. PPTP supports on-demand, multi-protocol, and virtual private networking over public networks, such as the Internet. The Prestige supports only one PPTP server connection at any given time. To configure a PPTP client, you must configure the User Name and Password fields for a PPP connection and the PPTP parameters for a PPTP connection.
User Name	Type the user name given to you by your ISP.

Table 6-6 PPTP Encapsulation

LABEL	DESCRIPTION
Password	Type the password associated with the User Name above.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Nailed-up Connection	Select Nailed-Up Connection if you do not want the connection to time out.
Idle Timeout	This value specifies the time in seconds that elapses before the Prestige automatically disconnects from the PPTP server.
PPTP Configuration	
Get Automatically from ISP	Select this option If your ISP did not assign you a fixed IP address.
Use fixed IP address	Select this option if your ISP already assigned you an IP address. This is the default selection.
My IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your Prestige automatically assigns a subnet mask based on the IP address typed in the previous field.
Server IP Address	Select this option if your ISP gave you an IP address. Otherwise select Server Domain Name . Type the IP address of the PPTP server as given by your ISP.
Server Domain Name	Select this option if your ISP gave you a domain name for your PPTP server. Otherwise select Server IP Address . Type the domain name of your PPTP server, for example "server.PPTP.com". Note that if Use fixed IP address is selected, this option is not available.
Connection ID/Name	Enter the connection ID or connection name in this field. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your ISP.

6.6 Configuring WAN IP

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

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

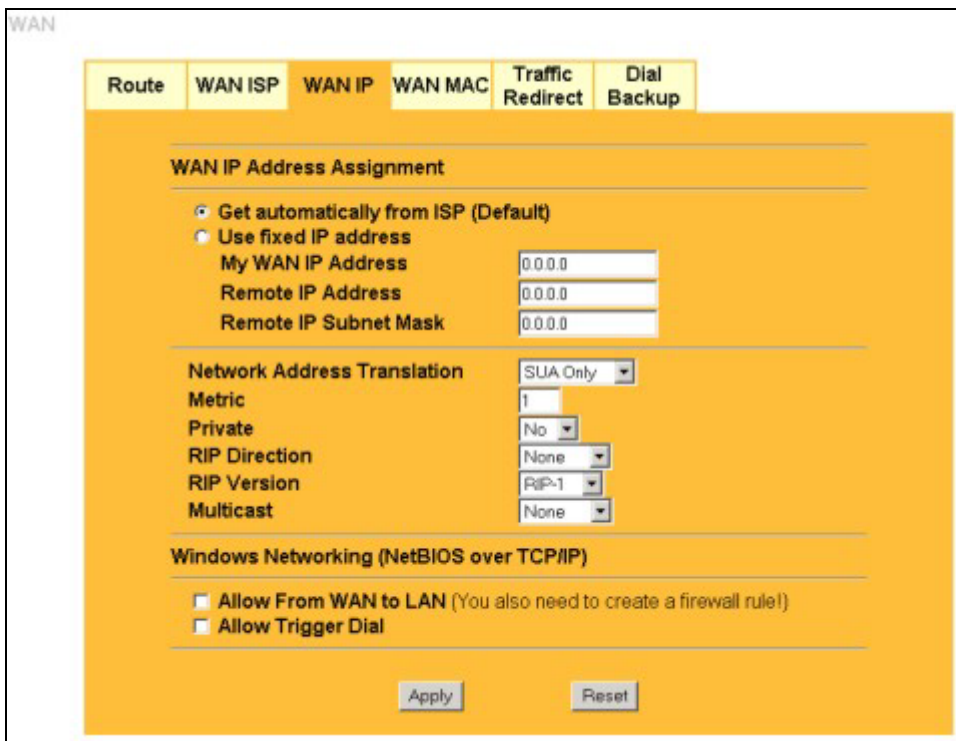


Figure 6-5 WAN: IP

The following table describes the labels in this screen.

Table 6-7 WAN: IP

LABEL	DESCRIPTION
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use fixed IP address	Select this option If the ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected Use Fixed IP Address .

Table 6-7 WAN: IP

LABEL	DESCRIPTION
My WAN IP Subnet Mask (Ethernet only)	Type your network's IP subnet Mask.
Remote IP Address	Enter the Remote IP Address (if your ISP gave you one) in this field.
Gateway/Remote IP Address	Enter the gateway IP address (if your ISP gave you one) in this field if you selected Use Fixed IP Address .
Network Address Translation	<p>Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).</p> <p>Choose None to disable NAT.</p> <p>Choose SUA Only if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: Many-to-One and Server.</p> <p>Choose Full Feature if you have multiple public IP addresses. Full Feature mapping types include: One-to-One, Many-to-One (SUA/PAT), Many-to-Many Overload, Many- One-to-One and Server. When you select Full Feature you must configure at least one address mapping set!</p> <p>For more information about NAT refer to the <i>NAT</i> chapter in this <i>User's Guide</i>.</p>
Metric (PPPoE and PPTP only)	<p>This field sets this route's priority among the routes the Prestige uses.</p> <p>The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".</p>
Private (PPPoE and PPTP only)	This parameter determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to Yes, this route is kept private and not included in RIP broadcast. If No, the route to this remote node will be propagated to other hosts through RIP broadcasts.

Table 6-7 WAN: IP

LABEL	DESCRIPTION
RIP Direction	<p>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.</p> <p>Choose Both, None, In Only or Out Only.</p> <p>When set to Both or Out Only, the Prestige will broadcast its routing table periodically.</p> <p>When set to Both or In Only, the Prestige will incorporate RIP information that it receives.</p> <p>When set to None, the Prestige will not send any RIP packets and will ignore any RIP packets received.</p> <p>By default, RIP Direction is set to Both.</p>
RIP Version	<p>The RIP Version field controls the format and the broadcasting method of the RIP packets that the Prestige sends (it recognizes both formats when receiving).</p> <p>Choose RIP-1, RIP-2B or RIP-2M.</p> <p>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. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, the RIP Version field is set to RIP-1.</p>
Multicast	<p>Choose None (default), IGMP-V1 or IGMP-V2. IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed information about interoperability between IGMP version 2 and version 1, please see sections 4 and 5 of RFC 2236.</p>
<p>Windows Networking (NetBIOS over TCP/IP):</p> <p>NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN. For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls. However it may sometimes be necessary to allow NetBIOS packets to pass through to the WAN in order to find a computer on the WAN.</p>	

Table 6-7 WAN: IP

LABEL	DESCRIPTION
Allow between WAN and LAN	Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to enable the default WAN to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN.
Allow Trigger Dial	Select this option to allow NetBIOS packets to initiate calls.
Apply	Click Apply to save your changes back to the Prestige.
Reset	Click Reset to begin configuring this screen afresh.

6.7 Configuring WAN MAC

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



Figure 6-6 MAC Setup

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

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

6.8 Traffic Redirect

Traffic redirect forwards WAN traffic to a backup gateway when the Prestige cannot connect to the Internet through its normal gateway. Connect the backup gateway on the WAN so that the Prestige still provides firewall protection.

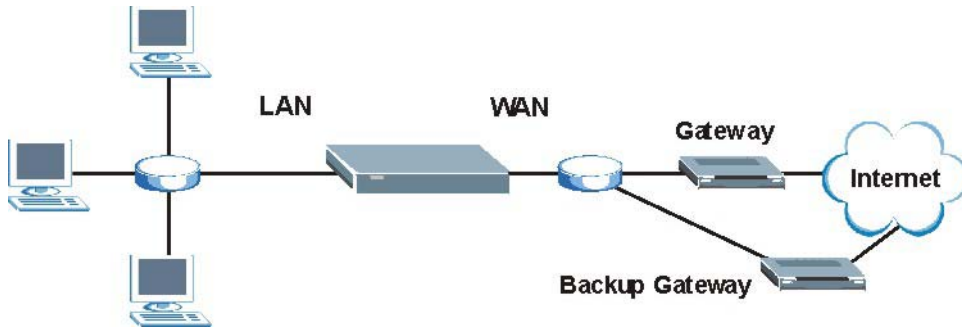


Figure 6-7 Traffic Redirect WAN Setup

The following network topology allows you to avoid triangle route security issues (see the *Appendices*) 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 a LAN to LAN/Prestige firewall rule that forwards packets from the protected LAN (Subnet 1) to the backup gateway (Subnet 2).

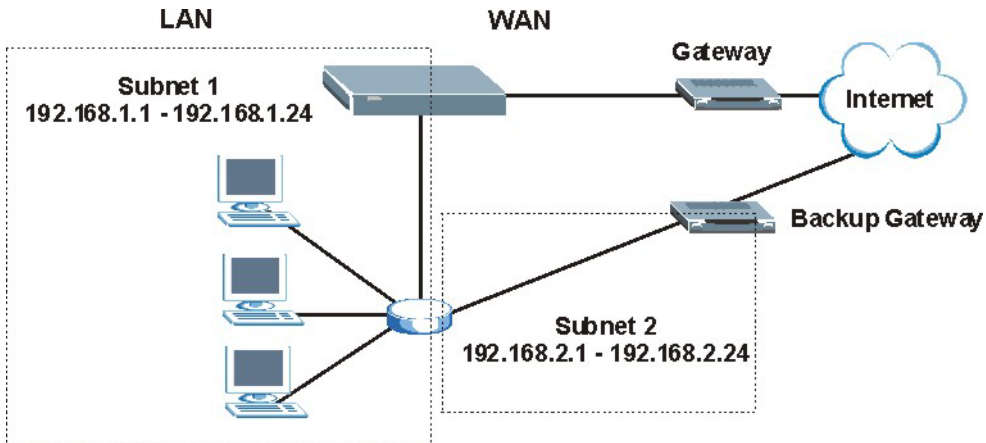


Figure 6-8 Traffic Redirect LAN Setup

6.9 Configuring Traffic Redirect

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

Figure 6-9 WAN: Traffic Redirect

The following table describes the labels in this screen.

Table 6-8 WAN: Traffic Redirect

LABEL	DESCRIPTION
Active	Select this check box to have the Prestige use traffic redirect if the normal WAN connection goes down.
Backup Gateway IP Address	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.
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".

Table 6-8 WAN: Traffic Redirect

LABEL	DESCRIPTION
Check WAN IP Address	Configuration of this field is optional. If you do not enter an IP address here, the Prestige will use the default gateway IP address. 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). If you are using PPTP or PPPoE Encapsulation, type "0.0.0.0" to configure the Prestige to check the PVC (Permanent Virtual Circuit) or PPTP tunnel.
Fail Tolerance	Type the number of times your Prestige may attempt and fail to connect to the Internet before traffic is forwarded to the backup gateway.
Period (seconds)	Type the number of seconds for the Prestige to wait between checks to see if it can connect to the WAN IP address (Check WAN IP Address field) or default gateway. Allow more time if your destination IP address handles lots of traffic.
Timeout (seconds)	Type the number of seconds for your Prestige to wait for a ping response from the IP Address in the Check WAN IP Address field before it times out. The WAN connection is considered "down" after the Prestige times out the number of times specified in the Fail Tolerance field. Use a higher value in this field if your network is busy or congested.
Apply	Click Apply to save your changes back to the Prestige.
Reset	Click Reset to begin configuring this screen afresh.

6.10 Configuring Dial Backup

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

WAN

Route WAN ISP WAN IP WAN MAC Traffic Redirect **Dial Backup**

Enable Dial Backup

Basic Settings

Login Name: ChangeMe
 Password:
 Retype to Confirm:
 Authentication Type: CHAP/PAP
 Primary Phone Number:
 Secondary Phone Number: (Optional)
 Dial Backup Port Speed: 115200
 AT Command Initial String: at&fs0=0
 Advanced Modem Setup:

TCP/IP Options

Priority (Metric): 15 (1(Highest) ~ 15(Lowest))
 Get IP Address Automatically from Remote Server
 Use Fixed IP Address
 My WAN IP Address: 0.0.0.0
 Remote Node IP Address: 0.0.0.0
 Remote IP Subnet Mask: 0.0.0.0

Enable SUA
 Enable RIP
 RIP Version: RIP-1
 RIP Direction: Both
 Broadcast Dial Backup Route

Enable Multicast
 Multicast Version: IGMPv1

PPP Options

PPP Encapsulation: Standard PPP
 Enable Compression

Budget

Always On
 Configure Budget
 Allocated Budget: 0 (Minutes)
 Period: 0 (Hours)
 Idle Timeout: 100 (Seconds)

Figure 6-10 Dial Backup Setup

The following table describes the labels in this screen.

Table 6-9 Dial Backup Setup

LABEL	DESCRIPTION
Enable Dial Backup	Select this check box to turn on dial backup.
Basic Settings	
Login Name	Type the login name assigned by your ISP.
Password	Type the password assigned by your ISP.
Retype to Confirm	Type your password again to make sure that you have entered is correctly.
Authentication Type	<p>Use the drop-down list box to select an authentication protocol for outgoing calls. Options are:</p> <p>CHAP/PAP - Your Prestige accepts either CHAP or PAP when requested by this remote node.</p> <p>CHAP - Your Prestige accepts CHAP only.</p> <p>PAP - Your Prestige accepts PAP only.</p>
Primary/ Secondary Phone Number	Type the first (primary) phone number from the ISP for this remote node. If the Primary Phone number is busy or does not answer, your Prestige dials the Secondary Phone number if available. Some areas require dialing the pound sign # before the phone number for local calls. Include a # symbol at the beginning of the phone numbers as required.
Dial Backup Port Speed	Use the drop-down list box to select the speed of the connection between the Dial Backup port and the external device. Available speeds are: 9600, 19200, 38400, 57600, 115200 or 230400 bps.
AT Command Initial String	Type the AT command string to initialize the WAN device. Consult the manual of your WAN device connected to your Dial Backup port for specific AT commands.
Advanced Modem Setup	Click Edit to display the Advanced Setup screen and edit the details of your dial backup setup.
TCP/IP Options	
Priority (Metric)	<p>This field sets this route's priority among the three routes the Prestige uses (normal, traffic redirect and dial backup). Type a number (1 to 15) to set the priority of the dial backup route for data transmission. The smaller the number, the higher the priority.</p> <p>If the three routes have the same metrics, the priority of the routes is as follows: WAN, Traffic Redirect, Dial Backup.</p>

Table 6-9 Dial Backup Setup

LABEL	DESCRIPTION
Get IP Address Automatically from Remote Server	Type the login name assigned by your ISP for this remote node.
Used Fixed IP Address	Select this check box if your ISP assigned you a fixed IP address, then enter the IP address in the following field.
My WAN IP Address	Leave the field set to 0.0.0.0 (default) to have the ISP or other remote router dynamically (automatically) assign your WAN IP address if you do not know it. Type your WAN IP address here if you know it (static). This is the address assigned to your local Prestige, not the remote router.
Remote Node IP Address	Leave this field set to 0.0.0.0 (default) to have the ISP or other remote router dynamically (automatically) send its IP address if you do not know it. Type the remote gateway's IP address here if you know it (static).
Remote IP Subnet Mask	Leave this field set to 0.0.0.0 (default) to have the ISP or other remote router dynamically send its subnet mask if you do not know it. Type the remote gateway's subnet mask here if you know it (static).
Enable SUA	<p>Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network to a different IP address known within another network.</p> <p>SUA (Single User Account) is a subset of NAT that supports two types of mapping: Many-to-One and Server. When you select this option the Prestige will use Address Mapping Set 255 in the SMT (see the section on menu 15.1 for more information).</p> <p>Select the check box to enable SUA. Clear the check box to disable SUA so the Prestige does not perform any NAT mapping for the dial backup connection.</p>
Enable RIP	Select this check box to turn on RIP (Routing Information Protocol), which allows a router to exchange routing information with other routers.

Table 6-9 Dial Backup Setup

LABEL	DESCRIPTION
RIP Version	<p>The RIP Version field controls the format and the broadcasting method of the RIP packets that the Prestige sends (it recognizes both formats when receiving). Choose RIP-1, RIP-2B or RIP-2M.</p> <p>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. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.</p>
RIP Direction	<p>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.</p> <p>Choose Both, In Only or Out Only.</p> <p>When set to Both or Out Only, the Prestige will broadcast its routing table periodically.</p> <p>When set to Both or In Only, the Prestige will incorporate RIP information that it receives.</p>
Broadcast Dial Backup Route	Select this check box to forward the backup route broadcasts to the WAN.
Enable Multicast	Select this check box to turn on IGMP (Internet Group Multicast Protocol). IGMP is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data.
Multicast Version	Select IGMP-v1 or IGMP-v2 . 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 <i>sections 4 and 5 of RFC 2236</i> .
PPP Options	
PPP Encapsulation	Select CISCO PPP from the drop-down list box if your dial backup WAN device uses Cisco PPP encapsulation, otherwise select Standard PPP .
Enable Compression	Select this check box to turn on stac compression.
Budget	
Always On	Select this check box to have the dial backup connection on all of the time.

Table 6-9 Dial Backup Setup

LABEL	DESCRIPTION
Configure Budget	Select this check box to have the dial backup connection on during the time that you select.
Allocated Budget	Type the amount of time (in minutes) that the dial backup connection can be used during the time configured in the Period field. Set an amount that is less than the time period configured in the Period field.
Period	Type the time period (in hours) for how often the budget should be reset. For example, to allow calls to this remote node for a maximum of 10 minutes every hour, set the Allocated Budget to 10 (minutes) and the Period to 1 (hour).
Idle Timeout	Type the number of seconds of idle time (when there is no traffic from the Prestige to the remote node) for the Prestige to wait before it automatically disconnects the dial backup connection. This option applies only when the Prestige initiates the call. The dial backup connection never times out if you set this field to "0" (it is the same as selecting Always On).
Apply	Click Apply to save your changes back to the Prestige.
Reset	Click Reset to begin configuring this screen afresh.

6.11 Advanced Modem Setup

6.11.1 AT Command Strings

For regular telephone lines, the default "Dial" string tells the modem that the line uses tone dialing. "ATDT" is the command for a switch that requires tone dialing. If your switch requires pulse dialing, change the string to "ATDP".

For ISDN lines, there are many more protocols and operational modes. Please consult the documentation of your TA. You may need additional commands in both "Dial" and "Init" strings.

6.11.2 DTR Signal

The majority of WAN devices default to hanging up the current call when the DTR (Data Terminal Ready) signal is dropped by the DTE. When the "Drop DTR When Hang Up" check box is selected, the Prestige uses this hardware signal to force the WAN device to hang up, in addition to issuing the drop command "ATH".

6.11.3 Response Strings

The response strings tell the Prestige the tags, or labels, immediately preceding the various call parameters sent from the WAN device. The response strings have not been standardized; please consult the documentation of your WAN device to find the correct tags.

6.12 Configuring Advanced Modem Setup

Click the **Edit** button in the **Dial Backup** screen to display the **Advanced Setup** screen shown next.

Consult the manual of your WAN device connected to your dial backup port for specific AT commands.

ADVANCED SETUP

AT Command Strings

Dial

Drop

Answer

Drop DTR When Hang Up

AT Response Strings

CLID

Called ID

Speed

Call Control

Dial Timeout (sec)

Retry Count

Retry Interval (sec)

Drop Timeout (sec)

Call Back Delay (sec)

Figure 6-11 Advanced Setup

The following table describes the labels in this screen.

Table 6-10 Advanced Setup

LABEL	DESCRIPTION	EXAMPLE
AT Command Strings		
Dial	Type the AT Command string to make a call.	atdt

Table 6-10 Advanced Setup

LABEL	DESCRIPTION	EXAMPLE
Drop	Type the AT Command string to drop a call. "~" represents a one second wait, for example, "~++++~ath" can be used if your modem has a slow response time.	~++++~ath
Answer	Type the AT Command string to answer a call.	ata
Drop DTR When Hang Up	Select this check box to have the Prestige drop the DTR (Data Terminal Ready) signal after the "AT Command String: Drop" is sent out.	
AT Response Strings		
CLID	Type the keyword that precedes the CLID (Calling Line Identification) in the AT response string. This lets the Prestige capture the CLID in the AT response string that comes from the WAN device. CLID is required for CLID authentication.	NMBR
Called ID	Type the keyword preceding the dialed number.	
Speed	Type the keyword preceding the connection speed.	CONNECT
Call Control		
Dial Timeout (sec)	Type a number of seconds for the Prestige to try to set up an outgoing call before timing out (stopping).	60
Retry Count	Type a number of times for the Prestige to retry a busy or no-answer phone number before blacklisting the number.	0
Retry Interval (sec)	Type a number of seconds for the Prestige to wait before trying another call after a call has failed. This applies before a phone number is blacklisted.	10
Drop Timeout (sec)	Type the number of seconds for the Prestige to wait before dropping the DTR signal if it does not receive a positive disconnect confirmation.	20
Call Back Delay (sec)	Type a number of seconds for the Prestige to wait between dropping a callback request call and dialing the corresponding callback call.	15
Apply	Click Apply to save your changes back to the Prestige.	
Cancel	Click Cancel to exit this screen without saving.	

Part III:

NAT and Static Route

This part covers Network Address Translation and setting up static routes.

Chapter 7

Network Address Translation (NAT)

Screens

This chapter discusses how to configure NAT on the Prestige.

7.1 NAT Overview

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

7.1.1 NAT Definitions

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

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

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

Table 7-1 NAT Definitions

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

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

7.1.2 What NAT Does

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

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

7.1.3 How NAT Works

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

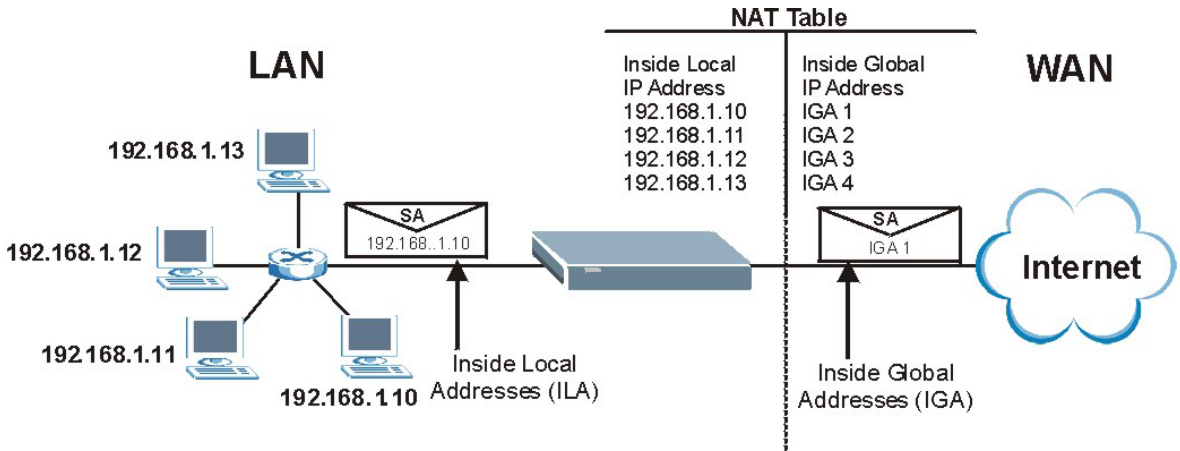


Figure 7-1 How NAT Works

7.1.4 NAT Application

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

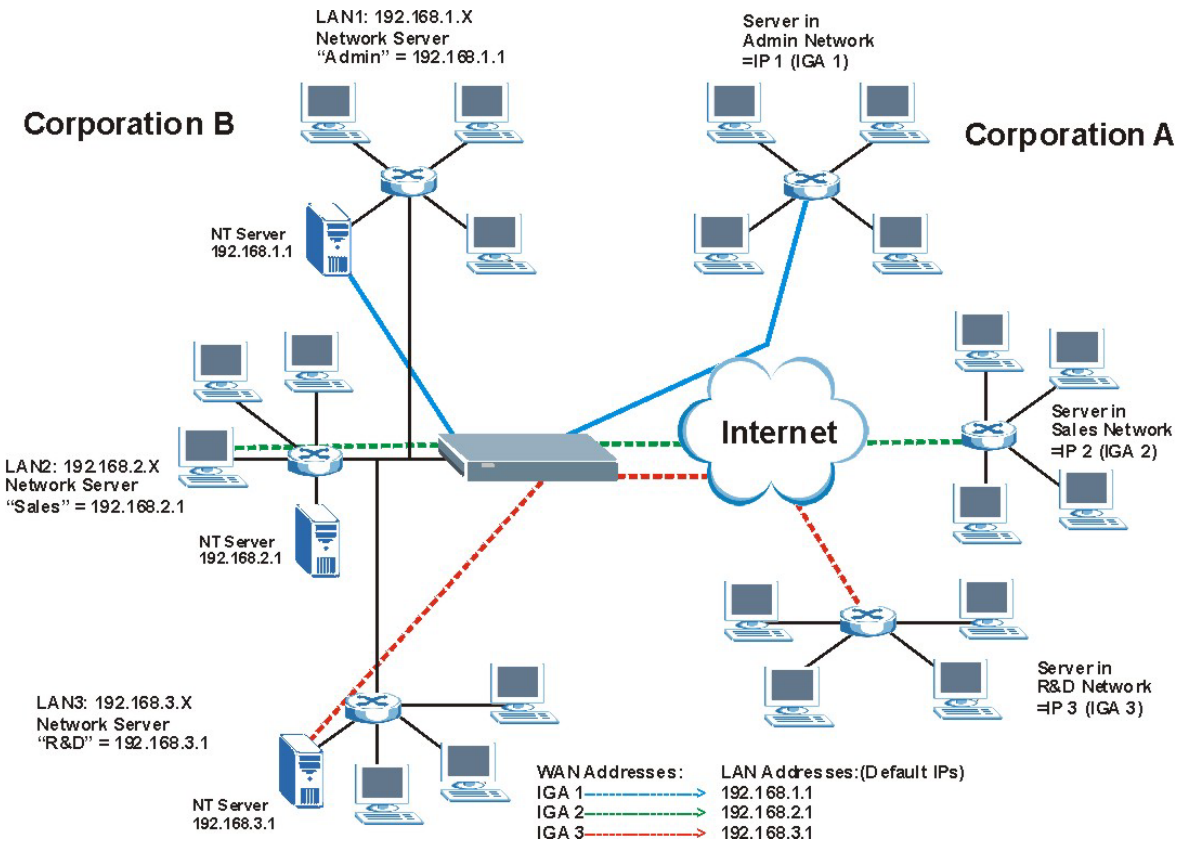


Figure 7-2 NAT Application With IP Alias

7.1.5 NAT Mapping Types

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

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

- **Many One-to-One:** In Many-One-to-One mode, the Prestige maps each local IP address to a unique global IP address.
- **Server:** This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.

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

The following table summarizes these types.

Table 7-2 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 One-to-One	ILA1↔ IGA1 ILA2↔ IGA2 ILA3↔ IGA3 ...	M-1-1
Server	Server 1 IP↔ IGA1 Server 2 IP↔ IGA1 Server 3 IP↔ IGA1	Server

7.2 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.

7.2.1 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**. The Prestige also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types. Select either **SUA Only** or **Full Feature** in the **WAN IP** screen.

7.3 SUA Server

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

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

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

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 a Default Server IP Address, the Prestige discards all packets received for ports that are not specified in this screen or remote management.

7.3.1 Port Forwarding: Services and Port Numbers

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

Use the **SUA Server** page to forward incoming service requests to the server(s) on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port

21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers.

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

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.

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

Table 7-3 Services and Port Numbers

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

7.3.2 Configuring Servers Behind SUA (Example)

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

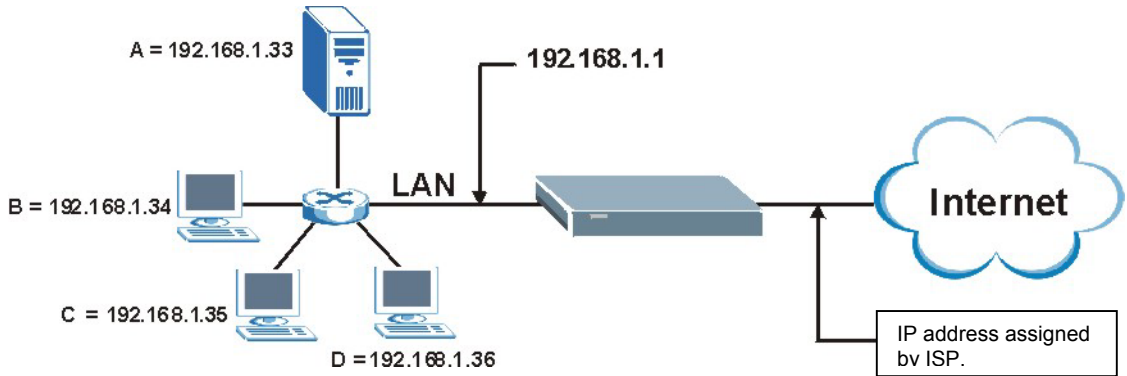


Figure 7-3 Multiple Servers Behind NAT Example

7.4 Configuring SUA Server

If you do not assign a Default Server IP Address, the Prestige discards all packets received for ports that are not specified in this screen or remote management.

Click SUA/NAT to open the SUA Server screen.

Refer to *Table 7-3* for port numbers commonly used for particular services.

SUA/NAT

SUA Server Address Mapping Trigger Port

Default Server

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

Figure 7-4 SUA/NAT Setup

The following table describes the labels in this screen.

Table 7-4 SUA/NAT Setup

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

Table 7-4 SUA/NAT Setup

LABEL	DESCRIPTION
Server IP Address	Enter the inside IP address of the server here.
Apply	Click Apply to save your changes back to the Prestige.
Reset	Click Reset to begin configuring this screen afresh.

7.5 Configuring Address Mapping

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

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

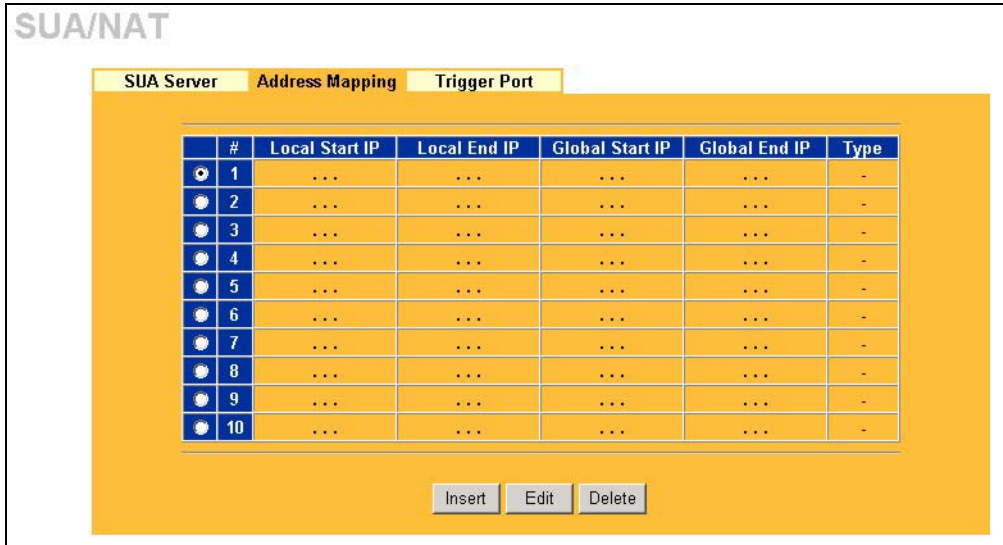


Figure 7-5 Address Mapping

The following table describes the labels in this screen.

Table 7-5 Address Mapping

LABEL	DESCRIPTION
Local Start IP	This refers to the Inside Local Address (ILA), which is the starting local IP address. If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the Local Start IP address. Local IP addresses are N/A for Server port mapping.
Local End IP	This is the end Inside Local Address (ILA). If the rule is for all local IP addresses, then this field displays 255.255.255.255 as the Local End IP address. This field is N/A for One-to-One and Server mapping types.
Global Start IP	This refers to the Inside Global IP Address (IGA). 0.0.0.0 is for a dynamic IP address from your ISP with Many-to-One and Server mapping types.
Global End IP	This is the ending Inside Global Address (IGA), which is the starting global IP address. This field is N/A for One-to-One , Many-to-One and Server mapping types.
Type	<ol style="list-style-type: none"> 1. One-to-One mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type. 2. 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. 3. Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. 4. Many One-to-One mode maps each local IP address to unique global IP addresses. 5. Server allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Insert	Click Insert to insert a new mapping rule before an existing one.
Edit	Click Edit to go to the Address Mapping Rule screen.
Delete	Click Delete to delete an address mapping rule.

Configuring Address Mapping

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

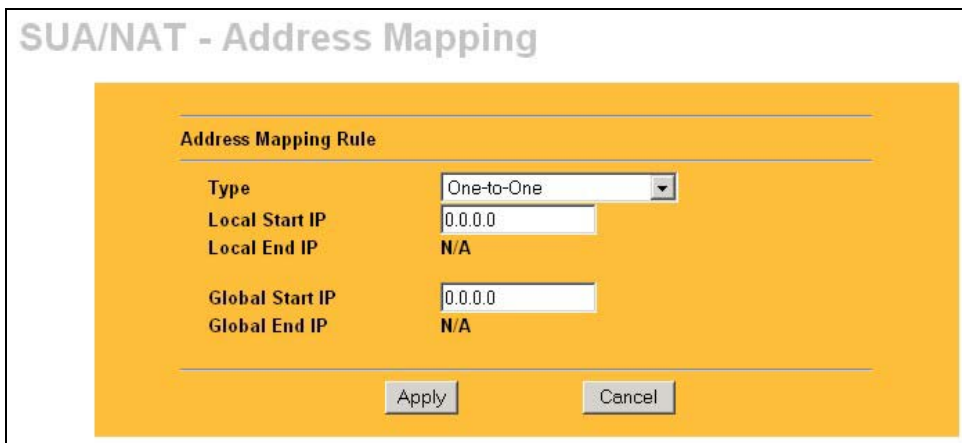


Figure 7-6 Address Mapping Edit

The following table describes the labels in this screen.

Table 7-6 Address Mapping Edit

LABEL	DESCRIPTION
Type	<p>Choose the port mapping type from one of the following.</p> <ol style="list-style-type: none"> 1. One-to-One: One-to-one mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-one NAT mapping type. 2. Many-to-One: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature. 3. Many-to-Many Overload: Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. 4. Many One-to-One: Many One-to-one mode maps each local IP address to unique global IP addresses. 5. Server: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Local Start IP	<p>This is the starting Inside Local IP Address (ILA). Local IP addresses are N/A for Server port mapping.</p>
Local End IP	<p>This is the end Inside Local IP Address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address.</p> <p>This field is N/A for One-to-One and Server mapping types.</p>

Table 7-6 Address Mapping Edit

LABEL	DESCRIPTION
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP.
Global End IP	This is the ending Inside Global IP Address (IGA). This field is N/A for One-to-One , Many-to-One and Server mapping types.
Apply	Click Apply to save your changes back to the Prestige.
Cancel	Click Cancel to return to the previous screen and not save your changes.

7.6 Trigger Port Forwarding

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

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

7.6.1 Trigger Port Forwarding Example

The following is an example of trigger port forwarding.

