

Prestige 791R

G.SHDSL Router

User's Guide

Version 3.40

June 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

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

Federal Communications Commission (FCC) Interference Statement

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

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

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

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

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. 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

Refer to the product page at www.zyxel.com.

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.

Safety Warnings

1. To reduce the risk of fire, use only No. 26 AWG or larger telephone wire.
2. Do not use this product near water, for example, in a wet basement or near a swimming pool.
3. Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightning.

Customer Support

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

- Product model and serial number.
- Information in **Menu 24.2.1 – System Information**.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

METHOD	E-MAIL SUPPORT/SALES	TELEPHONE/FAX	WEB SITE/ FTP SITE	REGULAR MAIL
LOCATION				
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.europe.zyxel.com	ZyXEL Communications Corp., 6 Innovation Road II, Science- Based Industrial Park, Hsinchu 300, Taiwan.
NORTH AMERICA	support@zyxel.com sales@zyxel.com	+1-714-632-0882 800-255-4101 +1-714-632-0858	www.zyxel.com ftp.zyxel.com	ZyXEL Communications Inc., 1650 Miraloma Avenue, Placentia, CA 92870, U.S.A.
SCANDINAVIA	support@zyxel.dk sales@zyxel.dk	+45-3955-0700 +45-3955-0707	www.zyxel.dk ftp.zyxel.dk	ZyXEL Communications A/S, Columbusvej 5, 2860 Soeborg, Denmark.
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 Wuersele, Germany

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.....	xiii
List of Tables.....	xvii
Preface.....	xix
What is DSL?.....	xxi
GETTING STARTED.....	I
Chapter 1 Getting to Know Your G.SHDSL Router.....	1-1
1.1 Features of the Prestige.....	1-1
1.2 Application Scenarios for the Prestige.....	1-3
1.2.1 Internet Access.....	1-3
1.2.2 LAN-to-LAN Application.....	1-4
Chapter 2 Hardware Installation.....	2-1
2.1 Installation Requirements.....	2-1
2.2 Front Panel.....	2-1
2.3 Rear Panel.....	2-3
2.3.1 DSL Port.....	2-3
2.3.2 LAN 10/100M.....	2-3
2.3.3 CON/AUX Port.....	2-3
2.3.4 Reset Button.....	2-4
2.3.5 Power Port.....	2-4
2.4 Turning On Your Prestige.....	2-4
Chapter 3 Initial Setup.....	3-1
3.1 Configuring Your Prestige For Internet Access.....	3-1
3.1.1 Procedure For SMT Configuration via Console Port.....	3-1
3.1.2 Procedure For SMT Configuration via Telnet.....	3-1
3.1.3 Connect to your Prestige Using the Web Configurator.....	3-2
3.1.4 Entering Password.....	3-2
3.2 Resetting the Prestige.....	3-2
3.2.1 Methods of Restoring Factory-Defaults.....	3-3
3.2.2 Prestige SMT Menu Overview.....	3-3
3.3 Navigating the SMT Interface.....	3-4
3.3.1 System Management Terminal Interface Summary.....	3-6
3.4 Changing the System Password.....	3-7
3.5 General Setup.....	3-8
3.5.1 Dynamic DNS.....	3-8

3.5.2	Procedure To Configure Menu 1.....	3-9
3.5.3	Procedure to Configure Dynamic DNS.....	3-10
Chapter 4	WAN.....	4-1
4.1	LAN and WAN Overview	4-1
4.1.1	LANs and WANs.....	4-1
4.1.2	LANs, WANs and the Prestige	4-1
4.2	WAN Setup.....	4-2
4.2.1	Service Type	4-2
4.2.2	Rate Adaption	4-2
4.2.3	Transfer Rates	4-3
4.2.4	Standard Mode	4-3
4.3	WAN Setup Screen	4-3
Chapter 5	Dial Backup	5-1
5.1	Dial Backup Overview.....	5-1
5.1.1	Configuring Dial Backup in Menu 2.....	5-1
5.1.2	Advanced WAN Setup.....	5-2
5.2	Remote Node Profile (Backup ISP)	5-4
5.2.1	Editing PPP Options	5-7
5.2.2	Editing TCP/IP Options	5-8
5.2.3	Remote Node Script Overview	5-9
5.2.4	Editing Remote Node Script	5-10
5.2.5	Editing Filter Sets	5-11
Chapter 6	LAN.....	6-1
6.1	LAN Overview	6-1
6.1.1	IP Address and Subnet Mask	6-1
6.1.2	Private IP Addresses	6-2
6.1.3	Factory Ethernet Defaults	6-2
6.1.4	RIP Setup	6-2
6.1.5	DHCP Configuration	6-3
6.1.6	IP Multicast.....	6-4
6.1.7	IP Policies	6-5
6.1.8	IP Alias	6-5
6.2	Ethernet Setup.....	6-6
6.2.1	LAN Port Filter Setup.....	6-6
6.2.2	IP Alias Setup	6-6
6.2.3	Route IP Setup	6-8
6.2.4	TCP/IP Ethernet Setup and DHCP.....	6-9
Chapter 7	Internet Access	7-1
7.1	Internet Access Overview	7-1
7.2	Encapsulation.....	7-1
7.2.1	ENET ENCAP	7-1

7.2.2	PPP over Ethernet	7-1
7.2.3	PPPoA	7-2
7.2.4	RFC 1483	7-2
7.3	IP Address Assignment	7-2
7.3.1	Using PPPoA or PPPoE Encapsulation	7-2
7.3.2	Using RFC 1483 Encapsulation	7-2
7.3.3	Using ENET ENCAP Encapsulation	7-2
7.4	VPI and VCI	7-3
7.5	Multiplexing	7-3
7.5.1	VC-based Multiplexing	7-3
7.5.2	LLC-based Multiplexing	7-3
7.6	Traffic Shaping	7-3
7.7	Internet Access Configuration	7-5
7.8	Internet Access Setup	7-6
ADVANCED APPLICATIONS.....		II
Chapter 8 Remote Node Configuration.....		8-1
8.1	Remote Node Overview	8-1
8.2	Remote Node Setup	8-1
8.2.1	Encapsulation and Multiplexing Scenarios	8-2
8.2.2	Outgoing Authentication Protocol	8-5
8.3	Remote Node Network Layer Options	8-5
8.3.1	My WAN Addr Sample IP Addresses	8-8
8.4	Remote Node Filter	8-8
8.4.1	Web Configurator Internet Security Filter Rules	8-9
8.4.2	Web Configurator Filter Sets	8-10
8.5	Editing ATM Layer Options	8-12
8.5.1	VC-based Multiplexing (non-PPP Encapsulation)	8-12
8.5.2	LLC-based Multiplexing or PPP Encapsulation	8-13
Chapter 9 Static Route Setup		9-1
9.1	Static Route Overview	9-1
Chapter 10 Bridging Setup.....		10-1
10.1	Bridging Overview	10-1
10.2	Bridge Ethernet Setup	10-1
10.2.1	Remote Node Bridging Setup	10-1
10.2.2	Bridge Static Route Setup	10-2
Chapter 11 Network Address Translation (NAT)		11-1
11.1	NAT Overview	11-1
11.1.1	NAT Definitions	11-1
11.1.2	What NAT Does	11-2
11.1.3	How NAT Works	11-2
11.1.4	NAT Application	11-3

11.1.5	NAT Mapping Types	11-4
11.1.6	SUA (Single User Account) Versus NAT	11-6
11.2	Applying NAT	11-6
11.3	NAT Setup	11-7
11.3.1	Address Mapping Sets	11-8
11.4	NAT Server Sets – Port Forwarding	11-14
11.4.1	Configuring a Server behind NAT	11-15
11.5	General NAT Examples	11-17
11.5.1	Example 1: Internet Access Only	11-17
11.5.2	Example 2: Internet Access with an Inside Server	11-19
11.5.3	Example 3: Multiple Public IP Addresses With Inside Servers	11-20
11.5.4	Example 4: NAT Unfriendly Application Programs	11-24
ADVANCED MANAGEMENT		III
Chapter 12 Filter Configuration		12-1
12.1	Filtering Overview	12-1
12.2	Filter Set Configuration	12-4
12.2.1	Filter Rules Summary Menus	12-8
12.3	Filter Rule Configuration	12-9
12.3.1	TCP/IP Filter Rule	12-10
12.3.2	Generic Filter Rule	12-14
12.4	Filter Types and NAT	12-16
12.5	Example Filter	12-16
12.6	Applying Filters and Factory Defaults	12-20
12.6.1	Ethernet Traffic	12-20
12.6.2	Remote Node Filters	12-21
Chapter 13 SNMP Configuration		13-1
13.1	SNMP Overview	13-1
13.2	Supported MIBs	13-2
13.3	SNMP Configuration	13-2
13.4	SNMP Traps	13-3
Chapter 14 System Maintenance		14-1
14.1	System Maintenance Overview	14-1
14.2	System Status	14-1
14.3	System Information	14-3
14.3.1	System Information	14-3
14.3.2	Console Port Speed	14-5
14.4	Log and Trace	14-5
14.4.1	Viewing Error Log	14-5
14.4.2	Syslog	14-6
14.5	Diagnostic	14-8
Chapter 15 Firmware and Configuration File Maintenance		15-1

15.1	Filename Conventions.....	15-1
15.2	Backup Configuration.....	15-2
15.2.1	Backup Configuration	15-3
15.2.2	Using the FTP Command from the Command Line.....	15-3
15.2.3	Example of FTP Commands from the Command Line.....	15-3
15.2.4	GUI-based FTP Clients	15-4
15.2.5	TFTP and FTP over WAN Will Not Work When.....	15-4
15.2.6	Backup Configuration Using TFTP	15-5
15.2.7	TFTP Command Example.....	15-5
15.2.8	GUI-based TFTP Clients.....	15-5
15.2.9	Backup Via Console Port	15-6
15.3	Restore Configuration	15-7
15.3.1	Restore Using FTP	15-8
15.3.2	Restore Using FTP Session Example.....	15-9
15.3.3	Restore Via Console Port	15-9
15.4	Uploading Firmware and Configuration Files.....	15-10
15.4.1	Firmware File Upload	15-10
15.4.2	Configuration File Upload	15-11
15.4.3	FTP File Upload Command from the DOS Prompt Example	15-12
15.4.4	FTP Session Example of Firmware File Upload.....	15-12
15.4.5	TFTP File Upload	15-12
15.4.6	TFTP Upload Command Example.....	15-13
15.4.7	Uploading Via Console Port.....	15-13
15.4.8	Uploading Firmware File Via Console Port.....	15-14
15.4.9	Example Xmodem Firmware Upload Using HyperTerminal.....	15-14
15.4.10	Uploading Configuration File Via Console Port.....	15-15
15.4.11	Example Xmodem Configuration Upload Using HyperTerminal.....	15-15
Chapter 16	System Maintenance and Information	16-1
16.1	Command Interpreter Mode	16-1
16.2	Call Control Support	16-2
16.2.1	Budget Management	16-2
16.3	Time and Date Setting.....	16-4
16.3.1	Resetting the Time	16-5
Chapter 17	IP Policy Routing.....	17-1
17.1	IP Policy Routing Overview	17-1
17.1.1	IP Policy Routing Benefits.....	17-1
17.1.2	Routing Policy.....	17-1
17.2	IP Routing Policy Setup	17-2
17.3	Applying an IP Policy	17-5
17.3.1	Ethernet IP Policies	17-5
17.4	IP Policy Routing Example.....	17-7

Chapter 18 Call Scheduling	18-1
18.1 Call Scheduling Overview	18-1
18.2 Schedule Setup.....	18-1
Chapter 19 Remote Management.....	19-1
19.1 Remote Management Overview.....	19-1
19.1.1 Remote Management and Telnet Services.....	19-1
19.1.2 Remote Management and FTP Services	19-1
19.1.3 Remote Management and Web Services.....	19-2
19.1.4 Disabling Remote Management.....	19-2
19.2 Remote Management Setup	19-2
19.2.1 Remote Management Limitations	19-3
19.3 Remote Management and NAT	19-3
19.4 System Timeout	19-3
ADDITIONAL INFORMATION	IV
Chapter 20 Universal Plug-and-Play (UPnP).....	20-1
20.1 Universal Plug and Play Overview	20-1
20.1.1 How do I know if I'm using UPnP?	20-1
20.1.2 NAT Transversal.....	20-1
20.1.3 Cautions with UPnP.....	20-1
20.1.4 UPnP and ZyXEL	20-2
20.2 Accessing the Prestige Web Configurator to Configure UPnP	20-2
20.2.1 Configuring UPnP.....	20-2
20.3 Installing UPnP in Windows Example.....	20-3
20.4 Using UPnP in Windows XP Example	20-6
Chapter 21 Troubleshooting.....	21-1
21.1 Problems Starting Up the Prestige	21-1
21.2 Problems with the LAN Interface	21-1
21.3 Problems with the WAN Interface.....	21-2
21.4 Problems with Internet Access.....	21-2
21.5 Problems with the Password	21-3
21.6 Problems with Telnet.....	21-3
Appendix A PPPoE	A
Appendix B Virtual Circuit Topology	C
Appendix C Power Adapter Specifications.....	D
Index	G

List of Figures

Figure 1-1 Internet Access Application	1-4
Figure 1-2 LAN-to-LAN Application	1-4
Figure 2-1 Front Panel	2-1
Figure 2-2 Rear Panel	2-3
Figure 3-1 Login Screen	3-2
Figure 3-2 Prestige SMT Menu Overview	3-4
Figure 3-3 SMT Main Menu	3-6
Figure 3-4 System Password	3-7
Figure 3-5 General Setup	3-9
Figure 3-6 Configure Dynamic DNS	3-10
Figure 4-1 LAN & WAN IPs	4-2
Figure 4-2 WAN Setup	4-3
Figure 5-1 Menu 2: Dial Backup Setup	5-1
Figure 5-2 Advanced WAN Setup	5-3
Figure 5-3 Remote Node Profile (Backup ISP)	5-5
Figure 5-4 Menu 11.2 - Remote Node PPP Options	5-7
Figure 5-5 Remote Node PPP Options Menu Fields	5-7
Figure 5-6 Remote Node Network Layer Options	5-8
Figure 5-7 Remote Node Script	5-11
Figure 5-8 Menu 11.5: Remote Node Filter (Ethernet)	5-12
Figure 6-1 Physical Network	6-5
Figure 6-2 Partitioned Logical Networks	6-5
Figure 6-3 TCP/IP Ethernet Setup	6-6
Figure 6-4 LAN Port Filter Setup	6-6
Figure 6-5 TCP/IP and DHCP Setup	6-7
Figure 6-6 IP Alias Setup	6-7
Figure 6-7 General Setup	6-8
Figure 6-8 TCP/IP and DHCP Ethernet Setup	6-9
Figure 7-1 Example of Traffic Shaping	7-4
Figure 7-2 Internet Access Setup	7-6
Figure 8-1 Remote Node Setup	8-2
Figure 8-2 Remote Node Profile	8-3
Figure 8-3 Remote Node Network Layer Options	8-6
Figure 8-4 Sample IP Addresses for a TCP/IP LAN-to-LAN Connection	8-8
Figure 8-5 Remote Node Filter (PPPoA or PPPoE Encapsulation)	8-9
Figure 8-6 Remote Node Filter (RFC1483 or ENET ENCAP Encapsulation)	8-9
Figure 8-7 Internet Security	8-10
Figure 8-8 Menu 21- Filer Set Configuration	8-11
Figure 8-9 Menu 21.11- WebSet 11	8-11

Figure 8-10 Menu 21.12- WebSet 12.....	8-11
Figure 8-11 Menu 11.6 for VC-based Multiplexing (non-PPP Encapsulation).....	8-12
Figure 8-12 Menu 11.6 for LLC-based Multiplexing or PPP Encapsulation	8-13
Figure 9-1 Sample Static Routing Topology Configuration	9-1
Figure 9-2 Static Route Setup.....	9-2
Figure 9-3 IP Static Route Setup.....	9-2
Figure 9-4 Edit IP Static Route.....	9-3
Figure 10-1 Remote Node Bridging Options.....	10-2
Figure 10-2 Bridge Static Route Setup.....	10-3
Figure 10-3 Edit Bridge Static Route.....	10-3
Figure 11-1 How NAT Works.....	11-3
Figure 11-2 NAT Application With IP Alias	11-4
Figure 11-3 Applying NAT for Internet Access	11-6
Figure 11-4 Applying NAT to the Remote Node	11-7
Figure 11-5 NAT Setup.....	11-8
Figure 11-6 Address Mapping Sets.....	11-9
Figure 11-7 Address Mapping Rules - SUA	11-9
Figure 11-8 Address Mapping Rules	11-11
Figure 11-9 Editing/Configuring an Individual Rule in a Set.....	11-13
Figure 11-10 NAT Server Sets	11-15
Figure 11-11 NAT Server Setup.....	11-16
Figure 11-12 Multiple Servers Behind NAT Example.....	11-17
Figure 11-13 NAT Example 1	11-18
Figure 11-14 Internet Access & NAT Example	11-18
Figure 11-15 NAT Example 2	11-19
Figure 11-16 NAT Example 2 - Menu 15.2.1	11-20
Figure 11-17 NAT Example 3	11-21
Figure 11-18 Example 3 - Menu 11.3	11-21
Figure 11-19 Example 3 - Menu 15.1.1.1	11-22
Figure 11-20 Example 3 - Final Menu 15.1.1	11-23
Figure 11-21 Example 3- Menu 15.2	11-24
Figure 11-22 NAT Example 4	11-24
Figure 11-23 Example 4 - Menu 15.1.1.1	11-25
Figure 11-24 Example 4 - Menu 15.1.1	11-26
Figure 12-1 Outgoing Packet Filtering Process	12-2
Figure 12-2 Filter Rule Process	12-3
Figure 12-3 Filter Set Configuration.....	12-4
Figure 12-4 NetBios WAN Filter Rules Summary	12-5
Figure 12-5 NetBios LAN Filter Rules Summary	12-5
Figure 12-6 Telnet WAN Filter Rules Summary.....	12-6
Figure 12-7 PPPoE Filter Rules Summary	12-6

Figure 12-8 FTP_WAN Filter Rules Summary	12-7
Figure 12-9 Web Set1 Filter Rules Summary	12-7
Figure 12-10 Web Set2 Filter Rules Summary	12-8
Figure 12-11 TCP/IP Filter Rule	12-10
Figure 12-12 Executing an IP Filter	12-13
Figure 12-13 Generic Filter Rule	12-14
Figure 12-14 Protocol and Device Filter Sets	12-16
Figure 12-15 Sample Telnet Filter	12-17
Figure 12-16 Sample Filter Rules Summary — Menu 21.1	12-18
Figure 12-17 Sample Filter Rules Summary — Menu 21.3.1	12-19
Figure 12-18 Sample Filter Rules Summary — Applying a Remote Node Filter Set	12-20
Figure 12-19 Filtering Ethernet Traffic	12-21
Figure 12-20 Filtering Remote Node Traffic	12-21
Figure 13-1 SNMP Management Model	13-1
Figure 13-2 SNMP Configuration	13-3
Figure 14-1 System Maintenance	14-1
Figure 14-2 System Maintenance — Status	14-2
Figure 14-3 System Information and Console Port Speed	14-3
Figure 14-4 System Maintenance — Information	14-4
Figure 14-5 System Maintenance – Change Console Port Speed	14-5
Figure 14-6 System Maintenance — Log and Trace	14-5
Figure 14-7 Sample Error and Information Messages	14-6
Figure 14-8 System Maintenance — Syslog and Accounting	14-6
Figure 14-9 System Maintenance — Diagnostic	14-8
Figure 15-1 System Maintenance - Backup Configuration	15-3
Figure 15-2 FTP Session Example	15-4
Figure 15-3 System Maintenance – Backup Configuration	15-6
Figure 15-4 System Maintenance – Starting Xmodem Download Screen	15-6
Figure 15-5 Backup Configuration Example	15-7
Figure 15-6 Successful Backup Confirmation Screen	15-7
Figure 15-7 System Maintenance - Restore Configuration	15-8
Figure 15-8 Restore Using FTP Session Example	15-9
Figure 15-9 System Maintenance – Restore Configuration	15-9
Figure 15-10 System Maintenance – Starting Xmodem Download Screen	15-9
Figure 15-11 Restore Configuration Example	15-10
Figure 15-12 Successful Restoration Confirmation Screen	15-10
Figure 15-13 System Maintenance - Upload System Firmware	15-11
Figure 15-14 Telnet Into Menu 24.7.2 – System Maintenance	15-11
Figure 15-15 FTP Session Example of Firmware File Upload	15-12
Figure 15-16 Menu 24.7.1 as seen using the Console Port	15-14
Figure 15-17 Example Xmodem Upload	15-14