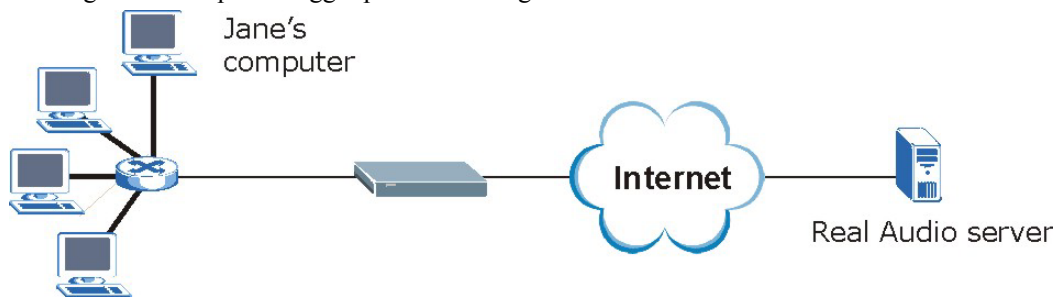


Figure 7-7 Trigger Port Forwarding Process: Example

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

7.6.2 Two Points To Remember About Trigger Ports

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

7.7 Configuring Trigger Port Forwarding

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

Only one LAN computer can use a trigger port (range) at a time.

SUA/NAT

SUA Server Address Mapping **Trigger Port**

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

Apply Reset

Figure 7-8 Trigger Port

The following table describes the labels in this screen.

Table 7-7 Trigger Port

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

Table 7-7 Trigger Port

LABEL	DESCRIPTION
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Apply	Click Apply to save your changes back to the Prestige.
Reset	Click Reset to begin configuring this screen afresh.

Chapter 8

Static Route Screens

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

8.1 Static Route Overview

Each remote node specifies only the network to which the gateway is directly connected, and the Prestige has no knowledge of the networks beyond. For instance, the Prestige knows about network N2 in the following figure through remote node router R1. However, the Prestige is unable to route a packet to network N3 because it doesn't know that there is a route through the same remote node router R1 (via gateway router R2). The static routes are for you to tell the Prestige about the networks beyond the remote nodes.

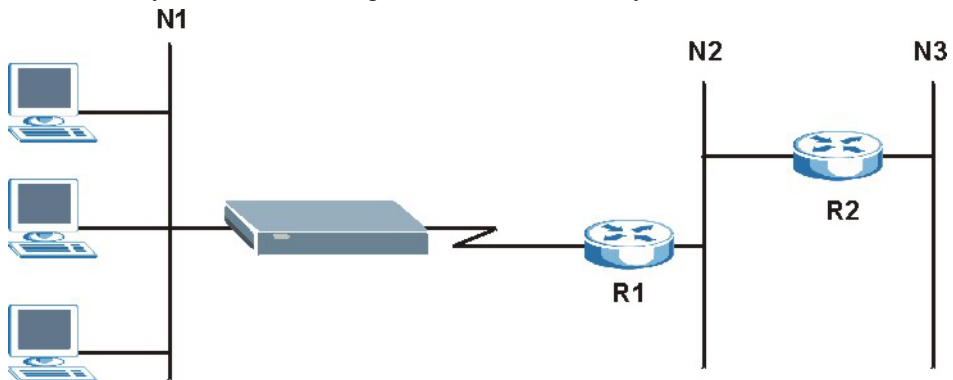


Figure 8-1 Example of Static Routing Topology

8.2 Configuring IP Static Route

Click **STATIC ROUTE** to open the screen as shown next.



Figure 8-2 Static Route

The following table describes the labels in this screen.

Table 8-1 Static Route

LABEL	DESCRIPTION
#	Number of an individual static route.
Name	Name that describes or identifies this route.
Active	This field shows whether this static route is active (Yes) or not (No).
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Gateway	This is the IP address of the gateway. The gateway is 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 the WAN, the gateway must be the IP address of one of the remote nodes.
Edit	Select a static route index number and then click Edit to set up a static route on the Prestige.

8.2.1 Configuring Route Entry

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

STATIC ROUTE - EDIT

Route Name

Active

Destination IP Address

IP Subnet Mask

Gateway IP Address

Metric

Private

Figure 8-3 Static Route: Edit

The following table describes the labels in this screen.

Table 8-2 Static Route: Edit

LABEL	DESCRIPTION
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	Enter the IP address of the gateway. The gateway is 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 the 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. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.

Table 8-2 Static Route: Edit

LABEL	DESCRIPTION
Private	This parameter determines if the Prestige will include this route to a remote node in its RIP broadcasts. Select this check box to keep this route private and not included in RIP broadcasts. Clear this checkbox to propagate this route to other hosts through RIP broadcasts.
Apply	Click Apply to save your changes back to the Prestige.
Cancel	Click Cancel to return to the previous screen and not save your changes.

Part IV:

UPnP and Firewall

This part provides information and configuration instructions for configuration of Universal Plug and Play, firewall and content filtering.

Chapter 9

UPnP

This chapter introduces the Universal Plug and Play feature.

9.1 Universal Plug and Play Overview

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.

9.1.1 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.

9.1.2 NAT Traversal

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

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

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

See the *SUA/NAT* chapter for further information about NAT.

9.1.3 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.

9.2 UPnP and ZyXEL

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

UPnP broadcasts are only allowed on the LAN.

Please see later in this *User's Guide* for examples of installing UPnP in Windows XP and Windows Me as well as an example of using UPnP in Windows.

9.3 Configuring UPnP

Click **UPnP** to display the screen shown next.

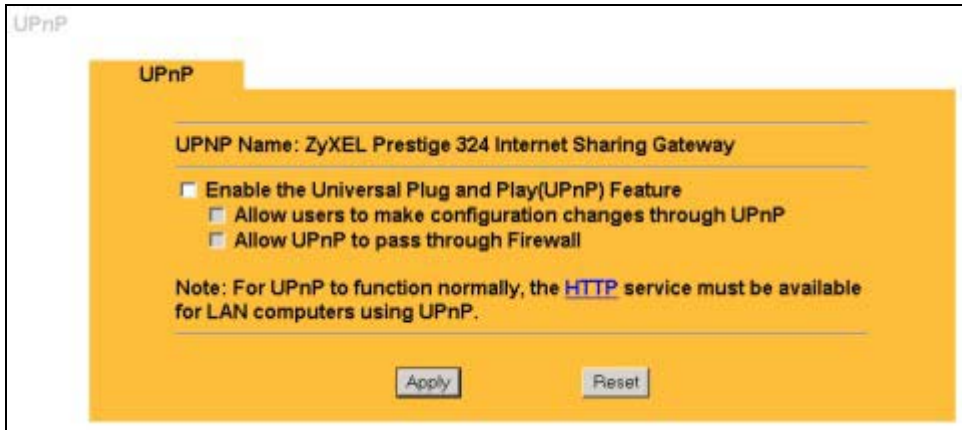


Figure 9-1 Configuring UPnP

The following table describes the labels in this screen.

Table 9-1 Configuring UPnP

LABEL	DESCRIPTION
Enable the Universal Plug and Play (UPnP) feature	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 Apply to save your changes back to the Prestige.
Reset	Click Reset to begin configuring this screen afresh.

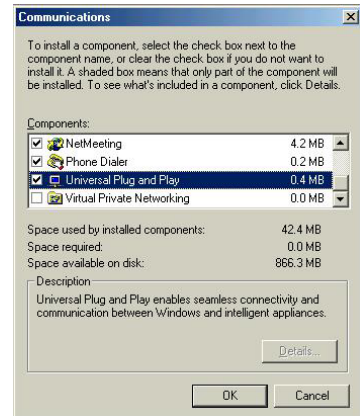
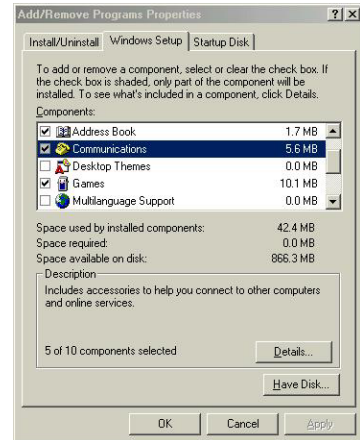
9.4 Installing UPnP in Windows Example

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

9.4.1 Installing UPnP in Windows Me

Follow the steps below to install UPnP in Windows Me.

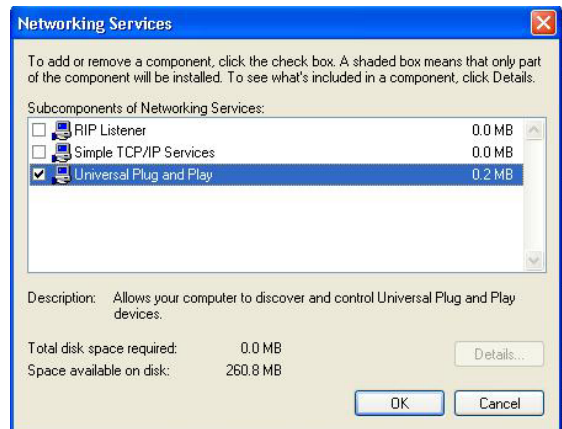
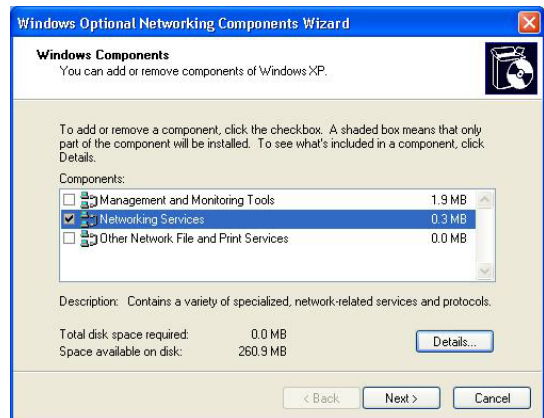
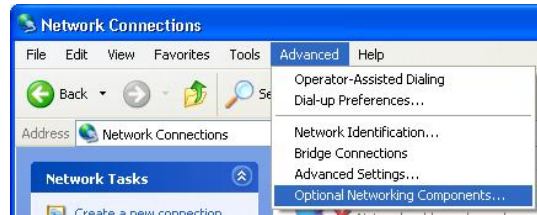
- Step 1.** Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.
- Step 2.** Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.
- Step 3.** In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.
- Step 4.** Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.
- Step 5.** Restart the computer when prompted.



9.4.2 Installing UPnP in Windows XP

Follow the steps below to install UPnP in Windows XP.

- Step 1.** Click **Start** and **Control Panel**.
- Step 2.** Double-click **Network Connections**.
- Step 3.** In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components ...**.
The **Windows Optional Networking Components Wizard** window displays.
- Step 4.** Select **Networking Service** in the **Components** selection box and click **Details**.
- Step 5.** In the **Networking Services** window, select the **Universal Plug and Play** check box.
- Step 6.** Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.



9.5 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 ZyXEL device.

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

9.5.1 Auto-discover Your UPnP-enabled Network Device

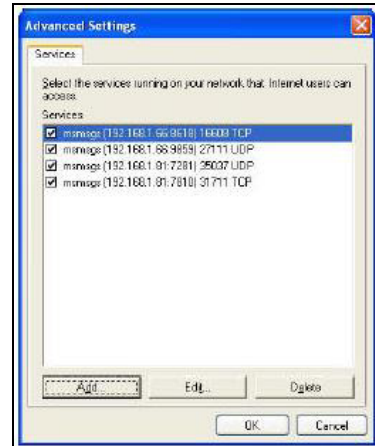
- Step 1.** Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.
- Step 2.** Right-click the icon and select **Properties**.



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



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



When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

Step 5. Select the **Show icon in notification area when connected** check box and click **OK**. An icon displays in the system tray



Step 6. Double-click the icon to display your current Internet connection status.

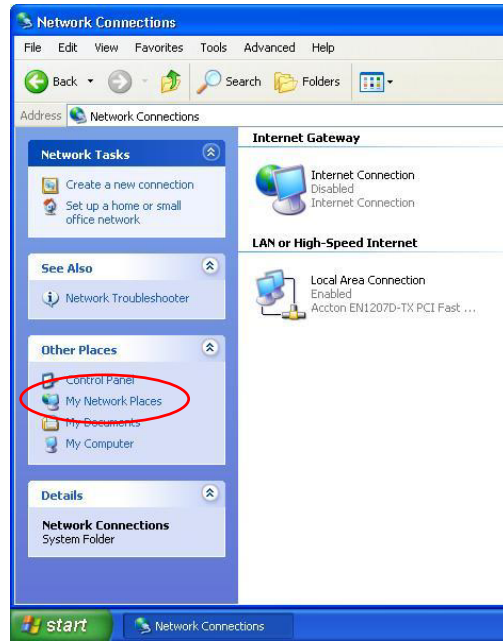


9.5.2 Web Configurator Easy Access

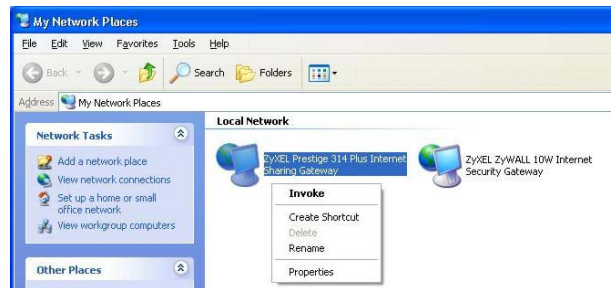
With UPnP, you can access the web-based configurator on the ZyXEL device without finding out the IP address of the ZyXEL device first. This is helpful if you do not know the IP address of the ZyXEL device.

Follow the steps below to access the web configurator.

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



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



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



Chapter 10

Firewall

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

10.1 Introduction

What is a Firewall?

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.

Stateful Inspection Firewall.

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

About the Prestige Firewall

The Prestige firewall is a stateful inspection firewall and is designed to protect against Denial of Service attacks when activated (click **FIREWALL** and then click the **Enable Firewall** check box). The Prestige's purpose is to allow a private Local Area Network (LAN) to be securely connected to the Internet. The

Prestige can be used to prevent theft, destruction and modification of data, as well as log events, which may be important to the security of your network.

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

The Prestige has one Ethernet WAN port and four Ethernet LAN ports, which are used to physically separate the network into two areas.

The WAN (Wide Area Network) port attaches to the broadband (cable or DSL) modem to the Internet.

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

10.1.1 Guidelines For Enhancing Security With Your Firewall

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

10.2 Firewall Settings Screen

From the **MAIN MENU**, click **FIREWALL** to open the **Settings** screen.

FIREWALL

Settings
Filter
Services

Enable Firewall
 Bypass Triangle Route

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

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

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

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

Trusted Computer IP Address:

Figure 10-1 Firewall: Settings

The following table describes the labels in this screen.

Table 10-1 Firewall: Settings

LABEL	DESCRIPTION
Enable Firewall	Select this check box to activate the firewall. The Prestige performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Bypass Triangle Route	Select this check box to have the Prestige firewall ignore the use of triangle route topology on the network. See the appendix for more on triangle route topology.
LAN to WAN	To log packets related to firewall rules, make sure that Access Control under Log is selected in the Logs, Log Settings screen.
Packets to Log	Choose what LAN to WAN packets to log. Choose from: <ul style="list-style-type: none"> ➤ No Log ➤ Log Blocked (blocked LAN to WAN services appear in the Blocked Services textbox in the Services screen (with Enable Services Blocking selected)) ➤ Log All (log all LAN to WAN packets)
WAN to LAN	To log packets related to firewall rules, make sure that Access Control under Log is selected in the Logs, Log Settings screen.
Packets to Log	Choose what WAN to LAN and WAN to WAN/Prestige packets to log. Choose from: <ul style="list-style-type: none"> ➤ No Log ➤ Log Forwarded (see how to forward WAN to LAN traffic in the next section) ➤ Log All (log all WAN to LAN packets).
Trusted Computer IP Address	You can allow a specific computer to access all Internet resources without restriction. Enter the IP address of the trusted computer in this field.
Apply	Click Apply to save the settings.
Reset	Click Reset to start configuring this screen again.

10.3 The Firewall, NAT and Remote Management

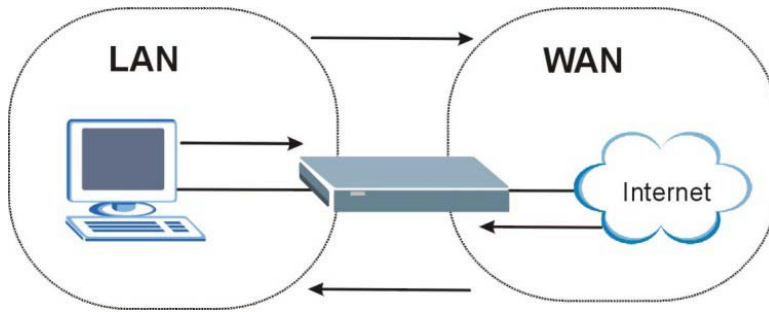


Figure 10-2 Firewall Rule Directions

10.3.1 LAN-to-WAN rules

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

How can you block certain LAN to WAN traffic?

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

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

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

10.3.2 WAN-to-LAN rules

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

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

- Configuring NAT port forwarding rules in the web configurator **SUA Server** screen or SMT NAT menus.
- Configuring **One-to-One** and **Many-One-to-One** NAT mapping rules in the web configurator **Address Mapping** screen or SMT NAT menus.
- Configuring **WAN** or **LAN & WAN** access for services in the **Remote Management** screens or SMT menus. When you allow remote management from the WAN, you are actually configuring WAN-to-WAN/Prestige firewall rules. WAN-to-WAN/Prestige firewall rules are Internet to the Prestige WAN interface firewall rules. The default is to block all such traffic. When you decide what WAN-to-LAN packets to log, you are in fact deciding what **WAN-to-LAN** and WAN-to-WAN/Prestige packets to log.
- Allow NetBIOS traffic from the WAN to the LAN using the **WAN IP** web screen or SMT menu 24.8 commands.

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

10.4 Configuring Content Filtering

Content filtering allows you to block web sites by URL keywords that you specify, for example, you can block access to all web sites with the word “bad” in the URL by specifying “bad” as a keyword. You can also block access to web proxies and pages containing Active X components, Java applets and cookies. Finally you can schedule when the Prestige performs content filtering by day and time.

Click on the **Filter** tab. The screen appears as shown next. Use this screen to restrict web features (Active X, Java, Cookies, Web Proxy), enable URL keyword blocking, enter/delete/modify keywords you want to block and the date/time you want to block them.

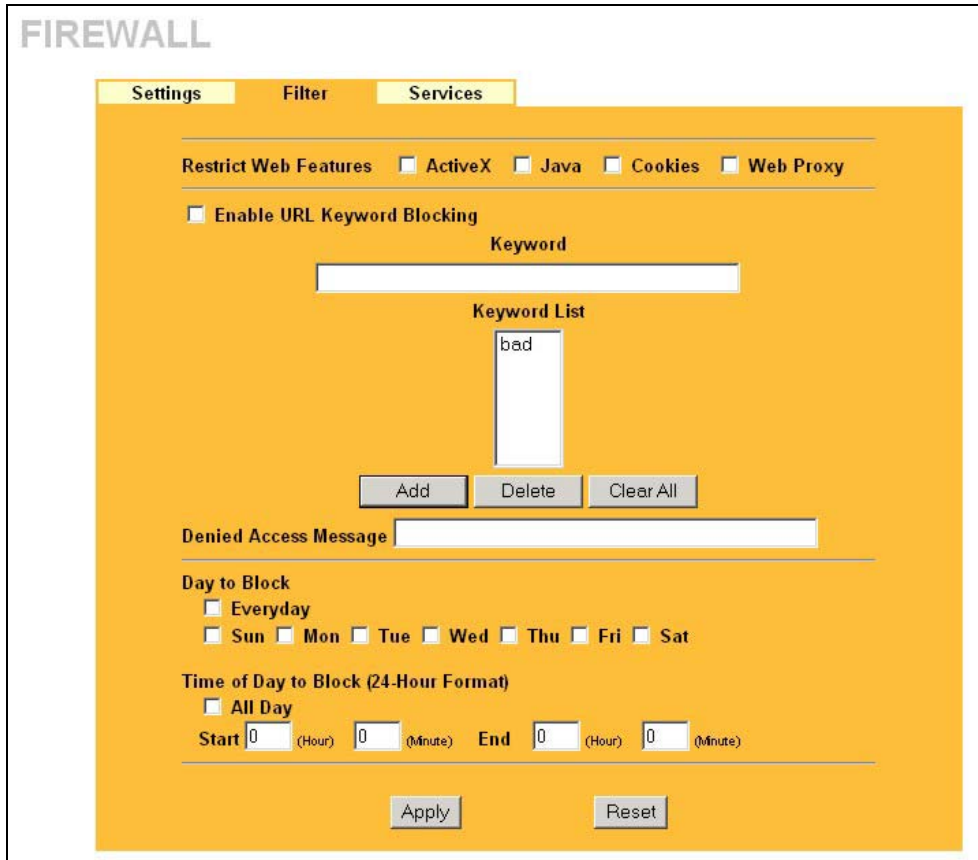


Figure 10-3 Firewall: Filter

The following table describes the labels in this screen.

Table 10-2 Firewall: Filter

LABEL	DESCRIPTION
Restricted Web Features	
ActiveX	ActiveX is a tool for building dynamic and active Web pages and distributed object applications. When you visit an ActiveX Web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again.

Table 10-2 Firewall: Filter

LABEL	DESCRIPTION
Java	Java is a programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds.
Cookies	Web servers that track usage and provide service based on ID use cookies.
Web Proxy	This is a server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN it is possible for LAN users to circumvent content filtering by pointing to this proxy server.
Enable URL Keyword Blocking	Select this option to block the URL containing the keywords in the keyword list.
Keyword	Type a keyword in this field. You may use any character (up to 64 characters). Wildcards are not allowed.
Keyword List	This is a list of keywords that will be inaccessible to computers on your LAN once you enable URL keyword blocking.
Add	Type a keyword in the Keyword field and click then Add to add a keyword to the Keyword List.
Delete	Select a keyword from the Keyword List and then click Delete to remove this keyword from the list.
Clear All	Click Clear All to empty the Keyword List .
Date to Block	Select everyday or the day(s) of the week to activate blocking.
Time of Day to Block	Select All Day or enter the start and end times in the hour-minute format to activate blocking.
Apply	Click Apply to save the settings.
Reset	Click Reset to start configuring this screen again.

10.5 Services

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

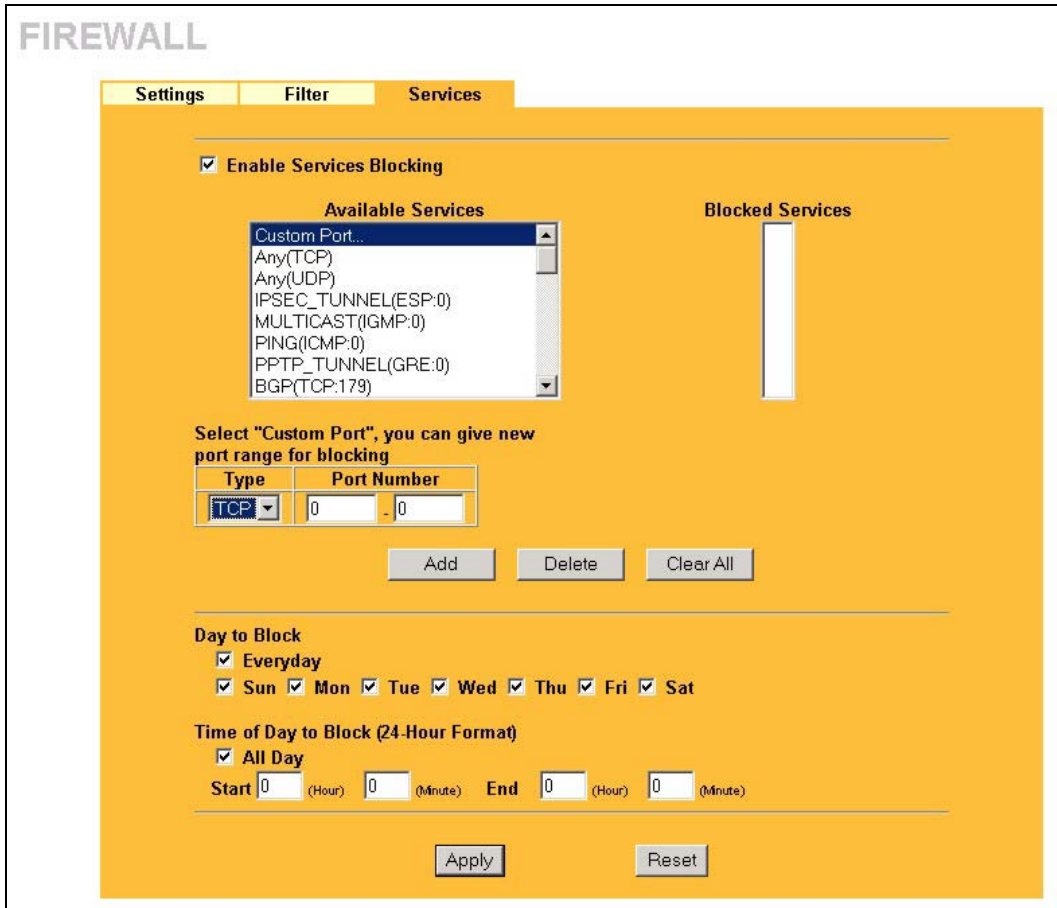


Figure 10-4 Firewall: Service

The following table describes the labels in this screen.

Table 10-3 Firewall: Service

ABEL	DESCRIPTION
Enable Services Blocking	Select this check box to enable this feature.

Table 10-3 Firewall: Service

ABEL	DESCRIPTION
Available Service	This is a list of pre-defined services (ports) you may prohibit your LAN computers from using. Select the port you want to block using the drop-down list and click Add to add the port to the Blocked Service field.
Blocked Service	This is a list of services (ports) that will be inaccessible to computers on your LAN once you enable service blocking. Choose the IP port (TCP , UDP or TCP/UDP) that defines your customized port from the drop down list box.
Custom Port	A custom port is a service that is not available in the pre-defined Available Services list and you must define using the next two fields.
Type	Services are either TCP and/or UDP . Select from either TCP or UDP .
Port Number	Enter the port number range that defines the service. For example, suppose you want to define the Gnutella service. Select TCP type and enter a port range from 6345-6349.
Add	Select a service from the Available Services drop-down list and then click Add to add a service to the Blocked Service.
Delete	Select a service from the Blocked Services List and then click Delete to remove this service from the list.
Clear All	Click Clear All to empty the Blocked Service .
Day to Block:	Select a check box to configure which days of the week (or everyday) you want the content filtering to be active.
Time of Day to Block (24-Hour Format)	Select the time of day you want service blocking to take effect. Configure blocking to take effect all day by selecting the All Day check box. You can also configure specific times that by entering the start time in the Start (hr) and Start (min) fields and the end time in the End (hr) and End (min) fields. Enter times in 24-hour format, for example, "3:00pm" should be entered as "15:00".
Apply	Click Apply to save the settings.
Reset	Click Reset to start configuring this screen again.

Part V:

Remote Management

This part provides information and configuration instructions for configuration of remote management.

Chapter 11

Remote Management Screens

This chapter provides information on the Remote Management screens.

11.1 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. Console port
2. Telnet
3. HTTP

11.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

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

11.1.2 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.

11.1.3 System Timeout

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

11.2 Configuring WWW

To change your Prestige's World Wide Web settings, click **REMOTE MGMT** to display the **WWW** screen.

REMOTE MANAGEMENT

WWW TELNET FTP SNMP DNS Security

WWW

Server Port

Server Access

Secured Client IP Address All Selected

Note: For [UPnP](#) to function normally, the HTTP service must be available for LAN computers using UPnP.

Figure 11-1 Remote Management: WWW

The following table describes the labels in this screen.

Table 11-1 Remote Management: WWW

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

11.3 Configuring Telnet

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

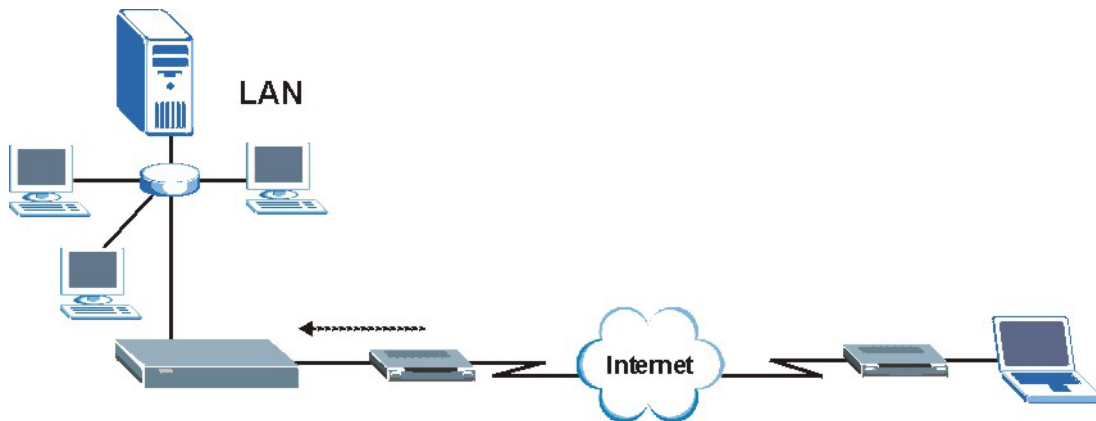


Figure 11-2 Telnet Configuration on a TCP/IP Network

11.4 Configuring TELNET

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

REMOTE MANAGEMENT

WWW
TELNET
FTP
SNMP
DNS
Security

TELNET

Server Port

Server Access

Secured Client IP Address All Selected

Figure 11-3 Remote Management: Telnet

The following table describes the labels in this screen.

Table 11-2 Remote Management: Telnet

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

11.5 Configuring FTP

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

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

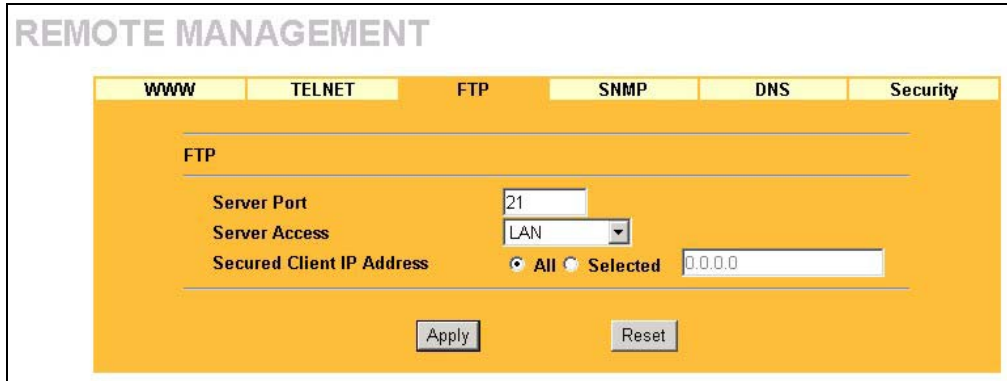


Figure 11-4 Remote Management: FTP

The following table describes the labels in this screen.

Table 11-3 Remote Management: FTP

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

11.6 SNMP

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

The Prestige supports SNMP version one (SNMPv1). The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

SNMP is only available if TCP/IP is configured.

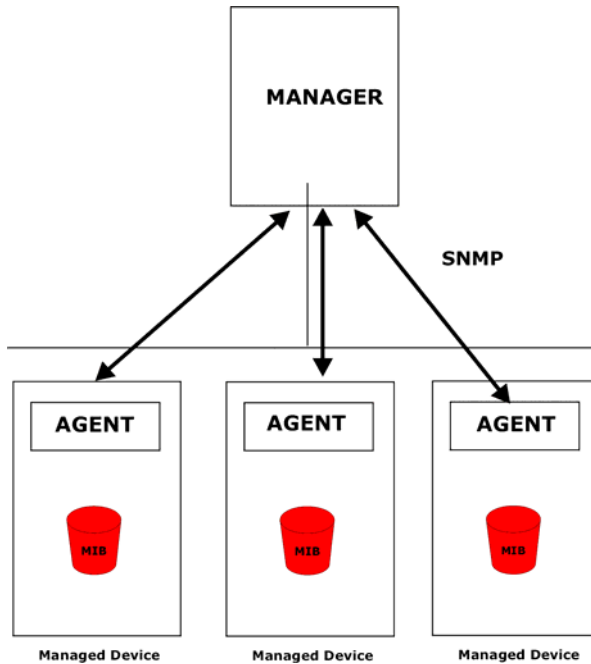


Figure 11-5 SNMP Management Model

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

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

The managed devices contain object variables/managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status

etc. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

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

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

11.6.1 Supported MIBs

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

11.6.2 SNMP Traps

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

Table 11-4 SNMP Traps

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

Table 11-4 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
6b	For fatal error :	A trap is sent with the message of the fatal code if the system reboots because of fatal errors.

11.6.3 Configuring SNMP

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

REMOTE MANAGEMENT

WWW TELNET FTP **SNMP** DNS Security

SNMP Configuration

Get Community public

Set Community public

Trap Community public

Destination 0.0.0.0

SNMP

Service Port 161

Service Access LAN

Secured Client IP Address All Selected 0.0.0.0

Apply Reset

Figure 11-6 Remote Management: SNMP

The following table describes the labels in this screen.

Table 11-5 Remote Management: SNMP

LABEL	DESCRIPTION
SNMP Configuration	
Get Community	Enter the Get Community , which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the Set community , which is the password for incoming Set requests from the management station. The default is public and allows all requests.
Trap	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Destination	Type the IP address of the station to send your SNMP traps to.
SNMP	
Service Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Service Access	Select the interface(s) through which a computer may access the Prestige using this service.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the Prestige using this service. Select All to allow any computer to access the Prestige using this service. Choose Selected to just allow the computer with the IP address that you specify to access the Prestige using this service.
Apply	Click Apply to save your customized settings and exit this screen.
Reset	Click Reset to begin configuring this screen afresh.

11.7 Configuring DNS

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa. Refer to the chapter on Wizard Setup for background information.

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

REMOTE MANAGEMENT

WWW TELNET FTP SNMP DNS **Security**

DNS

Service Port 53

Service Access LAN

Secured Client IP Address All Selected 0.0.0.0

Apply Reset

Figure 11-7 Remote Management: DNS

The following table describes the labels in this screen.

Table 11-6 Remote Management: DNS

LABEL	DESCRIPTION
Server Port	The DNS service port number is 53 and cannot be changed here.
Server Access	Select the interface(s) through which a computer may send DNS queries to the Prestige.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to send DNS queries to the Prestige. Select All to allow any computer to send DNS queries to the Prestige. Choose Selected to just allow the computer with the IP address that you specify to send DNS queries to the Prestige.
Apply	Click Apply to save your customized settings and exit this screen.
Reset	Click Reset to begin configuring this screen afresh.