Figure 15-18 Menu 24.7.2 as seen using the Console Port.....	15-15
Figure 15-19 Example Xmodem Upload.....	15-16
Figure 16-1 Command Mode in Menu 24	16-1
Figure 16-2 Valid Commands.....	16-2
Figure 16-3 Call Control.....	16-2
Figure 16-4 Budget Management	16-3
Figure 16-5 System Maintenance	16-4
Figure 16-6 System Maintenance — Time and Date Setting.....	16-4
Figure 17-1 IP Routing Policy Setup	17-2
Figure 17-2 Sample IP Routing Policy Setup	17-3
Figure 17-3 IP Routing Policy	17-4
Figure 17-4 TCP/IP and DHCP Ethernet Setup	17-6
Figure 17-5 Remote Node Network Layer Options.....	17-6
Figure 17-6 Example of IP Policy Routing.....	17-7
Figure 17-7 IP Routing Policy Example	17-8
Figure 17-8 IP Routing Policy	17-9
Figure 17-9 Applying IP Policies.....	17-9
Figure 18-1 Schedule Setup.....	18-1
Figure 18-2 Schedule Set Setup.....	18-2
Figure 18-3 Applying Schedule Set(s) to a Remote Node (PPPoE).....	18-4
Figure 19-1 Telnet Configuration on a TCP/IP Network	19-1
Figure 19-2 Remote Management Control	19-2
Figure 20-1 Configuring UPnP.....	20-3

List of Tables

Table 2-1 Front Panel LED Description.....	2-2
Table 3-1 Main Menu Commands.....	3-5
Table 3-2 Main Menu Summary	3-6
Table 3-3 General Setup.....	3-9
Table 3-4 Configure Dynamic DNS.....	3-11
Table 4-1 WAN Setup	4-4
Table 5-1 Menu 2: Dial Backup Setup	5-2
Table 5-2 Advanced WAN Port Setup: AT Commands Fields	5-3
Table 5-3 Advanced WAN Port Setup: Call Control Parameters	5-4
Table 5-4 Remote Node Profile (Backup ISP)	5-5
Table 5-5 Remote Node Network Layer Options.....	5-8
Table 5-6 Remote Node Script.....	5-11
Table 6-1 IP Alias Setup.....	6-8
Table 6-2 TCP/IP and DHCP Ethernet Setup	6-9
Table 7-1 Internet Account Information.....	7-5
Table 7-2 Internet Access Setup.....	7-6
Table 8-1 Remote Node Profile.....	8-3
Table 8-2 Remote Node Network Layer Options.....	8-6
Table 9-1 Edit IP Static Route	9-3
Table 10-1 Remote Node Bridging Options.....	10-2
Table 10-2 Edit Bridge Static Route.....	10-3
Table 11-1 NAT Definitions	11-1
Table 11-2 NAT Mapping Types	11-5
Table 11-3 Applying NAT to the Remote Node	11-7
Table 11-4 Address Mapping Rules - SUA	11-9
Table 11-5 Address Mapping Rules	11-11
Table 11-6 Editing/Configuring an Individual Rule in a Set.....	11-13
Table 11-7 Services & Port Numbers.....	11-14
Table 12-1 Abbreviations Used in the Filter Rules Summary Menu.....	12-8
Table 12-2 Rule Abbreviations Used	12-9
Table 12-3 TCP/IP Filter Rule.....	12-10
Table 12-4 Generic Filter Rule Menu Fields.....	12-15
Table 12-5 Filter Sets Table	12-20
Table 13-1 SNMP Configuration	13-3
Table 13-2 SNMP Traps.....	13-3
Table 14-1 System Maintenance — Status	14-2
Table 14-2 System Maintenance — Information	14-4
Table 14-3 System Maintenance Menu — Syslog Parameters.....	14-7
Table 14-4 System Maintenance Menu — Diagnostic.....	14-9

Table 15-1 Filename Conventions	15-2
Table 15-2 General Commands for GUI-based FTP Clients	15-4
Table 15-3 General Commands for GUI-based TFTP Clients	15-6
Table 16-1 Budget Management.....	16-3
Table 16-2 Time and Date Setting Fields.....	16-5
Table 17-1 IP Routing Policy Setup Abbreviations	17-3
Table 17-2 IP Routing Policy.....	17-4
Table 18-1 Schedule Set Setup	18-2
Table 19-1 Remote Management Control.....	19-2
Table 20-1 Configuring UPnP	20-3
Table 21-1 Troubleshooting the Start-Up of Your Prestige	21-1
Table 21-2 Troubleshooting the LAN Interface	21-1
Table 21-3 Troubleshooting the WAN Interface	21-2
Table 21-4 Troubleshooting Internet Access.....	21-2
Table 21-5 Troubleshooting the Password.....	21-3
Table 21-6 Troubleshooting Telnet	21-3

Preface

Congratulations on your purchase of the Prestige 791R G.SHDSL Router.

The Prestige is a high-performance router for Internet/LAN access via a telephone line. Your Prestige supports multi-protocol routing for TCP/IP, as well as transparent bridging for other protocols.

The Prestige supports symmetrical multi-rate data transmission speeds 72 Kbps up to 2312 Kbps. The actual rate depends on the copper category of your telephone wires, distance from the central office and the type of DSL service you subscribe to. Its 10/100M auto-negotiating LAN interface enables fast data transfer of either 10Mbps or 100Mbps in either half-duplex or full-duplex mode depending on your Ethernet network. See the following section for more background information on DSL.

The Prestige uses TC-PAM line code with echo cancellation for high data rate transmissions over a single-twisted telephone wire pair without being affected by bridge taps or mixed cable links. It also provides high immunity from background noise.

Your Prestige is easy to install and configure. All functions are configurable via the SMT (System Management Terminal) and web configurator. Advanced users may configure the Prestige using CLI (Command Line Interface) commands.

Please visit our web site at www.zyxel.com for the latest release notes and product information.

Don't forget to register your Prestige (fast, easy online registration at www.zyxel.com) for free future product updates and information.

About This User's Guide

This manual is designed to guide you through the configuration of your Prestige for its various applications. Primarily SMT menus are shown, but web configurator screens are shown for features that do not have SMT menus or the recommendation is to configure via web configurator.

Related Documentation

- Supporting Disk
Refer to the included CD for support documents.
- Quick Start Guide
The Quick Start Guide is designed to help you get up and running right away. It contains a detailed easy-to-follow connection diagram, default settings, handy checklists and information on setting up your network and configuring for Internet access.
- ZyXEL Web Site
The ZyXEL download library at www.zyxel.com contains additional support documentation. Please also refer to www.zyxel.com for an online glossary of networking terms.

Syntax Conventions

- “Type” means for you to type one or more characters and press the carriage return. “Select” or “Choose” means for you to use one predefined choices.
- The SMT menu titles and labels are in **Bold Times New Roman** font. Predefined field choices are in **Bold Arial** font. Command and arrow keys are enclosed in square brackets. [ENTER] means the Enter, or carriage return key; [ESC] means the Escape key and [SPACE BAR] means the Space Bar.
- For brevity’s sake, we will use “e.g.,” as a shorthand for “for instance”, and “i.e.,” for “that is” or “in other words” throughout this manual.
- The Prestige 791R may be referred to as the Prestige in this user’s guide.
- Images of Prestige 791R are used throughout this document unless otherwise specified.

The following section offers some background information on DSL. Skip to *Chapter 1* if you wish to begin working with your router right away.

What is DSL?

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

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

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

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

What is G.SHDSL?

G.SHDSL (Single-pair High-speed Digital Subscriber Line) is a symmetrical, bi-directional DSL service that operates on one twisted-pair wire and provides data rates up to 2.3 Mbits/sec. (The "G." in "G.SHDSL" is defined by the G.991.2 ITU (International Telecommunication Union) state-of-the-art industry standard).

Part I:

GETTING STARTED

This part covers Getting to Know Your Prestige, Hardware Installation, Initial Setup, WAN, Dial Backup, LAN and Internet Access.

Chapter 1

Getting to Know Your G.SHDSL Router

This chapter covers the key features and main applications of your Prestige.

The Prestige 791R Router can be used for high-speed LAN-to-LAN connections or Internet access through a G.SHDSL connection over the telephone line. You can use your Prestige for either IP routing or bridging depending on your ISP (Internet Service Provider) configuration.

1.1 Features of the Prestige

The following features make the Prestige a complete and the flexible networking solution for most users.

Scalability

One of the best features of G.SHDSL service is its scalability. You can increase the capacity of the Internet connection (within certain distance limitations) without changing your ISP or purchasing new equipment. G.SHDSL's high symmetrical speeds are ideal for applications like web hosting and videoconferencing as well as the two-way data traffic needs of businesses.

Symmetrical High Speed Internet Access

The Prestige 792H can support symmetrical transmission speeds of up to 2.3 Mbps. For NSP's (Network Service Provider) convenience, the Prestige also supports rate management depending on distance and service charges.

The table below lists the transmission speeds available on the Prestige.

SUPPORTED TRANSMISSION SPEEDS		
	Min (Kbps)	Max (Kbps)
SDSL	72	136
G.HDSL (G.991.2)	200	2312

SNMP (Simple Network Management Protocol – versions 1 and 2)

SNMP, a member of the TCP/IP protocol suite, allows you to exchange management information between network devices. Your Prestige supports SNMP agent functionality that allows a manager station to manage and monitor the Prestige through the network.

SNMP is only available if TCP/IP is configured on your Prestige.

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

IP Policy Routing

IP Policy Routing provides a mechanism to override the default routing behavior and alter packet forwarding based on the policies defined by the network administrator.

10/100MB Auto-negotiation Ethernet/Fast Ethernet Interface

This auto-negotiation feature allows the Prestige to detect the speed of incoming transmissions and adjust appropriately, providing a faster data transfer on the Ethernet network as required. It enables fast data transfer of either 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode depending on your Ethernet network.

Protocols Supported

- TCP/IP (Transmission Control Protocol/Internet Protocol) network layer protocol.
- PPP (Point-to-Point Protocol) link layer protocol.
- SUA™ (Single User Account) and NAT (Network Address Translation).

PAP and CHAP Security

The Prestige supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is available on more platforms.

DHCP Support

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

Encapsulation

The Prestige supports PPPoE, PPP over ATM (RFC-2364), Multiple Protocol over ATM (RFC-1483) and ENET ENCAP.

SUA for Single-IP Address Internet Access

The Prestige's SUA (Single User Account, equivalent to NAT) feature allows multiple user Internet access for the cost of a single ISP account and allows multiple users on the LAN (Local Area Network) to access the Internet concurrently. SUA supports popular Internet applications such as MS traceroute, CuSeeMe, IRC, ICQ, RealAudio, VDOLive, Quake and PPTP. No extra configuration is needed to support these applications. SUA address mapping can also be used for other LAN-to-LAN connections.

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.

Full Network Management

- Menu driven SMT (System Management Terminal) management
- SNMP manageable
- Web Configurator

Upgrade Firmware via LAN

In addition to the direct console port connection, the Prestige supports the up/downloading of firmware and configuration file over the LAN.

Packet Filtering

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

Ease of Installation

Your Prestige is designed for quick, easy and intuitive installation. Its compact size and light weight make it easy to position anywhere in your busy office.

Multiple PVC (Permanent Virtual Circuits) Support

Your Prestige supports up to 12 PVC's.

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.

1.2 Application Scenarios for the Prestige

This section provides examples on how your Prestige can be used.

1.2.1 Internet Access

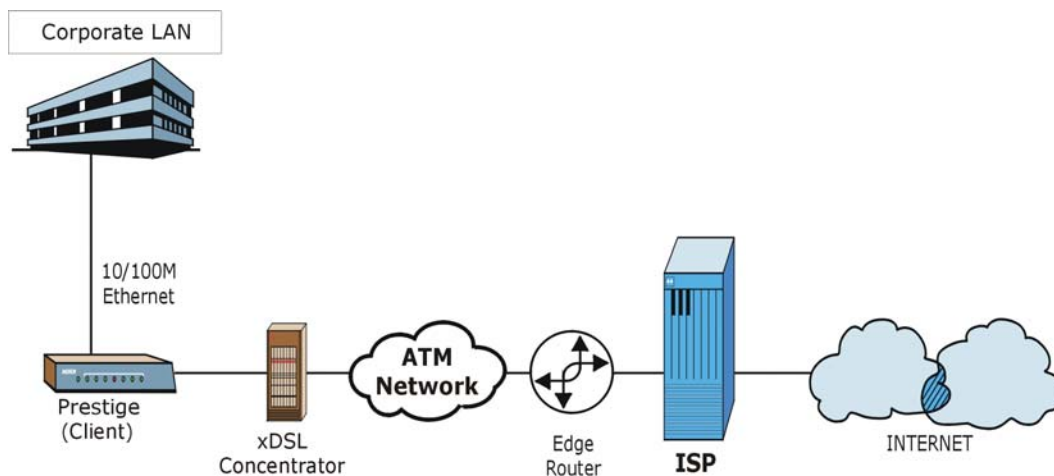


Figure 1-1 Internet Access Application

Your Prestige can act as either of the following:

- A bridge for multi-computer/MAC bridging (RFC-1483, bridged Ethernet/802.3).

1.2.2 LAN-to-LAN Application

You can use the Prestige to connect two geographically dispersed networks over the DSL line. A typical LAN-to-LAN application is shown next.

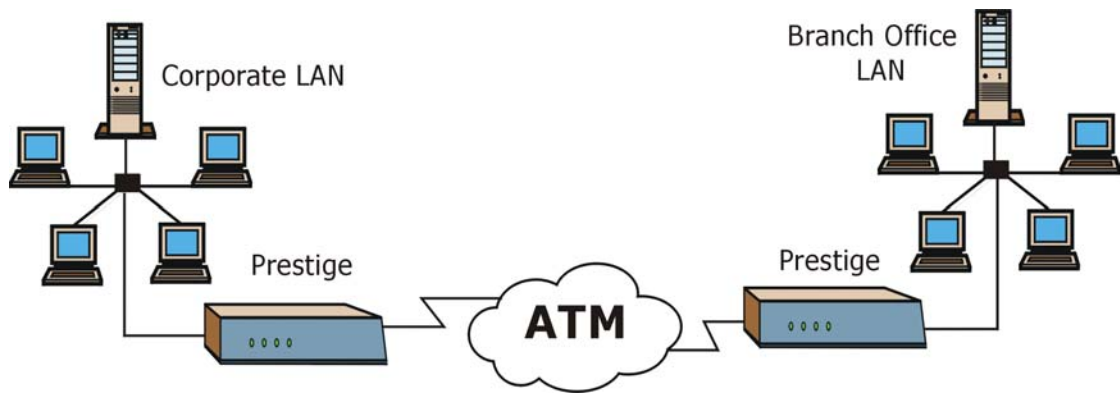


Figure 1-2 LAN-to-LAN Application

Chapter 2

Hardware Installation

This chapter introduces the Prestige hardware and shows you how to make cable connections.

2.1 Installation Requirements

In addition to your Prestige package, your computer should include the following hardware and software:

- An Ethernet 10/100Base-T NIC (Network Interface Card).
- Communications software configured as follows: VT100 terminal emulation; 9600 Baud; No parity, 8 Data bits, 1 Stop bit, no Flow Control.

2.2 Front Panel

The LED indicators on the front panel show the operational status of the Prestige.



Figure 2-1 Front Panel

Table 2-1 Front Panel LED Description

LED	COLOR	STATUS	DESCRIPTION
PWR	Green	On	The Prestige is receiving power.
		Off	The Prestige is not receiving power.
SYS	Green	On	The Prestige is functioning properly.
		Flashing	The Prestige is rebooting.
		Off	The system is not ready or has malfunctioned.
	Red	On	Power to the Prestige is too low.
10/100M LAN	Green	On	The Prestige has a successful 10Mb Ethernet connection.
		Flashing	The Prestige is sending/receiving data.
		Off	The Prestige does not have 10Mb Ethernet connection.
	Orange	On	The Prestige has a successful 100Mb Ethernet connection.
		Flashing	The Prestige is sending/receiving data.
		Off	The Prestige does not have 100Mb Ethernet connection.
CON/AUX	Green	On	The CON/AUX switch is set to CON and the CON/AUX port is connected to a management computer.
		Off	The CON/AUX link is not ready, or has failed.
	Orange	On	The CON/AUX switch is set to AUX and the CON/AUX port has an Internet connection through a dial-up modem.
		Flashing	The CON/AUX switch is set to AUX and the CON/AUX port is sending or receiving data through a dial-up modem.
		Off	The CON/AUX link is not ready, or has failed.
DSL	Green	On	The Prestige is linked successfully to a DSLAM.
		Flashing	The Prestige is initializing the DSL line.
		Off	The DSL link is down.
PPP/ACT	Green	Flashing	The Prestige is sending/receiving data.
		Off	The system is ready, but is not sending/receiving data.
	Orange	On	The Prestige is initiating a PPPoE connection.

2.3 Rear Panel



Figure 2-2 Rear Panel

2.3.1 DSL Port

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

2.3.2 LAN 10/100M

Ethernet 10Base-T/100Base-T networks use Shielded Twisted Pair (STP) cable with RJ-11 (POTS) connectors or RJ-45 (ISDN) connectors that look like a bigger telephone plug with 8 pins. The LAN port is auto-sensing, so you may use the crossover cable provided or a straight-through Ethernet cable to connect your Prestige to a computer/external hub.

2.3.3 CON/AUX Port

Set this switch to the “CON” side to use the CON/AUX port as a regular console port for local device configuration and management. Connect the 9-pin male end of the console cable to the console port of the Prestige and the other end (choice of 9-pin or 25-pin, depending on your computer) end to a serial port (COM1, COM2 or other COM port) of your computer. Your computer should have a terminal emulation communications program (such as HyperTerminal) set to VT100 terminal emulation, no parity, 8 data bits, 1 stop bit, no data flow and 9600 bps port speed.

Set this switch to the “AUX” side to use the CON/AUX port as an auxiliary dial-up WAN connection. Connect the 9-pin male end of the cable to the CON/AUX port and use the included CON/AUX converter on the other 9-pin end of the cable to connect to a modem or TA.

2.3.4 Reset Button

The Prestige comes with a reset button 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 addressed starting at 192.168.1.33.

Hold this button in for between 1 and 3 seconds to restart the Prestige. Upload the default configuration file by holding this button in for more than 3 seconds. Refer to section 3.2 for information on the resetting your Prestige.

2.3.5 Power Port

Connect the power adapter to the port labeled **POWER** on the rear panel of your Prestige. Push in the power button when you want to turn on the Prestige.

**To avoid damage to the Prestige, make sure you use the supplied power adapter.
Refer to the *Power Adapter Specification Appendix* for this information.**

2.4 Turning On Your Prestige

You can now turn on your Prestige by pushing in the power button (located on the back panel) to turn on your Prestige.

Chapter 3

Initial Setup

This chapter shows you how to set up your G.SHDSL connection using the SMT.

3.1 Configuring Your Prestige For Internet Access

Configure your Prestige for Internet access using:

- SMT (System Management Terminal).
- Web configurator (refer to the *Quick Start Guide*).

3.1.1 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”.

3.1.2 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.

3.1.3 Connect to your Prestige Using the Web Configurator

Step 1. Launch your web browser.

Step 2. Enter “192.168.1.1” as the URL.

Step 3. In the **User Name** field, type "admin". In the **Password** field, type “1234”. Click **OK**.

Click the **Help** button for online web configurator HTML help.

The remainder of this user’s guide shows you how to configure the Prestige for Internet access using SMT screens. There are also some sections in this guide that also focus on using Telnet to configure the Prestige.

3.1.4 Entering Password

The login screen appears after you press [ENTER], prompting you to enter the password, as shown next.