11.8 Configuring Security

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

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

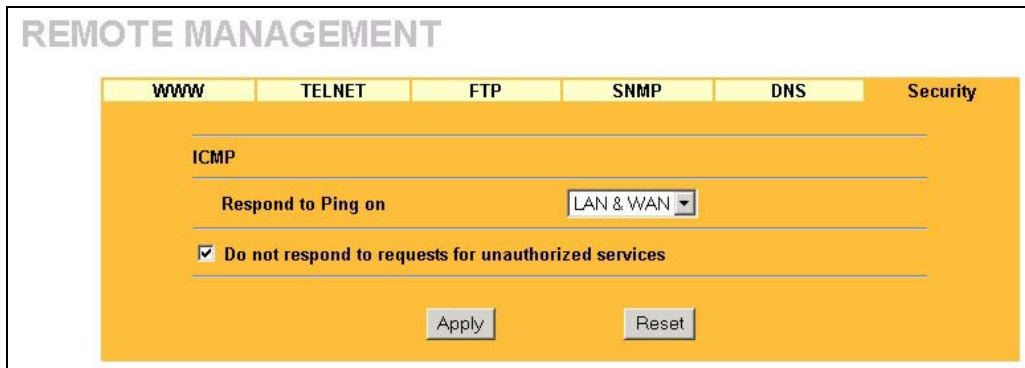


Figure 11-8 Security

The following table describes the labels in this screen.

Table 11-7 Security

LABEL	DESCRIPTION
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.
Respond to Ping on	The Prestige will not respond to any incoming Ping requests when Disable is selected. Select LAN to reply to incoming LAN Ping requests. Select WAN to reply to incoming WAN Ping requests. Otherwise select LAN & WAN to reply to both incoming LAN and WAN Ping requests.

Table 11-7 Security

LABEL	DESCRIPTION
Do not respond to requests for unauthorized services	<p>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.</p> <p>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 tcsrst rst [on off]" to change this policy. When the firewall mechanism blocks a UDP packet, it drops the packet without sending a response packet.</p>
Apply	Click Apply to save your customized settings and exit this screen.
Reset	Click Reset to begin configuring this screen afresh.

Part VI:

Logs and Maintenance

This part covers the centralized logs and maintenance screens.

Chapter 12

Centralized Logs

This chapter contains information about configuring general log settings and viewing the Prestige's logs. Refer to the appendices for example log message explanations.

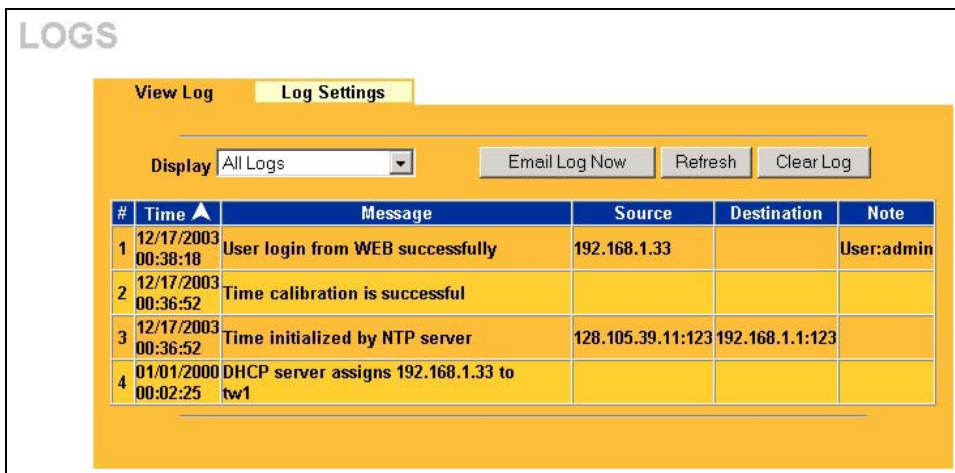
12.1 View Log

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

Click the **LOGS** in the navigation panel to open the **View Log** screen.

Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see *section 12.2*). Options include logs about system maintenance, system errors, access control, allowed or blocked web sites, blocked web features (such as ActiveX controls, java and cookies), attacks (such as DoS) and IPSec.

Log entries in red indicate system error logs. 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.



The screenshot shows the 'LOGS' interface with two tabs: 'View Log' and 'Log Settings'. Below the tabs is a 'Display' dropdown menu set to 'All Logs' and three buttons: 'Email Log Now', 'Refresh', and 'Clear Log'. A table with five columns is displayed below: '#', 'Time', 'Message', 'Source', 'Destination', and 'Note'. The table contains four log entries.

#	Time	Message	Source	Destination	Note
1	12/17/2003 00:38:18	User login from WEB successfully	192.168.1.33		User:admin
2	12/17/2003 00:36:52	Time calibration is successful			
3	12/17/2003 00:36:52	Time initialized by NTP server	128.105.39.11:123	192.168.1.1:123	
4	01/01/2000 00:02:25	DHCP server assigns 192.168.1.33 to tw1			

Figure 12-1 View Log

The following table describes the labels in this screen.

Table 12-1 View Log

LABEL	DESCRIPTION
Display	The categories that you select in the Log Settings page (see <i>section 12.2</i>) display in the drop-down list box. Select a category of logs to view; select All Logs to view logs from all of the log categories that you selected in the Log Settings page.
Time	This field displays the time the log was recorded. 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.
Note	This field displays additional information about the log entry.
Email Log Now	Click Email Log Now to send the log screen to the e-mail address specified in the Log Settings page (make sure that you have first filled in the Address Info fields in Log Settings , see <i>section 12.2</i>).
Refresh	Click Refresh to renew the log screen.
Clear Log	Click Clear Log to delete all the logs.

12.2 Log Settings

You can configure the Prestige's general log settings in one location.

Click the **LOGS** in the navigation panel and then the **Log Settings** tab to open the **Log Settings** screen.

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 to send.

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 or web sites with restricted web features such as cookies, active X and so on. 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.

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

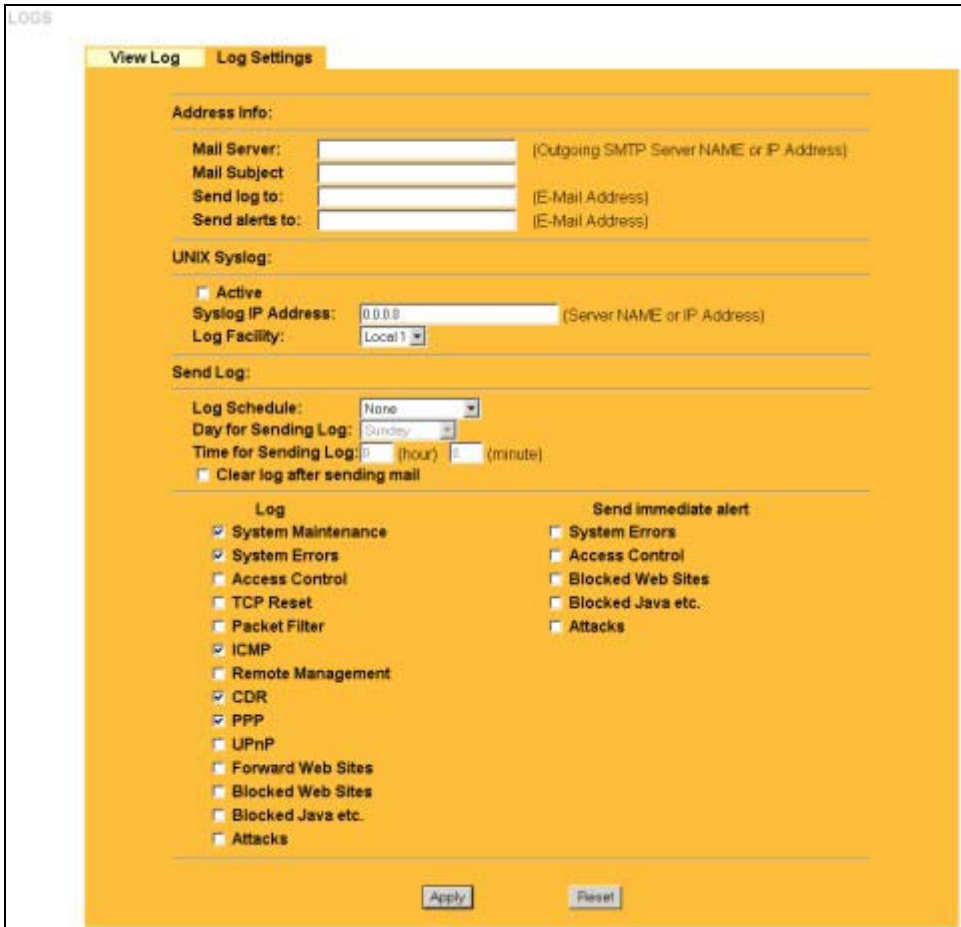


Figure 12-2 Log Settings

The following table describes the labels in this screen.

Table 12-2 Log Settings

LABEL	DESCRIPTION
Address Info	

Table 12-2 Log Settings

LABEL	DESCRIPTION
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.
Send Log To	The Prestige sends logs to the e-mail address specified in this field. If this field is left blank, the Prestige does not send logs via e-mail.
Send Alerts To	Alerts are real-time notifications that are sent as soon as an event, such as a DoS attack, system error, or forbidden web access attempt occurs. Enter the e-mail address where the alert messages will be sent. Alerts include system errors, attacks and attempted access to blocked web sites. If this field is left blank, alert messages will not be sent via e-mail.
Unix Syslog	The Prestige sends a log to an external syslog server.
Active	Click Active to enable syslog logging.
Syslog IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the syslog server manual for more information.
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"> • Daily • Weekly • Hourly • When Log is Full • None. <p>If you select Weekly or Daily, specify a time of day when the E-mail should be sent. If you select Weekly, then also specify which day of the week the E-mail should be sent. If you select When Log is Full, an alert is sent when the log fills up. If you select None, no log messages are sent</p>

Table 12-2 Log Settings

LABEL	DESCRIPTION
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.
Clear log after sending mail	Select the check box to clear all logs after logs and alert messages are sent via e-mail.
Log	Select the categories of logs that you want to record.
Send Immediate Alert	Select log categories for which you want the Prestige to send e-mail alerts immediately.
Apply	Click Apply to save your changes.
Reset	Click Reset to begin configuring this screen again.

Chapter 13

Maintenance

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

13.1 Maintenance Overview

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

13.2 Status Screen

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

The screenshot shows the 'SYSTEM STATUS' screen with a yellow background. At the top, there are five tabs: 'Status', 'DHCP Table', 'FW Upload', 'Configuration', and 'Restart'. The 'Status' tab is selected. Below the tabs, the screen displays the following information:

System Name :

Model Name : Prestige 324 ML
ZyNOS Firmware Version: V3.61(JF.0)b2 | 04/27/2004
Routing Protocols : IP

WAN Port :

IP Address : 0.0.0.0 DHCP : None
IP Subnet Mask : 0.0.0.0

LAN Port :

IP Address : 192.168.1.1 DHCP : Server
IP Subnet Mask : 255.255.255.0

At the bottom center, there is a button labeled 'Show Statistics'.

Figure 13-1 System Status

The following table describes the labels in this screen.

Table 13-1 System Status

LABEL	DESCRIPTION
System Name	This is the System Name you chose in the first Internet Access Wizard screen. It is for identification purposes
Model Name	The model name identifies your device type. The model name should also be on a sticker on your Prestige. If you are uploading firmware, be sure to upload firmware for this exact model name. This field is not available on all models.
ZyNOS Firmware Version	This is the ZyNOS Firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design.
Routing Protocols	This shows the routing protocol - IP for which the Prestige is configured. This field is not configurable in all Prestige router models.
WAN Port	
IP Address	This is the WAN port IP address.
IP Subnet Mask	This is the WAN port subnet mask.
DHCP	This is the WAN port DHCP role - Client or None .
LAN Port	
IP Address	This is the LAN port IP address.
IP Subnet Mask	This is the LAN port subnet mask.
DHCP	This is the LAN port DHCP role - Server , Relay or None .
Show Statistics	Click Show Statistics to display the real-time system statistics. Refer to <i>Section 13.2.1</i> for more information.

13.2.1 System Statistics

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

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	Down	0	0	0	0	0	00:00:00
LAN	100M/Full	1522	1625	0	5729	979	0:12:45

System Up Time : 0:12:51

Poll Interval(s) :

Figure 13-2 System Status: Show Statistics

The following table describes the labels in this screen.

Table 13-2 System Status: Show Statistics

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

Table 13-2 System Status: Show Statistics

LABEL	DESCRIPTION
Stop	Click Stop to stop refreshing statistics, click Stop .

13.3 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.

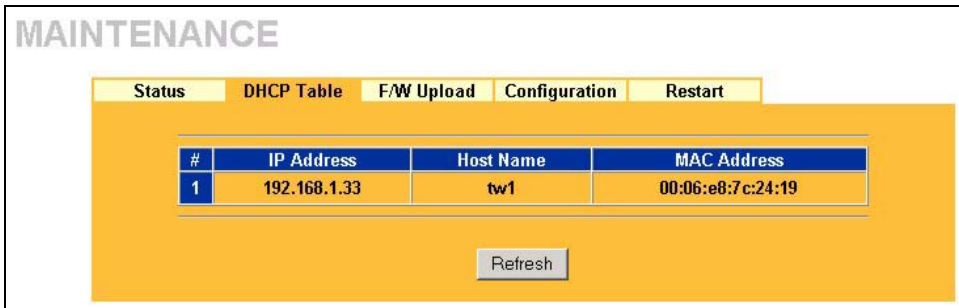


Figure 13-3 DHCP Table

The following table describes the labels in this screen.

Table 13-3 DHCP Table

LABEL	DESCRIPTION
#	This is the index number of the host computer.
IP Address	This field displays the IP address relative to the # field listed above.
Host Name	This field displays the computer host name.

Table 13-3 DHCP Table

LABEL	DESCRIPTION
MAC Address	This field shows the MAC address of the computer with the name in the Host Name field. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
Refresh	Click Refresh to renew the screen.

13.4 F/W Upload Screen

Find firmware at 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 the *Firmware and Configuration File Maintenance* chapter for upgrading firmware using FTP/TFTP commands.

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

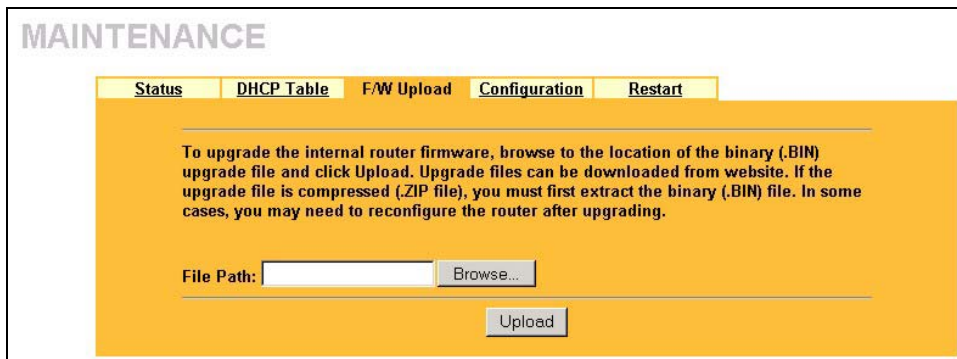


Figure 13-4 Firmware Upload

The following table describes the labels in this screen.

Figure 13-5 Firmware Upload

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

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.



Figure 13-6 Firmware Upload In Process

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.

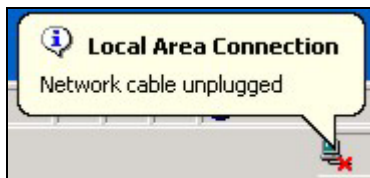


Figure 13-7 Network Temporarily Disconnected

After two minutes, log in again and check your new firmware version in the **System Status** screen. If the upload was not successful, the following screen will appear. Click **Return** to go back to the **F/W Upload** screen.

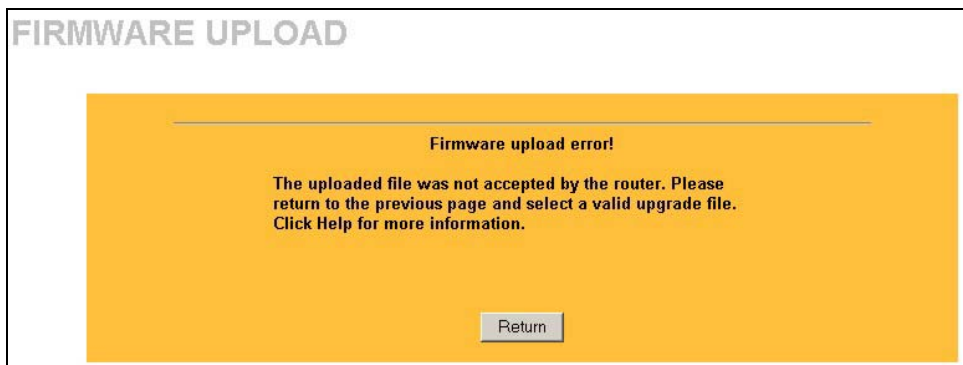


Figure 13-8 Firmware Upload Error

13.5 Configuration Screen

See the *Firmware and Configuration File Maintenance* chapter for transferring configuration files using FTP/TFTP commands.

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

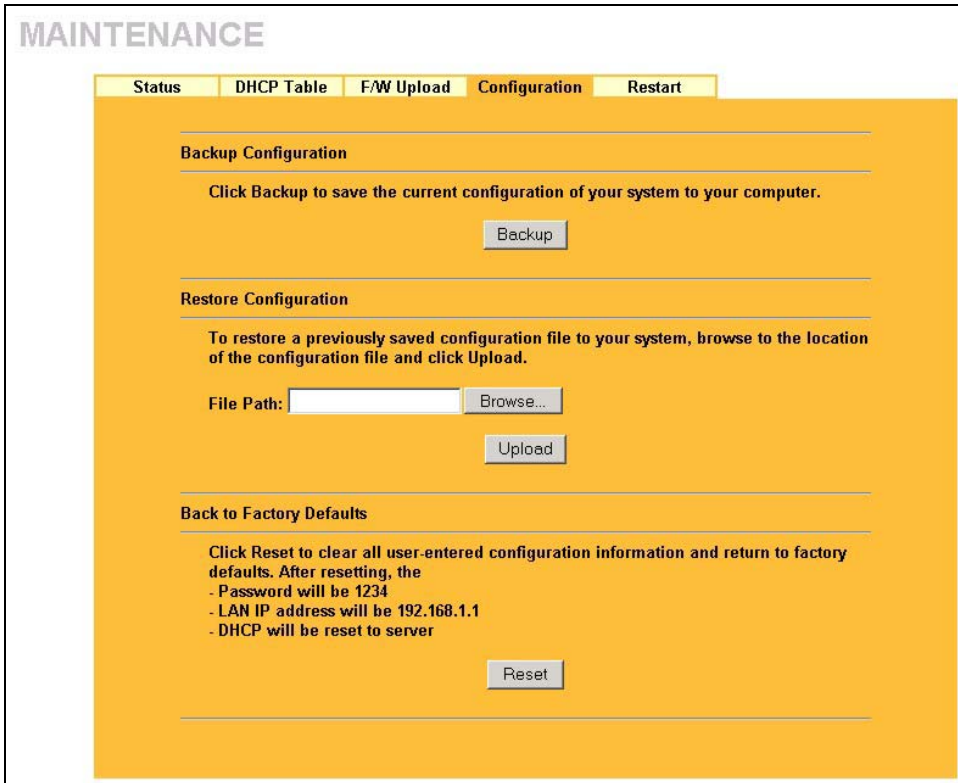


Figure 13-9 Configuration

13.5.1 Backup Configuration

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

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

13.5.2 Restore Configuration

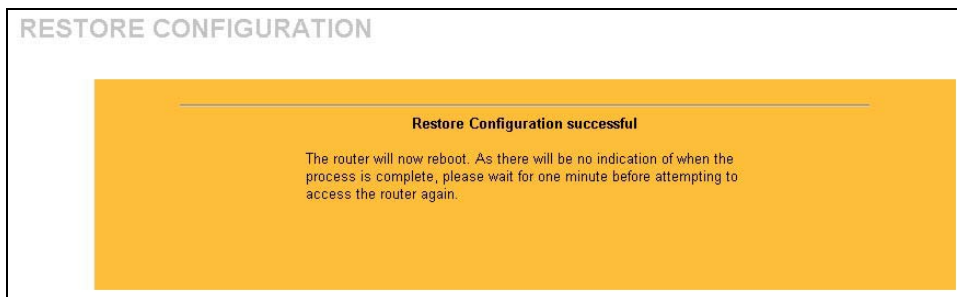
Restore configuration allows you to upload a new or previously saved configuration file from your computer to your Prestige.

Table 13-4 Restore Configuration

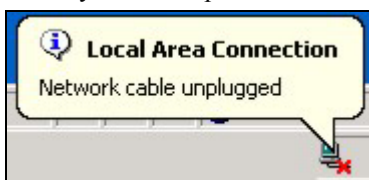
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click Browse ... to find it.
Browse...	Click Browse... to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click Upload to begin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

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

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

**Figure 13-10 Configuration Upload Successful**

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 13-11 Network Temporarily Disconnected**

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

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

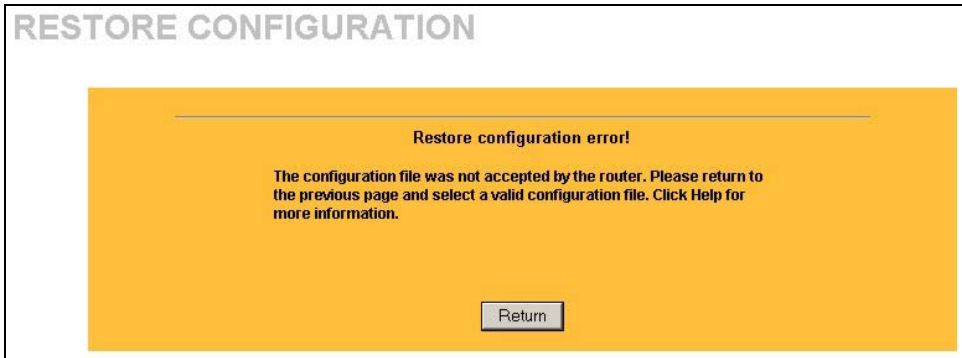


Figure 13-12 Restore Configuration Error

13.5.3 Back to Factory Defaults

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

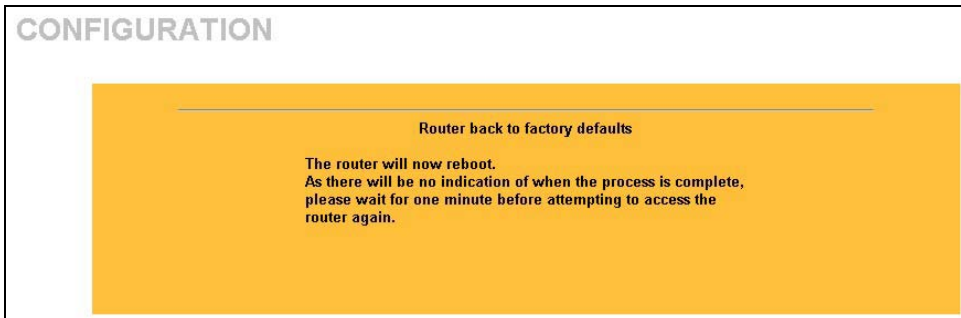


Figure 13-13 Reset Warning Message

You can also press the **RESET** button on the rear panel to reset the factory defaults of your Prestige. Refer to the *Hardware Installation* chapter for more information on the **RESET** button.

13.6 Restart Screen

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

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



Figure 13-14 Restart

Part VII:

SMT General Configuration

This part covers System Management Terminal configuration for general setup, WAN setup, LAN setup, Internet access, remote node, static route, NAT and enabling the firewall.

See the web configurator parts of this guide for background information on features configurable by web configurator and SMT.

Chapter 14

Introducing the SMT

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

14.1 SMT Introduction

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 (System Management Terminal) menus via console port, how to navigate the SMT and how to configure SMT menus.

14.1.1 Procedure for SMT Configuration via Console Port

Follow the steps below to access your Prestige via the console port.

Configure a terminal emulation communications program as follows: VT100 terminal emulation, no parity, 8 data bits, 1 stop bit, data flow set to none, 9600 bps port speed.

Press [ENTER] to display the SMT password screen. The default password is "1234".

14.1.2 Procedure for SMT Configuration via Telnet

The following procedure details how to telnet into your Prestige.

Step 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**.

Step 2. Enter "1234" in the **Password** field.

Step 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.

14.1.3 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.

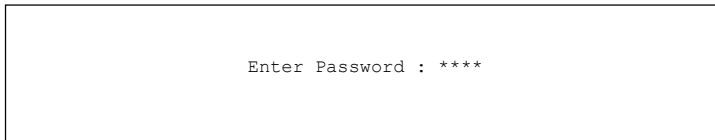


Figure 14-1 Login Screen

14.1.4 Prestige SMT Menu Overview

The following figure gives you an overview of the various SMT menu screens of your Prestige.

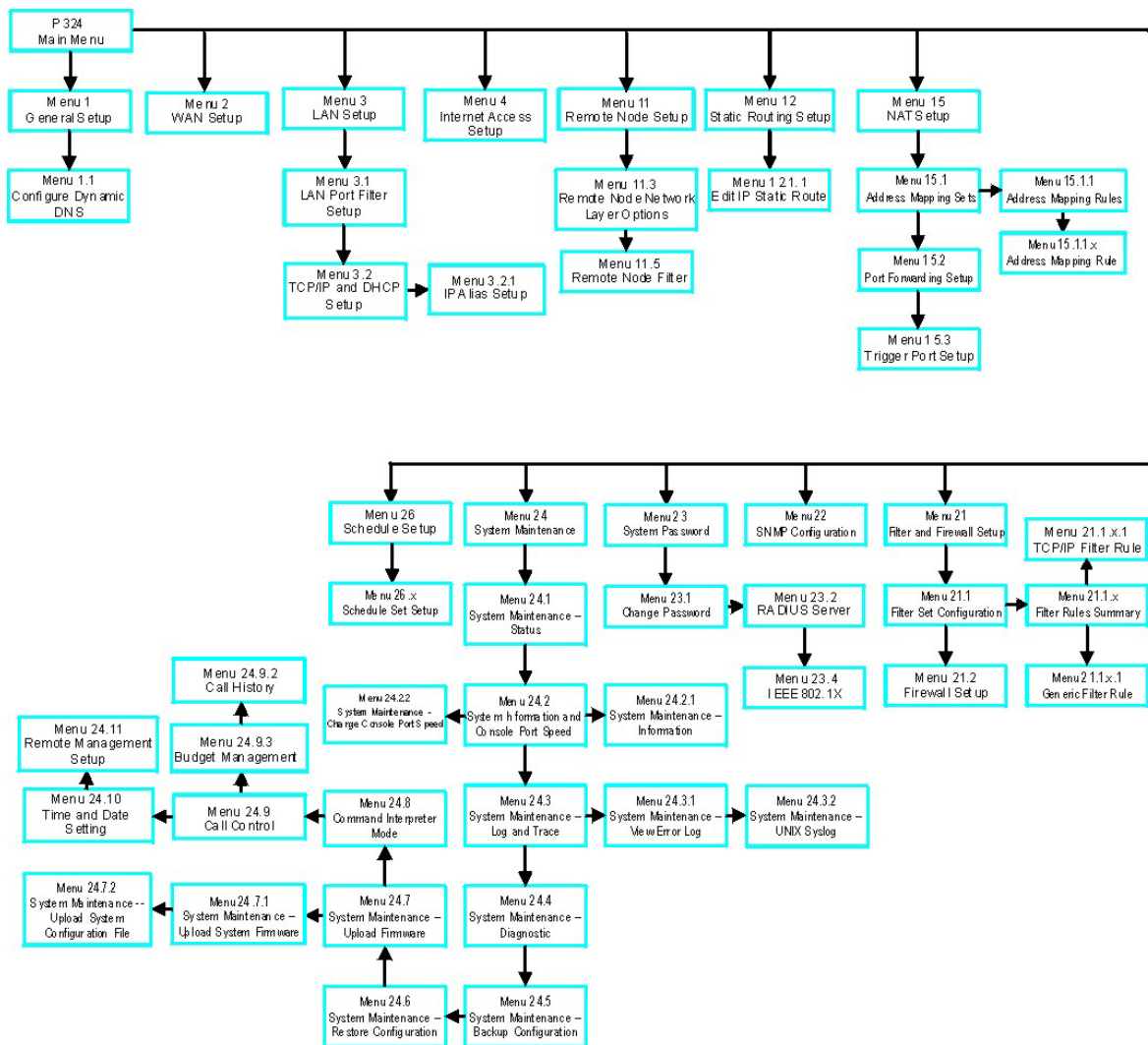


Figure 14-2 SMT Menu Overview

14.2 Navigating the SMT Interface

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

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

Table 14-1 Main Menu Commands

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

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


```

Copyright (c) 1994 - 2003 ZyXEL Communications Corp.

Prestige 324 Main Menu

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

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

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

99. Exit

Enter Menu Selection Number:

```

Figure 14-3 SMT Main Menu

14.2.1 System Management Terminal Interface Summary

Table 14-2 Main Menu Summary

#	MENU TITLE	DESCRIPTION
1	General Setup	Use this menu to set up your general information.
2	WAN Setup	Use this menu to clone a MAC address from a computer on your LAN.
3	LAN Setup	Use this menu to apply LAN filters, configure LAN DHCP and TCP/IP settings.
4	Internet Access Setup	Configure your Internet Access setup (Internet address, gateway, login, etc.) with this menu.
11	Remote Node Setup	Use this menu to configure detailed remote node settings (your ISP is also a remote node) as well as apply WAN filters.
12	Static Routing Setup	Use this menu to set up static routes.
15	NAT Setup	Use this menu to specify inside servers when NAT is enabled.
21	Filter and Firewall Setup	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 Password	Use this menu to change your password.

Table 14-2 Main Menu Summary

#	MENU TITLE	DESCRIPTION
24	System Maintenance	This menu provides system status, diagnostics, software upload, etc.
26	Schedule Setup	Use this menu to schedule outgoing calls.
99	Exit	Use this to exit from SMT and return to a blank screen.

14.3 Changing the System Password

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

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

```
Menu 23 - System Password

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

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

Figure 14-4 Menu 23 System Password

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

Note that as you type a password, the screen displays an “*” for each character you type.

Chapter 15

Menu 1 General Setup

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

15.1 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.

15.2 Procedure To Configure Menu 1

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

```

Menu 1 - General Setup

System Name=
Domain Name= zyxel.com.tw
First System DNS Server= From ISP
    IP Address= N/A
Second System DNS Server= From ISP
    IP Address= N/A
Third System DNS Server= From ISP
    IP Address= N/A
Edit Dynamic DNS= No

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

Figure 15-1 Menu 1 General Setup

Step 2. Fill in the required fields. Refer to the table shown next for more information about these fields.

Table 15-1 Menu 1 General Setup

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

Table 15-1 Menu 1 General Setup

FIELD	DESCRIPTION	EXAMPLE
First System DNS Server Second System DNS Server Third System DNS Server	<p>DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. The Prestige uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.</p> <p>Press [SPACE BAR] and then [ENTER] to select an option. Select From ISP if your ISP dynamically assigns DNS server information (and the Prestige's WAN IP address). The IP Address field below displays the (read-only) DNS server IP address that the ISP assigns.</p> <p>Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the IP Address field. If you select User-Defined, but leave the IP address set to 0.0.0.0, User-Defined changes to None after you save your changes. If you set a second choice to User-Defined, and enter the same IP address, the second User-Defined changes to None after you save your changes.</p> <p>Select None if you do not want to configure DNS servers. If you do not configure a system DNS server, you must use IP addresses when configuring VPN, DDNS and the time server.</p>	From ISP
Edit Dynamic DNS	Press [SPACE BAR] and then [ENTER] to select Yes or No (default). Select Yes to configure Menu 1.1: Configure Dynamic DNS discussed next.	No (default)
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		

15.2.1 Procedure to Configure Dynamic DNS

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

- Step 1.** 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.

```

Menu 1.1 - Configure Dynamic DNS

Service Provider= WWW.DynDNS.ORG
Active= No
DDNSType= DynamicDNS
Host1=
Host2=
Host3=
USER=
Password= *****
Enable Wildcard= No
Offline= N/A
Edit Update IP Address:
  Use Server Detected IP= No
  User Specified IP Address= No
  IP Address= N/A

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

Figure 15-2 Menu 1.1 Configure Dynamic DNS

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

Table 15-2 Menu 1.1 Configure Dynamic DNS

FIELD	DESCRIPTION	EXAMPLE
Service Provider	This is the name of your Dynamic DNS service provider.	WWW.DynDNS.ORG (default)
Active	Press [SPACE BAR] to select Yes and then press [ENTER] to make dynamic DNS active.	Yes
DDNS Type	Press [SPACE BAR] and then [ENTER] to select DynamicDNS if you have a dynamic IP address(es). Select StaticDNS if you have a static IP address(s). Select CustomDNS to have dyns.org provide DNS service for a domain name that you already have from a source other than dyndns.org.	DynamicDNS (default)
Host1-3	Enter your host name(s) in the fields provided. You can specify up to two host names separated by a comma in each field.	me.dyndns.org
USER	Enter your user name.	
Password	Enter the password assigned to you.	
Enable Wildcard	Your Prestige supports DYNDNS Wildcard. Press [SPACE BAR] and then [ENTER] to select Yes or No This field is N/A when you choose DDNS client as your service provider.	No

Table 15-2 Menu 1.1 Configure Dynamic DNS

FIELD	DESCRIPTION	EXAMPLE
Offline	This field is only available when CustomDNS is selected in the DDNS Type field. Press [SPACE BAR] and then [ENTER] to select Yes . When Yes is selected, http://www.dyndns.org/ traffic is redirected to a URL that you have previously specified (see www.dyndns.org for details).	Yes
<p>Edit Update IP Address:</p> <p>You can select Yes in either the Use Server Detected IP field (recommended) or the User Specified IP Addr field, but not both.</p> <p>With the Use Server Detected IP and User Specified IP Addr fields both set to No, the DDNS server automatically updates the IP address of the host name(s) with the Prestige's WAN IP address.</p> <p>DDNS does not work with a private IP address. When both fields are set to No, the Prestige must have a public WAN IP address in order for DDNS to work.</p>		
Use Server Detected IP	<p>Press [SPACE BAR] to select Yes and then press [ENTER] to have the DDNS server automatically update the IP address of the host name(s) with the public IP address that the Prestige uses or is behind.</p> <p>You can set this field to Yes whether the IP address is public or private, static or dynamic.</p>	Yes
User Specified IP Address	<p>Press [SPACE BAR] to select Yes and then press [ENTER] to update the IP address of the host name(s) to the IP address specified below.</p> <p>Only select Yes if the Prestige uses or is behind a static public IP address.</p>	No
IP Address	Enter the static public IP address if you select Yes in the User Specified IP Addr field.	N/A
<p>When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.</p>		

The IP address updates when you reconfigure menu 1 or perform DHCP client renewal.

Chapter 16

WAN and Dial Backup Setup

This chapter describes how to configure the WAN using menu 2 and dial-backup using menus 2.1 and 11.1.

16.1 Introduction to WAN

This chapter explains how to configure settings for your WAN port.

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

```

Menu 2 - WAN Setup
MAC Address:
Assigned By= Factory default
IP Address= N/A

Dial-Backup:
Active= No
Phone Number=
Port Speed= 9600
AT Command String:
Init=
Edit Advanced Setup= No

Press ENTER to Confirm or ESC to Cancel:

```

Figure 16-1 MAC Address Cloning in WAN Setup

The following table describes the fields in this screen.

Table 16-1 MAC Address Cloning in WAN Setup

FIELD	DESCRIPTION	EXAMPLE
MAC Address		
Assigned By	Press [SPACE BAR] and then [ENTER] to choose one of two methods to assign a MAC Address. Choose Factory Default to select the factory assigned default MAC Address. Choose IP address attached on LAN to use the MAC Address of that workstation whose IP you give in the following field.	IP address attached on LAN

Table 16-1 MAC Address Cloning in WAN Setup

FIELD	DESCRIPTION	EXAMPLE
IP Address	This field is applicable only if you choose the IP address attached on LAN method in the Assigned By field. Enter the IP address of the computer on the LAN whose MAC you are cloning.	192.168.1.35
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		

16.2 Dial Backup

The Dial Backup port can be used in reserve, as a traditional dial-up connection should the broadband connection to the WAN port fail. To set up the auxiliary port (Dial Backup) for use in the event that the regular WAN connection is dropped, first make sure you have set up the switch and port connection (see the *Quick Start Guide*), then configure

1. Menu 2 - WAN Setup,
2. Menu 2.1 - Advanced WAN Setup and
3. Menu 11.1 - Remote Node Profile (Backup ISP) as shown next

Refer also to the traffic redirect section for information on an alternate backup WAN connection.

16.3 Configuring Dial Backup in Menu 2

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

```

Menu 2 - WAN Setup

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

Dial-Backup:
Active= No
Phone Number=
Port Speed= 9600
AT Command String:
Init=
Edit Advanced Setup= No

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

Figure 16-2 Menu 2: Dial Backup Setup

The following table describes the fields in this menu.