For your first login, enter the default password “1234”. As you type the password, the screen displays an asterisk “*” for each character you type.

Please note that if there is no activity for longer than five minutes after you log in, your Prestige will automatically log you out.

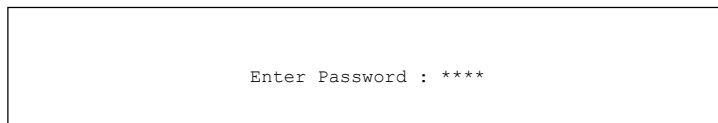


Figure 3-1 Login Screen

3.2 Resetting the Prestige

If you forget your password or cannot access the Prestige, you will need to reload the factory-default configuration file. This means that you will lose all configurations that you had previously; the password will be reset to “1234” and the LAN IP address to 192.168.1.1.

To obtain the default configuration file, download it from the ZyXEL FTP site, unzip it and save it in a folder.

3.2.1 Methods of Restoring Factory-Defaults

You can erase the current configuration and restore factory defaults in three ways:

1. Transfer the configuration file to your Prestige using:
 - the SMT menus. See later in this User's Guide for more information on this.
 - the web configurator to restore defaults (see the web configurator HTML help)
2. Use the **Reset** button on the rear panel of the Prestige to upload the default configuration file (hold this button in for more than 3 seconds). Use this method for cases when the password or IP address of the Prestige is not known.

3.2.2 Prestige SMT Menu Overview

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

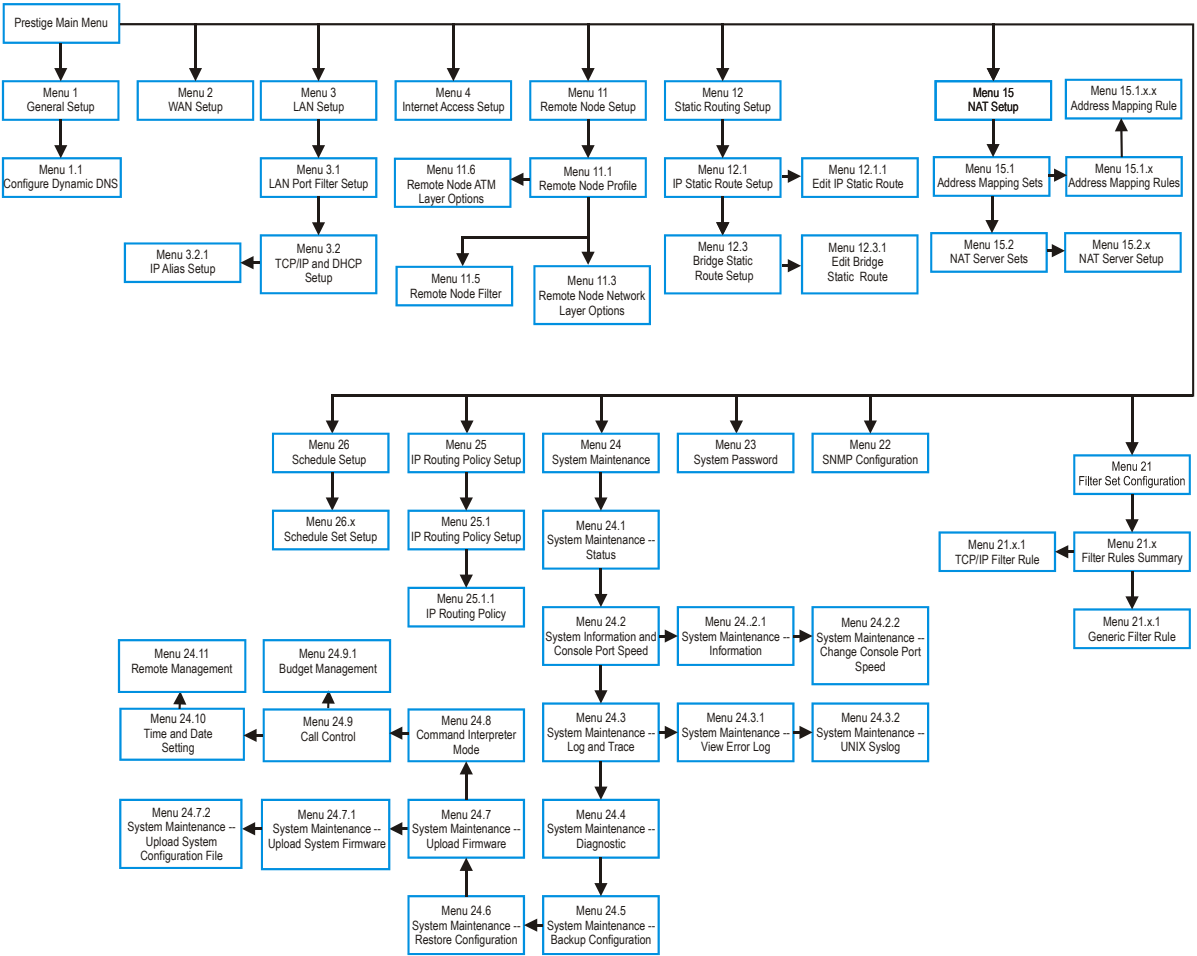


Figure 3-2 Prestige SMT Menu Overview

3.3 Navigating the SMT Interface

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

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

Table 3-1 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 791R 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 Set Configuration
  22. SNMP Configuration
  23. System Password
  24. System Maintenance
  25. IP Routing Policy Setup
  26. Schedule Setup

99. Exit

Enter Menu Selection Number:_
```

Figure 3-3 SMT Main Menu

The SMT menu continually improves and changes with new firmware upgrades. Check the release notes at www.zyxel.com to find the most recent upgrades and information.

3.3.1 System Management Terminal Interface Summary

Table 3-2 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 set up your WAN connection.
3	LAN Setup	Use this menu to set up your LAN connection.
4	Internet Access Setup	A quick and easy way to set up an Internet connection.
11	Remote Node Setup	Use this menu to set up the Remote Node for LAN-to-LAN connection, including Internet connection.
12	Static Routing Setup	Use this menu to set up static routes.
15	NAT Setup	Use this menu to specify inside servers when NAT is enabled.
21	Filter Set Configuration	Use this menu to set up filters to provide security, etc.
22	SNMP Configuration	Use this menu to set up SNMP related parameters.
23	System Password	Use this menu to change your password.

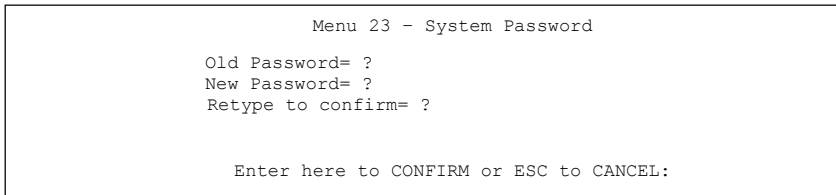
#	MENU TITLE	DESCRIPTION
24	System Maintenance	This menu provides system status, diagnostics, software upload, etc.
25	IP Routing Policy Setup	Use this menu to configure your IP routing policy.
26	Schedule Setup	Use this menu to schedule outgoing calls.
99	Exit	Use this to exit from SMT and return to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

3.4 Changing the System Password

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

Step 1. Enter 23 in the main menu to open **Menu 23 - System Password** as shown next.

Step 2. Type your existing system password (1234 is the default) in the **Old Password** field and press [ENTER].



```
Menu 23 - System Password

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

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

Figure 3-4 System Password

Step 3. Type your new system password in the **New Password** field (up to 30 alphanumeric characters. Do not use spaces, but dashes “-“ and underscores “_“ are accepted). Then 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 asterisk “*” for each character you type.

If you forget your password, use the reset button to restore the default password of 1234. This will allow you to enter the SMT. Then use the above instructions to set a new password.

3.5 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.

3.5.1 Dynamic DNS

Dynamic DNS (Domain Name System) 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 or other services). You can also access your FTP server or Web site on your own computer using a DNS-like address (for example, *myhost.dhs.org*, where *myhost* is a name of your choice) which 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 DNS name.

To use this service, you must register with the Dynamic DNS service provider. The Dynamic DNS service provider will give you a password or key. The Prestige supports www.dyndns.org. You can apply to this service provider for Dynamic DNS service.

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.

3.5.2 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= ?
Location=
Contact Person's Name=
Domain Name=
Edit Dynamic DNS= No

Route IP= Yes
Bridge= No

Press ENTER to Confirm or ESC to Cancel:

```

Figure 3-5 General Setup

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

Table 3-3 General Setup

FIELD	DESCRIPTION	EXAMPLE
System Name	Choose a descriptive name for identification purposes. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.	P650HW
Location (optional)	Enter the geographic location (up to 31 characters) of your Prestige.	MyHouse
Contact Person's Name (optional)	Enter the name (up to 30 characters) of the person in charge of this Prestige.	JohnDoe

FIELD	DESCRIPTION	EXAMPLE
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. You can go to menu 24.8 and type "sys domainname" to see the current domain name used by your gateway. If you want to clear this field just press the [SPACE BAR]. The domain name entered by you is given priority over the ISP assigned domain name.	zyxel.com.tw
Edit Dynamic DNS	Press the [SPACE BAR] to select Yes or No (default). Select Yes to configure Menu 1.1 — Configure Dynamic DNS (discussed next).	No
Route IP	Set this field to Yes to enable or No to disable IP routing. You must enable IP routing for Internet access.	Yes
Bridge	Turn on/off bridging for protocols not supported (for example, SNA) or not turned on in the previous Route IP field. Select Yes to turn bridging on; select No to turn bridging off.	No

3.5.3 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= Yes
Host= me.ddns.org
EMAIL= mail@mailserver
USER= username
Password= *****
Enable Wildcard= No

Press ENTER to confirm or ESC to cancel:
```

Figure 3-6 Configure Dynamic DNS

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

Table 3-4 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
Host	Enter the domain name assigned to your Prestige by your Dynamic DNS provider.	me.dyndns.org
EMAIL	Enter your e-mail address.	mail@mailserver
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
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 4

WAN

This chapter shows you how to configure the WAN settings of your Prestige.

4.1 LAN and WAN Overview

This section provides information on LANs, WANs, TCP/IP parameters and configuring your prestige for Internet access.

4.1.1 LANs and WANs

A LAN (Local Area Network) is a computer network limited to the immediate area, usually the same building or floor of a building. A WAN (Wide Area Network), on the other hand, is an outside connection to another network or the Internet.

4.1.2 LANs, WANs and the Prestige

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

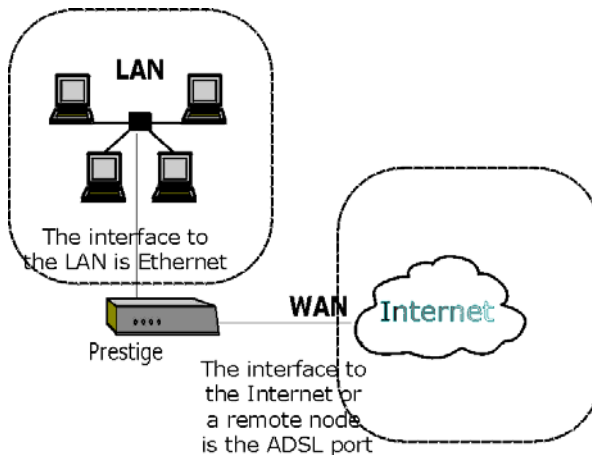


Figure 4-1 LAN & WAN IPs

4.2 WAN Setup

Use **Menu 2 – WAN Setup** to configure G.SHDSL settings for your WAN line. Different telephone companies deploy different types of G.SHDSL service. If you are unsure of any of this information, please check with your telephone company.

4.2.1 Service Type

Is your Prestige acting as a Server or Client?

1. The Prestige is a server if it is acting as a COE (Central Office Equipment). It will determine transfer rate and mode.
2. The Prestige is a client if it is acting as a CPE (Customer Premise Equipment).

4.2.2 Rate Adaption

Both the Prestige and the peer must have the same transmission rate. Rate Adaption allows the Prestige to auto-detect the peer transfer rate.

4.2.3 Transfer Rates

The Prestige supports the following symmetrical multi-rate data transmission speeds:

72, 136, 200, 264, 392, 520, 776, 1032, 1160, 1544, 1736, 2056 and 2312Kbps.

You can increase the capacity of the Internet connection (within certain limitations) without changing your ISP or buying new equipment.

For back-to-back applications make sure that your Prestige and its peer have the same **Transfer Max Rate** and the same **Transfer Min Rate**. Two (maximum and minimum) transfer rates are used to accommodate fluctuations in line speed. This is known as Dynamic Bandwidth Allocation.

4.2.4 Standard Mode

If your Prestige is a server, then select the mode that applies to your region: ANSI (American National Standards Institute) and ETSI (European Telecommunications Standards Institute). If your Prestige is a client, select the same **Standard Mode** that the server side selects. ANSI and ETSI create recommendations and standards for the telecommunications industry.

4.3 WAN Setup Screen

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

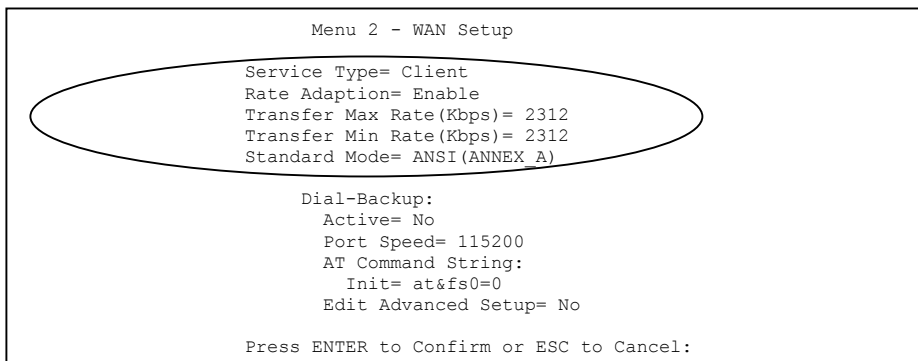


Figure 4-2 WAN Setup

Table 4-1 WAN Setup

FIELD	DESCRIPTION
Service Type	Press [SPACE BAR] to select Server (COE) or Client (CPE).
Rate Adaption	Press [SPACE BAR] to select Enable (activate) or Disable (deactivate).
Transfer Max Rate (2312 Kbps)	Press [SPACE BAR] to select a Transfer Max Rate greater than or equal to the Transfer Min Rate and press [ENTER] to continue.
Transfer Min Rate (2312 Kbps)	Press [SPACE BAR] to select a Transfer Min Rate less than or equal to the Transfer Max Rate and press [ENTER] to continue.
Standard Mode	Press [SPACE BAR] to select ANSI (ANNEX A) or ETSI (ANNEX B) and press [ENTER] to continue. The Client side must match the Server side.

Chapter 5

Dial Backup

This chapter shows you how to configure Dial Backup for your Prestige.

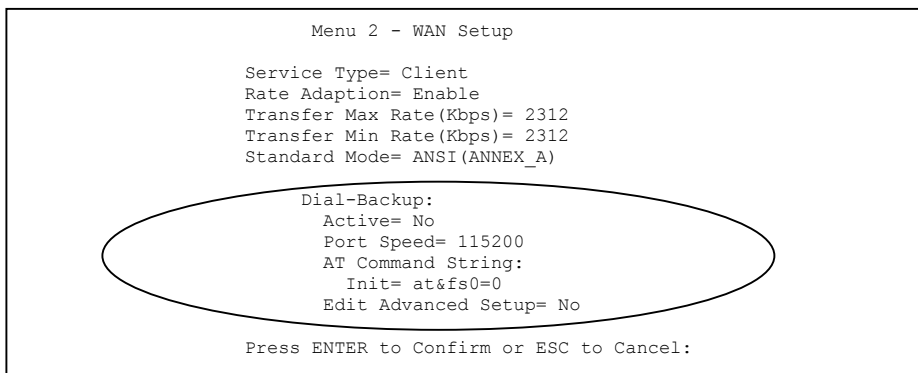
5.1 Dial Backup Overview

The Dial Backup port or CON/AUX port can be used in reserve, as a traditional dial-up connection, if the broadband connection to the WAN port fails. To set up the auxiliary port (Dial Backup or CON/AUX) 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 Hardware Installation chapter), 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

5.1.1 Configuring Dial Backup in Menu 2

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



```
Menu 2 - WAN Setup

Service Type= Client
Rate Adaption= Enable
Transfer Max Rate(Kbps)= 2312
Transfer Min Rate(Kbps)= 2312
Standard Mode= ANSI(ANNEX_A)

Dial-Backup:
Active= No
Port Speed= 115200
AT Command String:
Init= at&fs0=0
Edit Advanced Setup= No

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

Figure 5-1 Menu 2: Dial Backup Setup

Table 5-1 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
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.	115200
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.		

5.1.2 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:
Dial= atdt
Drop= ~++++~ath
Answer= ata

Drop DTR When Hang Up= Yes

AT Response Strings:
CLID= NMBR =
Called Id=
Speed= CONNECT

Call Control:
Dial Timeout(sec)= 60
Retry Count= 0
Retry Interval(sec)= N/A
Drop Timeout(sec)= 20
Call Back Delay(sec)= 15

Press ENTER to Confirm or ESC to Cancel:

```

Figure 5-2 Advanced WAN Setup**Table 5-2 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 String:		
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

Table 5-2 Advanced WAN Port Setup: AT Commands Fields

FIELD	DESCRIPTION	DEFAULT
Speed	Enter the keyword preceding the connection speed.	CONNECT

Table 5-3 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

5.2 Remote Node Profile (Backup ISP)

Enter **12** 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= 0.0.0.0
                                                Edit IP= No
Outgoing:                                       Edit Script Options= No
  My Login=                                     Telco Option:
  My Password= *****                       Allocated Budget (min)= 0
  Authen= CHAP/PAP                           Period(hr)= 0
  Pri Phone #= ?                             Nailed-Up Connection= No
  Sec Phone #=                               Session Options:
                                                Edit Filter Sets= No
                                                Idle Timeout(sec)= 100
Press ENTER to Confirm or ESC to Cancel:

```

Figure 5-3 Remote Node Profile (Backup ISP)

Table 5-4 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.	*****
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 5-4 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 5.2.1</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 5.2.2</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 5.2.3</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.	No (default)

Table 5-4 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.		

5.2.1 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:

Press Space Bar to Toggle.
```

Figure 5-4 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 5-5 Remote Node PPP Options Menu Fields

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)

5.2.2 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 - Network Layer Options**.

```
Menu 11.3 - Remote Node Network Layer Options

Rem IP Addr= 0.0.0.0
Rem Subnet Mask= 0.0.0.0
My WAN Addr= 0.0.0.0

NAT = None
Metric= 15
Private= No
RIP Direction= Both
Version= RIP-2B
Multicast= None

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

Figure 5-6 Remote Node Network Layer Options

Table 5-5 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 IP 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)
NAT	Press [SPACE BAR] and then [ENTER] to select either Full Feature , None or SUA Only . See the Network Address Translation (NAT) chapter for a full discussion on this feature.	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)

Table 5-5 Remote Node Network Layer Options

FIELD	DESCRIPTION	EXAMPLE
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.		

5.2.3 Remote Node Script Overview

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.

5.2.4 Editing Remote Node Script

Move the cursor to the **Edit Script Options** field in menu 11.1, then press [SPACE BAR] to select **Yes**. Press [ENTER] to open **Menu 11.4 – Remote Node Script**.

```

Menu 11.4 - Remote Node Script

Active= No

Set 1:                               Set 5:
  Expect=                             Expect=
  Send=                               Send=
Set 2:                               Set 6:
  Expect=                             Expect=
  Send=                               Send=
Set 3:
  Expect=
  Send=
Set 4:
  Expect=
  Send=

Enter here to CONFIRM or ESC to CANCEL:

Press Space Bar to Toggle.

```

Figure 5-7 Remote Node Script**Table 5-6 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

5.2.5 Editing Filter Sets

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=

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

Figure 5-8 Menu 11.5: Remote Node Filter (Ethernet)

Chapter 6

LAN

This chapter shows you how to configure the LAN settings for your Prestige.

6.1 LAN Overview

This section describes how to configure the Prestige for LAN connections.

6.1.1 IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, the machines on a LAN also share one common network number.

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

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 (ignoring the trailing zero). The Internet Assigned Number Authority (IANA) has 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 3 numbers specify the network number while the last number identifies an individual computer on that network.

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.

6.1.2 Private IP Addresses

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

10.0.0.0 – 10.255.255.255
172.16.0.0 – 172.31.255.255
192.168.0.0 – 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or 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*.

6.1.3 Factory Ethernet Defaults

The Ethernet 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).

6.1.4 RIP Setup

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

1. **Both** - the Prestige will broadcast its routing table periodically and incorporate the RIP information that it receives.
2. **In Only** - the Prestige will not send any RIP packets but will accept all RIP packets received.

3. **Out Only** - the Prestige will send out RIP packets but will not accept any RIP packets received.
4. **None** - the Prestige will not send any RIP packets and will ignore any RIP packets received.

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

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

6.1.5 DHCP Configuration

DHCP (Dynamic Host Configuration Protocol) allows the individual clients (computers) to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The Prestige has built-in DHCP server capability, enabled by default, which means it can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client. The Prestige can also act as a surrogate DHCP server where it relays IP address assignment from the actual DHCP server to the clients.

IP Pool Setup

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

DNS Server Address

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa, for example, 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 machine before you can access it. The DNS server addresses that you enter in the DHCP setup are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses. The first is for an ISP to tell a customer the DNS server addresses, usually in the form of an information sheet, when s/he signs up. If

your ISP does give you the DNS server addresses, enter them in the **DNS Server** fields in **DHCP Setup**, otherwise, leave them blank.

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

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

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

6.1.6 IP 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 is a third way to deliver IP packets to *a group* of hosts on the network - not everybody.

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 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 using menus 3.2 (LAN) and 11.3 (WAN). Select **None** to disable IP Multicasting on these interfaces.

6.1.7 IP Policies

Traditionally, routing is based on the destination address *only* and the router takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing. Create policies using SMT menu 25 (see *IP Policy Routing*) and apply them on the Prestige LAN and/or WAN interfaces using menus 3.2 (LAN) and 11.3 (WAN).

6.1.8 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. See *Section 6.2.2* to configure IP Alias on your Prestige.

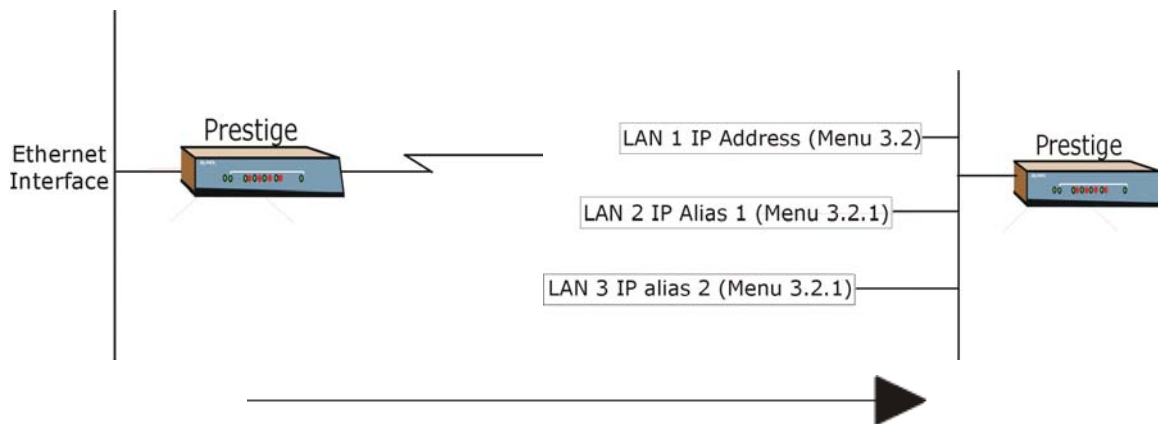


Figure 6-1 Physical Network

Figure 6-2 Partitioned Logical Networks

6.2 Ethernet Setup

This section describes how to configure the Ethernet using **Menu 3 – Ethernet Setup**. From the main menu, enter 3 to open the menu as follows.

```
Menu 3 - Ethernet Setup

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

Enter Menu Selection Number:
```

Figure 6-3 TCP/IP Ethernet Setup

6.2.1 LAN Port Filter Setup

In this menu type 1 to open **Menu 3.1- LAN Port Filter Setup**. Use this menu to specify filter set(s) that you want to apply to Ethernet traffic. You seldom need to filter Ethernet traffic; however, the filter sets may be useful for blocking certain packets, reducing traffic and preventing 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 6-4 LAN Port Filter Setup

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

6.2.2 IP Alias Setup

Use **Menu 3.2** to configure the first network. To edit **Menu 3.2**, enter 3 from the main menu to display **Menu 3 — Ethernet Setup**. When menu 3 appears, press 2 and press [ENTER] to display **Menu 3.2 —**

TCP/IP and DHCP Ethernet Setup as shown next. Move the cursor to **Edit IP Alias** field and press [SPACE BAR] to choose **Yes** and press [ENTER] to configure the second and third network.

```

Menu 3.2 - TCP/IP and DHCP Setup

DHCP Setup:
  DHCP= Server
  Client IP Pool Starting Address= 192.168.1.33
  Size of Client IP Pool= 32
  Primary DNS Server= 0.0.0.0
  Secondary DNS Server= 0.0.0.0
  Remote DHCP Server= N/A
TCP/IP Setup:
  IP Address= 192.168.1.1
  IP Subnet Mask= 255.255.255.0
  RIP Direction= None
  Version= N/A
  Multicast= None
  IP Policies=
  Edit IP Alias= No

Press ENTER to confirm or ESC to Cancel:

Press Space Bar to Toggle.

```

Figure 6-5 TCP/IP and DHCP Setup

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

```

Menu 3.2.1 - IP Alias Setup

IP Alias 1= No
  IP Address= N/A
  IP Subnet Mask= N/A
  RIP Direction= N/A
  Version= N/A
  Incoming protocol filters= N/A
  Outgoing protocol filters= N/A
IP Alias 2= No
  IP Address= N/A
  IP Subnet Mask= N/A
  RIP Direction= N/A
  Version= N/A
  Incoming protocol filters= N/A
  Outgoing protocol filters= N/A
Enter here to CONFIRM or ESC to CANCEL:

```

Figure 6-6 IP Alias Setup

Follow the instructions in the following table to configure IP Alias parameters.

Table 6-1 IP Alias Setup

FIELD	DESCRIPTION	EXAMPLE
IP Alias	Choose Yes to configure the LAN network for the Prestige.	Yes
IP Address	Enter the IP address of your Prestige in dotted decimal notation	192.168.2.1
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] to select the RIP direction. Choices are None , Both , In Only or Out Only .	None
Version	Press [SPACE BAR] to select the RIP version. Choices 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.	
Outgoing Protocol Filters	Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the Prestige.	
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		

6.2.3 Route IP Setup

You must enable IP routing for Internet access. You can enable IP routing in **Menu 1 — General Setup**. To edit menu 1, type in 1 in the main menu and press [ENTER]. Set the **Route IP** field to **Yes** by pressing [SPACE BAR].

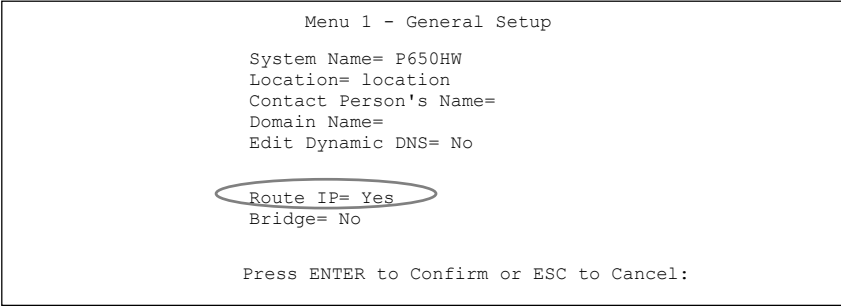


Figure 6-7 General Setup

6.2.4 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 — Ethernet Setup**. When menu 3 appears, press 2 and press [ENTER] to display **Menu 3.2 — TCP/IP and DHCP Ethernet Setup** as shown next:

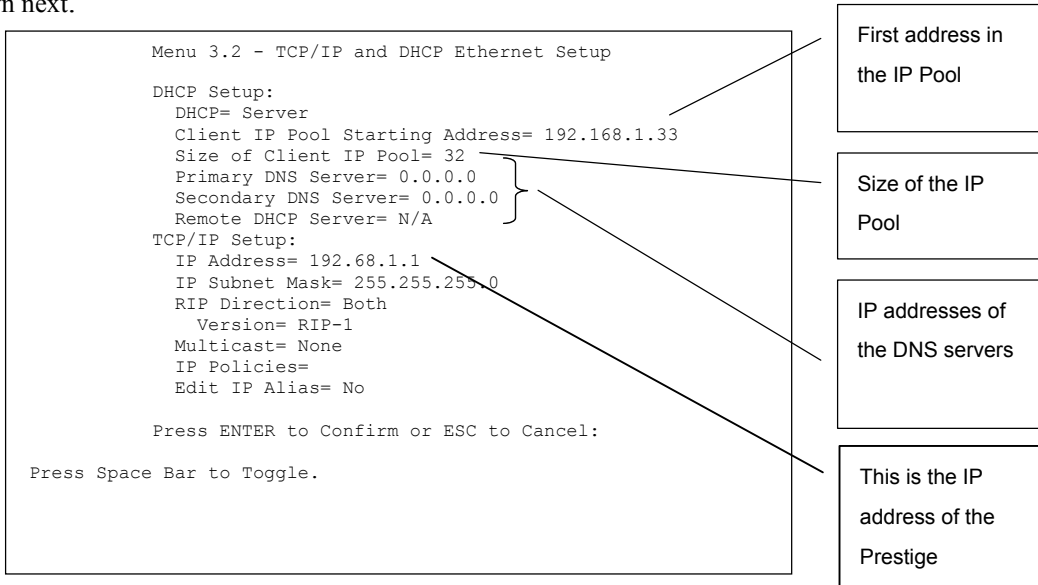


Figure 6-8 TCP/IP and DHCP Ethernet Setup

Table 6-2 TCP/IP and DHCP Ethernet Setup

FIELD	DESCRIPTION	EXAMPLE
DHCP Setup		

Table 6-2 TCP/IP and DHCP Ethernet Setup

FIELD	DESCRIPTION	EXAMPLE
DHCP	If set to Server, your Prestige can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client. If set to None, the DHCP server will be disabled. If set to Relay, the Prestige acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the Remote DHCP Server in this case. When DHCP is used, the following items need to be set:	Server (default)
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.	32
Primary DNS Server Secondary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.	
Remote DHCP Server	If Relay is selected in the DHCP field above then enter the IP address of the actual remote DHCP server here.	
TCP/IP Setup		
IP Address	Enter the (LAN) 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] to select the RIP direction. Choices are Both , In Only , Out Only or None .	Both (default)
Version	Press [SPACE BAR] to select the RIP version. Choices are RIP-1 , RIP-2B or RIP-2M .	RIP-1 (default)
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group. The Prestige supports both IGMP version 1 (IGMP-v1) and version 2 (IGMP-v2). Press the [SPACE BAR] to enable IP Multicasting or select None to disable it.	None (default)

Table 6-2 TCP/IP and DHCP Ethernet Setup

FIELD	DESCRIPTION	EXAMPLE
IP Policies	Create policies using SMT menu 25 (see the <i>IP Policy Routing chapter</i>) and apply them on the Prestige LAN interface here. You can apply up to four IP Policy sets (from twelve) by entering their numbers separated by commas.	2,4,7,9
Edit IP Alias	The Prestige supports three logical LAN interfaces via its single physical Ethernet interface with the Prestige itself as the gateway for each LAN network. Press [SPACE BAR] to change No to Yes and press [ENTER] to for menu 3.2.1	No (default)

Chapter 7

Internet Access

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

7.1 Internet Access Overview

This section provides information on configuring your Prestige for Internet access. It includes information on encapsulation types, IP address assignment and ATM networks.

7.2 Encapsulation

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

7.2.1 ENET ENCAP

The MAC Encapsulated Routing Link Protocol (ENET ENCAP) is only implemented with the IP network protocol. IP packets are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment for instance, it encapsulates routed Ethernet frames into bridged ATM cells. ENET ENCAP requires that you specify a gateway IP address in the **Ethernet Encapsulation Gateway** field in menu 4 and in the **Rem IP Addr** field in menu 11.1. You can get this information from your ISP.

7.2.2 PPP over Ethernet

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

7.2.3 PPPoA

Please refer to RFC 2364 for more information on PPP over ATM Adaptation Layer 5 (AAL5). Refer to RFC 1661 for more information on PPP.

7.2.4 RFC 1483

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

7.3 IP Address Assignment

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

7.3.1 Using PPPoA or PPPoE Encapsulation

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

7.3.2 Using RFC 1483 Encapsulation

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

7.3.3 Using ENET ENCAP Encapsulation

In this case you can have either a static or dynamic IP. For a static IP you must fill in all the **IP Address** and **ENET ENCAP Gateway** fields as supplied by your ISP. However for a dynamic IP, the Prestige acts

as a DHCP client on the WAN port and so the **IP Address** and **ENET ENCAP Gateway** fields are not applicable (N/A) as they are assigned to the Prestige by the DHCP server.

7.4 VPI and VCI

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

7.5 Multiplexing

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

7.5.1 VC-based Multiplexing

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

7.5.2 LLC-based Multiplexing

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

7.6 Traffic Shaping

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

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

Sustained Cell Rate (SCR) is the mean cell rate of a bursty, on-off traffic source that can be sent at the peak rate, and a parameter for burst-type traffic. SCR may not be greater than the PCR; the system default is 0 cells/sec.

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

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

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

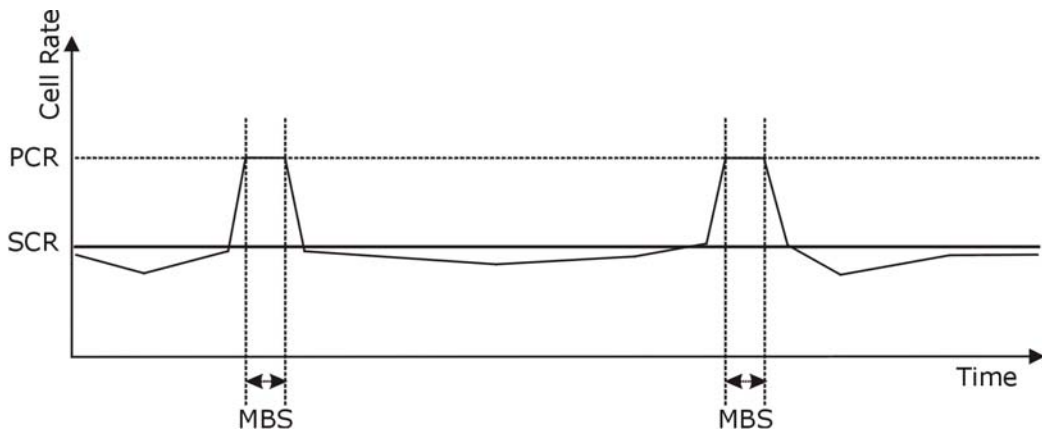


Figure 7-1 Example of Traffic Shaping

7.7 Internet Access Configuration

Menu 4 allows you to enter the Internet Access information in one screen. **Menu 4** is actually a simplified setup for one of the remote nodes that you can access in **Menu 11**. Before you configure your Prestige for Internet access, you need to collect your Internet account information from your ISP and telephone company.

Use the following table to record your Internet Account Information. Note that if you are using PPPoA or PPPoE encapsulation, then the only ISP information you need is a login name and password. You only need to know the Ethernet Encapsulation Gateway IP address if you are using ENET ENCAP encapsulation.

Table 7-1 Internet Account Information

FIELD	DESCRIPTION	YOUR INFO
System Name	Name of the Prestige (optional).	
Service Name (PPPoE Encapsulation)	Enter the PPPoE service name if the ISP supplies one. Enter "any" if the ISP does not assign you one.	
Encapsulation	PPPoE, RFC1483, PPPoA or ENET ENCAP.	
Multiplexing	LLC-based or VC-based. If this information is not given, use the default.	
VPI	Enter your Virtual Path Identifier here.	
VCI	Enter your Virtual Channel Identifier here.	
My Login	Enter the login name assigned by your ISP (for PPPoA/PPPoE only).	
My Password	Enter the password associated with your ISP assigned My Login (for PPPoA/PPPoE only).	
Idle Timeout (PPPoE or PPPoA)	Enter the time lapse, in seconds, before you automatically disconnect from the PPPoE or PPPoA server.	
IP Address	Enter if your IP address is not dynamically assigned.	
Network Address Translation	Full Feature, SUA Only or None.	

Table 7-1 Internet Account Information

FIELD	DESCRIPTION	YOUR INFO
DNS Server Address Assignment	Primary DNS server Secondary DNS server Enter when using RFC 1483 Encapsulation or a static IP address.	
ENET ENCAP Gateway	IP Address Gateway IP Address Enter when using ENET ENCAP Encapsulation.	

7.8 Internet Access Setup

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

```
Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
Encapsulation= ENET ENCAP
Multiplexing= LLC-based
VPI #= 8
VCI #= 35
ATM QoS Type= UBR
  Peak Cell Rate (PCR)= 0
  Sustain Cell Rate (SCR)= 0
  Maximum Burst Size (MBS)= 0
My Login= N/A
My Password= N/A
ENET ENCAP Gateway= N/A
IP Address Assignment= Dynamic
  IP Address= N/A
Network Address Translation= SUA Only
  Address Mapping Set= N/A

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

Figure 7-2 Internet Access Setup

Table 7-2 Internet Access Setup

FIELD	DESCRIPTION	EXAMPLE
ISP's Name	Enter the name of your Internet Service Provider. This information is for identification purposes only.	ChangeMe

Table 7-2 Internet Access Setup

FIELD	DESCRIPTION	EXAMPLE
Encapsulation	Press [SPACE BAR] to select the method of encapsulation used by your ISP. Choices are PPPoE , PPPoA , RFC 1483 or ENET ENCAP .	ENET ENCAP
Multiplexing	Press [SPACE BAR] to select the method of multiplexing used by your ISP. Choices are VC-based or LLC-based .	LLC-based
VPI #	Enter the Virtual Path Identifier (VPI) that the telephone company gives you.	8
VCI #	Enter the Virtual Channel Identifier (VCI) that the telephone company gives you.	35
ATM QoS Type	Press [SPACE BAR] and select CBR (Continuous Bit Rate) to specify fixed (always-on) bandwidth. Select UBR (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select VBR (Variable Bit Rate) for bursty traffic and bandwidth sharing with other applications.	UBR
Peak Cell Rate (PCR)	This is the maximum rate at which the sender can send cells. Type the PCR.	0
Sustain Cell Rate (SCR)= 0	Sustained Cell Rate is the mean cell rate of a bursty, on-off traffic source that can be sent at the peak rate, and a parameter for burst-type traffic. Type the SCR; it must be less than the PCR, unless both are set to zero.	0
Maximum Burst Size (MBS)= 0	Refers to the maximum number of cells that can be sent at the peak rate. Type the MBS. The MBS must be less than 65535.	0
My Login	Configure the My Login and My Password fields for PPPoA and PPPoE encapsulation only. Enter the login name that your ISP gives you. If you are using PPPoE encapsulation, then this field must be of the form user@domain where domain identifies your PPPoE service name.	N/A
My Password	Enter the password associated with the login name above.	N/A
ENET ENCAP Gateway	Enter the gateway IP address supplied by your ISP when you are using ENET ENCAP encapsulation.	N/A
Idle Timeout	This value specifies the number of idle seconds that elapse before the Prestige automatically disconnects the PPPoE session.	0

Table 7-2 Internet Access Setup

FIELD	DESCRIPTION	EXAMPLE
IP Address Assignment	Press [SPACE BAR] to select Static or Dynamic address assignment.	Dynamic
IP Address	Enter the IP address supplied by your ISP if applicable.	N/A
Network Address Translation	Press [SPACE BAR] to select None , SUA Only or Full Feature . Please see the <i>NAT Chapter</i> for more details on the SUA (Single User Account) feature.	SUA Only
Address Mapping Set	Type the numbers of mapping sets (1-8) to use with NAT. See the <i>NAT</i> chapter for details.	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.		