Table 16-2 Menu 2: Dial Backup Setup

FIELD	DESCRIPTION	EXAMPLE
Dial-Backup:		
Active	Use this field to turn the dial-backup feature on (Yes) or off (No).	No
Phone Number	Enter the telephone number assigned to your line by your telephone company. This field only accepts digits; do not include dashes and spaces.	1234567
Port Speed	Press [SPACE BAR] and then press [ENTER] to select the speed of the connection between the Dial Backup port and the external device. Available speeds are: 9600, 19200, 38400, 57600, 115200 or 230400 bps.	9600
AT Command String:		
Init	Enter the AT command string to initialize the WAN device. Consult the manual of your WAN device connected to your Dial Backup port for specific AT commands.	at&fs0=0
Edit Advanced Setup	To edit the advanced setup for the Dial Backup port, move the cursor to this field; press the [SPACE BAR] to select Yes and then press [ENTER] to go to Menu 2.1: Advanced Setup .	Yes
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		

16.4 Advanced WAN Setup

Consult the manual of your WAN device connected to your Dial Backup port for specific AT commands.

To edit the advanced setup for the Dial Backup port, move the cursor to the **Edit Advanced Setup** field in **Menu 2 - WAN Setup**, press the [SPACE BAR] to select **Yes** and then press [ENTER].

```

Menu 2.1 - Advanced WAN Setup

AT Command Strings:          Call Control:
Dial=                        Dial Timeout(sec)= 0
Drop=                        Retry Count= 0
Answer=                       Retry Interval(sec)= N/A
                               Drop Timeout(sec)= 0
                               Call Back Delay(sec)= 0

Drop DTR When Hang Up= No

AT Response Strings:
CLID=
Called Id=
Speed=

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

Figure 16-3 Menu 2.1 Advanced WAN Setup

The following table describes fields in this menu.

Table 16-3 Advanced WAN Port Setup: AT Commands Fields

FIELD	DESCRIPTION	DEFAULT
AT Command Strings:		
Dial	Enter the AT Command string to make a call.	atdt
Drop	Enter the AT Command string to drop a call. “~” represents a one second wait, e.g., “~++++~ath” can be used if your modem has a slow response time.	+++ath
Answer	Enter the AT Command string to answer a call.	ata
Drop DTR When Hang Up	Press the [SPACE BAR] to choose either Yes or No . When Yes is selected (the default), the DTR (Data Terminal Ready) signal is dropped after the “AT Command String: Drop” is sent out.	YES
AT Response Strings:		
CLID (Calling Line Identification)	Enter the keyword that precedes the CLID (Calling Line Identification) in the AT response string. This lets the Prestige capture the CLID in the AT response string that comes from the WAN device. CLID is required for CLID authentication.	NMBR =
Called Id	Enter the keyword preceding the dialed number.	TO
Speed	Enter the keyword preceding the connection speed.	CONNECT

Table 16-4 Advanced WAN Port Setup: Call Control Parameters

FIELD	DESCRIPTION	DEFAULT
Call Control		
Dial Timeout (sec)	Enter a number of seconds for the Prestige to keep trying to set up an outgoing call before timing out (stopping). The Prestige times out and stops if it cannot set up an outgoing call within the timeout value.	60 seconds
Retry Count	Enter a number of times for the Prestige to retry a busy or no-answer phone number before blacklisting the number.	0 to disable the blacklist control
Retry Interval (sec)	Enter a number of seconds for the Prestige to wait before trying another call after a call has failed. This applies before a phone number is blacklisted.	
Drop Timeout (sec)	Enter a number of seconds for the Prestige to wait before dropping the DTR signal if it does not receive a positive disconnect confirmation.	20 seconds
Call Back Delay (sec)	Enter a number of seconds for the Prestige to wait between dropping a callback request call and dialing the co-responding callback call.	15 seconds

16.5 Remote Node Profile (Backup ISP)

Enter **2** in **Menu 11 Remote Node Setup** to open **Menu 11.1 Remote Node Profile (Backup ISP)** (shown below) and configure the setup for your Dial Backup port connection.

```

Menu 11.1 - Remote Node Profile (Backup ISP)

Rem Node Name= ?           Edit PPP Options= No
Active= Yes                Rem IP Addr= ?
                            Edit IP= No
                            Edit Script Options= No

Outgoing:
  My Login=
  My Password= *****
  Retype to Confirm= *****
  Authen= CHAP/PAP
  Pri Phone #= ?
  Sec Phone #=

                            Telco Option:
                              Allocated Budget(min)= 0
                              Period(hr)= 0
                              Nailed-Up Connection= No

                            Session Options:
                              Edit Filter Sets= No
                              Idle Timeout(sec)= 100

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

Figure 16-4 Menu 11.1 Remote Node Profile (Backup ISP)

The following table describes the fields in this menu.

Table 16-5 Menu 11.1 Remote Node Profile (Backup ISP)

FIELD	DESCRIPTION	EXAMPLE
Rem Node Name	Enter a descriptive name for the remote node. This field can be up to eight characters.	LAoffice
Active	Press [SPACE BAR] and then [ENTER] to select Yes to enable the remote node or No to disable the remote node.	Yes
Outgoing		
My Login	Enter the login name assigned by your ISP for this remote node.	jim
My Password	Enter the password assigned by your ISP for this remote node.	*****
Retype to Confirm	Enter your password again to make sure that you have entered is correctly.	
Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are: CHAP/PAP - Your Prestige will accept either CHAP or PAP when requested by this remote node. CHAP - accept CHAP only. PAP - accept PAP only.	CHAP/PAP

Table 16-5 Menu 11.1 Remote Node Profile (Backup ISP)

FIELD	DESCRIPTION	EXAMPLE
Pri Phone # Sec Phone #	Enter the first (primary) phone number from the ISP for this remote node. If the Primary Phone number is busy or does not answer, your Prestige dials the Secondary Phone number if available. Some areas require dialing the pound sign # before the phone number for local calls. Include a # symbol at the beginning of the phone numbers as required.	
Edit PPP Options	Move the cursor to this field and use the space bar to select [Yes] and press [Enter] to edit the PPP options for this remote node. This brings you to Menu 11.2 - Remote Node PPP Options (see <i>section 16.6</i>).	No (default)
Rem IP Addr	Leave the field set to 0.0.0.0 (default) if the remote gateway has a dynamic IP address. Enter the remote gateway's IP address here if it is static.	0.0.0.0 (default)
Edit IP	This field leads to a "hidden" menu. Press [SPACE BAR] to select Yes and press [ENTER] to go to Menu 11.3 - Remote Node Network Layer Options . See <i>section 16.7</i> for more information.	No (default)
Edit Script Options	Press [SPACE BAR] to select Yes and press [ENTER] to edit the AT script for the dial backup remote node (Menu 11.4 - Remote Node Script). See <i>section 16.8</i> for more information.	No (default)
Telco Option		
Allocated Budget	Enter the maximum number of minutes that this remote node may be called within the time period configured in the Period field. The default for this field is 0 meaning there is no budget control and no time limit for accessing this remote node.	0 (default)
Period(hr)	Enter the time period (in hours) for how often the budget should be reset. For example, to allow calls to this remote node for a maximum of 10 minutes every hour, set the Allocated Budget to 10 (minutes) and the Period to 1 (hour).	0 (default)
Nailed-Up Connection	Press [SPACE BAR] to select Yes to set this connection to always be on, regardless of whether or not there is any traffic. Select No to have this connection act as a dial-up connection.	No (default)
Session Options		
Edit Filter sets	This field leads to another "hidden" menu. Use [SPACE BAR] to select Yes and press [ENTER] to open menu 11.5 to edit the filter sets. See <i>section 16.9</i> for more details.	No (default)

Table 16-5 Menu 11.1 Remote Node Profile (Backup ISP)

FIELD	DESCRIPTION	EXAMPLE
Idle Timeout	Enter the number of seconds of idle time (when there is no traffic from the Prestige to the remote node) that can elapse before the Prestige automatically disconnects the PPP connection. This option only applies when the Prestige initiates the call.	100 seconds (default)
Once you have configured this menu, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		

16.6 Editing PPP Options

The Prestige's dial back-up feature uses PPP. To edit the remote node PPP Options, move the cursor to the **[Edit PPP Options]** field in Menu 11.1 - Remote Node Profile, and use the space bar to select **[Yes]**. Press [Enter] to open Menu 11.2 as shown next.

```

Menu 11.2 - Remote Node PPP Options

Encapsulation= Standard PPP
Compression= No

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

Figure 16-5 Menu 11.2: Remote Node PPP Options

This table describes the Remote Node PPP Options Menu, and contains instructions on how to configure the PPP options fields.

Figure 16-6 Menu 11.2: Remote Node PPP Options

FIELD	DESCRIPTION	EXAMPLE
Encapsulation	Press [SPACE BAR] and then [ENTER] to select CISCO PPP if your Dial Backup WAN device uses Cisco PPP encapsulation, otherwise select Standard PPP .	Standard PPP (default)
Compression	Press [SPACE BAR] and then [ENTER] to select Yes to enable or No to disable Stac compression.	No (default)
Once you have configured this menu, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		

16.7 Editing TCP/IP Options

Move the cursor to the **Edit IP** field in menu 11.1, then press [SPACE BAR] to select **Yes**. Press [ENTER] to open **Menu 11.3 - Remote Node Network Layer Options**.

```

Menu 11.3 - Remote Node Network Layer Options

IP Address Assignment= Dynamic
em IP Addr= 0.0.0.0
Rem Subnet Mask= 0.0.0.0
My WAN Addr= 0.0.0.0

Network Address Translation= SUA Only
Metric= 15
Private= No
RIP Direction= None
  Version= N/A
Multicast= None

```

Figure 16-7 Menu 11.3: Remote Node Network Layer Options

The following table describes the fields in this menu.

Table 16-6 Menu 11.3: Remote Node Network Layer Options

FIELD	DESCRIPTION	EXAMPLE
Rem IP Address	Leave this field set to 0.0.0.0 to have the ISP or other remote router dynamically (automatically) send its IP address if you do not know it. Enter the remote gateway's IP address here if you know it (static).	0.0.0.0 (default)
Rem Subnet Mask	Leave this field set to 0.0.0.0 to have the ISP or other remote router dynamically send its subnet mask if you do not know it. Enter the remote gateway's subnet mask here if you know it (static).	0.0.0.0 (default)
My WAN Addr	Leave the field set to 0.0.0.0 to have the ISP or other remote router dynamically (automatically) assign your WAN IP address if you do not know it. Enter your WAN IP address here if you know it (static). This is the address assigned to your local Prestige, not the remote router.	0.0.0.0 (default)

Table 16-6 Menu 11.3: Remote Node Network Layer Options

FIELD	DESCRIPTION	EXAMPLE
Network Address Translation	<p>Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).</p> <p>Press [SPACE BAR] and then [ENTER] to select either Full Feature, None or SUA Only.</p> <p>Choose None to disable NAT.</p> <p>Choose SUA Only if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: Many-to-One and Server.</p> <p>Choose Full Feature if you have multiple public IP addresses. Full Feature mapping types include: One-to-One, Many-to-One (SUA/PAT), Many-to-Many Overload, Many- One-to-One and Server. When you select Full Feature you must configure at least one address mapping set!</p> <p>See the Network Address Translation (NAT) chapter for a full discussion on this feature.</p>	None (default)
Metric	Enter a number from 1 to 15 to set this route's priority among the Prestige's routes. The smaller the number, the higher priority the route has.	15 (default)
Private	This parameter determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to Yes , this route is kept private and not included in RIP broadcasts. If No , the route to this remote node will be propagated to other hosts through RIP broadcasts.	No (default)
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP Direction from Both/ None/In Only/Out Only and None .	Both (default)
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version from RIP-1/RIP-2B/RIP-2M .	RIP-1
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The Prestige supports both IGMP version 1 (IGMP-v1) and version 2 (IGMP-v2). Press the [SPACE BAR] to enable IP Multicasting or select None to disable it. See the LAN Setup chapter for more information on this feature.	None (default)
Once you have completed filling in Menu 11.3 Remote Node Network Layer Options , press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration and return to menu 11, or press [ESC] at any time to cancel.		

16.8 Editing Login Script

For some remote gateways, text login is required before PPP negotiation is started. The Prestige provides a script facility for this purpose. The script has six programmable sets; each set is composed of an 'Expect' string and a 'Send' string. After matching a message from the server to the 'Expect' field, the Prestige returns the set's 'Send' string to the server.

For instance, a typical login sequence starts with the server printing a banner, a login prompt for you to enter the user name and a password prompt to enter the password:

```
Welcome to Acme, Inc.
```

```
Login: myLogin
```

```
Password:
```

To handle the first prompt, you specify "ogin: " as the 'Expect' string and "myLogin" as the 'Send' string in set 1. The reason for leaving out the leading "L" is to avoid having to know exactly whether it is upper or lower case. Similarly, you specify "word: " as the 'Expect' string and your password as the 'Send' string for the second prompt in set 2.

You can use two variables, \$USERNAME and \$PASSWORD (all UPPER case), to represent the actual user name and password in the script, so they will not show in the clear. They are replaced with the outgoing login name and password in the remote node when the Prestige sees them in a 'Send' string. Please note that both variables must be entered exactly as shown. No other characters may appear before or after, either, i.e., they must be used alone in response to login and password prompts.

Please note that the ordering of the sets is significant, i.e., starting from set 1, the Prestige will wait until the 'Expect' string is matched before it proceeds to set 2, and so on for the rest of the script. When both the 'Expect' and the 'Send' fields of the current set are empty, the Prestige will terminate the script processing and start PPP negotiation. This implies two things: first, the sets must be contiguous; the sets after an empty one are ignored. Second, the last set should match the final message sent by the server. For instance, if the server prints:

```
login successful.
```

```
Starting PPP...
```

after you enter the password, then you should create a third set to match the final "PPP..." but without a "Send" string. Otherwise, the Prestige will start PPP prematurely right after sending your password to the server.

If there are errors in the script and it gets stuck at a set for longer than the "Dial Timeout" in menu 2 (default 60 seconds), the Prestige will timeout and drop the line. To debug a script, go to Menu 24.4 to initiate a manual call and watch the trace display to see if the sequence of messages and prompts from the server differs from what you expect.

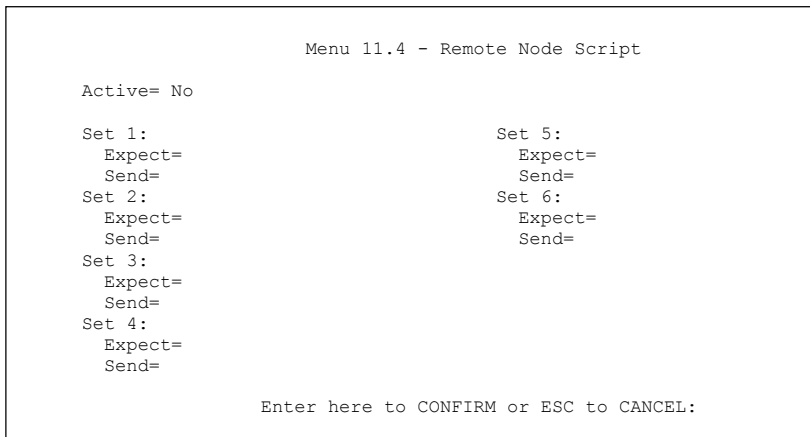


Figure 16-8 Menu 11.4: Remote Node Script

The following table describes the fields in this menu.

Table 16-7 Menu 11.4: Remote Node Script

FIELD	DESCRIPTION	EXAMPLE
Active	Press [SPACE BAR] and then [ENTER] to select either Yes to enable the AT strings or No to disable them.	No (default)
Set 1-6: Expect	Enter an Expect string to match. After matching the Expect string, the Prestige returns the string in the Send field.	
Set 1-6: Send	Enter a string to send out after the Expect string is matched.	0.0.0.0

16.9 Remote Node Filter

Move the cursor to the field **Edit Filter Sets** in menu 11.1, and then press [SPACE BAR] to set the value to **Yes**. Press [ENTER] to open **Menu 11.5 - Remote Node Filter**.

Use menu 11.5 to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the Prestige to prevent certain packets from triggering calls. You can specify up to four filter sets separated by commas, for example, 1, 5, 9, 12, in each filter field. Note that spaces are accepted in this field. Please refer to the *Filters* chapter for more information on defining the filters.

```
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:
```

Figure 16-9 Menu 11.5: Dial Backup Remote Node Filter

Chapter 17

Menu 3 LAN Setup

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

17.1 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.

```
Menu 3 - LAN Setup

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

Enter Menu Selection Number:
```

Figure 17-1 Menu 3 LAN Setup

17.1.1 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.

```
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:
```

Figure 17-2 Menu 3.1 LAN Port Filter Setup

If you need to define filters, please read the *Filter Set Configuration* chapter first, then return to this menu to define the filter sets.

17.2 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 the *Internet Access Application* chapter.
- For bridging Ethernet setup refer to the *Bridging Setup* chapter.

17.3 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:

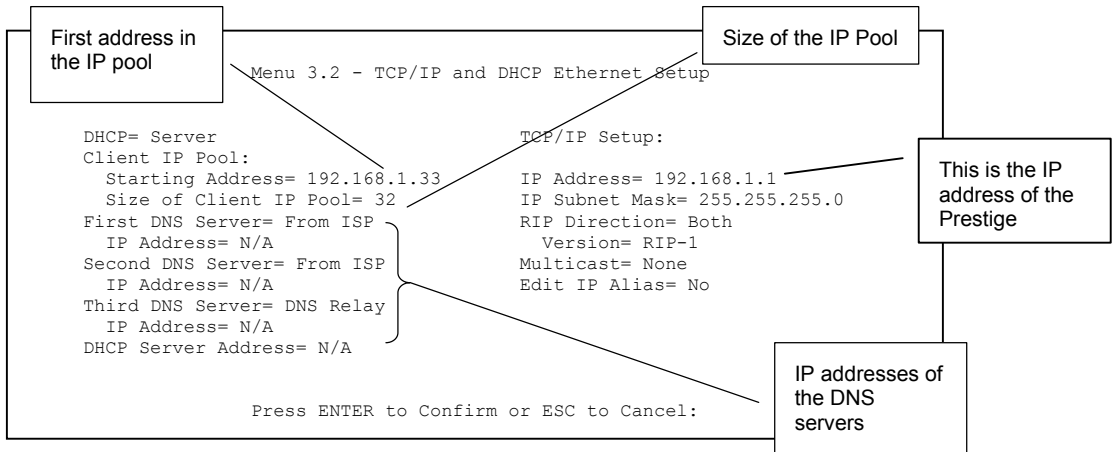


Figure 17-3 Menu 3.2 TCP/IP and DHCP Ethernet Setup

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

Table 17-1 Menu 3.2: DHCP Ethernet Setup Fields

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

Table 17-1 Menu 3.2: DHCP Ethernet Setup Fields

FIELD	DESCRIPTION	EXAMPLE
Client IP Pool:		
Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.	192.168.1.33
Size of Client IP Pool	This field specifies the size, or count of the IP address pool.	128
First DNS Server Second DNS Server Third DNS Server	<p>The Prestige passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients.</p> <p>Select From ISP if your ISP dynamically assigns DNS server information (and the Prestige's WAN IP address). The IP Address field below displays the (read-only) DNS server IP address that the ISP assigns.</p> <p>Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the IP Address field below. If you chose User-Defined, but leave the IP address set to 0.0.0.0, User-Defined changes to None after you save your changes. If you set a second choice to User-Defined, and enter the same IP address, the second User-Defined changes to None after you save your changes.</p> <p>Select DNS Relay to have the Prestige act as a DNS proxy. The Prestige's LAN IP address displays in the IP Address field below (read-only). The Prestige tells the DHCP clients on the LAN that the Prestige itself is the DNS server. When a computer on the LAN sends a DNS query to the Prestige, the Prestige forwards the query to the Prestige's system DNS server (configured in menu 1) and relays the response back to the computer. You can only select DNS Relay for one of the three servers; if you select DNS Relay for a second or third DNS server, that choice changes to None after you save your changes.</p> <p>Select None if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.</p>	From ISP
DHCP Server Address	If Relay is selected in the DHCP field above, then type the IP address of the actual, remote DHCP server here.	

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

Table 17-2 Menu 3.2: LAN TCP/IP Setup Fields

FIELD	DESCRIPTION	EXAMPLE
TCP/IP Setup:		
IP Address	Enter the IP address of your Prestige in dotted decimal notation	192.168.1.1 (default)
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.	255.255.255.0
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction. Options are: Both , In Only , Out Only or None .	Both (default)
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are: RIP-1 , RIP-2B or RIP-2M .	RIP-1 (default)
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The Prestige supports both IGMP version 1 (IGMP-v1) and version 2 (IGMP-v2). Press [SPACE BAR] and then [ENTER] to enable IP Multicasting or select None (default) to disable it.	None
Edit IP Alias	The Prestige supports three logical LAN interfaces via its single physical Ethernet interface with the Prestige itself as the gateway for each LAN network. Press [SPACE BAR] to select Yes and then press [ENTER] to display menu 3.2.1	No
When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm...] to save your configuration, or press [ESC] at any time to cancel.		

17.3.1 IP Alias Setup

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

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

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

```

Menu 3.2.1 - IP Alias Setup

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

Enter here to CONFIRM or ESC to CANCEL:

```

Figure 17-4 Menu 3.2.1: IP Alias Setup

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

Table 17-3 Menu 3.2.1: IP Alias Setup

FIELD	DESCRIPTION	EXAMPLE
IP Alias 1, 2	Choose Yes to configure the LAN network for the Prestige.	Yes
IP Address	Enter the IP address of your Prestige in dotted decimal notation.	192.168.1.1
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.	255.255.255.0
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP direction. Options are Both, In Only, Out Only or None .	None
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are RIP-1, RIP-2B or RIP-2M .	RIP-1
Incoming Protocol Filters	Enter the filter set(s) you wish to apply to the incoming traffic between this node and the Prestige.	1
Outgoing Protocol Filters	Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the Prestige.	2

Table 17-3 Menu 3.2.1: IP Alias Setup

FIELD	DESCRIPTION	EXAMPLE
When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm...] to save your configuration, or press [ESC] at any time to cancel.		

Chapter 18

Internet Access

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

18.1 Introduction to Internet Access Setup

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

18.2 Ethernet Encapsulation

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

If you choose **Ethernet** in menu 4 you will see the next menu.

```
Menu 4 - Internet Access Setup

ISP's Name= MyISP
Encapsulation= Ethernet
  Service Type= Standard
  My Login= N/A
  My Password= N/A
  Retype to Confirm= N/A
  Login Server= N/A
  Relogin Every (min)= N/A
IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Address= N/A
Network Address Translation= SUA Only

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

Figure 18-1 Menu 4 Internet Access Setup

The following table describes the fields in this menu.

Table 18-1 Menu 4: Internet Access Setup (Ethernet)

FIELD	DESCRIPTION
ISP's Name	Enter the name of your Internet Service Provider, e.g., myISP. This information is for identification purposes only.
Encapsulation	Press [SPACE BAR] and then press [ENTER] to choose Ethernet . The encapsulation method influences your choices for the IP Address field.
Service Type	Press [SPACE BAR] and then [ENTER] to select Standard , RR-Toshiba (RoadRunner Toshiba authentication method), RR-Manager (RoadRunner Manager authentication method), RR-Telstra or Telia Login . Choose a RoadRunner flavor if your ISP is Time Warner's RoadRunner; otherwise choose Standard .
Note: DSL users must choose the Standard option only. The My Login , My Password and Login Server fields are not applicable in this case.	
My Login	Enter the login name given to you by your ISP.
My Password	Type your password again for confirmation.
Retype to Confirm	Enter your password again to make sure that you have entered is correctly.
Login Server	The Prestige will find the RoadRunner Server IP if this field is left blank. If it does not, then you must enter the authentication server IP address.
Relogin Every (min)	This field is available when you select Telia Login in the Service Type field. The Telia server logs the Prestige out if the Prestige does not log in periodically. Type the number of minutes from 1 to 59 (30 recommended) for the Prestige to wait between logins.
IP Address Assignment	If your ISP did not assign you a fixed IP address, press [SPACE BAR] and then [ENTER] to select Dynamic , otherwise select Static and enter the IP address and subnet mask in the following fields.
IP Address	Enter the (fixed) IP address assigned to you by your ISP (static IP address assignment is selected in the previous field).
IP Subnet Mask	Enter the subnet mask associated with your static IP.
Gateway IP Address	Enter the gateway IP address associated with your static IP.

Table 18-1 Menu 4: Internet Access Setup (Ethernet)

FIELD	DESCRIPTION
Network Address Translation	<p>Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).</p> <p>Choose None to disable NAT.</p> <p>Choose SUA Only if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: Many-to-One and Server.</p> <p>Choose Full Feature if you have multiple public IP addresses. Full Feature mapping types include: One-to-One, Many-to-One (SUA/PAT), Many-to-Many Overload, Many- One-to-One and Server. When you select Full Feature you must configure at least one address mapping set!</p> <p>Please see the NAT chapter for a more detailed discussion on the Network Address Translation feature.</p>
<p>When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.</p>	

18.3 Configuring the PPTP Client

The Prestige supports only one PPTP server connection at any given time.

To configure a PPTP client, you must configure the **My Login** and **Password** fields for a PPP connection and the PPTP parameters for a PPTP connection.

After configuring **My Login** and **Password** for PPP connection, press [SPACE BAR] and then [ENTER] in the **Encapsulation** field in **Menu 4 -Internet Access Setup** to choose **PPTP** as your encapsulation option.

This brings up the following screen.

```

Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
Encapsulation= PPTP
Service Type= N/A
My Login=
My Password= *****
Retype to Confirm= *****
Idle Timeout= 100

IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Address= N/A
Network Address Translation= SUA Only

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

Figure 18-2 Internet Access Setup (PPTP)

The following table contains instructions about the new fields when you choose **PPTP** in the **Encapsulation** field in menu 4.

Table 18-2 New Fields in Menu 4 (PPTP) Screen

FIELD	DESCRIPTION	EXAMPLE
Encapsulation	Press [SPACE BAR] and then press [ENTER] to choose PPTP . The encapsulation method influences your choices for the IP Address field.	PPTP
Idle Timeout	This value specifies the time, in seconds, that elapses before the Prestige automatically disconnects from the PPTP server.	100 (default)

18.4 Configuring the PPPoE Client

If you enable PPPoE in menu 4, you will see the next screen. For more information on PPPoE, please see the appendix.


```

Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
Encapsulation= PPPoE
Service Type= N/A
My Login=
My Password= *****
Retype to Confirm= *****
Idle Timeout= 100

IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Address= N/A
Network Address Translation= SUA Only

Press ENTER to Confirm or ESC to Cancel:

```

Figure 18-3 Internet Access Setup (PPPoE)

The following table contains instructions about the new fields when you choose **PPPoE** in the **Encapsulation** field in menu 4.

Table 18-3 New Fields in Menu 4 (PPPoE) screen

FIELD	DESCRIPTION	EXAMPLE
Encapsulation	Press [SPACE BAR] and then press [ENTER] to choose PPPoE . The encapsulation method influences your choices in the IP Address field.	PPPoE
Idle Timeout	This value specifies the time in seconds that elapses before the Prestige automatically disconnects from the PPPoE server.	100 (default)

If you need a PPPoE service name to identify and reach the PPPoE server, please go to menu 11 and enter the PPPoE service name provided to you in the **Service Name** field.

18.5 Basic Setup Complete

Well done! You have successfully connected, installed and set up your Prestige to operate on your network as well as access the Internet.

When the firewall is activated, the default policy allows all communications to the Internet that originate from the LAN, and blocks all traffic to the LAN that originates from the Internet.

You may deactivate the firewall in menu 21.2 or via the Prestige embedded web configurator. You may also define additional firewall rules or modify existing ones but please exercise extreme caution in doing so. See the chapters on firewall for more information on the firewall.

Chapter 19

Remote Node Configuration

This chapter covers remote node configuration.

19.1 Introduction to Remote Node Setup

A remote node is required for placing calls to a remote gateway. A remote node represents both the remote gateway and the network behind it across a WAN connection. Note that when you use menu 4 to set up Internet access, you are actually configuring a remote node. The following describes how to configure **Menu 11.1 Remote Node Profile**, **Menu 11.3 - Remote Node Network Layer Options**, **Menu 11.5 - Remote Node Filter** and **Menu 11.6 - Traffic Redirect Setup**.

19.2 Remote Node Profile Setup

From the main menu, select menu option 11 to open **Menu 11 Remote Node Profile** (shown below).

The following explains how to configure the remote node profile menu.

19.2.1 Ethernet Encapsulation

There are two variations of menu 11 depending on whether you choose **Ethernet Encapsulation** or **PPPoE Encapsulation**. You must choose the **Ethernet** option when the WAN port is used as a regular Ethernet. The first menu 11.1 screen you see is for Ethernet encapsulation shown next.

```

Menu 11.1 - Remote Node Profile

Rem Node Name= MyISP           Route= IP
Active= Yes

Encapsulation= Ethernet       Edit IP= No
Service Type= Standard        Session Options:
Service Name= N/A             Edit Filter Sets= No
Outgoing:
  My Login= N/A
  My Password= N/A            Edit Traffic Redirect= No
  Retype to Confirm= N/A
  Server= N/A
  Relogin Every (min)= N/A

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

Figure 19-1 Menu 11.1 Remote Node Profile for Ethernet Encapsulation

The following table describes the fields in this menu.

Table 19-1 Menu 11.1 Remote Node Profile for Ethernet Encapsulation

FIELD	DESCRIPTION	EXAMPLE
Rem Node Name	Enter a descriptive name for the remote node. This field can be up to eight characters.	LAoffice
Active	Press [SPACE BAR] and then [ENTER] to select Yes (activate remote node) or No (deactivate remote node).	Yes
Encapsulation	Ethernet is the default encapsulation. Press [SPACE BAR] and then [ENTER] to change to PPPoE or PPTP encapsulation.	Ethernet
Service Type	Press [SPACE BAR] and then [ENTER] to select from Standard , RR-Toshiba (RoadRunner Toshiba authentication method), RR-Manager (RoadRunner Manager authentication method), RR-Telstra or Telia Login . Choose one of the RoadRunner methods if your ISP is Time Warner's RoadRunner; otherwise choose Standard .	Standard
Outgoing		
My Login	This field is applicable for PPPoE encapsulation only. Enter the login name assigned by your ISP when the Prestige calls this remote node. Some ISPs append this field to the Service Name field above (e.g., jim@poellc) to access the PPPoE server.	jim

Table 19-1 Menu 11.1 Remote Node Profile for Ethernet Encapsulation

FIELD	DESCRIPTION	EXAMPLE
My Password	Enter the password assigned by your ISP when the Prestige calls this remote node. Valid for PPPoE encapsulation only.	*****
Retype to Confirm	Type your password again to make sure that you have entered it correctly.	*****
Server	This field is valid only when RoadRunner is selected in the Service Type field. The Prestige will find the RoadRunner Server IP automatically if this field is left blank. If it does not, then you must enter the authentication server IP address here.	
Relogin Every (min)	This field is available when you select Telia Login in the Service Type field. The Telia server logs the Prestige out if the Prestige does not log in periodically. Type the number of minutes from 1 to 59 (30 recommended) for the Prestige to wait between logins.	
Route	This field refers to the protocol that will be routed by your Prestige – IP is the only option for the Prestige.	IP
Edit IP	This field leads to a “hidden” menu. Press [SPACE BAR] to select Yes and press [ENTER] to go to Menu 11.3 - Remote Node Network Layer Options .	No (default)
Session Options		
Edit Filter Sets	This field leads to another “hidden” menu. Use [SPACE BAR] to select Yes and press [ENTER] to open menu 11.5 to edit the filter sets. See the <i>Remote Node Filter</i> section for more details.	No (default)
Edit Traffic Redirect	Press [SPACE BAR] to select Yes or No . Select Yes and press [ENTER] to configure Menu 11.6 Traffic Redirect Setup . Select No (default) if you do not want to configure this feature.	
Once you have configured this menu, press [ENTER] at the message “Press ENTER to Confirm...” to save your configuration, or press [ESC] at any time to cancel.		

19.2.2 PPPoE Encapsulation

The Prestige supports PPPoE (Point-to-Point Protocol over Ethernet). You can only use PPPoE encapsulation when you're using the Prestige with a DSL modem as the WAN device. If you change the Encapsulation to **PPPoE**, then you will see the next screen. Please see the appendix for more information on PPPoE.

```
Menu 11.1 - Remote Node Profile

Rem Node Name= MyISP           Route= IP
Active= Yes

Encapsulation= PPPoE           Edit IP= No
Service Type= Standard         Telco Option:
Service Name=                   Allocated Budget(min)= 0
Outgoing:                       Period(hr)= 0
  My Login=                     Schedules=
  My Password= *****         Nailed-Up Connection= No
  Retype to Confirm= *****
  Authen= CHAP/PAP

                               Session Options:
                               Edit Filter Sets= No
                               Idle Timeout(sec)= 100

                               Edit Traffic Redirect= No

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

Figure 19-2 Menu 11.1 Remote Node Profile for PPPoE Encapsulation

Outgoing Authentication Protocol

Generally speaking, you should employ the strongest authentication protocol possible, for obvious reasons. However, some vendor's implementation includes a specific authentication protocol in the user profile. It will disconnect if the negotiated protocol is different from that in the user profile, even when the negotiated protocol is stronger than specified. If you encounter a case where the peer disconnects right after a successful authentication, please make sure that you specify the correct authentication protocol when connecting to such an implementation.

Nailed-Up Connection

A nailed-up connection is a dial-up line where the connection is always up regardless of traffic demand. The Prestige does two things when you specify a nailed-up connection. The first is that idle timeout is disabled.

The second is that the Prestige will try to bring up the connection when turned on and whenever the connection is down. A nailed-up connection can be very expensive for obvious reasons.

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

The following table describes the fields not already described in *Table 19-1*.

Table 19-2 Fields in Menu 11.1 (PPPoE Encapsulation Specific)

FIELD	DESCRIPTION	EXAMPLE
Service Name	If you are using PPPoE encapsulation, then type the name of your PPPoE service here. Only valid with PPPoE encapsulation.	poellc
Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are: CHAP/PAP - Your Prestige will accept either CHAP or PAP when requested by this remote node. CHAP - accept CHAP only. PAP - accept PAP only.	CHAP/PAP
Telco Option		
Allocated Budget	The field sets a ceiling for outgoing call time for this remote node. The default for this field is 0 meaning no budget control.	0 (default)
Period(hr)	This field is the time period that the budget should be reset. For example, if we are allowed to call this remote node for a maximum of 10 minutes every hour, then the Allocated Budget is (10 minutes) and the Period(hr) is 1 (hour).	0 (default)
Schedules	You can apply up to four schedule sets here. For more details please refer to the <i>Call Schedule Setup</i> chapter.	
Nailed-Up Connection	This field specifies if you want to make the connection to this remote node a nailed-up connection. More details are given earlier in this section.	No (default)
Session Options		
Idle Timeout	Type the length of idle time (when there is no traffic from the Prestige to the remote node) in seconds that can elapse before the Prestige automatically disconnects the PPPoE connection. This option only applies when the Prestige initiates the call.	100 seconds (default)

19.2.3 PPTP Encapsulation

If you change the Encapsulation to **PPTP** in menu 11.1, then you will see the next screen. Please see the appendix for information on PPTP.

```

Menu 11.1 - Remote Node Profile

Rem Node Name= MyISP           Route= IP
Active= Yes

Encapsulation= PPTP           Edit IP= No
Service Type= Standard        Telco Option:
Service Name= N/A              Allocated Budget(min)= 0
Outgoing:                      Period(hr)= 0
  My Login=                     Schedules=
  My Password= *****         Nailed-Up Connection= No
  Retype to Confirm= *****
  Authen= CHAP/PAP

PPTP:                          Session Options:
  My IP Addr=                   Edit Filter Sets= No
  My IP Mask=                   Idle Timeout(sec)= 100
  Server IP Addr=
  Connection ID/Name=           Edit Traffic Redirect= No

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

Figure 19-3 Menu 11.1 Remote Node Profile for PPTP Encapsulation

The next table shows how to configure fields in menu 11.1 not previously discussed.

Table 19-3 Menu 11.1 Remote Node Profile for PPTP Encapsulation

FIELD	DESCRIPTION	EXAMPLE
Encapsulation	Press [SPACE BAR] and then [ENTER] to select PPTP . You must also go to menu 11.3 to check the IP Address setting once you have selected the encapsulation method.	PPTP
My IP Addr	Enter the IP address of the WAN Ethernet port.	10.0.0.140
My IP Mask	Enter the subnet mask of the WAN Ethernet port.	255.255.255.0
Server IP Addr	Enter the IP address of the ANT modem.	10.0.0.138
Connection ID/Name	Enter the connection ID or connection name in the ANT. It must follow the "c:id" and "n:name" format. This field is optional and depends on the requirements of your DSL modem.	N:My ISP

19.3 Edit IP

Move the cursor to the **Edit IP** field in menu 11.1, then press [SPACE BAR] to select **Yes**. Press [ENTER] to open **Menu 11.3 - Remote Node Network Layer Options**.

```

Menu 11.3 - Remote Node Network Layer Options

IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Addr= N/A

Network Address Translation= SUA Only
Metric= 1
Private= N/A
RIP Direction= None
  Version= N/A
Multicast= None

Enter here to CONFIRM or ESC to CANCEL:

```

Figure 19-4 Menu 11.3 Remote Node Network Layer Options for Ethernet Encapsulation

This menu displays the **My WAN Addr** field for **PPPoE** and **PPTP** encapsulations and **Gateway IP Addr** field for **Ethernet** encapsulation. The following table describes the fields in this menu.

Table 19-4 Remote Node Network Layer Options

FIELD	DESCRIPTION	EXAMPLE
IP Address Assignment	If your ISP did not assign you an explicit IP address, press [SPACE BAR] and then [ENTER] to select Dynamic ; otherwise select Static and enter the IP address & subnet mask in the following fields.	Dynamic (default)
(Rem) IP Address	If you have a static IP Assignment, enter the IP address assigned to you by your ISP.	
(Rem) IP Subnet Mask	If you have a static IP Assignment, enter the subnet mask assigned to you.	
Gateway IP Addr	This field is applicable to Ethernet encapsulation only. Enter the gateway IP address assigned to you if you are using a static IP address.	

Table 19-4 Remote Node Network Layer Options

FIELD	DESCRIPTION	EXAMPLE
My WAN Addr	<p>This field is applicable to PPPoE and PPTP encapsulations only. Some implementations, especially the UNIX derivatives, require the WAN link to have a separate IP network number from the LAN and each end must have a unique address within the WAN network number. If this is the case, enter the IP address assigned to the WAN port of your Prestige.</p> <p>Note that this is the address assigned to your local Prestige, not the remote router.</p>	
Network Address Translation	<p>Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet).</p> <p>Choose None to disable NAT.</p> <p>Choose SUA Only if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: Many-to-One and Server.</p> <p>Choose Full Feature if you have multiple public IP addresses. Full Feature mapping types include: One-to-One, Many-to-One (SUA/PAT), Many-to-Many Overload, Many- One-to-One and Server. When you select Full Feature you must configure at least one address mapping set!</p> <p>See the <i>NAT chapter</i> for a full discussion on this feature.</p>	SUA Only (default)
Metric	<p>Enter a number from 1 to 15 to set this route's priority among the Prestige's routes (see the <i>Metric</i> section in the <i>WAN and Dial Backup Setup</i> chapter). The smaller the number, the higher priority the route has.</p>	1
Private	<p>This field is valid only for PPTP/PPPoE encapsulation. This parameter determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to Yes, this route is kept private and not included in RIP broadcast. If No, the route to this remote node will be propagated to other hosts through RIP broadcasts.</p>	No
RIP Direction	<p>Press [SPACE BAR] and then [ENTER] to select the RIP direction from Both/ None/In Only/Out Only. See the <i>LAN Setup</i> chapter for more information on RIP. The default for RIP on the WAN side is None. It is recommended that you do not change this setting.</p>	None (default)
Version	<p>Press [SPACE BAR] and then [ENTER] to select the RIP version from RIP-1/RIP-2B/RIP-2M or None.</p>	N/A

Table 19-4 Remote Node Network Layer Options

FIELD	DESCRIPTION	EXAMPLE
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group. The Prestige supports both IGMP version 1 (IGMP-v1) and version 2 (IGMP-v2). Press [SPACE BAR] to enable IP Multicasting or select None to disable it. See the <i>LAN Setup</i> chapter for more information on this feature.	None (default)
Once you have completed filling in Menu 11.3 Remote Node Network Layer Options , press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration and return to menu 11, or press [ESC] at any time to cancel.		

19.4 Remote Node Filter

Move the cursor to the field **Edit Filter Sets** in menu 11.1, and then press [SPACE BAR] to set the value to **Yes**. Press [ENTER] to open **Menu 11.5 - Remote Node Filter**.

Use menu 11.5 to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the Prestige to prevent certain packets from triggering calls. You can specify up to 4 filter sets separated by commas, for example, 1, 5, 9, 12, in each filter field. Note that spaces are accepted in this field. For more information on defining the filters, please refer to the Filters chapter. For PPPoE or PPTP encapsulation, you have the additional option of specifying remote node call filter sets.

```

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 19-5 Menu 11.5: Remote Node Filter (Ethernet Encapsulation)

```

Menu 11.5 - Remote Node Filter

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

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

Figure 19-6 Menu 11.5: Remote Node Filter (PPPoE or PPTP Encapsulation)

19.4.1 Traffic Redirect Setup

Configure parameters that determine when the Prestige will forward WAN traffic to the backup gateway using **Menu 11.6 — Traffic Redirect Setup**.

```

Menu 11.6 - Traffic Redirect Setup

Active= Yes
Configuration:
  Backup Gateway IP Address= 0.0.0.0
  Metric= 14
  Check WAN IP Address= 0.0.0.0
  Fail Tolerance= 2
  Period(sec)= 5
  Timeout(sec)= 3

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

Figure 19-7 Menu 11.6: Traffic Redirect Setup

The following table describes the fields in this screen.

Table 19-5 Menu 11.6: Traffic Redirect Setup

FIELD	DESCRIPTION	EXAMPLE
Active	Press [SPACE BAR] and select Yes (to enable) or No (to disable) traffic redirect setup. The default is No .	Yes

Table 19-5 Menu 11.6: Traffic Redirect Setup

FIELD	DESCRIPTION	EXAMPLE
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.	0.0.0.0
Metric	Enter a number from 1 to 15 to set this route's priority among the Prestige's routes (see the <i>Metric</i> section in the <i>WAN and Dial Backup Setup</i> chapter) The smaller the number, the higher priority the route has.	15 (default)
Check WAN IP Address	Enter the IP address of a reliable nearby computer (for example, your ISP's DNS server address) to test your Prestige's WAN accessibility. The Prestige uses the default gateway IP address if you do not enter an IP address here. If you are using PPTP or PPPoE Encapsulation, enter "0.0.0.0" to configure the Prestige to check the PVC (Permanent Virtual Circuit) or PPTP tunnel.	0.0.0.0
Fail Tolerance	Enter the number of times your Prestige may attempt and fail to connect to the Internet before traffic is forwarded to the backup gateway. Two to five is usually a good number.	2
Period (sec)	Enter the time interval (in seconds) between WAN connection checks. Five to 60 is usually a good number.	5
Timeout (sec)	Enter the number of seconds the Prestige waits for a ping response from the IP Address in the Check WAN IP Address field before it times out. The number in this field should be less than the number in the Period field. Three to 50 is usually a good number. The WAN connection is considered "down" after the Prestige times out the number of times specified in the Fail Tolerance field.	3
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

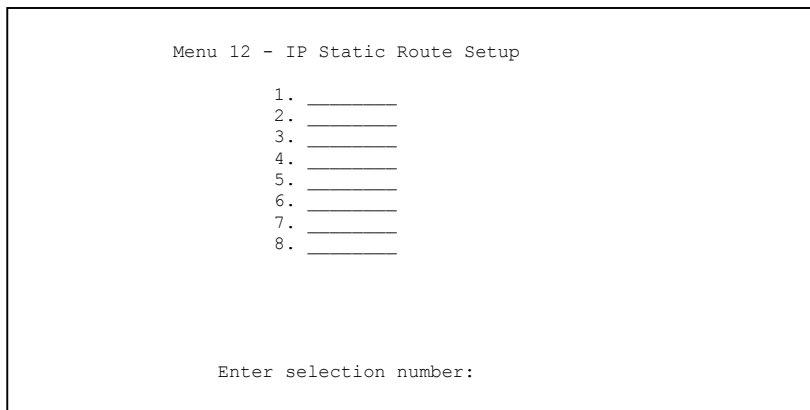
Chapter 20

Static Route Setup

This chapter shows how to setup IP static routes.

20.1 IP Static Route Setup

Step 1. To configure an IP static route, use **Menu 12 – Static Routing Setup** (shown next).



```
Menu 12 - IP Static Route Setup

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____

Enter selection number:
```

Figure 20-1 Menu 12 IP Static Route Setup

Step 3. Now, type the route number of a static route you want to configure.

```

Menu 12.1 - 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:
    
```

Figure 20-2 Menu12.1 Edit IP Static Route

The following table describes the fields for **Menu 12.1 – Edit IP Static Route Setup**.

Table 20-1 Menu12.1 Edit IP Static Route

FIELD	DESCRIPTION
Route #	This is the index number of the static route that you chose in menu 12.1.
Route Name	Type a descriptive name for this route. This is for identification purpose only.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Type the subnet mask for this destination. Follow the discussion on <i>IP Subnet Mask</i> in this manual.
Gateway IP Address	Type the IP address of the gateway. The gateway is an immediate neighbor of your Prestige that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your Prestige; over WAN, the gateway must be the IP address of one of the remote nodes.
Metric	Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Type a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.

Table 20-1 Menu12.1 Edit IP Static Route

FIELD	DESCRIPTION
Private	This parameter determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to Yes , this route is kept private and is not included in RIP broadcasts. If No , the route to this remote node will be propagated to other hosts through RIP broadcasts.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

Chapter 21

Network Address Translation (NAT)

This chapter discusses how to configure NAT on the Prestige.

21.1 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.

21.1.1 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 21.3.1* for 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.

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

21.2 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**.

```
Menu 4 - Internet Access Setup

ISP's Name= MyISP
Encapsulation= Ethernet
Service Type= Standard
My Login= N/A
My Password= N/A
Retype to Confirm= N/A
Login Server= N/A
Relogin Every (min)= N/A
IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Address= N/A
Network Address Translation= SUA Only

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

Figure 21-1 Menu 4 Applying NAT for Internet Access

The following figure shows how you apply NAT to the remote node in menu 11.1.

- Step 1.** Enter 11 from the main menu.
- Step 2.** When menu 11 appears, as shown in the following figure, type the number of the remote node that you want to configure.
- Step 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**.

```

Menu 11.3 - Remote Node Network Layer Options

IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Addr= N/A

Network Address Translation= SUA Only
Metric= 1
Private= N/A
RIP Direction= None
  Version= N/A
Multicast= None

Enter here to CONFIRM or ESC to CANCEL:

```

Figure 21-2 Menu 11.3 Applying NAT to the Remote Node

The following table describes the options for Network Address Translation.

Table 21-1 Applying NAT in Menus 4 & 11.3

FIELD	DESCRIPTION	EXAMPLE
NAT	Press [SPACE BAR] and then [ENTER] to select Full Feature if you have multiple public WAN IP addresses for your Prestige. The SMT uses the address mapping set that you configure and enter in the Address Mapping Set field (menu 15.1 - see section 21.3.1).	Full Feature
	Select None to disable NAT.	None
	When you select SUA Only , the SMT uses Address Mapping Set 255 (menu 15.1 - see section 21.3.1). Choose SUA Only if you have just one public WAN IP address for your Prestige.	SUA Only

21.3 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.

```
Menu 15 - NAT Setup

1. Address Mapping Sets
2. Port Forwarding Setup
3. Trigger Port Setup

Enter Menu Selection Number:
```

Figure 21-3 Menu 15 NAT Setup

21.3.1 Address Mapping Sets

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

```
Menu 15.1 - Address Mapping Sets

1. NAT_SET
255. SUA (read only)

Enter Menu Selection Number:
```

Figure 21-4 Menu 15.1 Address Mapping Sets

SUA Address Mapping Set

Enter 255 to display the next screen (see also *section 21.1.1*). The fields in this menu cannot be changed.

```

Menu 15.1.255 - Address Mapping Rules

Set Name= SUA

Idx  Local Start IP  Local End IP  Global Start IP  Global End IP  Type
-----
1.   0.0.0.0          255.255.255.255  0.0.0.0          0.0.0.0          M-1
2.
3.
4.
5.
6.
7.
8.
9.
10.

Press ENTER to Confirm or ESC to Cancel:

```

Figure 21-5 Menu 15.1.255 SUA Address Mapping Rules

The following table explains the fields in this menu.

Menu 15.1.255 is read-only.

Table 21-2 SUA Address Mapping Rules

FIELD	DESCRIPTION	EXAMPLE
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.	SUA
Idx	This is the index or rule number.	1
Local Start IP	Local Start IP is the starting local IP address (ILA).	0.0.0.0
Local End IP	Local End IP is the ending local IP address (ILA). If the rule is for all local IPs, then the Start IP is 0.0.0.0 and the End IP is 255.255.255.255.	255.255.255.255
Global Start IP	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the Global Start IP .	0.0.0.0
Global End IP	This is the ending global IP address (IGA).	
Type	These are the mapping types. Server allows us to specify multiple servers of different types behind NAT to this machine. See later for some examples.	Server

Table 21-2 SUA Address Mapping Rules

FIELD	DESCRIPTION	EXAMPLE
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

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.

```

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:
    
```

Figure 21-6 Menu 15.1.1 First Set

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.

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 21-3 Menu 15.1.1 First Set

FIELD	DESCRIPTION	EXAMPLE
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.	NAT_SET
Action	The default is Edit . Edit means you want to edit a selected rule (see following field). Insert Before means to insert a rule before the rule selected. The rules after the selected rule will then be moved down by one rule. Delete means to delete the selected rule and then all the rules after the selected one will be advanced one rule. None disables the Select Rule item.	Edit
Select Rule	When you choose Edit , Insert Before or Delete in the previous field the cursor jumps to this field to allow you to select the rule to apply the action in question.	1

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.

```

Menu 15.1.1.1 Address Mapping Rule

Type= One-to-One

Local IP:
  Start= 0.0.0.0
  End = N/A

Global IP:
  Start= 0.0.0.0
  End = N/A

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

Figure 21-7 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set

The following table explains the fields in this menu.

Table 21-4 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set

FIELD	DESCRIPTION	EXAMPLE
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. Server allows you to specify multiple servers of different types behind NAT to this computer. See <i>section 21.5.3</i> for an example.	One-to-One
Local IP	Only local IP fields are N/A for server; Global IP fields MUST be set for Server .	
Start	This is the starting local IP address (ILA).	0.0.0.0
End	This is the ending local IP address (ILA). If the rule is for all local IPs, then put the Start IP as 0.0.0.0 and the End IP as 255.255.255.255. This field is N/A for One-to-One and Server types.	N/A
Global IP		
Start	This is the starting inside global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the Global IP Start . Note that Global IP Start can be set to 0.0.0.0 only if the types are Many-to-One or Server .	0.0.0.0
End	This is the ending inside global IP address (IGA). This field is N/A for One-to-One , Many-to-One and Server types.	N/A
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

21.4 Configuring a Server behind NAT

Follow these steps to configure a server behind NAT:

Step 1. Enter 15 in the main menu to go to **Menu 15 - NAT Setup**.

Step 2. Enter 2 to display **Menu 15.2 - NAT Server Setup** as shown next.

Menu 15.2 - NAT Server Setup			
Rule	Start Port No.	End Port No.	IP Address
1.	Default	Default	0.0.0.0
2.	21	25	192.168.1.33
3.	0	0	0.0.0.0
4.	0	0	0.0.0.0
5.	0	0	0.0.0.0
6.	0	0	0.0.0.0
7.	0	0	0.0.0.0
8.	0	0	0.0.0.0
9.	0	0	0.0.0.0
10.	0	0	0.0.0.0
11.	0	0	0.0.0.0
12.	0	0	0.0.0.0

Press ENTER to Confirm or ESC to Cancel:

Figure 21-8 Menu 15.2.1 NAT Server Setup

Step 3. Enter a port number in an unused **Start Port No** field. To forward only one port, enter it again in the **End Port No** field. To specify a range of ports, enter the last port to be forwarded in the **End Port No** field.

Step 4. Enter the inside IP address of the server in the **IP Address** field. In the following figure, you have a computer acting as an FTP, Telnet and SMTP server (ports 21, 23 and 25) at 192.168.1.33.

Step 5. Press [ENTER] at the “Press ENTER to confirm ...” prompt to save your configuration after you define all the servers or press [ESC] at any time to cancel.

You assign the private network IP addresses. The NAT network appears as a single host on the Internet. A is the FTP/Telnet/SMTP server.

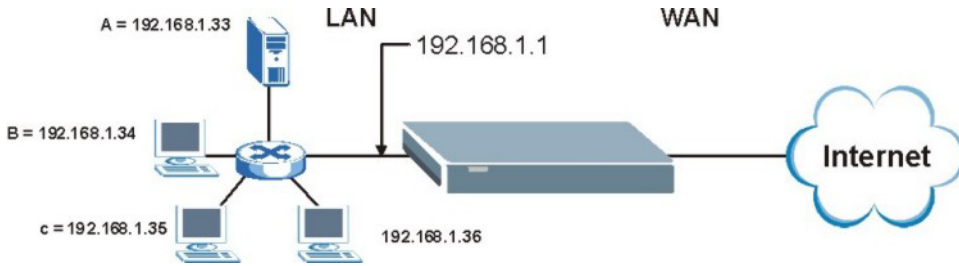


Figure 21-9 Multiple Servers Behind NAT Example

21.5 General NAT Examples

The following are some examples of NAT configuration.

21.5.1 Example 1: Internet Access Only

In the following Internet access example, you only need one rule where the ILAs (Inside Local Addresses) of computers A through D map to one dynamic IGA (Inside Global Address) assigned by your ISP.

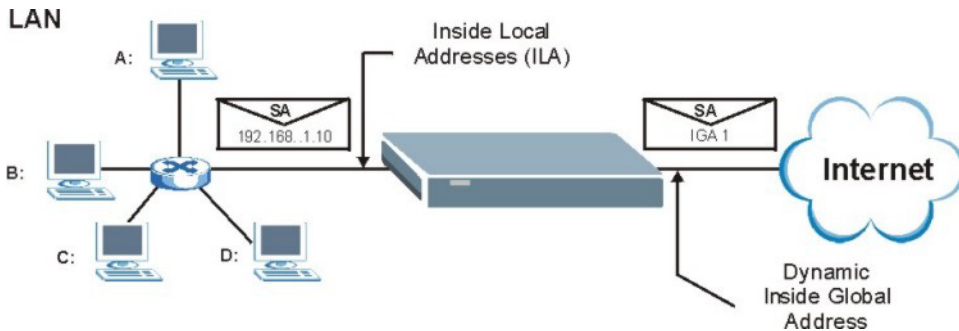


Figure 21-10 NAT Example 1

```

Menu 4 - Internet Access Setup

ISP's Name= MyISP
Encapsulation= Ethernet
Service Type= Standard
My Login= N/A
My Password= N/A
Retype to Confirm= N/A
Login Server= N/A
Relogin Every (min)= N/A
IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Address= N/A
Network Address Translation= SUA Only

Press ENTER to Confirm or ESC to Cancel:

```

Figure 21-11 Menu 4 Internet Access & NAT Example

From menu 4, choose the **SUA Only** option from the **Network Address Translation** field. This is the Many-to-One mapping discussed in *section 21.5*. 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.

21.5.2 Example 2: Internet Access with an Inside Server

The dynamic Inside Global Address is assigned by the ISP.

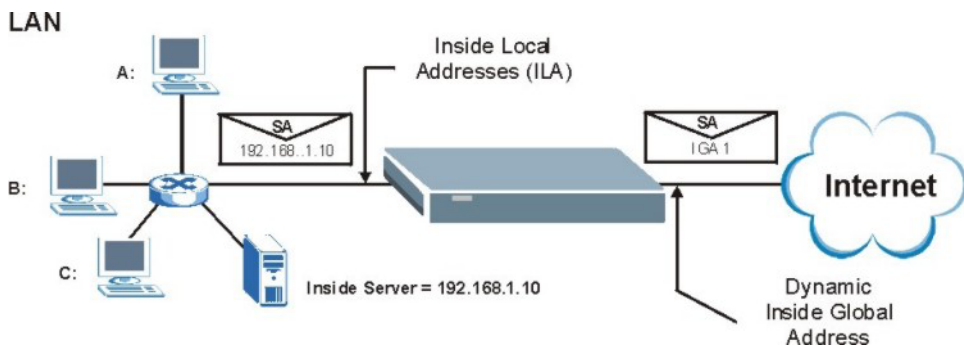


Figure 21-12 NAT Example 2

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.

Menu 15.2.1 - NAT Server Setup			
Rule	Start Port No.	End Port No.	IP Address
1.	Default	Default	192.168.1.10
2.	0	0	0.0.0.0
3.	0	0	0.0.0.0
4.	0	0	0.0.0.0
5.	0	0	0.0.0.0
6.	0	0	0.0.0.0
7.	0	0	0.0.0.0
8.	0	0	0.0.0.0
9.	0	0	0.0.0.0
10.	0	0	0.0.0.0
11.	0	0	0.0.0.0
12.	0	0	0.0.0.0

Press ENTER to Confirm or ESC to Cancel:

Figure 21-13 Menu 15.2.1 Specifying an Inside Server

21.5.3 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.

- Rule 1.** Map the first IGA to the first inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).
- Rule 2.** Map the second IGA to our second inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).
- Rule 3.** Map the other outgoing LAN traffic to IGA3 (**Many : 1** mapping).
- Rule 4.** You also map your third IGA to the web server and mail server on the LAN. Type **Server** allows you to specify multiple servers, of different types, to other computers behind NAT on the LAN.

The example situation looks somewhat like this:

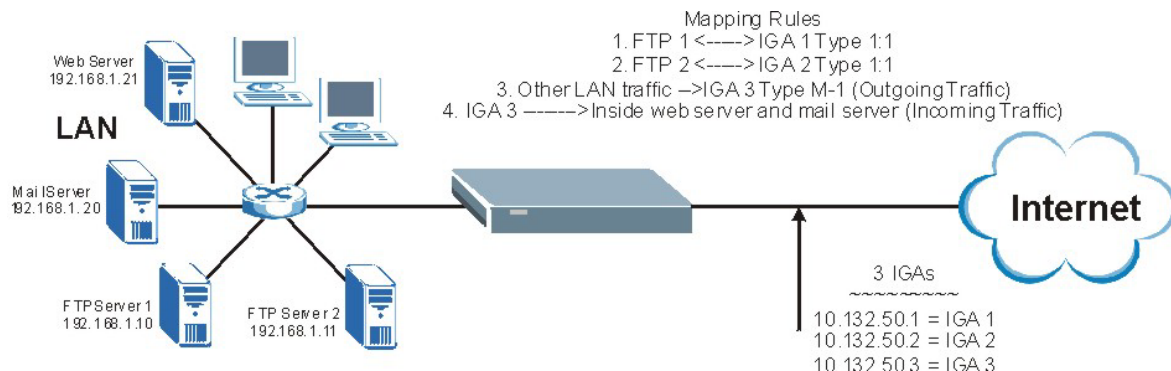


Figure 21-14 NAT Example 3

- Step 1.** In this case you need to configure Address Mapping Set 1 from **Menu 15.1 - Address Mapping Sets**. Therefore you must choose the **Full Feature** option from the **Network Address Translation** field (in menu 4 or menu 11.3) in *Figure 21-15*.
- Step 2.** Then enter 15 from the main menu.
- Step 3.** Enter 1 to configure the Address Mapping Sets.
- Step 4.** Enter 1 to begin configuring this new set. Enter a Set Name, choose the **Edit Action** and then enter 1 for the **Select Rule** field. Press [ENTER] to confirm.
- Step 5.** Select **Type** as **One-to-One** (direct mapping for packets going both ways), and enter the local **Start IP** as 192.168.1.10 (the IP address of FTP Server 1), the global **Start IP** as 10.132.50.1 (our first IGA). (See *Figure 21-16*).
- Step 6.** Repeat the previous step for rules 2 to 4 as outlined above.
- Step 7.** When finished, menu 15.1.1 should look like as shown in *Error! Reference source not found.*

```
Menu 11.3 - Remote Node Network Layer Options

IP Address Assignment= Dynamic
IP Address= N/A
IP Subnet Mask= N/A
Gateway IP Addr= N/A

Network Address Translation= Full Feature
Metric= 1
Private= N/A
RIP Direction= None
  Version= N/A
Multicast= None

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

Figure 21-15 Example 3: Menu 11.3

The following figures show how to configure the first rule.

```
Menu 15.1.1.1 Address Mapping Rule

Type= One-to-One

Local IP:
  Start= 192.168.1.10
  End = N/A

Global IP:
  Start= 10.132.50.1
  End = N/A

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 21-16 Example 3: Menu 15.1.1.1


```
Menu 15.1.1 - Address Mapping Rules

Set Name= NAT_SET

Idx  Local Start IP  Local End IP  Global Start IP  Global End IP  Type
-----
1.   192.168.1.10    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= None      Select Rule= N/A

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

Figure 21-17 Example 3: Final Menu 15.1.1

Now configure the IGA3 to map to our web server and mail server on the LAN.

Step 8. Enter 15 from the main menu.

Step 9. Enter 2 in **Menu 15 - NAT Setup**.

Step 10. Enter 1 in **Menu 15.2 - NAT Server Sets** to see the following menu. Configure it as shown.

Menu 15.2.1 - NAT Server Setup

Rule	Start Port No.	End Port No.	IP Address
1.	Default	Default	0.0.0.0
2.	80	80	192.168.1.21
3.	25	25	192.168.1.20
4.	0	0	0.0.0.0
5.	0	0	0.0.0.0
6.	0	0	0.0.0.0
7.	0	0	0.0.0.0
8.	0	0	0.0.0.0
9.	0	0	0.0.0.0
10.	0	0	0.0.0.0
11.	0	0	0.0.0.0
12.	0	0	0.0.0.0

Press ENTER to Confirm or ESC to Cancel:

Example 3: Menu 15.2.1

21.5.4 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.

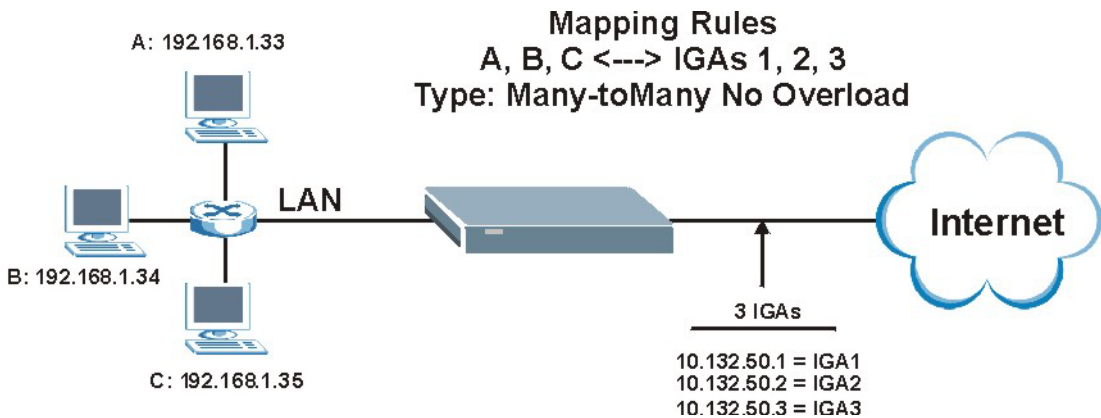


Figure 21-18 NAT Example 4

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.

```

Menu 15.1.1.1 Address Mapping Rule

Type= Many-One-to-One

Local IP:
  Start= 192.168.1.10
  End   = 192.168.1.12

Global IP:
  Start= 10.132.50.1
  End   = 10.132.50.3

Press ENTER to Confirm or ESC to Cancel:

```

Figure 21-19 Example 4: Menu 15.1.1.1 Address Mapping Rule

After you've configured your rule, you should be able to check the settings in menu 15.1.1 as shown next.

```

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:

```

Figure 21-20 Example 4: Menu 15.1.1 Address Mapping Rules

21.6 Configuring Trigger Port Forwarding

Only one LAN computer can use a trigger port (range) at a time.

Enter 3 in menu 15 to display **Menu 15.3 — Trigger Port Setup**, shown next.

Menu 15.3 - Trigger Port Setup						
Rule	Name	Incoming		Trigger		
		Start Port	End Port	Start Port	End Port	
1.	Real Audio	6970	7170	7070	7070	
2.		0	0	0	0	
3.		0	0	0	0	
4.		0	0	0	0	
5.		0	0	0	0	
6.		0	0	0	0	
7.		0	0	0	0	
8.		0	0	0	0	
9.		0	0	0	0	
10.		0	0	0	0	
11.		0	0	0	0	
12.		0	0	0	0	

Press ENTER to Confirm or ESC to Cancel:

Figure 21-21 Menu 15.3 Trigger Port Setup

The following table describes the fields in this screen.

Table 21-5 Menu 15.3 Trigger Port Setup

FIELD	DESCRIPTION	EXAMPLE
Rule	This is the rule index number.	1
Name	Enter a unique name for identification purposes. You may enter up to 15 characters in this field. All characters are permitted - including spaces.	Real Audio
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The Prestige forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.	
Start Port	Enter a port number or the starting port number in a range of port numbers.	6970
End Port	Enter a port number or the ending port number in a range of port numbers.	7170
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the Prestige to record the IP address of the LAN computer that sent the traffic to a server on the WAN.	
Start Port	Enter a port number or the starting port number in a range of port numbers.	7070

Table 21-5 Menu 15.3 Trigger Port Setup

FIELD	DESCRIPTION	EXAMPLE
End Port	Enter a port number or the ending port number in a range of port numbers.	7070
Press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		

Chapter 22

Enabling the Firewall

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

22.1 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.

22.2 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.