If all your settings are correct your Prestige should connect automatically to the Internet. If the connection fails, note the error message that you receive on the screen and take the appropriate troubleshooting steps.

Part II:

ADVANCED APPLICATIONS

This part shows how to configure Remote Nodes, Static Routes, Bridging and NAT.

Chapter 8

Remote Node Configuration

This chapter covers remote node configuration.

8.1 Remote Node Overview

This section describes the protocol-independent parameters for a remote node. A remote node is required for placing calls to a remote gateway. A remote node represents both the remote gateway and the network behind it across a WAN connection. When you use Menu 4 to set up Internet access, you are configuring one of the remote nodes.

You first choose a remote node in **Menu 11- Remote Node Setup**. You can then edit that node's profile in menu 11.1, as well as configure specific settings in three submenus: edit IP and bridge options in menu 11.3; edit ATM options in menu 11.6; and edit filter sets in menu 11.5.

8.2 Remote Node Setup

To configure a remote node, follow these steps:

- Step 1.** From the Main Menu, select menu option **11 Remote Node Setup**.
- Step 2.** When Menu 11 appears as shown in the following figure, type the number of the remote node that you want to configure.

Menu 11 - Remote Node Setup

1. MyISP (ISP, SUA)

2. _____

3. _____

4. _____

5. _____

6. _____

7. _____

8. _____

9. _____

10. _____

11. _____

12. _____

Enter Node # to Edit:

Figure 8-1 Remote Node Setup

8.2.1 Encapsulation and Multiplexing Scenarios

For Internet access you should use the encapsulation and multiplexing methods used by your ISP. For LAN-to-LAN applications, for example, between a branch office and corporate headquarters, prior agreement on methods is necessary because encapsulation and multiplexing cannot be automatically determined. What method(s) you use depends on how many VCs you have and how many different network protocols you need. The extra overhead that ENET ENCAP encapsulation entails makes it a poor choice in a LAN-to-LAN application. Here are some examples of more suitable combinations in such an application.

Scenario 1. One VC, Multiple Protocols

PPPoA (RFC-2364) encapsulation with **VC-based** multiplexing is the best combination because no extra protocol identifying headers are needed. The **PPP** protocol already contains this information.

Scenario 2. One VC, One Protocol (IP)

Selecting **RFC-1483** encapsulation with **VC-based** multiplexing requires the least amount of overhead (0 octets). However, if there is a potential need for multiple protocol support in the future, it may be safer to select **PPPoA** encapsulation instead of **RFC-1483**, so you do not need to reconfigure either computer later.

Scenario 3. Multiple VCs

If you have an equal number (or more) of VCs than the number of protocols, then select **RFC-1483** encapsulation and **VC-based** multiplexing.

Menu 11.1 - Remote Node Profile

Rem Node Name= myISP Active= Yes Encapsulation= RFC-1483 Multiplexing= VC-based Incoming: Rem Login= N/A Rem Password= N/A Outgoing: My Login= N/A My Password= N/A Authen= N/A	Route= IP Bridge= No Edit IP/Bridge= No Edit ATM Options= No Telco Option: Allocated Budget(min)= N/A Period(hr)= N/A Schedule Sets= N/A Nailed-Up Connection= N/A Session Options: Edit Filter Sets= No Idle Timeout(sec)= N/A
---	--

DELETE PROFILE:

Press Space Bar to Toggle.

Edit IP/Bridge Options
in menu 11.3.

Edit ATM Options in
menu 11.6.

Edit Filter Sets in menu
11.5.

Figure 8-2 Remote Node Profile

Table 8-1 Remote Node Profile

FIELD	DESCRIPTION	EXAMPLE
Rem Node Name	Type a unique, descriptive name of up to eight characters for this node.	myISP
Active	Press [SPACE BAR] and then [ENTER] to select Yes to activate or No to deactivate this node. Inactive nodes are displayed with a minus sign “-“ in SMT menu 11.	Yes
Encapsulation	PPPoA refers to RFC-2364 (PPP Encapsulation over ATM Adaptation Layer 5). PPPoE refers to RFC 2516 (PPP Encapsulation over Ethernet). If RFC-1483 (Multiprotocol Encapsulation over ATM Adaptation Layer 5) or ENET ENCAP are selected, then the Rem Login , Rem Password , My Login , My Password and Authen fields are not applicable (N/A).	ENET ENCAP
Multiplexing	Press [SPACE BAR] and then [ENTER] to select the method of multiplexing that your ISP uses, either VC-based or LLC-based .	LLC-based
Service Name	When using PPPoE encapsulation, type the name of your PPPoE service here.	N/A
Incoming: Rem Login	Type the login name that this remote node will use to call your Prestige. The login name and the Rem Password will be used to authenticate this node.	

Table 8-1 Remote Node Profile

FIELD	DESCRIPTION	EXAMPLE
Rem Password	Type the password used when this remote node calls your Prestige.	
Outgoing: My Login	Type the login name assigned by your ISP when the Prestige calls this remote node.	
My Password	Type the password assigned by your ISP when the Prestige calls this remote node.	
Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are: CHAP/PAP – Your Prestige will accept either CHAP or PAP when requested by this remote node. CHAP – accept CHAP (Challenge Handshake Authentication Protocol) only. PAP – accept PAP (Password Authentication Protocol) only.	CHAP
Route	This field determines the protocol used in routing. Options are IP and None .	IP
Bridge	When bridging is enabled, your Prestige will forward any packet that it does not route to this remote node; otherwise, the packets are discarded. Select Yes to enable and No to disable.	No
Edit IP/Bridge	Press [SPACE BAR] to select Yes and press [ENTER] to display Menu 11.3 – Remote Node Network Layer Options .	No
Edit ATM Options	Press [SPACE BAR] to select Yes and press [ENTER] to display Menu 11.6 – Remote Node ATM Layer Options .	No
Telco Option Allocated Budget (min)	This sets a ceiling for outgoing call time for this remote node. The default for this field is 0 meaning no budget control.	10
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).	1

Table 8-1 Remote Node Profile

FIELD	DESCRIPTION	EXAMPLE
Schedule Sets	This field is only applicable for PPPoE and PPPoA encapsulation. You can apply up to four schedule sets here. For more details please refer to the <i>Call Schedule Setup</i> chapter.	
Nailed up Connection	This field is only applicable for PPPoE and PPPoA encapsulation. This field specifies if you want to make the connection to this remote node a nailed-up connection. More details are given earlier in this section.	
Session Options Edit Filter Sets	Use [SPACE BAR] to choose Yes and press [ENTER] to open menu 11.5 to edit the filter sets. See the <i>Remote Node Filter</i> section for more details.	No (default)
Idle Timeout (sec)	Type the number of seconds (0-9999) that can elapse when the Prestige is idle (there is no traffic going to the remote node), before the Prestige automatically disconnects the remote node. 0 means that the session will not timeout.	
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.		

8.2.2 Outgoing Authentication Protocol

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

8.3 Remote Node Network Layer Options

Perform the following steps to edit **Menu 11.3 – Remote Node Network Layer Options** as shown next.

Step 1. In menu 11.1, make sure **IP** is among the protocols in the **Route** field.

Step 2. Move the cursor to the **Edit IP/Bridge** field, press [SPACE BAR] to select **Yes**, then press [ENTER] to display **Menu 11.3 – Remote Node Network Layer Options**.

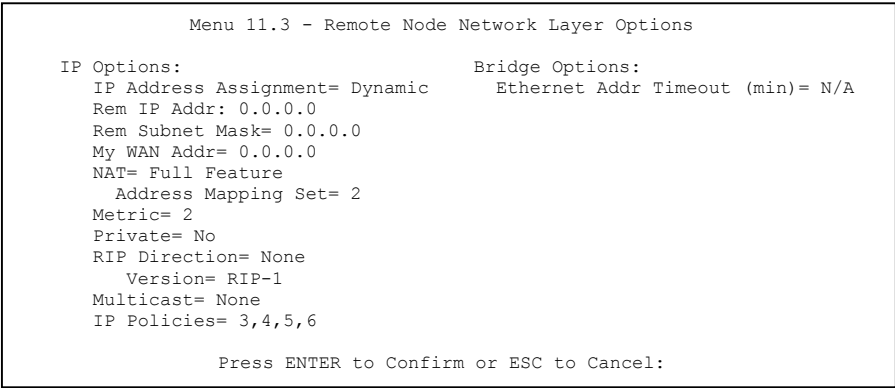


Figure 8-3 Remote Node Network Layer Options

Table 8-2 Remote Node Network Layer Options

FIELD	DESCRIPTION	EXAMPLE
IP Options		
IP Address Assignment	Press [SPACE BAR] and then [ENTER] to select Dynamic if the remote node is using a dynamically assigned IP address or Static if it is using a static (fixed) IP address. You will only be able to configure this in the ISP node (also the one you configure in Menu 4). All other nodes are set to Static .	Dynamic
Rem IP Addr	This is the IP address you entered in the previous menu.	
Rem Subnet Mask	Type the subnet mask assigned to the remote node.	
My WAN Addr	Some implementations, especially UNIX derivatives, require separate IP network numbers for the WAN and LAN links and each end to have a unique address within the WAN network number. In that case, type the IP address assigned to the WAN port of your Prestige. This address refers to the local Prestige address, not the remote router address.	

Table 8-2 Remote Node Network Layer Options

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. Select SUA Only if you have just one public WAN IP address for your Prestige. The SMT uses Address Mapping Set 255 (menu 15.1 - see section 11.3.1). Select None to disable NAT.	SUA Only
Address Mapping Set	When Full Feature is selected in the NAT field, configure address mapping sets in menu 15.1. Select one of the NAT server sets (2-10) in menu 15.2 (see the <i>NAT</i> chapter for details) and type that number here. When SUA Only is selected in the NAT field, the SMT uses NAT server set 1 in menu 15.2 (see the <i>NAT</i> chapter for details).	2
Metric	The metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the cost measurement, with a minimum of 1 for directly connected networks. Type a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.	2
Private	This determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to Yes , this route is kept private and not included in RIP broadcast. If No , the route to this remote node will be propagated to other hosts through RIP broadcasts.	No
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
Multicast	IGMP-v1 sets IGMP to version 1, IGMP-v2 sets IGMP to version 2 and None disables IGMP.	None
IP Policies	You can apply up to four IP Policy sets (from 12) by typing in their numbers separated by commas. Configure the filter sets in menu 25 first (see the <i>IP Policy Routing</i> chapter) and then apply them here.	3, 4, 5, 6
Bridge Options		
Ethernet Addr Timeout (min)	See the chapter on Bridging Setup for information on bridging.	
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.		

8.3.1 My WAN Addr Sample IP Addresses

The following diagram explains the sample IP addresses to help you understand the field of **My Wan Addr** in Menu 11.3. **My WAN Addr** indicates the local Prestige WAN IP while **Rem IP Addr** indicates the peer WAN IP.

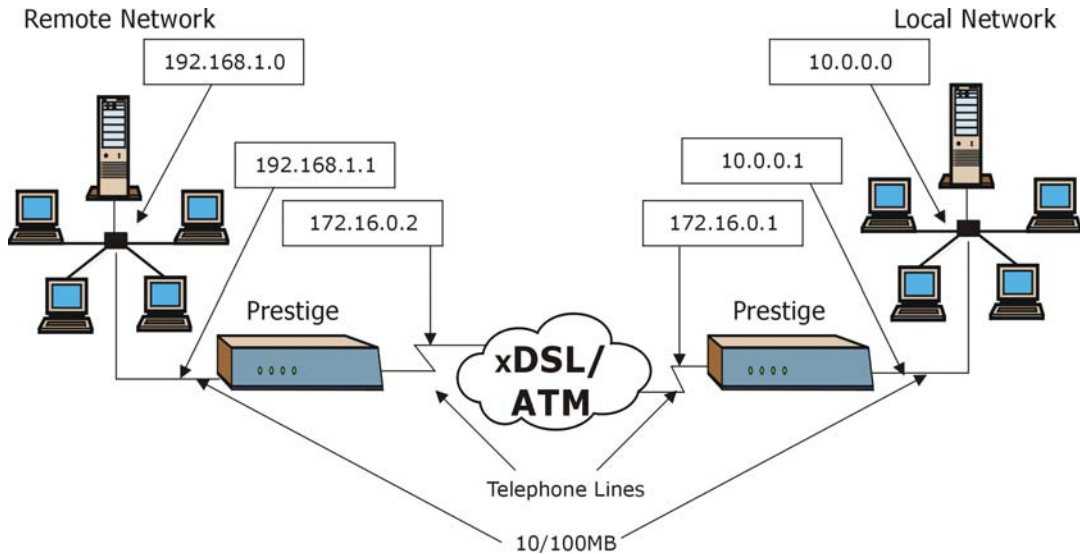


Figure 8-4 Sample IP Addresses for a TCP/IP LAN-to-LAN Connection

8.4 Remote Node Filter

Move the cursor to the **Edit Filter Sets** field in menu 11.1, then press [SPACE BAR] to select **Yes**. Press [ENTER] to display **Menu 11.5 – Remote Node Filter**.

Use **Menu 11.5 – Remote Node Filter** to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the Prestige and also to prevent certain packets from triggering calls. You can specify up to 4 filter sets separated by comma, for example, 1, 5, 9, 12, in each filter field.

Note that spaces are accepted in this field. The Prestige has prepackaged filter sets; refer to the chapter on Filter Configuration for details. Include these in the call filter sets if you want to prevent NetBIOS packets from triggering calls to a remote node.

```
Menu 11.5 - Remote Node Filter

Input Filter Sets:
  protocol filters= 12, 11
  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 8-5 Remote Node Filter (PPPoA or PPPoE Encapsulation)

```
Menu 11.5 - Remote Node Filter

Input Filter Sets:
  protocol filters= 12, 11
  device filters=
Output Filter Sets:
  protocol filters=
  device filters=

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

Figure 8-6 Remote Node Filter (RFC1483 or ENET ENCAP Encapsulation)

8.4.1 Web Configurator Internet Security Filter Rules

In the web configurator, open the **Internet Security** screen as shown next. Select the predefined filter rules and click **Apply**.

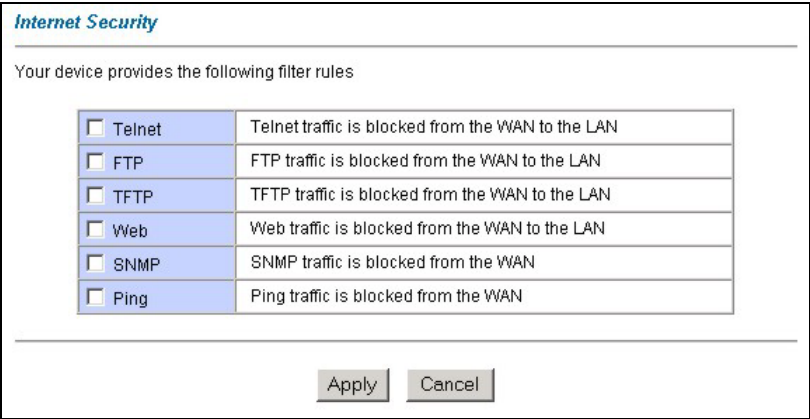


Figure 8-7 Internet Security

Once you apply the filter rules in the web configurator, filter sets 11 and 12 are automatically applied in the **protocol filters** field under **Input Filter Sets** in SMT menu 11.5.

SMT input protocol filter set numbers that were previously applied are erased after you apply the Internet Security filter rules in the web configurator. To reapply them or apply new filter sets, you need to enter the filter set numbers again along with filter sets 11 and 12. For example, to apply filter sets 1 and 2, you enter “1, 2, 11, 12”.

8.4.2 Web Configurator Filter Sets

When you apply filter rules using the web configurator, filter sets 11 and 12 are automatically generated in SMT menu 21.

```

Menu 21 - Filter Set Configuration

Filter Set #      Comments      Filter Set #      Comments
-----
1      NetBIOS_WAN
2      NetBIOS_LAN
3      TELNET_WAN
4      PPPoE
5      FTP_WAN
6      _____

Enter Filter Set Number to Configure= 0
Edit Comments= N/A
Press ENTER to Confirm or ESC to Cancel:

```

Figure 8-8 Menu 21- Filer Set Configuration

The following figures display the filter rules in filter sets 11 and 12.

```

Menu 21.11 - Filter Rules Summary
Filter Rules
# A Type ----- M m n
- - -
1 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=161      N D N
2 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=162      N D F
3 N
4 N
5 N
6 N

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

```

Figure 8-9 Menu 21.11- WebSet 11

```

Menu 21.12 - Filter Rules Summary
Filter Rules
# A Type ----- M m n
- - -
1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23      N D N
2 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=21      N D N
3 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=69      N D N
4 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=80      N D N
5 Y IP   Pr=1, SA=0.0.0.0, DA=0.0.0.0, DP=0        N D N
6 N

Enter Filter Rule Number (1-6) to Configure

```

Figure 8-10 Menu 21.12- WebSet 12

Do not edit filter sets 11 and 12. They are used exclusively by the web configurator. Any rules you configured in sets 11 and 12 will be erased and replaced when you apply the web configurator-generated filter rules.

8.5 Editing ATM Layer Options

Follow these steps to edit **Menu 11.6 – Remote Node ATM Layer Options**.

- Step 1.** In Menu 11.1, move the cursor to the **Edit ATM Options** then press [SPACE BAR] to toggle and set the value to **Yes**.
- Step 2.** Press [ENTER] to open **Menu 11.6 – Remote Node ATM Layer Options**.

There are two versions of Menu 11.6 for the Prestige, depending on whether you chose **VC-based** or **LLC-based** multiplexing and **PPP** (either PPPoA or PPPoE) encapsulation in menu 11.1.

8.5.1 VC-based Multiplexing (non-PPP Encapsulation)

For **VC-based** multiplexing, by prior agreement, a protocol is assigned a specific virtual circuit, e.g., VC1 will carry IP, VC2 will carry IPX, etc. Separate VPI and VCI numbers must be specified for each protocol.

Menu 11.6 - Remote Node ATM Layer Options
VPI/VCI (VC-Multiplexing)

VC Options for IP:

VC Options for Bridge:

VPI # = 0
VCI # = 38

VPI # = N/A
VCI # = N/A

ATM QoS Type = UBR
Peak Cell Rate (PCR) = 0
Sustain Cell Rate (SCR) = 0
Maximum Burst Size (MBS) = 0

ATM QoS Type = N/A
Peak Cell Rate (PCR) = N/A
Sustain Cell Rate (SCR) = N/A
Maximum Burst Size (MBS) = N/A

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

Separate VPI and VCI numbers must be specified.

Figure 8-11 Menu 11.6 for VC-based Multiplexing (non-PPP Encapsulation)

8.5.2 LLC-based Multiplexing or PPP Encapsulation

For **LLC-based** multiplexing or **PPP** encapsulation, one VC carries multiple protocols with protocol identifying information being contained in each packet header.

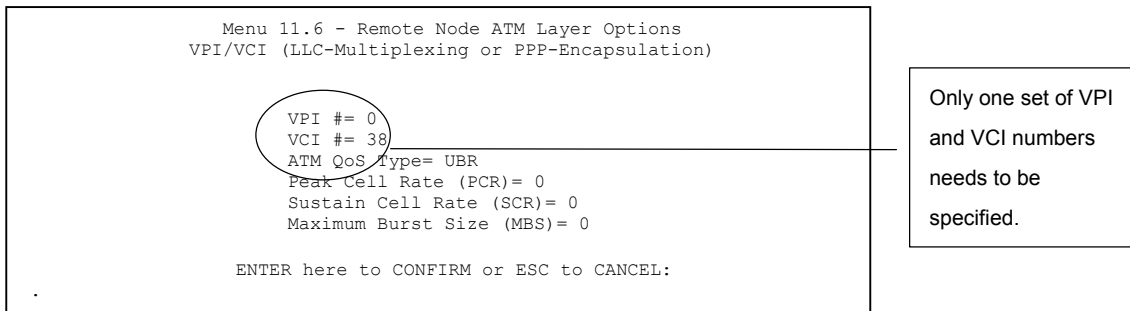


Figure 8-12 Menu 11.6 for LLC-based Multiplexing or PPP Encapsulation

In this case, only one set of VPI and VCI numbers need be specified for all protocols. The valid range for the VPI is 0 to 255 and for the VCI is 32 to 65535 (1 to 31 is reserved for local management of ATM traffic).