22.3 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.

```
Menu 21.2 - Firewall Setup

The firewall protects against Denial of Service (DoS) attacks when
it is active.

Your network is vulnerable to attacks when the firewall is turned off.

Refer to the User's Guide for details about the firewall default
policies.

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

Active: No

You can use the Web Configurator to configure the firewall.

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

Figure 22-1 Menu 21.2 Firewall Setup

Use the web configurator or the command interpreter to configure the firewall rules.

Part VIII:

SMT Advanced Management

This part discusses filtering setup, SNMP, system security, system information and diagnosis, firmware and configuration file maintenance, system maintenance, remote management and call scheduling.

See the web configurator parts of this guide for background information on features configurable by web configurator and SMT.

Chapter 23

Filter Configuration

This chapter shows you how to create and apply filters.

23.1 Introduction to Filters

Your Prestige uses filters to decide whether 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 the 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 LAN side. Call filtering is used to determine if a packet should be allowed to trigger a call. Remote node call filtering is only applicable when using PPPoE encapsulation. Outgoing packets must undergo data filtering before they encounter call filtering as shown in the following figure.

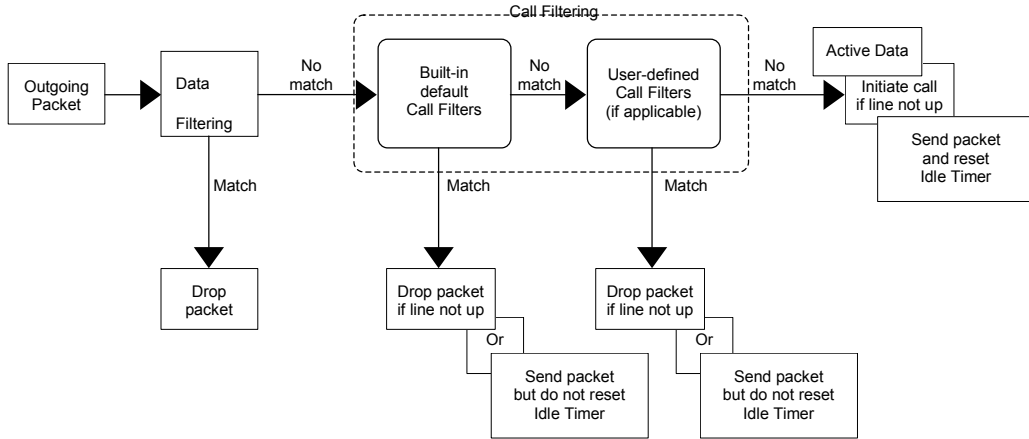


Figure 23-1 Outgoing Packet Filtering Process

For incoming packets, your Prestige applies data filters only. Packets are processed depending upon whether a match is found. The following sections describe how to configure filter sets.

23.1.1 The Filter Structure of the Prestige

A filter set consists of one or more filter rules. Usually, you would group related rules, e.g., all the rules for NetBIOS, into a single set and give it a descriptive name. The Prestige allows you to configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system. You cannot mix device filter rules and protocol filter rules within the same set. You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

Sets of factory default filter rules have been configured in menu 21 to prevent NetBIOS traffic from triggering calls and to prevent incoming telnet sessions. 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. See also *Figure 23-7* for the logic flow when executing an IP filter.

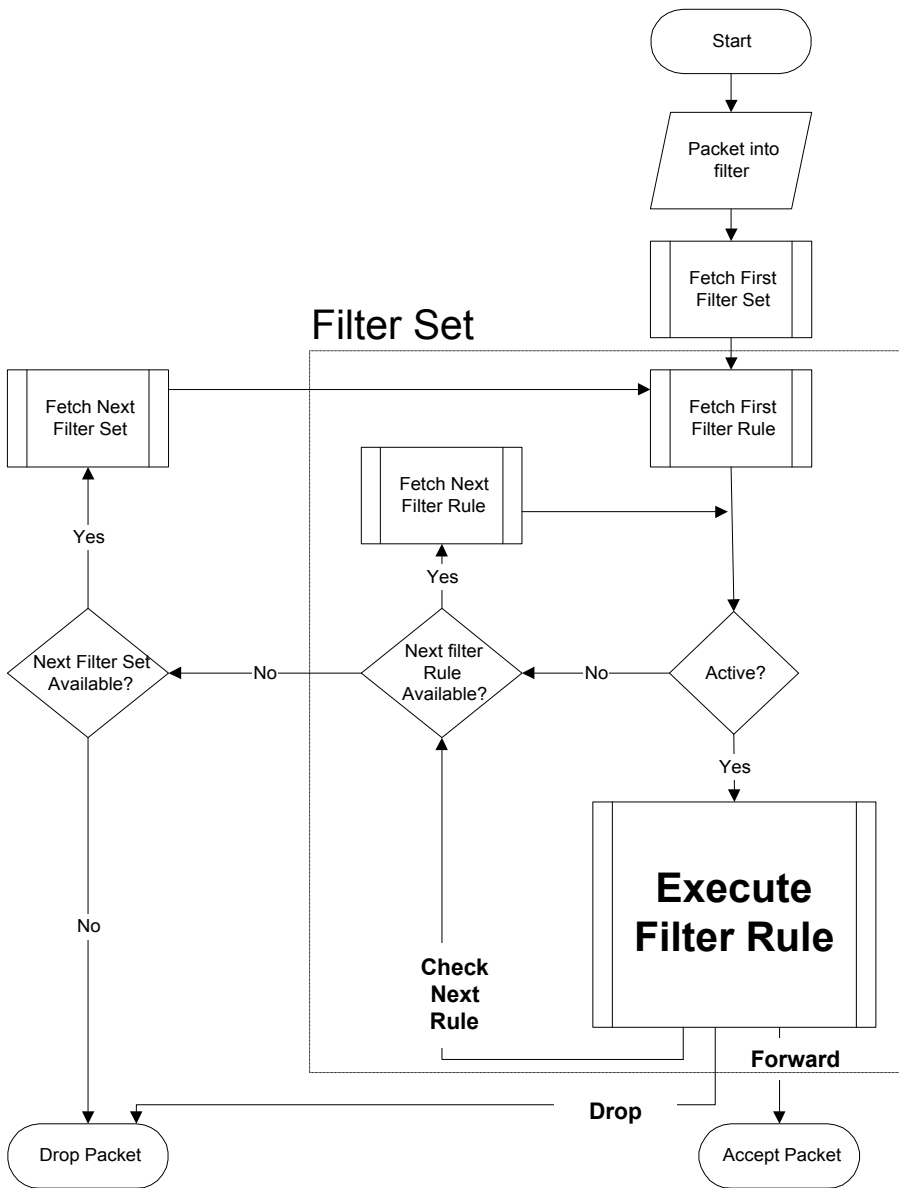


Figure 23-2 Filter Rule Process

You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

23.2 Configuring a Filter Set

The Prestige includes filtering for NetBIOS over TCP/IP packets by default. To configure another filter set, follow the procedure below.

Step 1. Enter 21 in the main menu to open menu 21.

```
Menu 21 - Filter and Firewall Setup

1. Filter Setup
2. Firewall Setup

Enter Menu Selection Number:
```

Figure 23-4 Menu 21: Filter and Firewall Setup

Step 2. Enter 1 to bring up the following menu.

```
Menu 21.1 - Filter Set Configuration

Filter Set #      Comments      Filter Set #      Comments
-----
1      _____      7      _____
2      _____      8      _____
3      _____      9      _____
4      _____     10     _____
5      _____     11     _____
6      _____     12     _____

Enter Filter Set Number to Configure= 0
Edit Comments= N/A

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

Figure 23-5 Menu 21.1: Filter Set Configuration

- Step 3.** Select the filter set you wish to configure (1-12) and press [ENTER].
- Step 4.** Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].
- Step 5.** Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.1 - Filter Rules Summary**.

This screen shows the summary of the existing rules in the filter set. The following tables contain a brief description of the abbreviations used in the previous menus.

Table 23-1 Abbreviations Used in the Filter Rules Summary Menu

FIELD	DESCRIPTION
#	The filter rule number: 1 to 6.
A	Active: "Y" means the rule is active. "N" means the rule is inactive.
Type	The type of filter rule: "GEN" for Generic, "IP" for TCP/IP.
Filter Rules	These parameters are displayed here.
M	More. "Y" means there are more rules to check which form a rule chain with the present rule. An action cannot be taken until the rule chain is complete. "N" means there are no more rules to check. You can specify an action to be taken i.e., forward the packet, drop the packet or check the next rule. For the latter, the next rule is independent of the rule just checked.
m	Action Matched. "F" means to forward the packet immediately and skip checking the remaining rules. "D" means to drop the packet. "N" means to check the next rule.
n	Action Not Matched. "F" means to forward the packet immediately and skip checking the remaining rules. "D" means to drop the packet. "N" means to check the next rule.

The protocol dependent filter rules abbreviation are listed as follows:

Table 23-2 Rule Abbreviations Used

ABBREVIATION	DESCRIPTION
IP	Pr Protocol
	SA Source Address
	SP Source Port number
	DA Destination Address
	DP Destination Port number
GEN	Off Offset
	Len Length

Refer to the next section for information on configuring the filter rules.

23.2.1 Configuring a Filter Rule

To configure a filter rule, type its number in **Menu 21.1.1 - Filter Rules Summary** and press [ENTER] to open menu 21.1.1.1 for the rule.

To speed up filtering, all rules in a filter set must be of the same class, i.e., protocol filters or generic filters. The class of a filter set is determined by the first rule that you create. When applying the filter sets to a port, separate menu fields are provided for protocol and device filter sets. If you include a protocol filter set in a device filter field or vice versa, the Prestige will warn you and will not allow you to save.

23.2.2 Configuring a TCP/IP Filter Rule

This section shows you how to configure a TCP/IP filter rule. TCP/IP rules allow you to base the rule on the fields in the IP and the upper layer protocol, for example, UDP and TCP headers.

To configure TCP/IP rules, select **TCP/IP Filter Rule** from the **Filter Type** field and press [ENTER] to open **Menu 21.1.1.1 - TCP/IP Filter Rule**, as shown next.

```

Menu 21.1.1.1 - TCP/IP Filter Rule

Filter #: 1,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 0      IP Source Route= No
Destination: IP Addr= 0.0.0.0
              IP Mask= 0.0.0.0
              Port #= 137
              Port # Comp= Equal
Source: IP Addr= 0.0.0.0
        IP Mask= 0.0.0.0
        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:

```

Figure 23-6 Menu 21.1.1.1 TCP/IP Filter Rule

The following table describes how to configure your TCP/IP filter rule.

Table 23-3 TCP/IP Filter Rule

FIELD	DESCRIPTION	OPTIONS
Active	Press [SPACE BAR] and then [ENTER] to select Yes to activate the filter rule or No to deactivate it.	Yes No
IP Protocol	Protocol refers to the upper layer protocol, e.g., TCP is 6, UDP is 17 and ICMP is 1. Type a value between 0 and 255. A value of 0 matches ANY protocol.	0-255
IP Source Route	Press [SPACE BAR] and then [ENTER] to select Yes to apply the rule to packets with an IP source route option. Otherwise the packets must not have a source route option. The majority of IP packets do not have source route.	Yes No
Destination		
IP Address	Enter the destination IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.	0.0.0.0

Table 23-3 TCP/IP Filter Rule

FIELD	DESCRIPTION	OPTIONS
IP Mask	Enter the IP mask to apply to the Destination: IP Addr.	0.0.0.0
Port #	Enter the destination port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.	0-65535
Port # Comp	Press [SPACE BAR] and then [ENTER] to select the comparison to apply to the destination port in the packet against the value given in Destination: Port #.	None Less Greater Equal Not Equal
Source		
IP Address	Enter the source IP Address of the packet you wish to filter. This field is ignored if it is 0.0.0.0.	0.0.0.0
IP Mask	Enter the IP mask to apply to the Source: IP Addr.	0.0.0.0
Port #	Enter the source port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is ignored if it is 0.	0-65535
Port # Comp	Press [SPACE BAR] and then [ENTER] to select the comparison to apply to the source port in the packet against the value given in Source: Port #.	None Less Greater Equal Not Equal
TCP Estab	This field is applicable only when the IP Protocol field is 6, TCP. Press [SPACE BAR] and then [ENTER] to select Yes , to have the rule match packets that want to establish a TCP connection (SYN=1 and ACK=0); if No , it is ignored.	Yes No
More	Press [SPACE BAR] and then [ENTER] to select Yes or No . If Yes , a matching packet is passed to the next filter rule before an action is taken; if No , the packet is disposed of according to the action fields. If More is Yes , then Action Matched and Action Not Matched will be N/A .	Yes No

Table 23-3 TCP/IP Filter Rule

FIELD	DESCRIPTION	OPTIONS
Log	Press [SPACE BAR] and then [ENTER] to select a logging option from the following: None – No packets will be logged. Action Matched - Only packets that match the rule parameters will be logged. Action Not Matched - Only packets that do not match the rule parameters will be logged. Both – All packets will be logged.	None Action Matched Action Not Matched Both
Action Matched	Press [SPACE BAR] and then [ENTER] to select the action for a matching packet.	Check Next Rule Forward Drop
Action Not Matched	Press [SPACE BAR] and then [ENTER] to select the action for a packet not matching the rule.	Check Next Rule Forward Drop
When you have Menu 21.1.1.1 - TCP/IP Filter Rule configured, press [ENTER] at the message "Press ENTER to Confirm" to save your configuration, or press [ESC] to cancel. This data will now be displayed on Menu 21.1.1 - Filter Rules Summary .		

The following figure illustrates the logic flow of an IP filter.

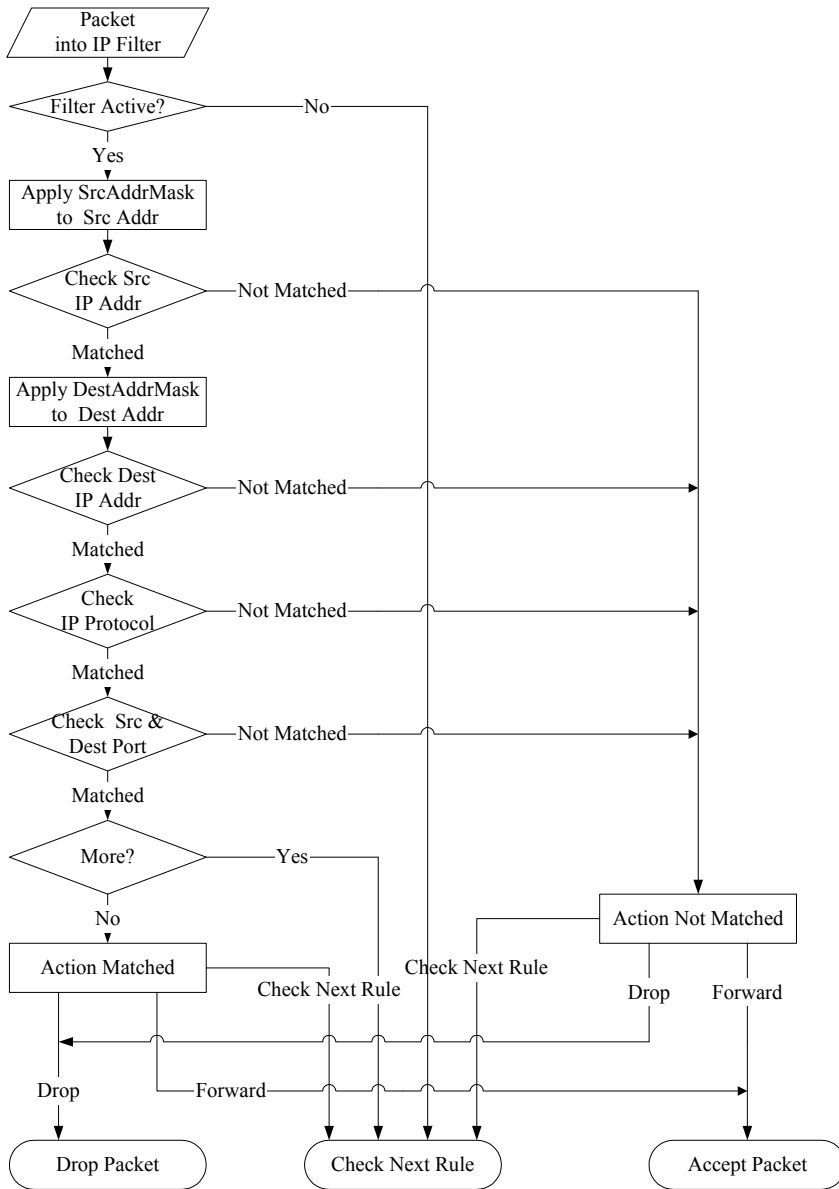


Figure 23-7 Executing an IP Filter

23.2.3 Configuring a Generic Filter Rule

This section shows you how to configure a generic filter rule. The purpose of generic rules is to allow you to filter non-IP packets. For IP, it is generally easier to use the IP rules directly.

For generic rules, the Prestige treats a packet as a byte stream as opposed to an IP or IPX packet. You specify the portion of the packet to check with the **Offset** (from 0) and the **Length** fields, both in bytes. The Prestige applies the Mask (bit-wise ANDing) to the data portion before comparing the result against the Value to determine a match. The **Mask** and **Value** are specified in hexadecimal numbers. Note that it takes two hexadecimal digits to represent a byte, so if the length is 4, the value in either field will take 8 digits, for example, FFFFFFFF.

To configure a generic rule, select **Generic Filter Rule** in the **Filter Type** field in menu 21.1.4.1 and press [ENTER] to open Generic Filter Rule, as shown below.

```

Menu 21.1.4.1 - Generic Filter Rule

Filter #: 4,1
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:

```

Figure 23-8 Menu 21.1.4.1 Generic Filter Rule

The following table describes the fields in the Generic Filter Rule menu.

Table 23-4 Generic Filter Rule Menu Fields

FIELD	DESCRIPTION	OPTIONS
Filter #	This is the filter set, filter rule co-ordinates, i.e., 2,3 refers to the second filter set and the third rule of that set.	

Table 23-4 Generic Filter Rule Menu Fields

FIELD	DESCRIPTION	OPTIONS
Filter Type	Use [SPACE BAR] and then [ENTER] to select a rule type. Parameters displayed below each type will be different. TCP/IP filter rules are used to filter IP packets while generic filter rules allow filtering of non-IP packets.	Generic Filter Rule TCP/IP Filter Rule
Active	Select Yes to turn on the filter rule or No to turn it off.	Yes / No
Offset	Enter the starting byte of the data portion in the packet that you wish to compare. The range for this field is from 0 to 255.	0-255
Length	Enter the byte count of the data portion in the packet that you wish to compare. The range for this field is 0 to 8.	0-8
Mask	Enter the mask (in Hexadecimal notation) to apply to the data portion before comparison.	
Value	Enter the value (in Hexadecimal notation) to compare with the data portion.	
More	If Yes , a matching packet is passed to the next filter rule before an action is taken; else the packet is disposed of according to the action fields. If More is Yes , then Action Matched and Action Not Matched will be No .	Yes No
Log	Select the logging option from the following: None - No packets will be logged. Action Matched - Only packets that match the rule parameters will be logged. Action Not Matched - Only packets that do not match the rule parameters will be logged. Both - All packets will be logged.	None Action Matched Action Not Matched Both
Action Matched	Select the action for a packet matching the rule.	Check Next Rule Forward Drop
Action Not Matched	Select the action for a packet not matching the rule.	Check Next Rule Forward Drop
Once you have completed filling in Menu 21.4.1.1 - Generic Filter Rule , press [ENTER] at the message "Press ENTER to Confirm" to save your configuration, or press [ESC] to cancel. This data will now be displayed on Menu 21.1.1 - Filter Rules Summary .		

23.3 Example Filter

Let's look at an example to block outside users from accessing the Prestige via telnet.

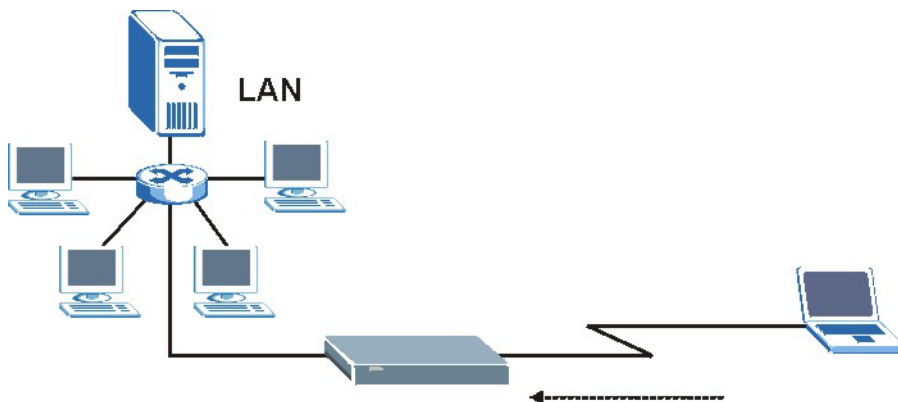


Figure 23-9 Telnet Filter Example

- Step 1.** Enter 21 from the main menu to open **Menu 21 - Filter and Firewall Setup**.
- Step 2.** Enter 1 to open **Menu 21.1 - Filter Set Configuration**.
- Step 3.** Enter the index of the filter set you wish to configure (say 3) and press [ENTER].
- Step 4.** Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].
- Step 5.** Press [ENTER] at the message [Press ENTER to confirm] to open **Menu 21.1.3 - Filter Rules Summary**.

Step 6. Enter 1 to configure the first filter rule (the only filter rule of this set). Make the entries in this menu as shown in the following figure.

```

Menu 21.1.3.1 - TCP/IP Filter Rule

Filter #: 3,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 6          IP Source Route= No
Destination: IP Addr= 0.0.0.0
                IP Mask= 0.0.0.0
                Port # = 23
                Port # Comp= Equal
Source: IP Addr= 0.0.0.0
                IP Mask= 0.0.0.0
                Port # = 0
                Port # Comp= None
TCP Estab= No
More= No              Log= None
Action Matched= Drop
Action Not Matched= Forward

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

Press [SPACE BAR] and then [ENTER] to choose this filter rule type. The first filter rule type determines all subsequent filter types within a set.

Select **Yes** to make the rule active.

6 is the TCP protocol.

The port number for the telnet service (TCP protocol) is **23**. See *RFC 1060* for port numbers of well-known services.

There are no more rules to check.

Select **Drop** here so that the packet will be dropped if its destination is the telnet port.

Select **Equal** here as you are looking for packets going to port 23 only.

Select **Forward** here so that the packet will be forwarded if its destination is not the telnet port.

Figure 23-10 Example Filter: Menu 21.1.3.1

When you press [ENTER] to confirm, you will see the following screen. Note that there is only one filter rule in this set.

Menu 21.1.3 - Filter Rules Summary

#	A	Type	Filter Rules	M	m	n
1	Y	IP	Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23	-	-	-
2	N			N	D	F
3	N					
4	N					
5	N					
6	N					

Enter Filter Rule Number (1-6) to Configure:

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 23-11 Example Filter Rules Summary: Menu 21.1.3

After you've created the filter set, you must apply it.

- Step 1.** Enter 11 from the main menu to go to menu 11.
- Step 2.** Go to the **Edit Filter Sets** field, press [SPACE BAR] to select **Yes** and press [ENTER].
- Step 3.** This brings you to menu 11.5. Apply a filter set (our example filter set 3) as shown in *Figure 23-14*.
- Step 4.** Press [ENTER] to confirm after you enter the set numbers and to leave menu 11.5.

23.4 Filter Types and NAT

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

Generic and TCP/IP filter rules are discussed in more detail in the next section. When NAT (Network Address Translation) is enabled, the inside IP address and port number are replaced on a connection-by-connection basis, which makes it impossible to know the exact address and port on the wire. Therefore, the Prestige applies the protocol filters to the “native” IP address and port number before NAT for outgoing packets and after NAT for incoming packets. On the other hand, the generic, or device filters are applied to the raw packets that appear on the wire. They are applied at the point when the Prestige is receiving and sending the packets; i.e. the interface. The interface can be an Ethernet port or any other hardware port. The following diagram illustrates this.

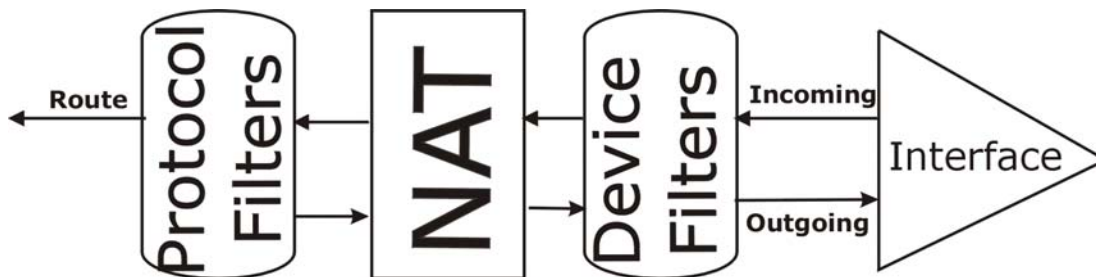


Figure 23-12 Protocol and Device Filter Sets

23.5 Firewall Versus Filters

Firewall configuration is discussed in the *firewall* chapters of this manual. Further comparisons are also made between filtering, NAT and the firewall.

23.6 Applying a Filter

This section shows you where to apply the filter(s) after you design it (them). The Prestige already has filters to prevent NetBIOS traffic from triggering calls, and block incoming telnet, FTP and HTTP connections.

If you do not activate the firewall, it is advisable to apply filters.

23.6.1 Applying LAN Filters

LAN traffic filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 3.1 (shown next) and enter the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by entering their numbers separated by commas, e.g., 3, 4, 6, 11. Input filter sets filter incoming traffic to the Prestige and output filter sets filter outgoing traffic from the Prestige. For PPPoE or PPTP encapsulation, you have the additional option of specifying remote node call filter sets.

```
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:
```

Figure 23-13 Filtering LAN Traffic

23.6.2 Applying Remote Node Filters

Go to menu 11.5 (shown below – note that call filter sets are only present for PPPoE encapsulation) and enter the number(s) of the filter set(s) as appropriate. You can cascade up to four filter sets by entering their numbers separated by commas. The Prestige already has filters to prevent NetBIOS traffic from triggering calls, and block incoming telnet, FTP and HTTP connections.

```
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 23-14 Filtering Remote Node Traffic

Chapter 24

SNMP Configuration

This chapter explains SNMP Configuration menu 22.

24.1 About SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your Prestige supports SNMP agent functionality, which allows a manager station to manage and monitor the Prestige through the network. The Prestige supports SNMP version one (SNMPv1) and version two c (SNMPv2c). The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

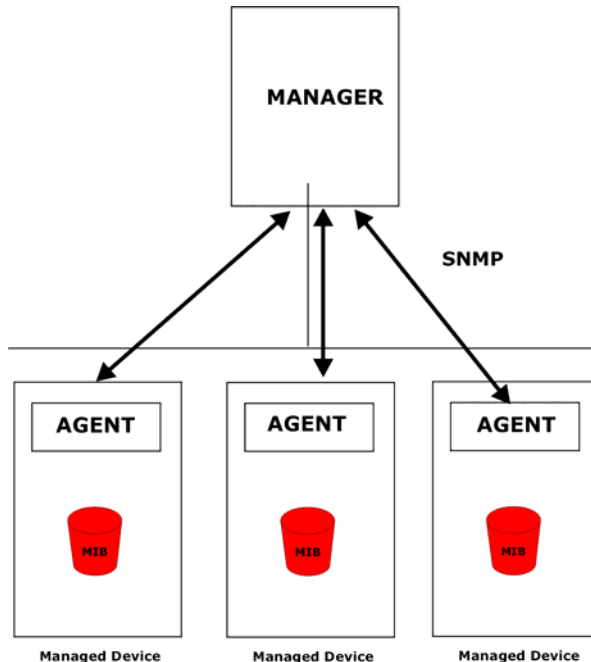


Figure 24-1 SNMP Management Model

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.

24.2 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.

24.3 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.

```

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:

```

Figure 24-2 Menu 22 SNMP Configuration

The following table describes the SNMP configuration parameters.

Table 24-1 Menu 22 SNMP Configuration

FIELD	DESCRIPTION	EXAMPLE
SNMP:		
Get Community	Type the Get Community , which is the password for the incoming Get- and GetNext requests from the management station.	public
Set Community	Type the Set community, which is the password for incoming Set requests from the management station.	public
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.	0.0.0.0
Trap:		
Community	Type the trap community, which is the password sent with each trap to the SNMP manager.	public
Destination	Type the IP address of the station to send your SNMP traps to.	0.0.0.0
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

24.4 SNMP Traps

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

Table 24-2 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.
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 24-3 Ports and Permanent Virtual Circuits

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

Chapter 25

System Information and Diagnosis

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

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.

```
Menu 24 - System Maintenance

1. System Status
2. System Information and Console Port Speed
3. Log and Trace
4. Diagnostic
5. Backup Configuration
6. Restore Configuration
7. Upload Firmware
8. Command Interpreter Mode
9. Call Control
10. Time and Date Setting
11. Remote Management Setup

Enter Menu Selection Number:
```

Figure 25-1 Menu 24 System Maintenance

25.1 System Status

The first selection, System Status gives you information on the status and statistics of the ports, as shown next. System Status is a tool that can be used to monitor your Prestige. Specifically, it gives you information on your ADSL telephone line status, number of packets sent and received.

To get to 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.


```

Menu 24.1 - System Maintenance - Status                                07:33:32
                                                                    Wed. Dec. 24, 2003

Port  Status      TxPkts      RxPkts      Cols      Tx B/s      Rx B/s      Up Time
WAN   100M/Full     15982       938667      0          78          2520       2:07:57
LAN   100M/Full     22381       21235       0          2399        128        6:55:05

Port  Ethernet Address      IP Address      IP Mask      DHCP
WAN   00:A0:C5:01:23:46     172.1.2.3      255.255.0.0  Client
LAN   00:A0:C5:01:23:45     192.168.1.1    255.255.255.0  Server

System up Time:      6:55:10

Name:
Routing: IP
ZyNOS F/W Version: V3.61(JF.0) | 5/10/2004

Press Command:
COMMANDS: 1-Drop WAN 9-Reset Counters  ESC-Exit
    
```

Figure 25-2 Menu 24.1 System Maintenance : Status

The following table describes the fields present in **Menu 24.1 — System Maintenance — Status**. These fields are READ-ONLY and meant for diagnostic purposes. The upper right corner of the screen shows the time and date according to the format you set in menu 24.10.

Table 25-1 System Maintenance: Status Menu Fields

FIELD	DESCRIPTION
Port	Identifies a port (WAN or LAN) on the Prestige.
Status	Shows the port speed and duplex setting if you're using Ethernet Encapsulation and Down (line is down), idle (line (ppp) idle), dial (starting to trigger a call) and drop (dropping a call) if you're using PPPoE Encapsulation .
TxPkts	The number of transmitted packets on this port.
RxPkts	The number of received packets on this port.
Cols	The number of collisions on this port.
Tx B/s	Shows the transmission speed in Bytes per second on this port.
Rx B/s	Shows the reception speed in Bytes per second on this port.
Up Time	Total amount of time the line has been up.
Ethernet Address	The Ethernet address of the port listed on the left.
IP Address	The IP address of the port listed on the left.

Table 25-1 System Maintenance: Status Menu Fields

FIELD	DESCRIPTION
IP Mask	The IP mask of the port listed on the left.
DHCP	The DHCP setting of the port listed on the left.
System up Time	The total time the Prestige has been on.
Name	This is the Prestige's system name + domain name assigned in menu 1. For example, System Name= xxx; Domain Name= baboo.mickey.com Name= xxx.baboo.mickey.com
Routing	Refers to the routing protocol used.
ZyNOS F/W Version	The ZyNOS Firmware version and the date created.
You may enter 1 to drop the WAN connection, 9 to reset the counters or [ESC] to return to menu 24.	

25.2 System Information

To get to the System Information:

- Step 1.** Enter 24 to display **Menu 24 — System Information and Console Port Speed**.
- Step 2.** Enter 2 to display **Menu 24.2 — System Information**.
- Step 3.** From this menu you have two choices as shown in the next figure:

```

Menu 24.2 - System Information and Console Port Speed
1. System Information
2. Console Port Speed

Please enter selection:

```

Figure 25-3 Menu 24.2 System Information and Console Port Speed

25.2.1 System Information

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

```

Menu 24.2.1 - System Maintenance - Information

Name:
Routing: IP
ZyNOS F/W Version: V3.61(JF.0)b1 | 04/15/2004

LAN
Ethernet Address: 00:A0:C5:01:23:45
IP Address: 192.168.1.1
IP Mask: 255.255.255.0
DHCP: Server

Press ESC or RETURN to Exit:
    
```

Figure 25-4 Menu 24.2.1 System Maintenance : Information

The following table describes the fields in this menu.

Table 25-2 Menu 24.2.1 System Maintenance : Information

FIELD	DESCRIPTION
Name	Displays the system name of your Prestige. This information can be changed in Menu 1 – General Setup .
Routing	Refers to the routing protocol used.
ZyNOS F/W Version	Refers to the ZyNOS (ZyXEL Network Operating System) system firmware version. ZyNOS is a registered trademark of ZyXEL Communications Corporation.
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.

25.2.2 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.

```

Menu 24.2.2 - System Maintenance - Change Console Port Speed

      Console Port Speed: 9600

      Press ENTER to Confirm or ESC to Cancel:

```

Figure 25-5 Menu 24.2.2 System Maintenance : Change Console Port Speed

25.3 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.

25.3.1 Syslog Logging

The Prestige uses the syslog facility to log the CDR (Call Detail Record) and system messages to a syslog server. Syslog and accounting can be configured in **Menu 24.3.2 — System Maintenance - Syslog Logging**, as shown next.

```

Menu 24.3.2 - System Maintenance - Syslog Logging

      Syslog:
      Active= No
      Syslog Server IP Address= 0.0.0.0
      Log Facility= Local 1

      Press ENTER to Confirm or ESC to Cancel:

```

Figure 25-6 Menu 24.3.2 System Maintenance : Syslog Logging

You need to configure the syslog parameters described in the following table to activate syslog then choose what you want to log.

Table 25-3 Menu 24.3.2 System Maintenance : Syslog and Accounting

PARAMETER	DESCRIPTION
Syslog:	
Active	Press [SPACE BAR] and then [ENTER] to turn syslog on or off.

Table 25-3 Menu 24.3.2 System Maintenance : Syslog and Accounting

PARAMETER	DESCRIPTION
Syslog Server IP Address	Enter the IP Address of the server that will log the CDR (Call Detail Record) and system messages i.e., the syslog server.
Log Facility	Press [SPACE BAR] and then [ENTER] to select a Local option. The log facility allows you to log the message to different files in the server. Please refer to the documentation of your syslog program for more details.
When finished configuring this screen, press [ENTER] to confirm or [ESC] to cancel.	

Your Prestige sends five types of syslog messages. Some examples (not all Prestige specific) of these syslog messages with their message formats are shown next:

1. CDR

```

CDR Message Format
SdcmSyslogSend( 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.)
      L02 Tunnel Connected(L2TP)
      C02 OutCall Connected xxxx (means connected speed) xxxxx (means Remote Call Number)
      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

```

Packet triggered Message Format
SdcmSyslogSend( 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=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a6b6c6d6e6f707172
7374
Jul 19 11:28:56 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600220008cd40000020405b4
Jul 19 11:29:06 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=45000028240140001f06ac12c0a86614ca849a7b0427001700195b451d1430135004000077600000
    
```

3. Filter log

```

Filter log Message Format
SdcmSyslogSend(SYSLOG_FILLOG, SYSLOG_NOTICE, String );
String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx] S04>R01mD

IP[...] is the packet header and S04>R01mD means filter set 4 (S) and rule 1 (R), match (m) drop (D).

Src: Source Address
Dst: Destination Address
prot: Protocol ("TCP", "UDP", "ICMP")
spo: Source port
dpo: Destination port
Mar 03 10:39:43 202.132.155.97 ZyXEL:
GEN[fffffffffnordff0080] }S05>R01mF
Mar 03 10:41:29 202.132.155.97 ZyXEL:
GEN[00a0c5f502fnord010080] }S05>R01mF
Mar 03 10:41:34 202.132.155.97 ZyXEL:
IP[Src=192.168.2.33 Dst=202.132.155.93 ICMP]}S04>R01mF
Mar 03 11:59:20 202.132.155.97 ZyXEL:
GEN[00a0c5f502fnord010080] }S05>R01mF
Mar 03 12:00:52 202.132.155.97 ZyXEL:
GEN[fffffffffff0080] }S05>R01mF
Mar 03 12:00:57 202.132.155.97 ZyXEL:
GEN[00a0c5f502010080] }S05>R01mF
Mar 03 12:01:06 202.132.155.97 ZyXEL:
IP[Src=192.168.2.33 Dst=202.132.155.93 TCP spo=01170 dpo=00021]}S04>R01mF

```

4. PPP log

```

PPP Log Message Format
SdcmSyslogSend( SYSLOG_PPLOG, 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

```

5. Firewall log

Firewall Log Message Format

```
SdcmdSyslogSend(SYSLOG_FIREWALL, SYSLOG_NOTICE, buf);
buf = IP[Src=xx.xx.xx.xx : spo=xxxx Dst=xx.xx.xx.xx : dpo=xxxx | prot | rule | action]
Src: Source Address
spo: Source port (empty means no source port information)
Dst: Destination Address
dpo: Destination port (empty means no destination port information)
prot: Protocol ("TCP","UDP","ICMP", "IGMP", "GRE", "ESP")
rule: <a,b> where a means "set" number; b means "rule" number.
Action: nothing(N) block (B) forward (F)
08-01-2000      11:48:41 Local1.Notice      192.168.10.10      RAS: FW 172.21.1.80      :137  -
>172.21.1.80   :137 |UDP|default permit:<2,0>|B
08-01-2000      11:48:41 Local1.Notice      192.168.10.10      RAS: FW 192.168.77.88    :520  -
>192.168.77.88 :520 |UDP|default permit:<2,0>|B
08-01-2000      11:48:39 Local1.Notice      192.168.10.10      RAS: FW 172.21.1.50      ->172.21.1.50
|IGMP<2>|default permit:<2,0>|B
08-01-2000      11:48:39 Local1.Notice      192.168.10.10      RAS: FW 172.21.1.25     ->172.21.1.25
|IGMP<2>|default permit:<2,0>|B
```

25.3.2 Call-Triggering Packet

Call-Triggering Packet displays information about the packet that triggered a dial-out call in an easy readable format. Equivalent information is available in menu 24.1 in hex format. An example is shown next.