Chapter 9

Static Route Setup

This chapter shows how to setup IP static routes.

9.1 Static Route Overview

Static routes tell the Prestige routing information that it cannot learn automatically through other means. This can arise in cases where RIP is disabled on the LAN or a remote network is beyond the one that is directly connected to a remote node.

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

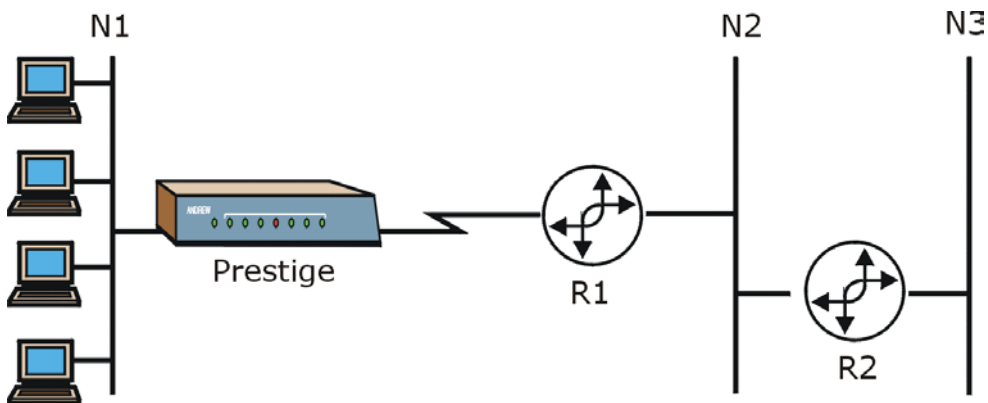


Figure 9-1 Sample Static Routing Topology Configuration

Step 1. To configure an IP static route, use **Menu 12 – Static Route Setup** (shown next). See the bridging chapter for more information on Bridge Static Routes.

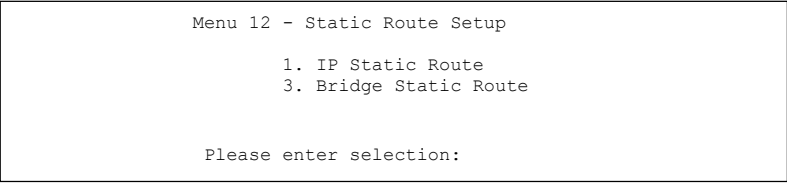


Figure 9-2 Static Route Setup

Step 2. From Menu 12, select **1** to open **Menu 12.1 – IP Static Route Setup**, as shown next.

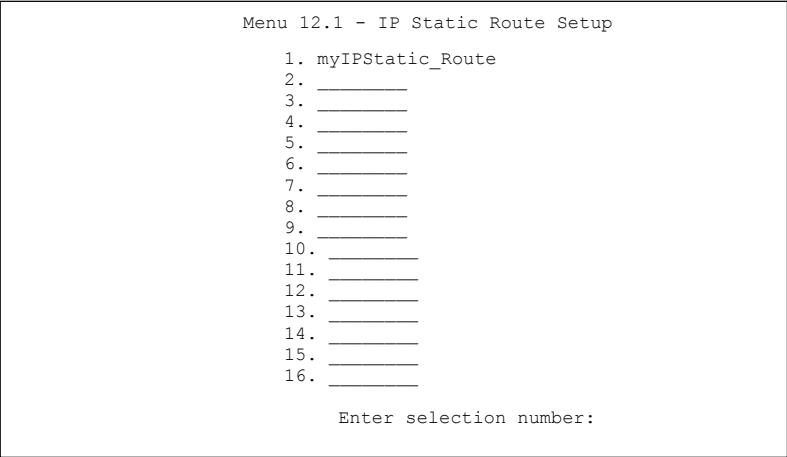


Figure 9-3 IP Static Route Setup

Now, type the index number of one of the static routes you want to configure.

```

Menu 12.1.1 - Edit IP Static Route

Route #: 1
Route Name= myIPStatic_Route
Active= No
Destination IP Address= ?
IP Subnet Mask= ?
Gateway IP Address= ?
Metric= 2
Private= No

Press ENTER to Confirm or ESC to Cancel:

```

Figure 9-4 Edit IP Static Route**Table 9-1 Edit IP Static Route**

FIELD	DESCRIPTION
Route #	This is the index number of the static route that you chose in menu 12.1.
Route Name	Type a descriptive name for this route. This is for identification purpose only.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Type the subnet mask for this destination. Follow the discussion on <i>IP Subnet Mask</i> in this manual.
Gateway IP Address	Type the IP address of the gateway. The gateway is an immediate neighbor of your Prestige that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your Prestige; over WAN, the gateway must be the IP address of one of the remote nodes.
Metric	Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Type a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Private	This parameter determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to 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 10

Bridging Setup

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

10.1 Bridging Overview

Bridging bases the forwarding decision on the MAC (Media Access Control), or hardware address, while routing does it on the network layer (IP) address. Bridging allows the Prestige to transport packets of network layer protocols that it does not route, for example, SNA, from one network to another. The caveat is that, compared to routing, bridging generates more traffic for the same network layer protocol, and it also demands more CPU cycles and memory.

For efficiency reasons, do *not* turn on bridging unless you need to support protocols other than IP on your network. For IP, enable the routing if you need it; do not bridge what the Prestige can route.

10.2 Bridge Ethernet Setup

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

10.2.1 Remote Node Bridging Setup

Follow the procedure in another section to configure the protocol-independent parameters in **Menu 11.1 – Remote Node Profile**. For bridging-related parameters, you need to configure **Menu 11.3 – Remote Node Network Layer Options**.

To setup **Menu 11.3 – Remote Node Network Layer Options** shown in the next figure, follow these steps:

- Step 1.** In menu 11.1, make sure the **Bridge** field is set to **Yes**.
- Step 2.** Move the cursor to the **Edit IP/Bridge** field, then press [SPACE BAR] to set the value to **Yes** and press [ENTER] to edit **Menu 11.3 – Remote Node Network Layer Options**.

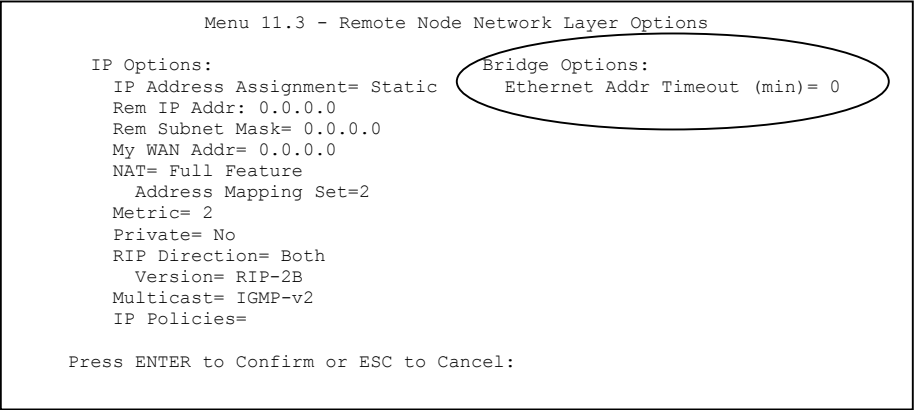


Figure 10-1 Remote Node Bridging Options

Table 10-1 Remote Node Bridging Options

FIELD	DESCRIPTION
Bridge (menu 11.1)	Make sure this field is set to Yes .
Edit IP/Bridge (menu 11.1)	Press [SPACE BAR] to select Yes and press [ENTER] to display menu 11.3.
Ethernet Addr Timeout (min.) (menu 11.3)	Type the time (in minutes) for the Prestige to retain the Ethernet Address information in its internal tables while the line is down. If this information is retained, your Prestige will not have to recompile the tables when the line comes back up.
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.	

10.2.2 Bridge Static Route Setup

Similar to IP layer static routes, a bridging static route tells the Prestige the route to a node before a connection is established. Go to menu 12, choose option 3 to see menu 12.3 shown next.

```

Menu 12.3 - Bridge Static Route Setup

1. _____
2. _____
3. _____
4. _____

Enter selection number:

```

Figure 10-2 Bridge Static Route Setup

Choose a static route to edit in menu 12.3. You configure bridge static routes in menu 12.3.1 as shown next.

```

Menu 12.3.1 - Edit Bridge Static Route

Route #: 1
Route Name=
Active= No
Ether Address= ?
IP Address=
Gateway Node= 1

Press ENTER to Confirm or ESC to Cancel:

```

Figure 10-3 Edit Bridge Static Route**Table 10-2 Edit Bridge Static Route**

FIELD	DESCRIPTION
Route #	This is the route index number you typed in Menu 12.3 – Bridge Static Route Setup .
Route Name	Type a name for the bridge static route for identification purposes.
Active	Indicates whether the static route is active (Yes) or not (No).
Ether Address	Type the MAC address of the destination computer that you want to bridge the packets to.
IP Address	If available, type the IP address of the destination computer that you want to bridge the packets to.
Gateway Node	Press [SPACE BAR] and then [ENTER] to select the number of the remote node (one to eight) that is the gateway of this static route.

FIELD	DESCRIPTION
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 11

Network Address Translation (NAT)

This chapter discusses how to configure NAT on the Prestige.

11.1 NAT Overview

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

11.1.1 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 11-1 NAT Definitions

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

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

11.1.2 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. Although you can make designated servers on the LAN accessible to the outside world, it is strongly recommended that you attach those servers to the DMZ port instead. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping – see *Table 11-2*), 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)*.

11.1.3 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.

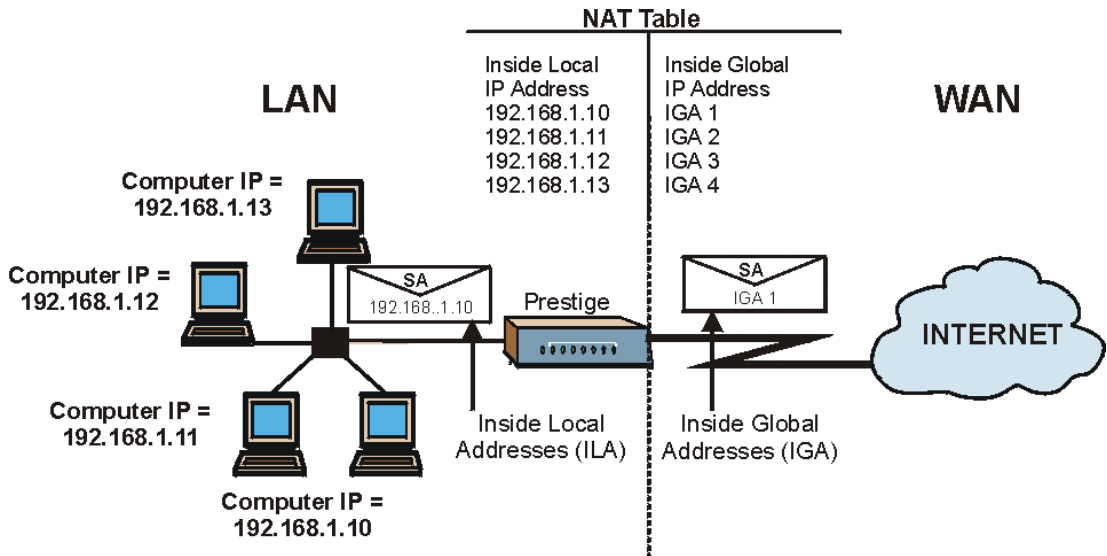


Figure 11-1 How NAT Works

11.1.4 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.

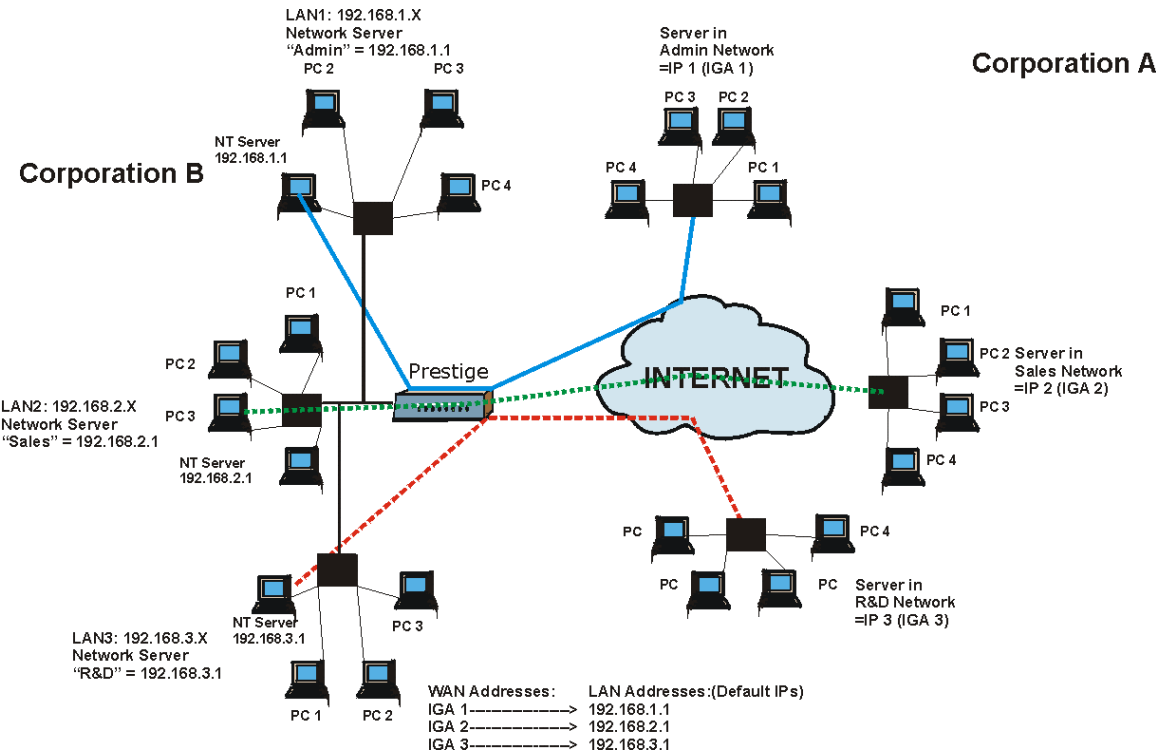


Figure 11-2 NAT Application With IP Alias

11.1.5 NAT Mapping Types

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

1. **One to One:** In One-to-One mode, the Prestige maps one local IP address to one global IP address.
2. **Many to One:** In Many-to-One mode, the Prestige maps multiple local IP addresses to one global IP address. This is equivalent to SUA (for instance, PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported (the **SUA Only** option in today's routers).
3. **Many to Many Overload:** In Many-to-Many Overload mode, the Prestige maps the multiple local IP addresses to shared global IP addresses.

4. **Many-to-Many No Overload:** In Many-to-Many No Overload mode, the Prestige maps each local IP address to a unique global IP address.
5. **Server:** This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world although, it is highly recommended that you use the DMZ port for these servers instead.

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

The following table summarizes these types.

Table 11-2 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-to-Many No Overload	ILA1↔ IGA1 ILA2↔ IGA2 ILA3↔ IGA3 ...	M:M No OV
Server	Server 1 IP↔ IGA1 Server 2 IP↔ IGA1 Server 3 IP↔ IGA1	Server

11.1.6 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 11.3.1 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 as outlined in *Table 11-2*.

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.**

11.2 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**. Use the space bar to toggle through the selections for NAT and choose the option you want.

```
Menu 4 - Internet Access Setup

ISP's Name= test
Encapsulation= RFC 1483
Multiplexing= LLC-based
VPI #= 1
VCI #= 1
Service Name= N/A
My Login= N/A
My Password= N/A
NAT= SUA Only
Address Mapping Set= N/A
IP Address Assignment= Static
IP Address= 0.0.0.0
ENET ENCAP Gateway= N/A

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 11-3 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 and choose a node number.

Step 2. Move the cursor to the **Edit IP/IPX/Bridge** field, press [SPACE BAR] to select **Yes** and then press [ENTER] to bring up **Menu 11.3 - Remote Node Network Layer Options**. Use the space bar to toggle through the selections for NAT and choose the option you want.

```

Menu 11.3 - Remote Node Network Layer Options

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

Enter here to CONFIRM or ESC to CANCEL:

```

Figure 11-4 Applying NAT to the Remote Node

Table 11-3 Applying NAT to the Remote Node

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 11.3.1).	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 11.3.1). Choose SUA Only if you have just one public WAN IP address for your Prestige.	SUA Only

11.3 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. You can see two NAT Address Mapping sets in menu 15.1. You can only configure **Set 1**. **Set 255** is used for SUA. When you select **Full Feature** in menu 4 or 11.3, the

SMT will use **Set 1**, which supports all mapping types as outlined in Table 11-2. When you select **SUA Only**, the SMT will use the pre-configured **Set 255** (read only).

The Server Set is a list of LAN side servers mapped to external ports. To use this set (one set for the Prestige 10), a server rule must be set up inside the NAT Address Mapping set. Please see *section 11.4* for further information on these menus. To configure NAT, enter 15 from the main menu to bring up the following screen.

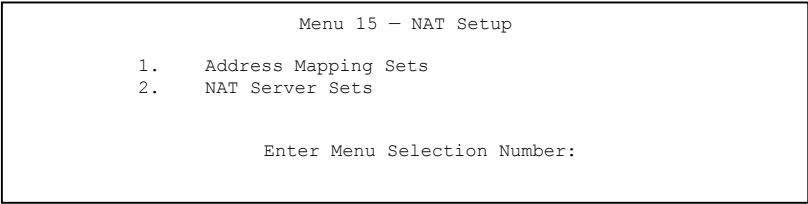


Figure 11-5 NAT Setup

11.3.1 Address Mapping Sets

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

```

Menu 15.1 - Address Mapping Sets

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

Enter Menu Selection Number:

Enter Menu Selection Number:

```

Figure 11-6 Address Mapping Sets

Enter 255 to display the next screen (see also *section 11.1.6*). The fields in this menu cannot be changed.

```

Menu 15.1.255 - Address Mapping Rules

Set Name=

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

Press ENTER to Confirm or ESC to Cancel:

```

Figure 11-7 Address Mapping Rules - SUA**Table 11-4 Address Mapping Rules - SUA**

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

Table 11-4 Address Mapping Rules - SUA

FIELD	DESCRIPTION	EXAMPLE
Idx	This is the index or rule number.	1
Local Start IP Local End IP	Local Start IP is the starting local IP address (ILA) (see <i>Figure 11-1</i>). 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.	0.0.0.0 255.255.255.255
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 discussed above (see <i>Table 11-2</i>). Server allows us to specify multiple servers of different types behind NAT to this machine. See later for some examples.	Server
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= ?

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 11-8 Address Mapping Rules

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 11-5 Address Mapping Rules

FIELD	DESCRIPTION	EXAMPLE
Set Name	Enter a name for this set of rules. This is a required field. If this field	NAT_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=
  End  = N/A

Global IP:
  Start=
  End  = N/A

Server Mapping Set= N/A

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

```

Figure 11-9 Editing/Configuring an Individual Rule in a Set**Table 11-6 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 Table 11-2. Server allows you to specify multiple servers of different types behind NAT to this computer. See <i>section 11.5.3</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 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 global IP address (IGA). This field is N/A for One-to-One , Many-to-One and Server types.	N/A
Server Mapping Set	Only available when Type is set to Server . Type a number from 1 to 10 to choose a server set from menu 15.2.	
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

11.4 NAT Server Sets – Port Forwarding

A NAT 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 NAT makes your whole inside network appear as a single machine to the outside world.

Use **Menu 15 - NAT Setup** 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 included disk for more examples and details on NAT.

Table 11-7 Services & Port Numbers

SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21
Telnet	23
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79

SERVICES	PORT NUMBER
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

11.4.1 Configuring a Server behind NAT

Follow these steps to configure a server behind NAT:

Step 3. Enter 15 in the main menu to go to **Menu 15 - NAT Setup**.