```

IP Frame: ENET0-RECV Size: 44/ 44   Time: 17:02:44.262
Frame Type:

  IP Header:
    IP Version           = 4
    Header Length        = 20
    Type of Service      = 0x00 (0)
    Total Length         = 0x002C (44)
    Identification      = 0x0002 (2)
    Flags                = 0x00
    Fragment Offset      = 0x00
    Time to Live         = 0xFE (254)
    Protocol             = 0x06 (TCP)
    Header Checksum      = 0xFB20 (64288)
    Source IP            = 0xC0A80101 (192.168.1.1)
    Destination IP      = 0x00000000 (0.0.0.0)

  TCP Header:
    Source Port          = 0x0401 (1025)
    Destination Port     = 0x000D (13)
    Sequence Number      = 0x05B8D000 (95997952)
    Ack Number           = 0x00000000 (0)
    Header Length        = 24
    Flags                = 0x02 (...S.)
    Window Size          = 0x2000 (8192)
    Checksum             = 0xE06A (57450)
    Urgent Ptr           = 0x0000 (0)
    Options              =
      0000: 02 04 02 00

  RAW DATA:
    0000: 45 00 00 2C 00 02 00 00-FE 06 FB 20 C0 A8 01 01  E.....
    0010: 00 00 00 00 04 01 00 0D-05 B8 D0 00 00 00 00 00  .....
    0020: 60 02 20 00 E0 6A 00 00-02 04 02 00

Press any key to continue...

```

Figure 25-7 Call-Triggering Packet Example

25.4 Diagnostic

The diagnostic facility allows you to test the different aspects of your Prestige to determine if it is working properly. Menu 24.4 allows you to choose among various types of diagnostic tests to evaluate your system, as shown in the following figure.

Follow the procedure next to get to Diagnostic:

- Step 1.** From the main menu, type 24 to open **Menu 24 – System Maintenance**.
- Step 2.** From this menu, type 4 to open **Menu 24.4 – System Maintenance – Diagnostic**.


```

Menu 24.4 - System Maintenance - Diagnostic

TCP/IP
 1. Ping Host
 2. WAN DHCP Release
 3. WAN DHCP Renewal
 4. Internet Setup Test

System
 11. Reboot System

Enter Menu Selection Number:

Host IP Address= N/A
    
```

Figure 25-8 Menu 24.4 System Maintenance : Diagnostic

25.4.1 WAN DHCP

DHCP functionality can be enabled on the LAN or WAN as shown in *Figure 25-9*. LAN DHCP has already been discussed. The Prestige can act either as a WAN DHCP client (**IP Address Assignment** field in menu 4 or menu 11.3 is **Dynamic** and the **Encapsulation** field in menu 4 or menu 11 is **Ethernet**) or **None**, (when you have a static IP). The **WAN Release** and **Renewal** fields in menu 24.4 conveniently allow you to release and/or renew the assigned WAN IP address, subnet mask and default gateway in a fashion similar to winipcfg.

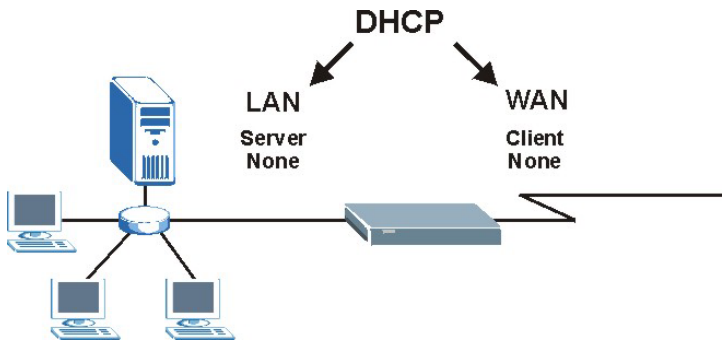


Figure 25-9 LAN & WAN DHCP

The following table describes the diagnostic tests available in menu 24.4 for your Prestige and associated connections.

Table 25-4 System Maintenance Menu Diagnostic

FIELD	DESCRIPTION
Ping Host	Enter 1 to ping any machine (with an IP address) on your LAN or WAN. Enter its IP address in the Host IP Address field below.
WAN DHCP Release	Enter 2 to release your WAN DHCP settings.
WAN DHCP Renewal	Enter 3 to renew your WAN DHCP settings.
Internet Setup Test	Enter 4 to test the Internet setup. You can also test the Internet setup in Menu 4 - Internet Access . Please refer to the <i>Internet Access</i> chapter for more details. This feature is only available for dial-up connections using PPPoE or PPTP encapsulation.
Reboot System	Enter 11 to reboot the Prestige.
Host IP Address=	If you entered 1 in Ping Host , then enter the IP address of the computer you want to ping in this field.
Enter the number of the selection you would like to perform or press [ESC] to cancel.	

Chapter 26

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.

26.1 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 26-1 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

26.2 Backup Configuration

Option 5 from **Menu 24 – System Maintenance** allows you to backup the current Prestige configuration to your computer. Backup is highly recommended once your Prestige is functioning properly. FTP is the preferred methods for backing up your current configuration to your computer since they are faster.

Please note that terms “download” and “upload” are relative to the computer. Download means to transfer from the Prestige to the computer, while upload means from your computer to the Prestige.

26.2.1 Backup Configuration

Follow the instructions as shown in the next screen.

```
Menu 24.5 - System Maintenance - Backup Configuration

To transfer the configuration file to your workstation, follow the procedure
below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your Prestige. Then type "root" and
   SMT password as requested.
3. Locate the 'rom-0' file.
4. Type 'get rom-0' to back up the current Prestige configuration to
   your workstation.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on backup using TFTP (note that you must remain
in this menu to back up using TFTP), please see your Prestige manual.

Press ENTER to Exit:
```

Figure 26-1 Telnet in Menu 24.5

26.2.2 Using the FTP Command from the Command Line

- Step 1.** Launch the FTP client on your computer.
- Step 2.** Enter “open”, followed by a space and the IP address of your Prestige.
- Step 3.** Press [ENTER] when prompted for a username.
- Step 4.** Enter your password as requested (the default is “1234”).
- Step 5.** Enter “bin” to set transfer mode to binary.
- Step 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.
- Step 7.** Enter “quit” to exit the ftp prompt.

26.2.3 Example of FTP Commands from the Command Line

```

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
    
```

Figure 26-2 FTP Session Example

26.2.4 GUI-based FTP Clients

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

Table 26-2 General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	<p>Anonymous.</p> <p>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.</p> <p>Normal.</p> <p>The server requires a unique User ID and Password to login.</p>
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode. Configuration and firmware files should be transferred in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

26.2.5 TFTP and FTP Management Limitations

TFTP, FTP and Telnet over WAN will not work when:

1. You have disabled Telnet service in menu 24.11.
2. You have applied a filter in menu 3.1 (LAN) or in menu 11.5 (WAN) to block Telnet service.

3. 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.
4. You have an SMT console session running.

26.2.6 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.

- Step 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.
- Step 2.** Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
- Step 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.
- Step 4.** Launch the TFTP client on your computer and connect to the Prestige. Set the transfer mode to binary before starting data transfer.
- Step 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.

26.2.7 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.

26.2.8 GUI-based TFTP Clients

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

Table 26-3 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 26.2.5* to read about configurations that disallow TFTP and FTP over WAN.

26.3 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.

WARNING!
**DO NOT INTERRUPT THE FILE TRANSFER PROCESS AS THIS MAY
PERMANENTLY DAMAGE YOUR PRESTIGE.**

26.3.1 Restore Using FTP

For details about backup using (T)FTP please refer to earlier sections on FTP and TFTP file upload in this chapter.

```
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:
```

Figure 26-3 Telnet into Menu 24.6

- Step 1.** Launch the FTP client on your computer.
- Step 2.** Enter “open”, followed by a space and the IP address of your Prestige.
- Step 3.** Press [ENTER] when prompted for a username.
- Step 4.** Enter your password as requested (the default is “1234”).
- Step 5.** Enter “bin” to set transfer mode to binary.
- Step 6.** Find the “rom” file (on your computer) that you want to restore to your Prestige.
- Step 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.
- Step 8.** Enter “quit” to exit the ftp prompt. The Prestige will automatically restart after a successful restore process.

26.3.2 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
```

Figure 26-4 Restore Using FTP Session Example

Refer to *section 26.2.5* to read about configurations that disallow TFTP and FTP over WAN.

26.4 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 the previous *Restore Configuration* section or by following the instructions in **Menu 24.7.2 – System Maintenance – Upload System Configuration File**.

WARNING!
**DO NOT INTERRUPT THE FILE TRANSFER PROCESS AS THIS MAY
PERMANENTLY DAMAGE YOUR PRESTIGE.**

26.4.1 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.

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

To upload the system firmware, follow the procedure below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your system. Then type "root" and
   SMT password as requested.
3. Type "put firmware filename ras" where "firmwarefilename" is the name
   of your firmware upgrade file on your workstation and "ras" is the
   remote file name on the system.
4. The system reboots automatically after a successful firmware upload.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP),
please see your manual.

Press ENTER to Exit:
```

Figure 26-5 Telnet Into Menu 24.7.1 Upload System Firmware

26.4.2 Configuration File Upload

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

```
Menu 24.7.2 - System Maintenance - Upload System Configuration File

To upload the system configuration file, follow the procedure below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your system. Then type "root" and
   SMT password as requested.
3. Type "put configuration filename rom-0" where "configurationfilename"
   is the name of your system configuration file on your workstation, which
   will be transferred to the "rom-0" file on the system.
4. The system reboots automatically after the upload system configuration
   file process is complete.

For details on FTP commands, please consult the documentation of your FTP
client program. For details on uploading system firmware using TFTP (note
that you must remain on this menu to upload system firmware using TFTP),
please see your manual.

Press ENTER to Exit:
```

Figure 26-6 Telnet Into Menu 24.7.2 System Maintenance

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

26.4.3 FTP File Upload Command from the DOS Prompt Example

- Step 1.** Launch the FTP client on your computer.
- Step 2.** Enter “open”, followed by a space and the IP address of your Prestige.
- Step 3.** Press [ENTER] when prompted for a username.
- Step 4.** Enter your password as requested (the default is “1234”).
- Step 5.** Enter “bin” to set transfer mode to binary.
- Step 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.
- Step 7.** Enter “quit” to exit the ftp prompt.

The Prestige automatically restarts after a successful file upload.

26.4.4 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
```

Figure 26-7 FTP Session Example of Firmware File Upload

More commands (found in GUI-based FTP clients) are listed earlier in this chapter.

Refer to *section 26.2.5* to read about configurations that disallow TFTP and FTP over WAN.

26.4.5 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.

- Step 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.
- Step 2.** Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
- Step 3.** Enter the command “sys stdio 0” to disable the console timeout, so the TFTP transfer will not be interrupted. Enter “command sys stdio 5” to restore the five-minute console timeout (default) when the file transfer is complete.
- Step 4.** Launch the TFTP client on your computer and connect to the Prestige. Set the transfer mode to binary before starting data transfer.
- Step 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.

26.4.6 TFTP Upload Command Example

The following is an example TFTP command:

```
tftp [-i] host put firmware.bin ras
```

where “i” specifies binary image transfer mode (use this mode when transferring binary files), “host” is the Prestige’s IP address and “put” transfers the file source on the computer (firmware.bin – name of the firmware on the computer) to the file destination on the remote host (ras - name of the firmware on the Prestige).

Commands that you may see in GUI-based TFTP clients are listed earlier in this chapter.

Chapter 27

System Maintenance

This chapter leads you through SMT menus 24.8 to 24.10.

27.1 Command Interpreter Mode

The Command Interpreter (CI) is a part of the main system firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. Enter the CI from the SMT by selecting menu 24.8. See the included disk or the zyxel.com web site for more detailed information on CI commands. Enter 8 from **Menu 24 — System Maintenance**. A list of valid commands can be found by typing `help` or `?` at the command prompt. Type “exit” to return to the SMT main menu when finished.

```
Menu 24 - System Maintenance

1. System Status
2. System Information and Console Port Speed
3. Log and Trace
4. Diagnostic
5. Backup Configuration
6. Restore Configuration
7. Firmware Update
8. Command Interpreter Mode
9. Call Control
10. Time and Date Setting
11. Remote Management Setup

Enter Menu Selection Number:
```

Figure 27-1 Command Mode in Menu 24

27.1.1 Command Syntax

The command keywords are in `courier new` font.

Enter the command keywords exactly as shown, do not abbreviate.

The required fields in a command are enclosed in angle brackets `<>`.

The optional fields in a command are enclosed in square brackets `[]`.

The | symbol means “or”.

For example,

```
sys filter netbios config <type> <on|off>
```

means that you must specify the type of netbios filter and whether to turn it on or off.

27.1.2 Command Usage

A list of commands can be found by typing `help` or `?` at the command prompt. Always type the full command. Type `exit` to return to the SMT main menu when finished.

```
Copyright (c) 1994 - 2003 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys          exit          device          ether
poe         pptp          config         ip
ipsec       ppp           hdap
ras>
```

Figure 27-2 Valid Commands

27.2 Call Control Support

The Prestige provides two call control functions: budget management and call history. Please note that this menu is only applicable when **Encapsulation** is set to **PPPoE** in menu 4 or menu 11.1.

The budget management function allows you to set a limit on the total outgoing call time of the Prestige within certain times. When the total outgoing call time exceeds the limit, the current call will be dropped and any future outgoing calls will be blocked.

To access the call control menu, select option 9 in menu 24 to go to **Menu 24.9 — System Maintenance — Call Control**, as shown in the next table.

```
Menu 24.9 - System Maintenance - Call Control

1. Budget Management
2. Call History

Enter Menu Selection Number:
```

Figure 27-3 Menu 24.9 System Maintenance : Call Control

27.2.1 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.

```

Menu 24.9.1 - Budget Management

Remote Node      Connection Time/Total Budget      Elapsed Time/Total Period
1. MyISP         No Budget                        No Budget

Reset Node (0 to update screen):

```

Figure 27-4 Budget Management

The total budget is the time limit on the accumulated time for outgoing calls to a remote node. When this limit is reached, the call will be dropped and further outgoing calls to that remote node will be blocked. After each period, the total budget is reset. The default for the total budget is 0 minutes and the period is 0 hours, meaning no budget control. You can reset the accumulated connection time in this menu by entering the index of a remote node. Enter 0 to update the screen. The budget and the reset period can be configured in menu 11.1 for the remote node.

Table 27-1 Budget Management

FIELD	DESCRIPTION	EXAMPLE
Remote Node	Enter the index number of the remote node you want to reset (just one in this case)	1
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).	5/10 means that 5 minutes out of a total allocation of 10 minutes have lapsed.
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.	0.5/1 means that 30 minutes out of the 1-hour time period has lapsed.
Enter "0" to update the screen or press [ESC] to return to the previous screen.		

27.2.2 Call History

This is the second option in **Menu 24.9 - System Maintenance - Call Control**. It displays information about past incoming and outgoing calls. Enter 2 from **Menu 24.9 - System Maintenance - Call Control** to bring up the following menu.

Menu 24.9.2 - Call History						
Phone Number	Dir	Rate	#call	Max	Min	Total
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						
Enter Entry to Delete(0 to exit):						

Figure 27-5 Call History

The following table describes the fields in this screen.

Table 27-2 Call History Fields

FIELD	DESCRIPTION
Phone Number	The PPPoE service names are shown here.
Dir	This shows whether the call was incoming or outgoing.
Rate	This is the transfer rate of the call.
#call	This is the number of calls made to or received from that telephone number.
Max	This is the length of time of the longest telephone call.
Min	This is the length of time of the shortest telephone call.
Total	This is the total length of time of all the telephone calls to/from that telephone number.
You may enter an entry number to delete it or "0" to exit.	

27.3 Time and Date Setting

The Real Time Chip (RTC) keeps track of the time and date (not available on all models). 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.

```
Menu 24 - System Maintenance

1. System Status
2. System Information and Console Port Speed
3. Log and Trace
4. Diagnostic
5. Backup Configuration
6. Restore Configuration
7. Upload Firmware
8. Command Interpreter Mode
9. Call Control
10. Time and Date Setting
11. Remote Management Setup

Enter Menu Selection Number:
```

Figure 27-6 Menu 24: System Maintenance

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.

```
Menu 24.10 - System Maintenance - Time and Date Setting

Time Protocol= NTP (RFC-1305)
Time Server Address= time-b.nist.gov

Current Time:                08 : 07 : 14
New Time (hh:mm:ss):        08 : 06 : 48

Current Date:                2003 - 12 - 24
New Date (yyyy-mm-dd):      2003 - 12 - 24

Time Zone= GMT

Daylight Saving= No
Start Date (mm-dd):         01 - 01
End Date (mm-dd):           01 - 01

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

Figure 27-7 Menu 24.10 System Maintenance: Time and Date Setting

The following table describes the fields in this screen.

Table 27-3 Time and Date Setting Fields

FIELD	DESCRIPTION
Time Protocol	<p>Enter the time service protocol that your timeserver sends when you turn on the Prestige. Not all timeservers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main differences between them are the format.</p> <p>Daytime (RFC 867) format is day/month/year/time zone of the server.</p> <p>Time (RFC-868) format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.</p> <p>NTP (RFC-1305) the default, is similar to Time (RFC-868).</p> <p>None enter the time manually.</p>
Time Server Address	Enter the IP address or domain name of your timeserver. Check with your ISP/network administrator if you are unsure of this information. The default is tick.stdtime.gov.tw
Current Time	This field displays 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 reenter 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	Daylight Saving Time is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daylight time in the evenings. If you use daylight savings time, then choose Yes .
Start Date	Enter the month and day that your daylight-savings time starts on if you selected Yes in the Daylight Saving field.
End Date	Enter the month and day that your daylight-savings time ends on if you selected Yes in the Daylight Saving field.
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.	

27.3.1 Resetting the Time

The Prestige resets the time in three instances:

- i. On leaving menu 24.10 after making changes.

- ii. When the Prestige starts up, if there is a timeserver configured in menu 24.10.
- iii. 24-hour intervals after starting.

Chapter 28

Remote Management

This chapter covers remote management (SMT menu 24.11).

28.1 Remote Management

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

You may manage your Prestige from a remote location via:

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

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.

Enter 11 from menu 24 to bring up **Menu 24.11 – Remote Management Control**.

```
Menu 24.11 - Remote Management Control

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

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

Web Server:         Port = 80          Access = ALL
                   Secure Client IP = 0.0.0.0

SNMP Service:       Port = 161         Access = LAN only
                   Secure Client IP = 0.0.0.0

DNS Service:        Port = 53          Access = LAN only
                   Secure Client IP = 0.0.0.0

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

Figure 28-1 Menu 24.11 – Remote Management Control

The following table describes the fields in this screen.

Table 28-1 Menu 24.11 – Remote Management Control

FIELD	DESCRIPTION	EXAMPLE
Telnet Server FTP Server Web Server SNMP Service DNS Service	Each of these read-only labels denotes a service or protocol.	
Port	This field shows the port number for the service or protocol. You may change the port number if needed, but you must use the same port number to access the Prestige.	23
Access	Select the access interface (if any) by pressing [SPACE BAR], then [ENTER] to choose from: LAN only , WAN only , ALL or Disable .	LAN Only (default)
Secure Client IP	The default 0.0.0.0 allows any client to use this service or protocol to access the Prestige. Enter an IP address to restrict access to a client with a matching IP address.	0.0.0.0
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.		

28.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

1. A filter in menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
2. You have disabled that service in menu 24.11.
3. The IP address in the **Secure Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the Prestige will disconnect the session immediately.
4. There is an SMT console session running.
5. 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.
6. There is a firewall rule that blocks it.

Chapter 29

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.

29.1 Introduction to Call Scheduling

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.

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:

Figure 29-1 Menu 26 Schedule Setup

Lower numbered sets take precedence over higher numbered sets thereby avoiding scheduling conflicts. For example, if sets 1, 2, 3 and 4 in are applied in the remote node then set 1 will take precedence over set 2, 3 and 4 as the Prestige, by default, applies the lowest numbered set first. Set 2 will take precedence over set 3 and 4, and so on.

You can design up to 12 schedule sets but you can only apply up to four schedule sets for a remote node.

To delete a schedule set, enter the set number and press [SPACE BAR] and then [ENTER] (or delete) in the Edit Name field.

To setup a schedule set, select the schedule set you want to setup from menu 26 (1-12) and press [ENTER] to see **Menu 26.1 — Schedule Set Setup** as shown next.

```

Menu 26.1 - Schedule Set Setup

Active= Yes
Start Date (yyyy/mm/dd) = 2000 - 01 - 01
How Often= Once
Once:
  Date (yyyy/mm/dd)= 2000 - 01 - 01
Weekdays:
  Sunday= N/A
  Monday= N/A
  Tuesday= N/A
  Wednesday= N/A
  Thursday= N/A
  Friday= N/A
  Saturday= N/A
Start Time (hh:mm)= 00 : 00
Duration (hh:mm)= 00 : 00
Action= Forced On

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

Figure 29-2 Menu 26.1 Schedule Set Setup

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 29-1 Menu 26.1 Schedule Set Setup

FIELD	DESCRIPTION	EXAMPLE
Active	Press [SPACE BAR] to select Yes or No . Choose Yes and press [ENTER] to activate the schedule set.	Yes
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.	2000-01-01
How Often	Should this schedule set recur weekly or be used just once only? Press the [SPACE BAR] and then [ENTER] to select Once or Weekly . Both these options are mutually exclusive. If Once is selected, then all weekday settings are N/A . When Once is selected, the schedule rule deletes automatically after the scheduled time elapses.	Once

Table 29-1 Menu 26.1 Schedule Set Setup

FIELD	DESCRIPTION	EXAMPLE
Once: Date	If you selected Once in the How Often field above, then enter the date the set should activate here in year-month-date format.	2000-01-01
Weekday: Day	If you selected Weekly in the How Often field above, then select the day(s) when the set should activate (and recur) by going to that day(s) and pressing [SPACE BAR] to select Yes , then press [ENTER].	Yes No N/A
Start Time	Enter the start time when you wish the schedule set to take effect in hour-minute format.	09:00
Duration	Enter the maximum length of time this connection is allowed in hour-minute format.	08:00
Action	<p>Forced On means that the connection is maintained whether or not there is a demand call on the line and will persist for the time period specified in the Duration field.</p> <p>Forced Down means that the connection is blocked whether or not there is a demand call on the line.</p> <p>Enable Dial-On-Demand means that this schedule permits a demand call on the line. Disable Dial-On-Demand means that this schedule prevents a demand call on the line.</p>	Forced 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] to cancel and go back to the previous screen.		

Once your schedule sets are configured, you must then apply them to the desired remote node(s). Enter 11 from the **Main Menu** and then enter the target remote node index. Using [SPACE BAR], select **PPPoE** or **PPPoA** in the **Encapsulation** field and then press [ENTER] to make the schedule sets field available as shown next.

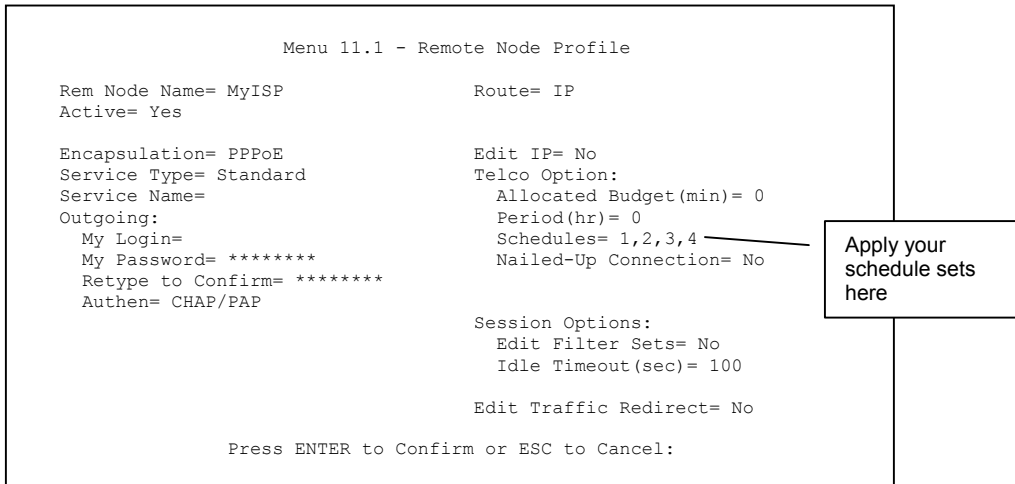


Figure 29-3 Applying Schedule Set(s) to a Remote Node (PPPoE)

You can apply up to four schedule sets, separated by commas, for one remote node. Change the schedule set numbers to your preference(s).

Part IX:

Appendices and Index

This section provides some Appendices and an Index.

Appendix A

PPPoE

PPPoE in Action

An ADSL modem bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your PC to an ATM PVC (Permanent Virtual Circuit) that connects to an xDSL Access Concentrator where the PPP session terminates (see the next figure). 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:

1. It provides you with a familiar dial-up networking (DUN) user interface.
2. 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 & ISDN), the switching fabric is already in place.
3. 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 PCs use traditional dial-up networking.

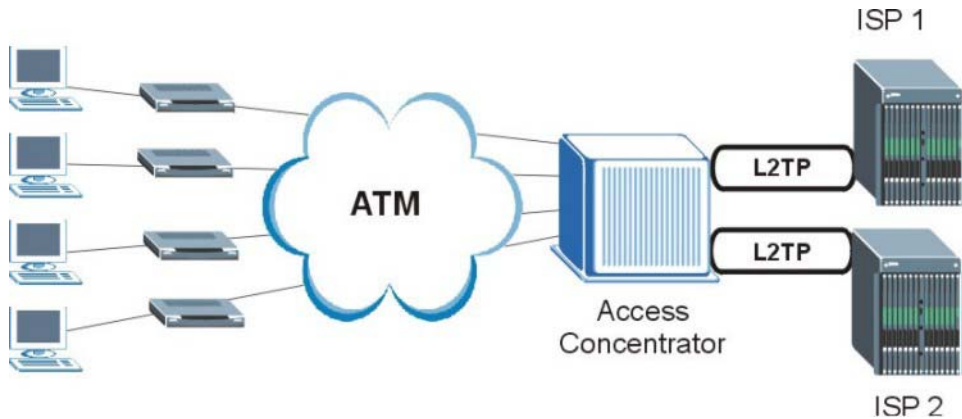


Diagram A-1 Single-PC per Modem Hardware Configuration

How PPPoE Works

The PPPoE driver makes the Ethernet appear as a serial link to the PC and the PC 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 PC and the ISP.

The Prestige as a PPPoE Client

When using the Prestige as a PPPoE client, the PCs 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 PCs.

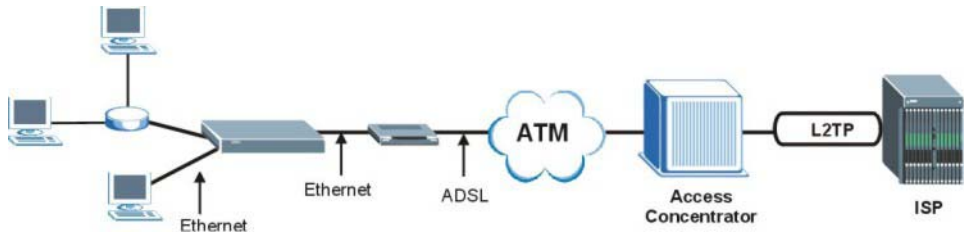


Diagram A-2 The Prestige as a PPPoE Client

Appendix B

PPTP

What is PPTP?

PPTP (Point-to-Point Tunneling Protocol) is a Microsoft proprietary protocol (RFC 2637 for PPTP is informational only) to tunnel PPP frames.

How can we transport PPP frames from a PC to a broadband modem over Ethernet?

A solution is to build PPTP into the ANT (ADSL Network Termination) where PPTP is used only over the short haul between the PC and the modem over Ethernet. For the rest of the connection, the PPP frames are transported with PPP over AAL5 (RFC 2364). The PPP connection, however, is still between the PC and the ISP. The various connections in this setup are depicted in the following diagram. The drawback of this solution is that it requires one separate ATM VC per destination.

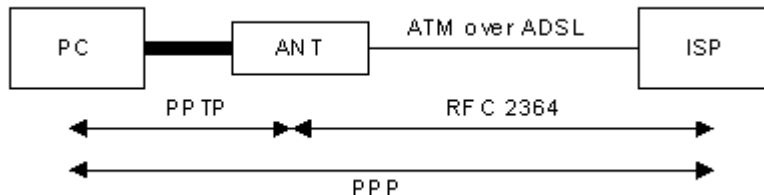


Diagram B-1 Transport PPP frames over Ethernet

PPTP and the Prestige

When the Prestige is deployed in such a setup, it appears as a PC to the ANT (ADSL Network Termination).

In Windows VPN or PPTP Pass-Through feature, the PPTP tunneling is created from Windows 95, 98 and NT clients to an NT server in a remote location. The pass-through feature allows users on the network to access a different remote server using the Prestige's Internet connection. In NAT mode, the Prestige is able to pass the PPTP packets to the internal PPTP server (i.e. NT server) behind the NAT. Users need to forward PPTP packets to port 1723 by configuring the server in **Menu 15.2 - Server Set Setup**. In the case above as the PPTP connection is initialized by the remote PPTP Client, the user must configure the PPTP clients. The Prestige initializes the PPTP connection hence, there is no need to configure the remote PPTP clients.

PPTP Protocol Overview

PPTP is very similar to L2TP, since L2TP is based on both PPTP and L2F (Cisco's Layer 2 Forwarding). Conceptually, there are three parties in PPTP, namely the PNS (PPTP Network Server), the PAC (PPTP Access Concentrator) and the PPTP user. The PNS is the box that hosts both the PPP and the PPTP stacks and forms one end of the PPTP tunnel. The PAC is the box that dials/answers the phone calls and relays the PPP frames to the PNS. The PPTP user is not necessarily a PPP client (can be a PPP server too). Both the PNS and the PAC must have IP connectivity; however, the PAC must in addition have dial-up capability. The phone call is between the user and the PAC and the PAC tunnels the PPP frames to the PNS. The PPTP user is unaware of the tunnel between the PAC and the PNS.

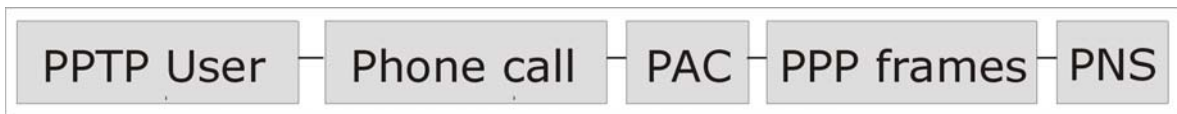


Diagram B-2 PPTP Protocol Overview

Microsoft includes PPTP as a part of the Windows OS. In Microsoft's implementation, the PC, and hence the Prestige, is the PNS that requests the PAC (the ANT) to place an outgoing call over AAL5 to an RFC 2364 server.

Control & PPP connections

Each PPTP session has distinct control connection and PPP data connection.

Call Connection

The control connection runs over TCP. Similar to L2TP, a tunnel control connection is first established before call control messages can be exchanged. Please note that a tunnel control connection supports multiple call sessions.

The following diagram depicts the message exchange of a successful call setup between a PC and an ANT.

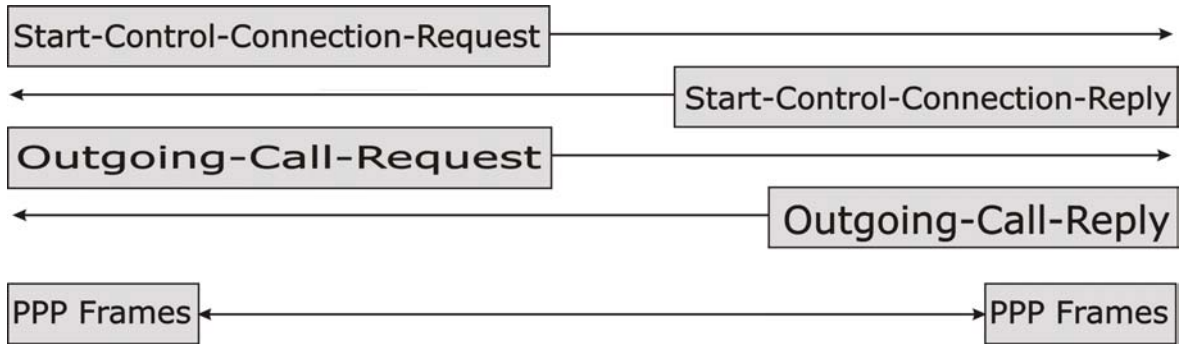


Diagram B-3 Example Message Exchange between PC and an ANT

PPP Data Connection

The PPP frames are tunneled between the PNS and PAC over GRE (General Routing Encapsulation, RFC 1701, 1702). The individual calls within a tunnel are distinguished using the Call ID field in the GRE header.

Appendix C

NetBIOS Filter Commands

The following describes the NetBIOS packet filter commands.

Introduction

NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN.

For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls.

You can configure NetBIOS filters to:

- Allow or disallow the sending of NetBIOS packets from the LAN to the WAN and from the WAN to the LAN.
- Allow or deny NetBIOS packets to be sent through VPN connections.
- Block or forward NetBIOS packets from initiating calls.

Display NetBIOS Filter Settings

Syntax: `sys filter netbios disp`

This command displays the current NetBIOS filter settings.