Step 4. Enter 2 to display **Menu 15.2 - NAT Server Sets** as shown next.

```
Menu 15.2 - NAT Server Sets

1. Server Set 1 (Used for SUA Only)
2. Server Set 2
3. Server Set 3
4. Server Set 4
5. Server Set 5
6. Server Set 6
7. Server Set 7
8. Server Set 8
9. Server Set 9
10. Server Set 10

Enter Set Number to Edit:
```

Figure 11-10 NAT Server Sets

Step 5. Enter 1 to go to **Menu 15.2 NAT Server Setup** as follows.

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 11-11 NAT Server Setup

- Step 6.** 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 7.** 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 8.** 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.

The NAT network appears as
a single host on the Internet

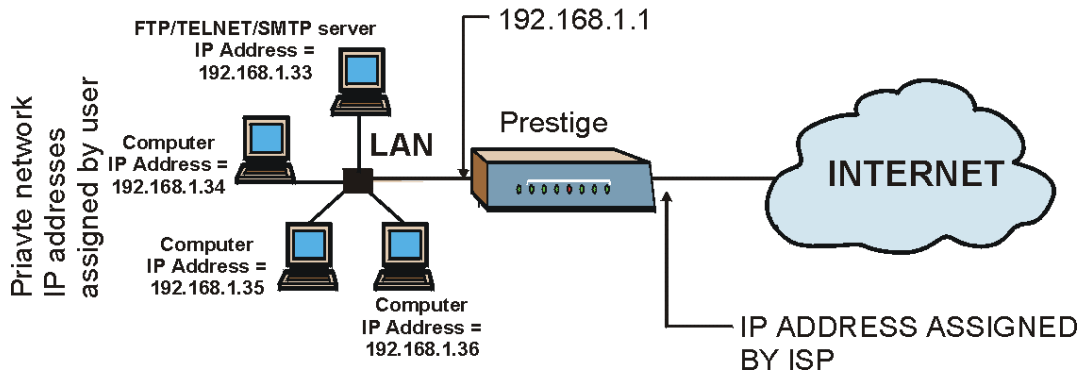


Figure 11-12 Multiple Servers Behind NAT Example

11.5 General NAT Examples

This section provides some examples with Network Address Translation.

11.5.1 Example 1: Internet Access Only

In the following Internet access example, you only need one rule where your ILAs (Inside Local addresses) all map to one dynamic IGA (Inside Global Address) assigned by your ISP.

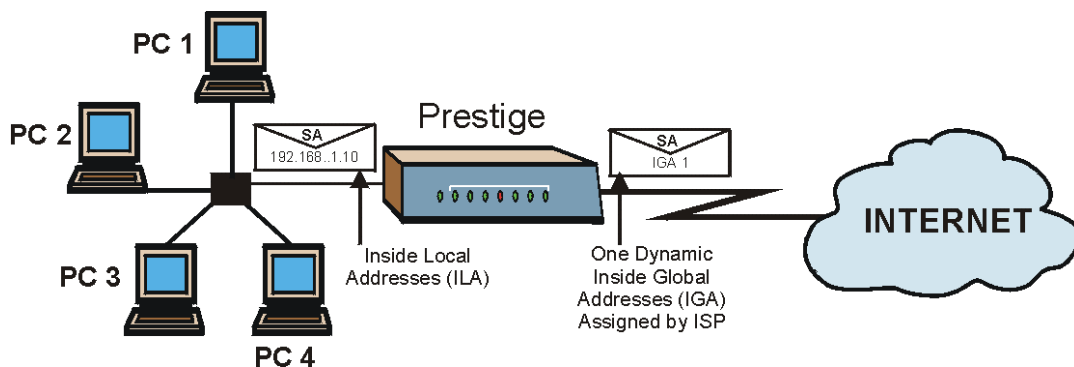


Figure 11-13 NAT Example 1

```

Menu 4 - Internet Access Setup

ISP's Name= ChangeMe
Encapsulation= RFC-1483
Multiplexing= LLC-based
VPI #= 1
VCI #= 1
ATM QoS Type= UBR
  Peak Cell Rate (PCR)= 5500
  Sustained Cell Rate (SCR)= 0
  Maximum Burst Size (MBS)= 0
My Login= N/A
My Password= N/A
ENET ENCAP Gateway= N/A
IP Address Assignment= Static
  IP Address= 0.0.0.0
  Network Address Translation= SUA Only
  Address Mapping Set=
    
```

Figure 11-14 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 11.5*. 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.

11.5.2 Example 2: Internet Access with an Inside Server

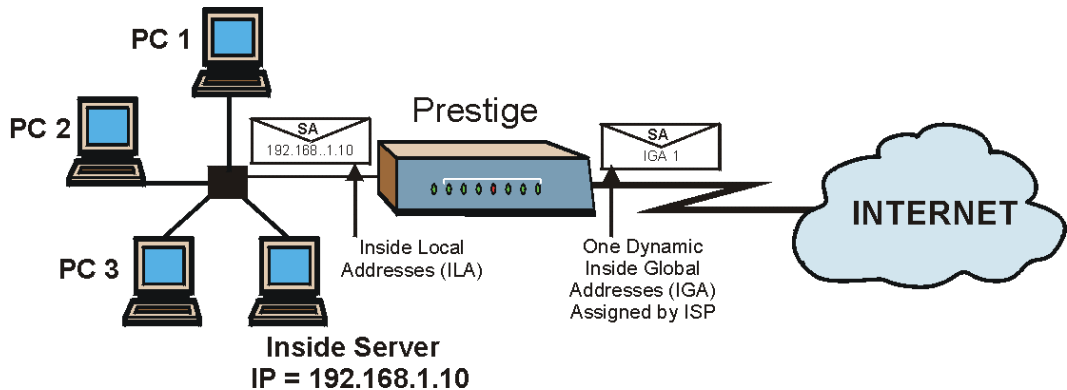
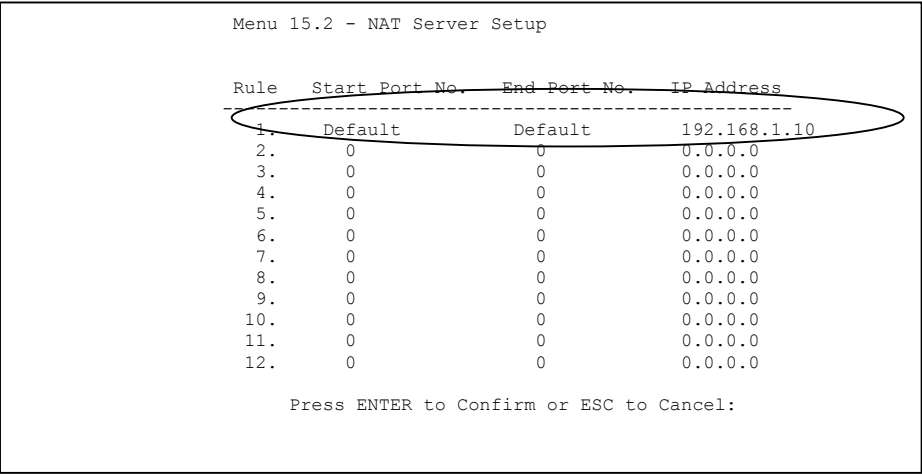


Figure 11-15 NAT Example 2

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 - 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 11-16 NAT Example 2 - Menu 15.2.1

11.5.3 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 uni-directional 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:

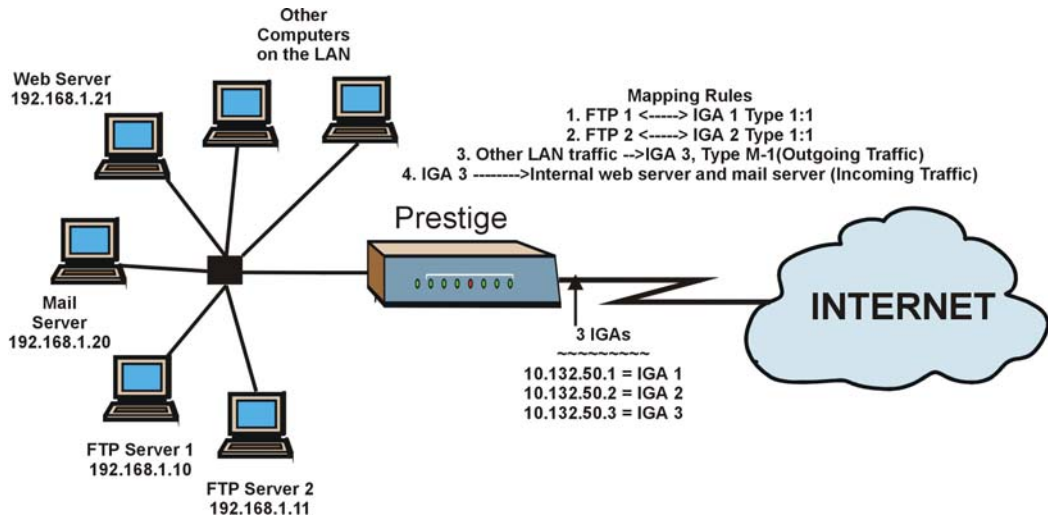


Figure 11-17 NAT Example 3

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). See the figure below.

```

Menu 11.3 - Remote Node Network Layer Options

IP Options:                               Bridge Options:
IP Address Assignment= Static              Ethernet Addr Timeout (min)= 0
Rem IP Addr= 0.0.0.0
Rem Subnet Mask= 0.0.0.0
My WAN Addr= 0.0.0.0
NAT= Full Feature
Address Mapping Set= 2
Metric= 2
Private= No
RIP Direction= Both
Version= RIP-2B
Multicast= IGMP-v2
IP Policies=

Press ENTER to Confirm or ESC to Cancel:

```

Figure 11-18 Example 3 - Menu 11.3

- 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.** In menu 15.1.1.1, select **Type** as **One-to-One** (direct mapping for packets going both ways), and set the local **Start IP** as 192.168.1.10 (the IP address of FTP Server 1) and the global **Start IP** as 10.132.50.1 (our first IGA). See the figure below.

```
Menu 15.1.1.1 Address Mapping Rule

Type= One-to-One
Local IP:
  Start= 192.168.1.10
  End   = N/A
Global IP:
  Start= 10.132.50.1
  End   = N/A
Server Mapping Set= N/A

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

Figure 11-19 Example 3 - Menu 15.1.1.1

- Step 6.** Repeat the previous step for rules 2 to 4 as outlined above.
- Step 7.** When finished, menu 15.1.1 should look as follows.

Menu 15.1.1 - Address Mapping Rules

Set Name= Example3

Idx	Local Start IP	Local End IP	Global Start IP	Global End IP	Type
1.	192.168.1.10		10.132.50.1		1-1
2.	192.168.1.11		10.132.50.2		1-1
3.	0.0.0.0	255.255.255.255	10.132.50.3		M-1
4.			10.132.50.3		Server
5.					
6.					
7.					
8.					
9.					
10.					

Action= Edit Select Rule=

Press ENTER to Confirm or ESC to Cancel:

Figure 11-20 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** and enter 1 again to see the following menu.
Configure it as shown.

Menu 15.2 - NAT Server Setup

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

Press ENTER to Confirm or ESC to Cancel:

Figure 11-21 Example 3- Menu 15.2

11.5.4 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.

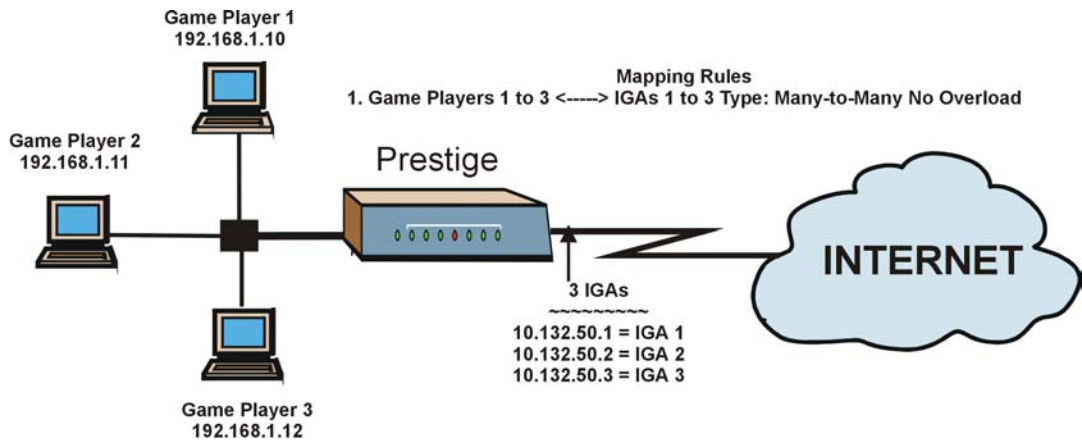


Figure 11-22 NAT Example 4

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-to-Many No Overload

Local IP:
  Start= 192.168.1.10
  End  = 192.168.1.12

Global IP:
  Start= 10.132.50.1
  End  = 10.132.50.3

Server Mapping Set= N/A

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

Figure 11-23 Example 4 - Menu 15.1.1.1

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 11-24 Example 4 - Menu 15.1.1

Part III:

ADVANCED MANAGEMENT

This part discusses Filter Configuration, SNMP, System Maintenance and IP Policy Routing, Call Scheduling and Remote Management.

Chapter 12

Filter Configuration

This chapter shows you how to create and apply filters.

12.1 Filtering Overview

Your Prestige uses filters to decide whether or not to allow passage of a data packet and/or to make a call. There are two types of filter applications: data filtering and call filtering. Filters are subdivided into device and protocol filters, which are discussed later.

Data filtering screens 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 Ethernet side. Call filtering is used to determine if a packet should be allowed to trigger a call.

Outgoing packets must undergo data filtering before they encounter call filtering. Call filters are divided into two groups, the built-in call filters and user-defined call filters. Your Prestige has built-in call filters that prevent administrative, e.g., RIP packets from triggering calls. These filters are always enabled and not accessible to you. Your Prestige applies the built-in filters first and then the user-defined call filters, if applicable, as shown next.

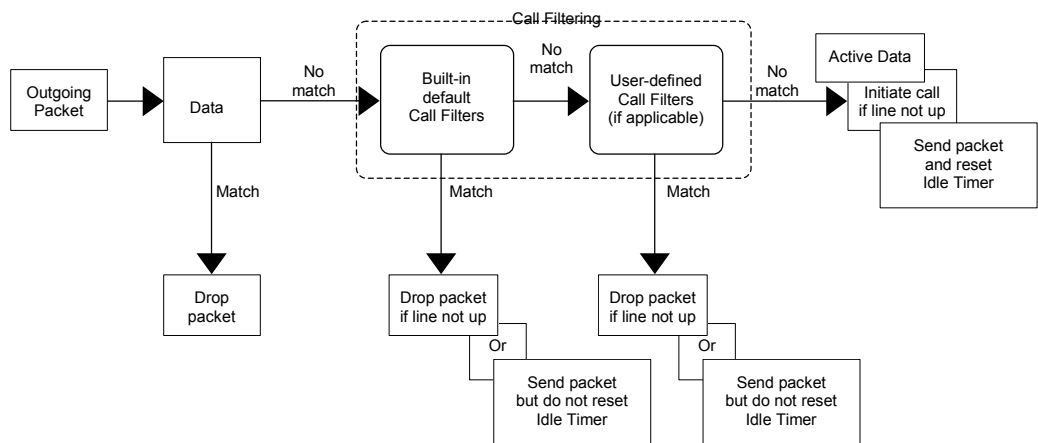


Figure 12-1 Outgoing Packet Filtering Process

Two sets of factory filter rules have been configured in Menu 21 to prevent NetBIOS traffic from triggering calls. A summary of their filter rules is shown in the figures that follow.

The following figure illustrates the logic flow when executing a filter rule.

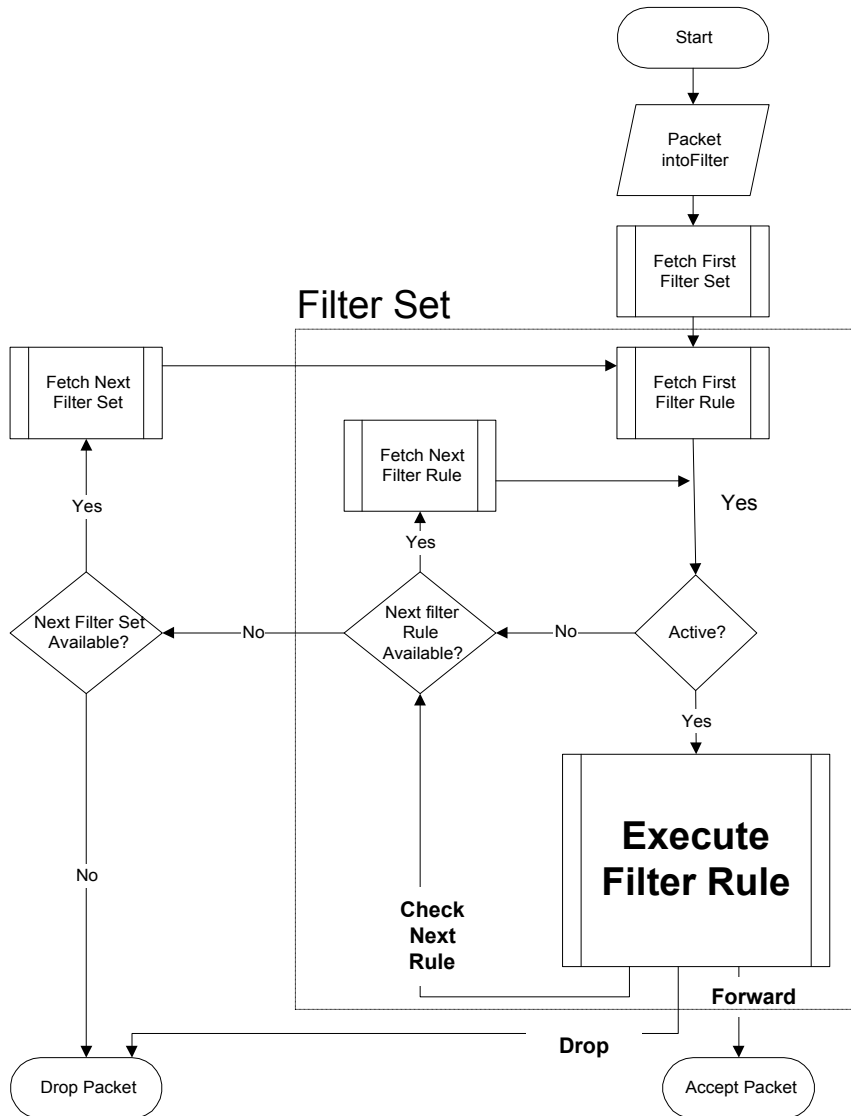


Figure 12-2 Filter Rule Process

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

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

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. You can configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system.

You can apply up to 4 filter sets to a particular port to block multiple types of packets. Because each filter set can have up to 6 rules, you can have a maximum of 24 rules active for a single port.

12.2 Filter Set Configuration

To configure a filter set, follow the procedures indicated:

Step 1. Type 21 in the main menu to open Menu 21.

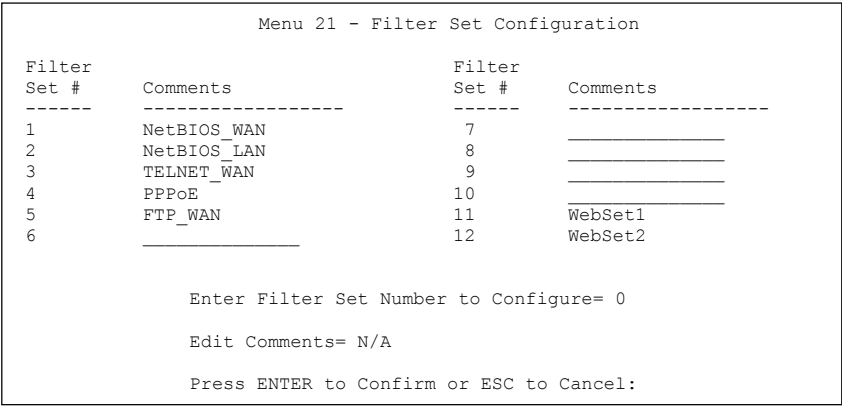


Figure 12-3 Filter Set Configuration

Step 2. Type the filter set to configure (no. 1 to 12) and press [ENTER].

Filter rule set 11 and 12 are used by the web configurator. Your custom configurator may be lost if you use rule 11 or 12.

Step 3. Type a descriptive name or comment in the **Edit Comments** field and press [ENTER].

Step 4. Press [ENTER] at the message “Press ENTER to confirm...” to display **Menu 21.1 – Filter Rules Summary** (that is, if you selected filter set 1 in menu 21).

Menu 21.1 - Filter Rules Summary						
#	A	Type	Filter Rules			M m n
1	Y	IP	Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=137			N D N
2	Y	IP	Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=138			N D N
3	Y	IP	Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=139			N D N
4	Y	IP	Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=137			N D N
5	Y	IP	Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=138			N D N
6	Y	IP	Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=139			N D F

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

Figure 12-4 NetBios WAN Filter Rules Summary

Menu 21.2 - Filter Rules Summary						
#	A	Type	Filter Rules			M m n
1	Y	IP	Pr=17, SA=0.0.0.0, SP=137, DA=0.0.0.0, DP=53			N D F
2	Y					
3	Y					
4	Y					
5	Y					
6	Y					

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

Figure 12-5 NetBios LAN Filter Rules Summary

Menu 21.3 - Filter Rules Summary			
#	A	Type	Filter Rules
1	Y	IP	Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23
2	N		
3	N		
4	N		
5	N		
6	N		

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

Figure 12-6 Telnet_WAN Filter Rules Summary

Menu 21.4 - Filter Rules Summary			
#	A	Type	Filter Rules
1	Y	Gen	Off=12, Len=2, Mask=ffff, Value=8863
2	Y	Gen	Off=12, Len=2, Mask=ffff, Value=8864
3	N		
4	N		
5	N		
6	N		

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

Figure 12-7 PPPoE Filter Rules Summary

Menu 21.5 - 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=21	N	D	F
2	N					
3	N					
4	N					
5	N					
6	N					

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

Figure 12-8 FTP_WAN Filter Rules Summary

Menu 21.11 - Filter Rules Summary						
#	A	Type	Filter Rules	M	m	n
1	Y	IP	Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=161	N	D	N
2	Y	IP	Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=162	N	D	F
3	N					
4	N					
5	N					
6	N					

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

Figure 12-9 Web Set1 Filter Rules Summary

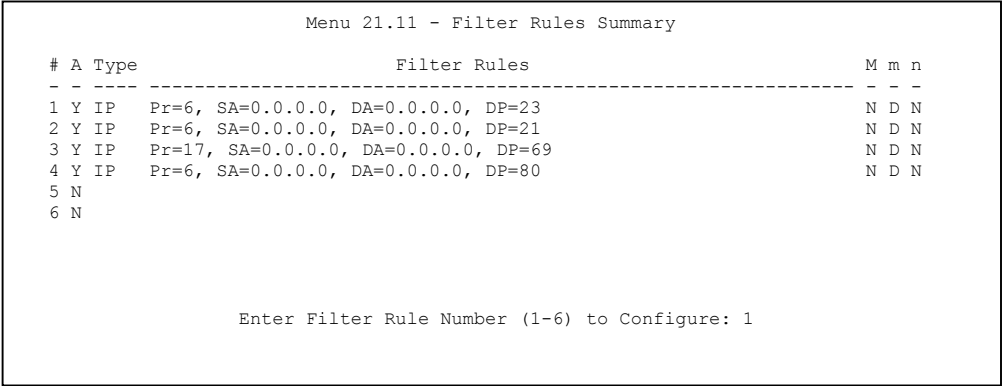


Figure 12-10 Web Set2 Filter Rules Summary

12.2.1 Filter Rules Summary Menus

The following tables briefly describe the abbreviations used in menus 21.1 and 21.2.

Table 12-1 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 for instance, forward the packet, drop the packet or check the next rule. For the latter, the next rule is independent of the rule just checked.
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.

FIELD	DESCRIPTION
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 12-2 Rule Abbreviations Used

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

12.3 Filter Rule Configuration

To configure a filter rule, type its number in **Menu 21.1 – Filter Rules Summary** and press [ENTER] to open menu 21.1.1 for the rule.

There are two types of filter rules: **TCP/IP** and **Generic**. Depending on the type of rule, the parameters for each type will be different. Use [SPACE BAR] to select the type of rule that you want to create in the **Filter Type** field and press [ENTER] to open the respective menu.

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

12.3.1 TCP/IP Filter Rule

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

To configure TCP/IP rules, select TCP/IP Filter Rule from the **Filter Type** field and press [ENTER] to open **Menu 21.1.1 – TCP/IP Filter Rule**, as shown next.