```
===== NetBIOS Filter Status =====  
Between LAN and WAN: Block  
IPSec Packets: Forward  
Trigger Dial: Disabled
```

Diagram C-1 NetBIOS Display Filter Settings Command

The filter types and their default settings are as follows.

Table C-1 NetBIOS Filter Default Settings

NAME	DESCRIPTION	EXAMPLE
Between LAN and WAN	This field displays whether NetBIOS packets are blocked or forwarded from the LAN to the WAN or from the WAN to the LAN.	Forward
IPSec Packets	This field displays whether NetBIOS packets sent through a VPN connection are blocked or forwarded.	Forward
Trigger dial	This field displays whether NetBIOS packets are allowed to initiate calls. Disabled means that NetBIOS packets are blocked from initiating calls.	Disabled

NetBIOS Filter Configuration

Syntax: `sys filter netbios config <type> <on|off>`

where

`<type>` = Identify which NetBIOS filter (numbered 0-3) to configure.

0 = LAN to WAN and WAN to LAN

3 = IPSec Packets

4 = Trigger dial

`<on|off>` = For type 0, use `on` to enable the filter and block NetBIOS packets. Use `off` to disable the filter and forward NetBIOS packets.

For type 3, use `on` to block NetBIOS packets from being sent through a VPN connection. Use `off` to allow NetBIOS packets to be sent through a VPN connection.

For type 4, use `on` to allow NetBIOS packets to initiate dial backup calls. Use `off` to block NetBIOS packets from initiating dial backup calls.

Example commands

Command: `sys filter netbios config 0 on`

This command blocks LAN to WAN and WAN to LAN NetBIOS packets

Command: `sys filter netbios config 3 on`

This command blocks IPSec NetBIOS packets

Command: `sys filter netbios config 4 off`

This command stops NetBIOS commands from initiating calls.

Appendix D

Log Descriptions

Configure centralized logs using the embedded web configurator; see the online help for details.

This appendix describes some of the log messages.

Chart 1 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.

Chart 2 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.
DHCP client gets %s	A DHCP client got a new IP address from the DHCP server.
DHCP client IP expired	A DHCP client's IP address has expired.
DHCP server assigns %s	The DHCP server assigned an IP address to a client.
SMT Login Successfully	Someone has logged on to the router's SMT interface.
SMT Login Fail	Someone has failed to log on to the router's SMT interface.
WEB Login Successfully	Someone has logged on to the router's web configurator interface.
WEB Login Fail	Someone has failed to log on to the router's web configurator interface.

Chart 2 System Maintenance Logs

LOG MESSAGE	DESCRIPTION
TELNET Login Successfully	Someone has logged on to the router via telnet.
TELNET Login Fail	Someone has failed to log on to the router via telnet.
FTP Login Successfully	Someone has logged on to the router via ftp.
FTP Login Fail	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.
!! Phase 1 ID type mismatch	The ID type of an incoming packet does not match the local's peer ID type.
!! Phase 1 ID content mismatch	The ID content of an incoming packet does not match the local's peer ID content.
!! No known phase 1 ID type found	The ID type of an incoming packet does not match any known ID type.

Chart 3 UPnP Logs

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

Chart 4 Content Filtering Logs

CATEGORY	LOG MESSAGE	DESCRIPTION
URLFOR	IP/Domain Name	The Prestige allows access to this IP address or domain name and forwarded traffic addressed to the IP address or domain name.
URLBLK	IP/Domain Name	The Prestige blocked access to this IP address or domain name due to a forbidden keyword. All web traffic is disabled except for trusted domains, untrusted domains, or the cybernot list.

Chart 4 Content Filtering Logs

CATEGORY	LOG MESSAGE	DESCRIPTION
JAVBLK	IP/Domain Name	The Prestige blocked access to this IP address or domain name because of a forbidden service such as: ActiveX, a Java applet, a cookie, or a proxy.

Chart 5 ICMP Type and Code Explanations

TYPE	CODE	DESCRIPTION
0	0	Echo Reply 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

Chart 5 ICMP Type and Code Explanations

TYPE	CODE	DESCRIPTION
	0	Echo message
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp Reply
	0	Timestamp reply message
15		Information Request
	0	Information request message
16		Information Reply
	0	Information reply message

Appendix E

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.

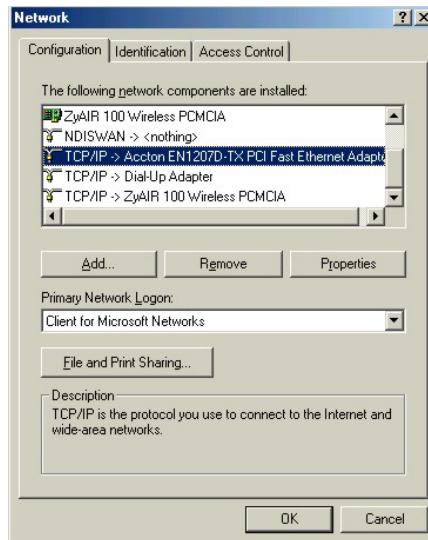
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

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 (192.168.1.2 to 192.168.1.254 range with a subnet mask of 255.255.255.0.) as the default Prestige's LAN port IP address (192.168.1.1).

Windows 95/98/Me

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



2. 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:

- a. In the **Network** window, click **Add**.
- b. Select **Adapter** and then click **Add**.
- c. Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

- a. In the **Network** window, click **Add**.
- b. Select **Protocol** and then click **Add**.
- c. Select **Microsoft** from the list of **manufacturers**.
- d. Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

- a. Click **Add**.
- b. Select **Client** and then click **Add**.
- c. Select **Microsoft** from the list of manufacturers.

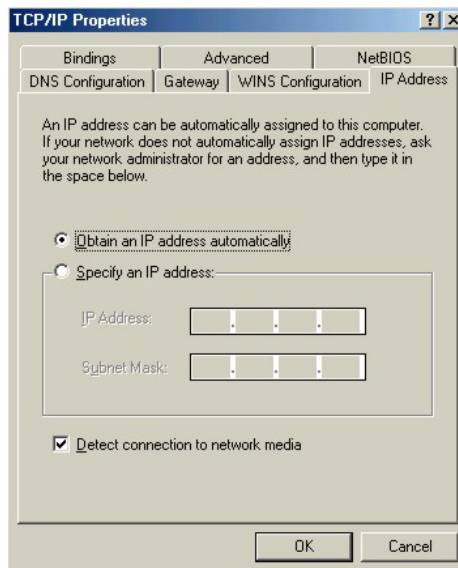
- d. Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
- e. Restart your computer so the changes you made take effect.

In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**.

1. Click the **IP Address** tab.

-To have your computer assigned a dynamic IP address, select **Obtain an IP address automatically**.

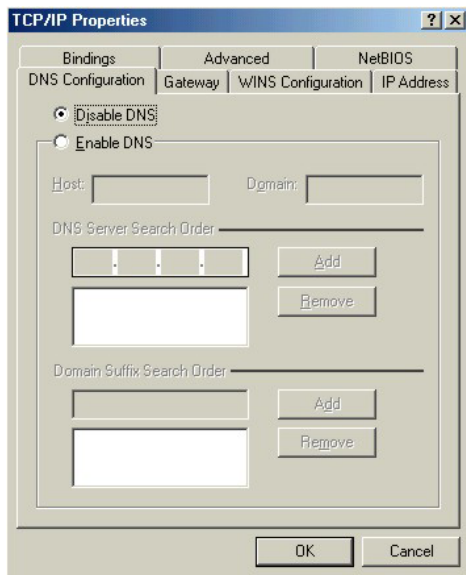
-To give your computer a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.



2. Click the **DNS Configuration** tab.

-If you do not know your DNS information, select **Disable DNS**.

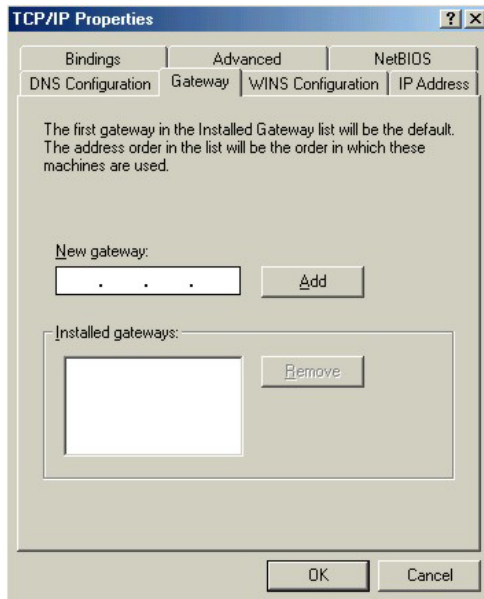
-If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).



3. 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**.



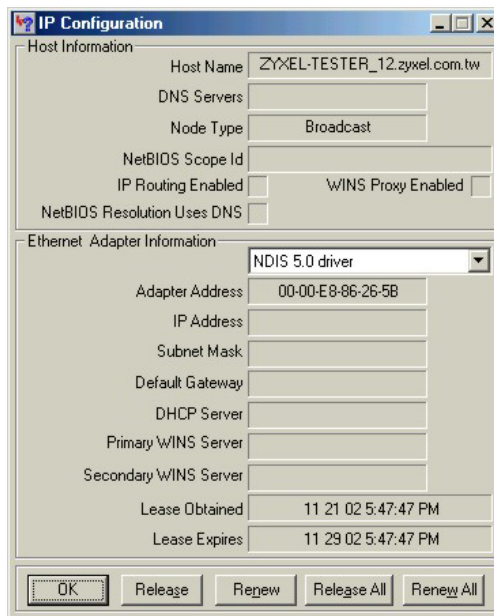
4. Click **OK** to save and close the **TCP/IP Properties** window.

5. Click **OK** to close the **Network** window. Insert the Windows CD if prompted.
6. Turn on your Prestige and restart your computer when prompted.

Checking/Modifying Your Computer's IP Address

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 (static) IP address, subnet mask and default gateway in this screen. Verify that your computer's static IP address is in the correct subnet (192.168.1.2 to 192.168.1.254 if using the default Prestige LAN IP address). Alternatively, to have the Prestige assign your computer a new IP address (from the IP pool), make sure your Prestige is turned on and click **Renew** in this screen.

Your computer can now communicate with the Prestige using the LAN port.

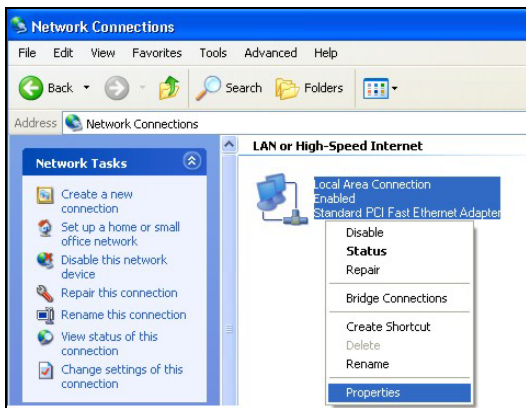


Windows 2000/NT/XP

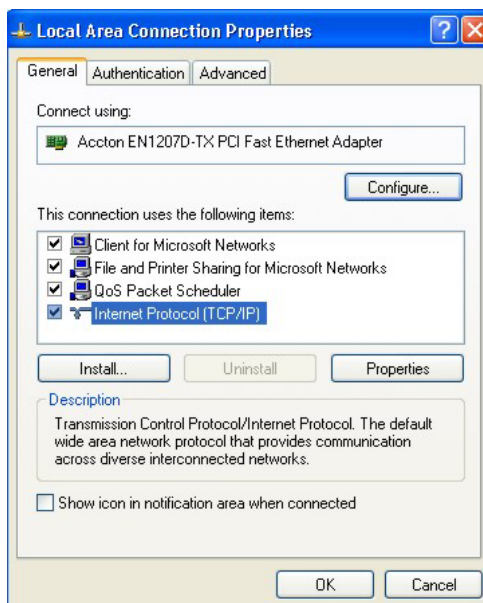
1. In Windows XP, click **start**, **Control Panel**.
In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.



2. In Windows XP, click **Network Connections**.
In Windows 2000/NT, click **Network and Dial-up Connections**.
3. Right-click **Local Area Connection** and then click **Properties**.



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

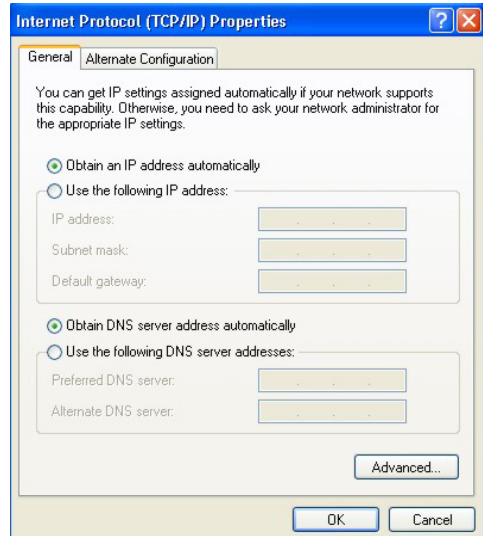


5. The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

- To have your computer assigned 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** to go to the **Advanced TCP/IP Settings** screen shown next.



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.

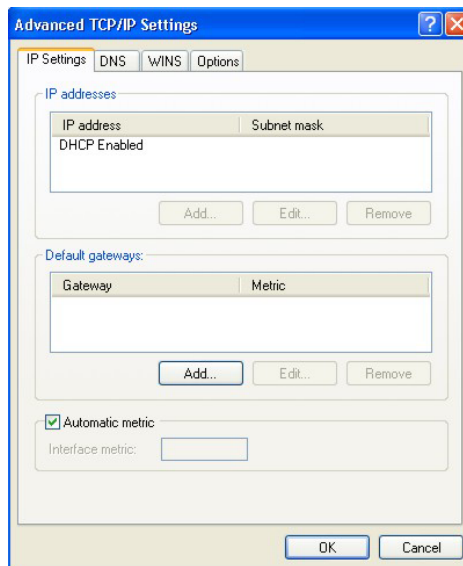
-Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.

-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.

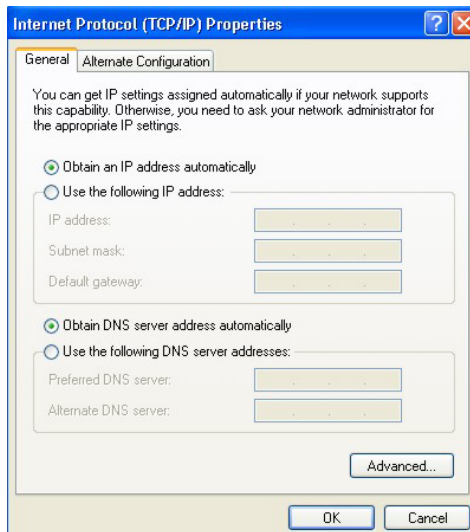


7. In the **Internet Protocol TCP/IP Properties** window (the **General tab** in Windows XP):

-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 wish to have more than two DNS servers, click **Advanced**, the **DNS** tab and then configure them using **Add**.



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).

Checking/Modifying Your Computer's IP Address

1. Click **Start, All Programs, Accessories** and then **Command Prompt**.
2. In the **Command Prompt** window, type "ipconfig" and then press **ENTER** to verify that your computer's static IP address is in the correct subnet (192.168.1.2 to 192.168.1.254 if using the default Prestige LAN IP address). Alternatively, to have the Prestige assign your computer a new IP address (from the IP pool), make sure your Prestige is turned on, type "ipconfig/renew" and then press **ENTER**.

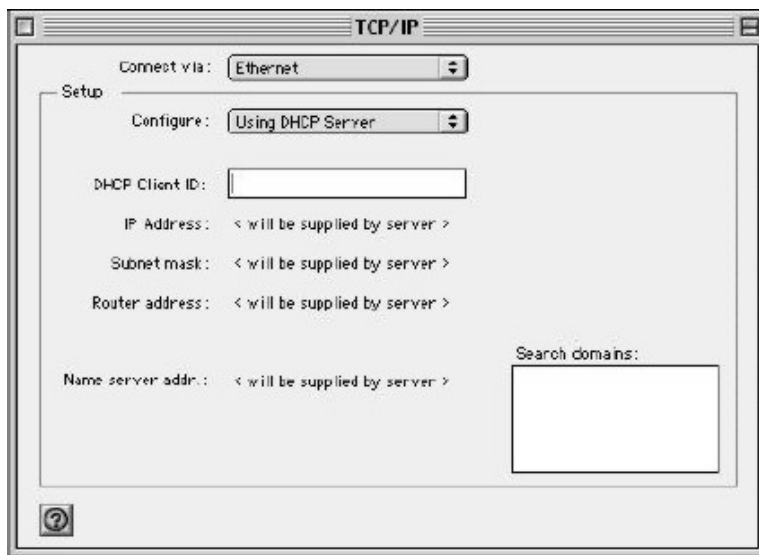
Your computer can now communicate with the Prestige using the LAN port.

Macintosh OS 8/9

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



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



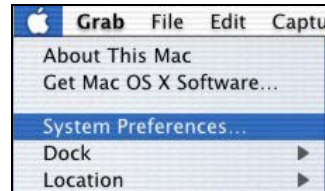
3. For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.
4. For statically assigned settings, do the following:
 - From the **Configure** box, select **Manually**.
 - Type your IP address in the **IP Address** box.
 - Type your subnet mask in the **Subnet mask** 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 Your Computer's IP Address

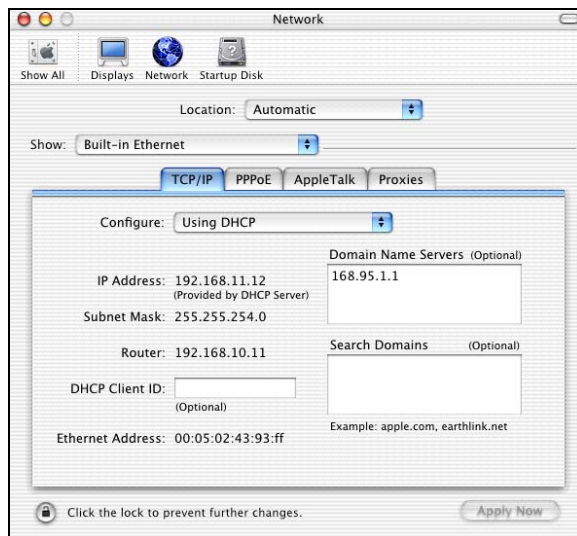
Check your TCP/IP properties in the **TCP/IP Control Panel** window.

Macintosh OS X

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



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.
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 Your Computer's IP Address

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

Appendix F

Brute-Force Password Guessing Protection

The following describes the commands for enabling, disabling and configuring the brute-force password guessing protection mechanism for the password. See other *appendices* for information on the command structure.

Chart 6 Brute-Force Password Guessing Protection Commands

COMMAND	DESCRIPTION
<code>sys pwderrtm</code>	This command displays the brute-force guessing password protection settings.
<code>sys pwderrtm 0</code>	This command turns off the password's protection from brute-force guessing. The brute-force password guessing protection is turned off by default.
<code>sys pwderrtm N</code>	This command sets the password protection to block all access attempts for N (a number from 1 to 60) minutes after the third time an incorrect password is entered.

Example

<code>sys pwderrtm 5</code>	This command sets the password protection to block all access attempts for five minutes after the third time an incorrect password is entered.
-----------------------------	--

Appendix G

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.

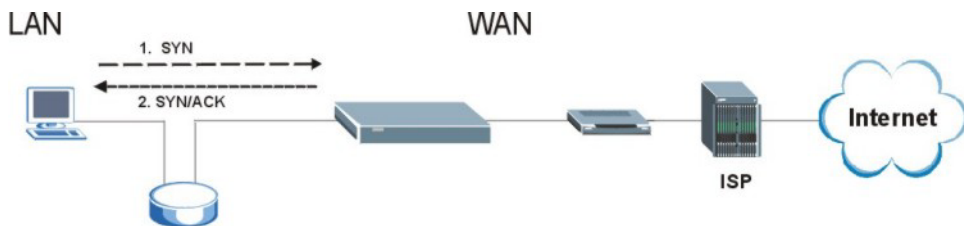


Diagram G-1 Ideal Setup

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.

- Step 1.** A computer on the LAN initiates a connection by sending out a SYN packet to a receiving server on the WAN.
- Step 2.** The Prestige reroutes the SYN packet through Gateway **B** on the LAN to the WAN.
- Step 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.

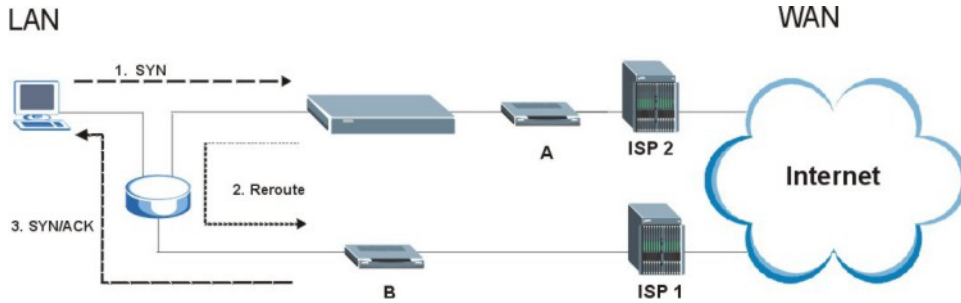


Diagram G-2 “Triangle Route” Problem

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.

- Step 1.** A computer on the LAN initiates a connection by sending a SYN packet to a receiving server on the WAN.
- Step 2.** The Prestige reroutes the packet to Gateway **B** which is in Subnet 2.
- Step 3.** The reply from WAN goes through the Prestige to the computer on the LAN in Subnet 1.

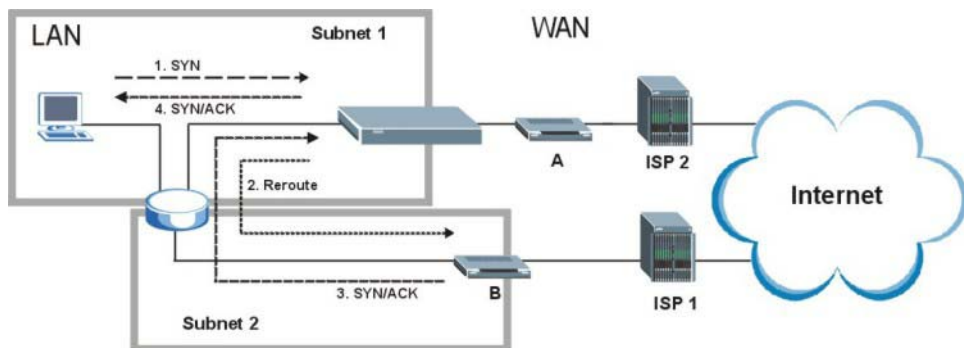


Diagram G-3 IP Alias

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.

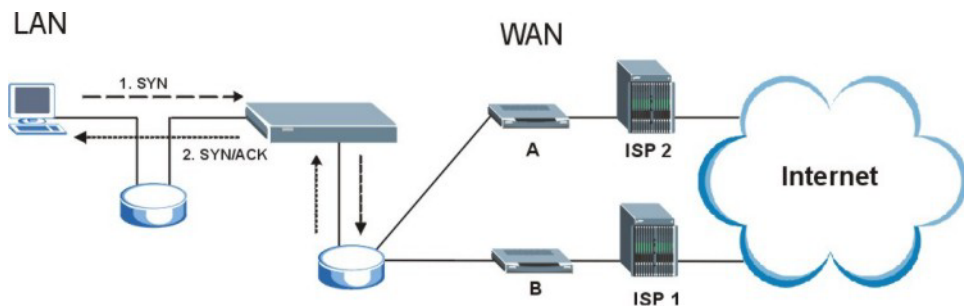


Diagram G-4 Gateways on the WAN Side

How To Configure Triangle Route:

- Step 1.** From the SMT main menu, enter 24.
- Step 2.** Enter “8” in menu 24 to enter CI command mode.

Step 3. Use the following commands to allow/disallow triangle route.

<code>sys firewall ignore triangle all off</code>	This command allows triangle route.
<code>sys firewall ignore triangle all on</code>	This command disallows triangle route.

Appendix H

Index

A

Active.....16-6, 16-8, 19-2
 Address Assignment.....3-8, 3-9, 6-1
 Allocated Budget 16-7, 19-5
 Applications 1-4
 AT command16-3, 16-4, 26-1
 Authen.....16-6, 19-5
 Authentication16-6, 19-4, 19-5
 Authentication Protocol..... 19-4
 auto-negotiation..... 1-1

B

Backup 13-8, 26-2
 Bridging..... 17-2
 Budget Management..... 27-3

C

Call Back Delay 16-5
 Call Control 27-2
 Call History..... 27-4
 Call Scheduling..... 1-3, 29-1
 Maximum Number of Schedule Sets 29-1
 PPPoE 29-3
 Precedence 29-1
 Precedence Example *See precedence*
 Call-Trigerring Packet 25-8
 Canada iv
 Caution..... iv
 CDR (Call Detail Record)..... 25-5
 CHAP 16-6, 19-5
 Command Interpreter Mode..... 27-1
 Community 24-2
 Computer Name 15-1
 Computer's IP Address E-1

Conditions that prevent TFTP and FTP from
 working over WAN..... 26-4
 Configuration 5-1, 13-4
 Connection ID/Name 19-6
 Content Filtering..... 1-2
 Copyright.....ii
 Cost Of Transmission 20-2
 Customer Supportvi

D

DDNS Type..... 15-4
 Default..... 13-10
 Denial of Service 22-1
 DHCP.....3-1, 3-9, 4-3, 5-1, 5-3, 13-4, 17-2, 25-4
 DHCP (Dynamic Host Configuration Protocol)
 1-4
 Diagnostic Tools 25-1
 Dial Timeout..... 16-5
 Disclaimerii
 DNS 11-10, 17-3
 Domain Name.....3-1, 3-9, 7-7, 25-3
 DoS (Denial of Service)..... 1-2
 Drop Timeout..... 16-5
 DSL Modem 1-4, 19-4
 DTR..... 6-22, 16-4
 Dynamic DNS..... 4-2, 4-3, 15-3
 Dynamic DNS Support 1-3
 DYNDNS Wildcard 4-3

E

e.g. *See Syntax Conventions*
 ECHO 7-7
 Edit IP..... 16-7, 19-3
 Enable Wildcard 15-4
 Encapsulation..... 18-2, 19-2, 19-6

PPP over Ethernet.....A-1
Enter *See Syntax Conventions*
Ethernet 3-2, 3-4, 10-2
Ethernet Encapsulation.....7-6, 18-1, 19-1, 19-2,
 19-9

F

Factory Default 16-1
Factory LAN Defaults 5-1
Fail Tolerance..... 19-11
FCC..... iii
Filename Conventions 26-1
Filter..... 16-12, 17-1, 19-9
 Applying..... 23-16
 Configuring 23-4
 Example..... 23-13
 Generic Filter Rule 23-11
 Generic Rule..... 23-11
 NAT..... 23-15
 Remote Node..... 23-17
 Structure 23-2
 TCP/IP Rule 23-7

Filters

 Executing a Filter Rule 23-2
 IP Filter Logic Flow 23-9

Finger..... 7-7

Firewall..... 1-2, 10-1, 10-2
 Access Methods..... 22-1
 Remote Management..... 22-1
 SMT Menus..... 22-1

Firmware File

 Maintenance 13-5, 13-7

FTP.....4-2, 5-1, 7-6, 7-7, 10-2, 11-2, 11-5, 28-2
FTP File Transfer 26-8
FTP Restrictions 11-2, 26-4, 28-2
FTP Server 1-4, 21-13
Full Network Management 1-4

G

Gateway 20-2
Gateway IP Addr 19-7

Gateway IP Address 18-2
General Setup 3-1, 4-1, 15-1
Global 7-1

H

Hidden Menus..... 14-4
Hop Count..... 20-2
Host..... 4-5, 15-4
How PPPoE Works A-2
HTTP 7-7

I

i.e. *See Syntax Conventions*
Idle Timeout..... 16-7, 16-8, 19-4, 19-5
IGMP 5-2
Incoming Protocol Filters 17-5
Industry Canada..... iv
Inside 7-1
Inside Global Address 7-1
Inside Local Address 7-1
Internet access..... 18-1
Internet Access..... 17-2, 18-1
 ISP's Name 18-2
Internet Access Setup..... 18-1, 18-2, 21-1
Internet Security Gateway 1-1
Introduction to Filters..... 23-1
IP address..... 16-7, 16-9
IP Address... 3-8, 5-2, 5-4, 6-1, 6-2, 7-6, 7-8, 7-9,
 13-4, 17-4, 17-5, 18-2, 19-7, 20-2, 25-4
 Remote 16-9
IP Address Assignment 19-7
IP Address Assignment 18-2
IP Alias 1-3, 17-5
IP Alias Setup..... 17-4
IP Multicast..... 1-3
 Internet Group Management Protocol (IGMP)
 1-3
IP Pool 5-3, 5-4, 17-3
IP Pool Setup..... 5-1
IP Static Route 20-1
IP Static Route Setup 20-1

IP Subnet Mask	16-9, 17-5
Remote	16-9
IPSec standard	1-2
IPSec VPN Capability	1-2
ISP's Name	18-2

L

LAN Setup	5-1, 6-1
LAN TCP/IP	5-1
Local	7-1
Log Facility	25-6
Logging	1-4
Login Name	<i>See My Login Name</i>

M

MAC Address	16-1
Main Menu	14-4
Management Information Base (MIB) 11-8, 24-2	
Many to Many No Overload	<i>See NAT</i>
Many to Many Overload	<i>See NAT</i>
Many to One	<i>See NAT</i>
Message Logging	25-5
Metric	6-1, 8-3, 16-10, 19-8, 20-2
Multicast	5-2, 5-5, 16-10, 17-4, 19-9
My IP Addr	19-6
My Login	16-6, 19-2
My Login Name	18-2
My Password	16-6, 18-2, 19-3
My Server IP Addr	19-6
My WAN Address	16-9

N

Nailed-up Connection	19-4
Nailed-Up Connection	16-7, 19-5
NAT	3-4, 7-6, 7-7, 7-8, 7-9, 16-10, 19-8, 23-16
Applying NAT in the SMT Menus	21-1
Configuring.....	21-3
Definitions	7-1
Examples	21-10
How NAT Works.....	7-2

Mapping Types.....	7-4
Non NAT Friendly Application Programs	21-16
Ordering Rules	21-6
Server Sets	7-6
What NAT does.....	7-2
NAT Traversal	9-1, 9-2, 9-3
Navigation Panel	2-3
Network Address Translation	18-3
Network Address Translation (NAT) ..	1-3, 21-1
Network Management	7-7
NNTP	7-7
Notice	iii

O

Offline	15-5
One to One	<i>See NAT</i>
Online Registration	v
Outgoing Protocol Filters	17-5
Outside	7-1

P

Packing List Card	xxv
PAP	16-6, 19-5
Password	4-4, 14-1, 14-6, 24-2. <i>See My Password</i>
Period(hr)	16-7, 19-5
Ping	25-11
Point-to-Point Tunneling Protocol 3-6, 7-7. <i>See PPTP</i>	
POP3	7-7
Port Forwarding	1-4
Port Numbers	7-7
PPP	16-8
PPPoE	1-3, 3-2, 3-4
PPPoE Encapsulation 18-1, 18-5, 19-1, 19-4, 19-5	
PPTP	3-2, 3-4, 3-6, 7-7
Client	18-3, 18-4
Configuring a Client	18-3, 18-4
PPTP and the Prestige	B-1
PPTP Encapsulation	1-3, 3-6, 19-6

PPTP Protocol Overview.....B-2
PPTP, What is it?.....B-1
Prestige as a PPPoE Client.....A-3
Private.....8-4, 16-10, 19-8, 20-3
Private IP Address..... 3-8, 6-2
Protocol Filters..... 17-5
 Incoming..... 17-5
 Outgoing..... 17-5

Q

Quick Start Guide..... 2-1

R

RAS 25-4
Related Documentationxxv
Relay 17-2
Rem IP Address.....16-9
Rem Node Name 16-6, 16-8, 19-2
Remote Management
 Firewall..... 22-1
Remote Management and NAT 11-2
Remote Management Limitations 11-2, 28-2
Remote Node 19-1
Remote Node Filter..... 16-12, 19-9
Remote Node Traffic 23-18
Repairs.....v
Replacementv
Required fields 14-4
Reset Button 1-2
Resetting the Time 27-6
Restore 13-8
Restore Configuration 26-6
retry count..... 16-5
retry interval..... 16-5
Return Material Authorization Numberv
RIP 5-2, 16-10, 17-4, 17-5, 19-8
 Direction..... 17-5
 Version 17-5, 19-8
RoadRunner Support 1-4
Route..... 19-3
RTC..... See Real Time Chip

S

Schedule Sets
 Duration29-2
Schedules 19-5
Select..... See Syntax Conventions
Server..4-6, 7-5, 18-2, 19-3, 21-3, 21-4, 21-5, 21-8, 21-9, 21-11, 21-12, 27-6
Server IP..... 19-3
Service v
Service Name..... 19-5
Service Type..... 18-2, 19-2
Services 7-6, 7-7, 10-8
setup a schedule29-2
SMT Menu Overview 14-2
SMTP..... 7-7
SNMP..... 7-7, 10-2, 11-6
 Community..... 24-3
 Configuration 24-2
 Get..... 11-8, 24-2
 Manager 11-7, 24-2
 MIBs 11-8, 24-2
 Trap 11-8, 24-2
 Trusted Host..... 24-3
SNMP (Simple Network Management Protocol)..... 1-3
Stateful Inspection..... 1-2, 10-1
Static Route8-1
SUA..... 7-6, 7-7, 7-9
SUA (Single User Account)..See NAT. See NAT
Subnet Mask . 3-8, 5-2, 5-4, 16-9, 17-4, 18-2, 19-7, 20-2, 25-4
Support Disk xxv
Syntax Conventions..... xxvi
Syslog 25-5
Syslog IP Address 25-6
Syslog Server..... 25-5
System
 Console Port Speed 25-4
 Diagnostic 25-9
 Log and Trace..... 25-5
 Syslog and Accounting 25-5

System Information	25-3
System Status.....	25-1
System Information.....	25-3
System Information & Diagnosis.....	25-1
System Maintenance . 12-2, 25-1, 25-2, 25-3, 25-11, 26-2, 26-5, 26-11, 27-1, 27-2, 27-3, 27-4, 27-5	
System Management Terminal	14-4
System Name	4-1, 15-2
System Status.....	25-2
System Timeout.....	11-2

T

TCP/IP5-4, 11-4, 16-9, 17-3, 19-7, 23-6, 23-7, 23-9, 23-12, 23-15	
Setup	17-3
TCP/IP filter rule	23-6
Telnet.....	11-4
Telnet Configuration.....	11-4
TFTP and FTP over WAN Will Not Work	
When.....	26-4
TFTP and FTP Over WAN}.....	11-2, 28-2
TFTP File Transfer	26-10
TFTP Restrictions.....	11-2, 26-4, 28-2
Time and Date	1-2
Time and Date Setting	27-5, 27-6
Time Zone	4-5, 27-6
Timeout	16-7, 16-8, 18-4, 18-5, 19-5
Trace Records.....	25-5
Tracing.....	1-4
Trademarks	ii
Traffic Redirect.....	1-3, 6-15
Setup	19-10
Triangle.....	G-1
Triangle Route\ Solutions.....	G-2

Trigger Port Forwarding	21-18
Process.....	7-13

U

Universal Plug and Play (UPnP).....	9-1, 9-3
UNIX Syslog	25-5
UNIX syslog parameters	25-5
Upload Firmware.....	26-8
UPnP Examples.....	9-4
Use Server Detected IP	15-5
User Name	4-4, 15-4
User Specified IP Addr.....	15-5

V

Virtual Private Network.....	1-2
VPN	6-7

W

WAN DHCP	25-10, 25-11
WAN Setup.....	3-9, 6-2, 16-1
Warranty	v
Web	11-2
Web Configurator.....	2-1, 2-2, 22-2
What is PPTP?	B-1
Wizard Setup.....	3-1, 3-2, 3-8
www.dyndns.org	15-5
www.zyxel.com	v

Z

ZyNOS.....	25-3, 26-1, 26-2
ZyNOS F/W Version	25-3, 26-1
ZyXEL Limited Warranty	
Note	v
ZyXEL website.....	v