```
Menu 21.1.1 - TCP/IP Filter Rule
Filter #: 1,1
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 #= 137
              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= Check Next Rule
Action Not Matched= Check Next Rule

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 12-11 TCP/IP Filter Rule

Table 12-3 TCP/IP Filter Rule

FIELD	DESCRIPTION	EXAMPLE
Filter #	This is the filter set, filter rule coordinates, for instance, 2, 3 refers to the second filter set and the third filter rule of that set.	1,1
Filter Type	Use [SPACE BAR] and then [ENTER] to choose a rule. Parameters displayed for each type will be different. Choices are TCP/IP Filter Rule or Generic Filter Rule .	TCP/IP Filter Rule
Active	Select Yes to activate or No to deactivate the filter rule.	No (default)

Table 12-3 TCP/IP Filter Rule

FIELD	DESCRIPTION	EXAMPLE
IP Protocol	This is the upper layer protocol, for example, TCP is 6, UDP is 17 and ICMP is 1. The value must be between 0 and 255. A value of 0 matches ANY protocol.	0 to 255
IP Source Route	IP Source Route is an optional header that dictates the route an IP packet takes from its source to its destination. If Yes , the rule applies to any packet with an IP source route. The majority of IP packets do not have source route.	No (default)
Destination: IP Addr	Type the destination IP address of the packet you want to filter. This field is ignored if it is 0.0.0.0.	IP address
IP Mask	Type the IP mask to apply to the Destination: IP Addr field.	IP mask
Port #	Type the destination port of the packets you want to filter. The field range is 0 to 65535. A 0 field is ignored.	0 to 65535
Port # Comp	Select the comparison to apply to the destination port in the packet against the value given in Destination: Port # . Choices are None , Less , Greater , Equal or Not Equal .	None
Source: IP Addr	Type the source IP Address of the packet you want to filter. A 0.0.0.0 field is ignored.	IP address
IP Mask	Type the IP mask to apply to the Source: IP Addr field.	IP mask
Port #	Type the source port of the packets you want to filter. The range of this field is 0 to 65535. A 0 field is ignored.	0 to 65535
Port # Comp	Select the comparison to apply to the source port in the packet against the value given in Source: Port # field. Choices are None , Less , Greater , Equal or Not Equal .	None
TCP Estab	This applies only when the IP Protocol field is 6, TCP. If Yes , the rule matches packets that want to establish TCP connection(s) (SYN=1 and ACK=0); else it is ignored.	No (default)
More	If Yes , a matching packet is passed to the next filter rule before an action is taken or else the packet is disposed of according to the action fields. If More is Yes , then Action Matched and Action Not Matched will be N/A.	No (default)

Table 12-3 TCP/IP Filter Rule

FIELD	DESCRIPTION	EXAMPLE
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	Select the action for a matching packet. Choices are Check Next Rule , Forward or Drop .	Check Next Rule (default)
Action Not Matched	Select the action for a packet not matching the rule. Choices are Check Next Rule , Forward or Drop .	Check Next Rule (default)
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.		

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

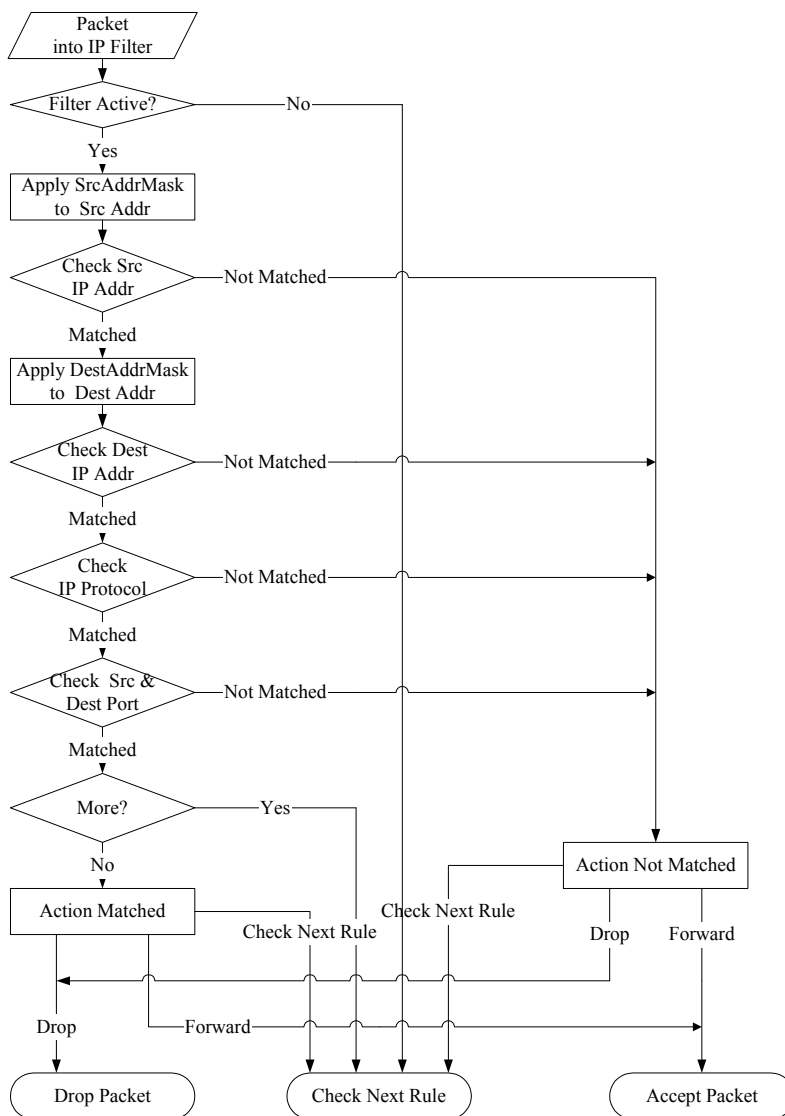


Figure 12-12 Executing an IP Filter

12.3.2 Generic Filter Rule

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

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

To configure a generic rule select an empty filter set in menu 21, for example 7. Select **Generic Filter Rule** in the **Filter Type** field and press [ENTER] to open **Menu 21.5.1 – Generic Filter Rule**, as shown in the following figure.

```
Menu 21.7.1 - Generic Filter Rule

Filter #: 7,1
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:

Press Space Bar to Toggle.
```

Figure 12-13 Generic Filter Rule

Table 12-4 Generic Filter Rule Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Filter #	This is the filter set, filter rule coordinates, for instance, 2, 3 refers to the second filter set and the third rule of that set.	5,1
Filter Type	Press [SPACE BAR] and then [ENTER] to select a type of rule. Parameters displayed below each type will be different. Choices are Generic Filter Rule or TCP/IP Filter Rule .	Generic Filter Rule
Active	Select Yes to turn on or No to turn off the filter rule.	No (default)
Offset	Type the starting byte of the data portion in the packet that you want to compare. The range for this field is from 0 to 255.	0 (default)
Length	Type the byte count of the data portion in the packet that you want to compare. The range for this field is 0 to 8.	0 (default)
Mask	Type the mask (in Hexadecimal) to apply to the data portion before comparison.	
Value	Type the value (in Hexadecimal) to compare with the data portion.	
More	If Yes , a matching packet is passed to the next filter rule before an action is taken or else the packet is disposed of according to the action fields. If More is Yes , then Action Matched and Action Not Matched will be N/A .	No (default)
Log	Select the logging option from the following: None – No packets will be logged. Action Matched – Only matching packets and rules will be logged. Action Not Matched – Only packets that do not match the rule parameters will be logged. Both – All packets will be logged.	None
Action Matched	Select the action for a matching packet. Choices are Check Next Rule , Forward or Drop .	Check Next Rule (default)
Action Not Matched	Select the action for a packet not matching the rule. Choices are Check Next Rule , Forward or Drop .	Check Next Rule (default)
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.		

12.4 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 IP packets.

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

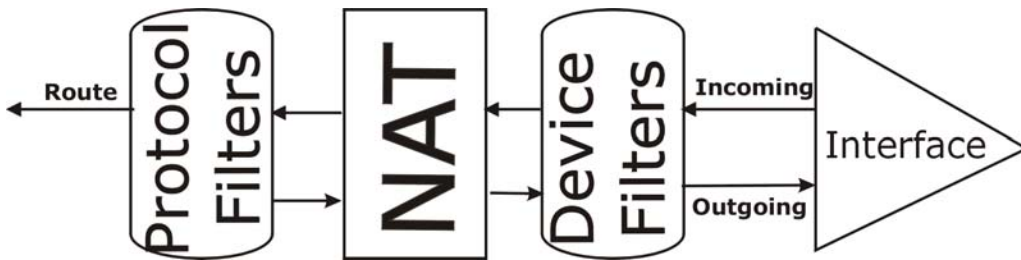


Figure 12-14 Protocol and Device Filter Sets

12.5 Example Filter

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

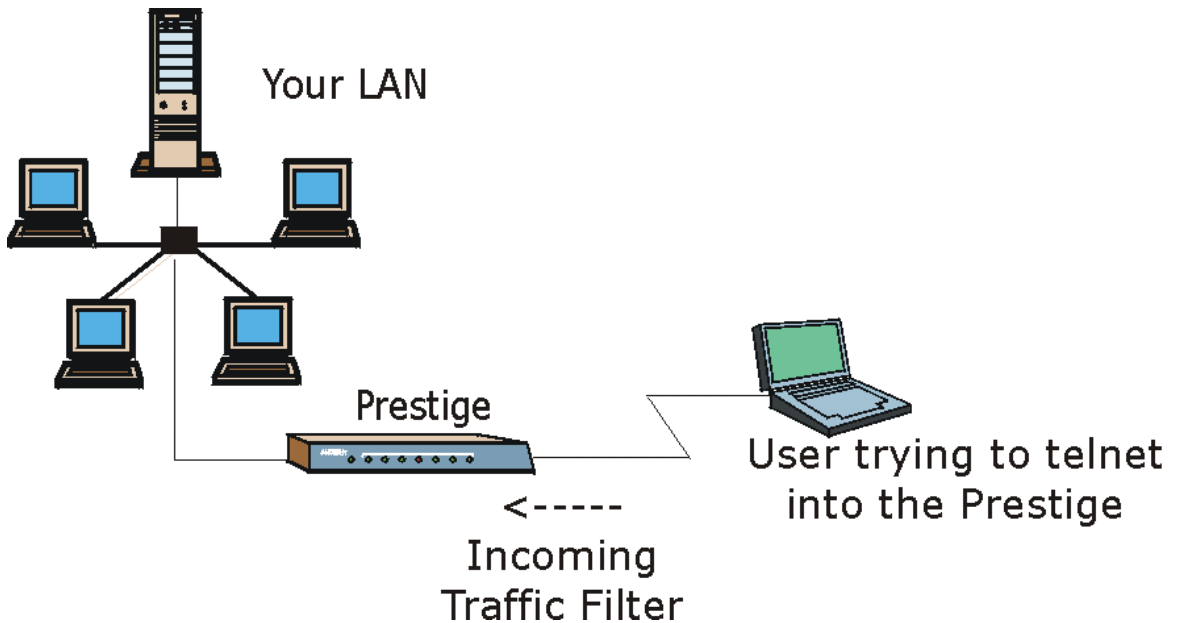


Figure 12-15 Sample Telnet Filter

- Step 1.** Enter 21 from the main menu to open **Menu 21 — Filter Set Configuration**.
- Step 2.** Enter the index number of the filter set you want to configure (in this case 3).
- Step 3.** Type a descriptive name or comment in the **Edit Comments** field (for example, TELNET_WAN) and press [ENTER].
- Step 4.** Press [ENTER] at the message “Press [ENTER] to confirm or [ESC] to cancel” to open **Menu 21.3 — Filter Rules Summary**.

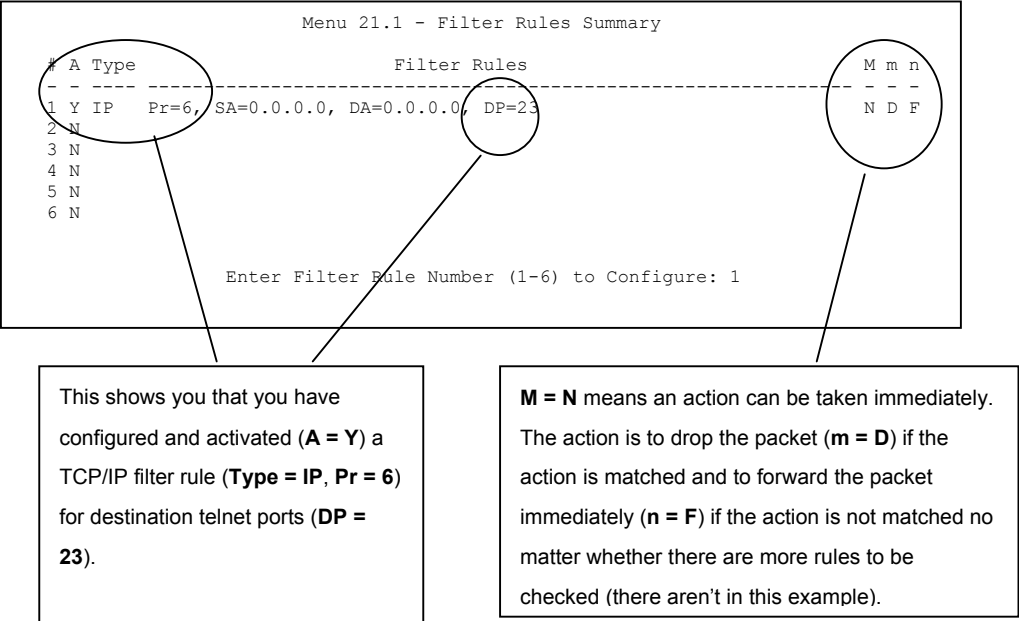


Figure 12-16 Sample Filter Rules Summary — Menu 21.1

Step 5. Type 1 to configure the first filter rule. Make the entries in this menu as shown next. When you press [ENTER] to confirm, the following screen appears. Note that there is only one filter rule in this set.

Menu 21.3.1 - 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 # =
                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 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 we 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 and there are no more rules in this filter set to check. Select **Next** if there are more rules to check.

Figure 12-17 Sample Filter Rules Summary — Menu 21.3.1

After you have created the filter set, you must apply it.

Step 1. Enter 11 in the main menu to display menu 11 and type the remote node number to edit it.

Step 2. Go to the **Edit Filter Sets** field, press [SPACE BAR] to choose **Yes** and press [ENTER].

Step 3. This brings you to menu 11.5. Enter the example filter set number in this menu as shown in the following figure.

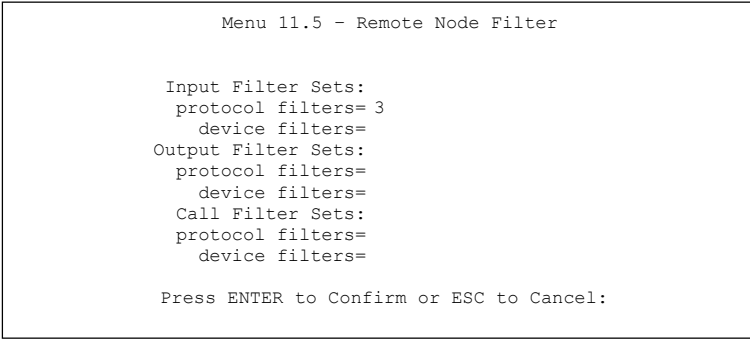


Figure 12-18 Sample Filter Rules Summary — Applying a Remote Node Filter Set

12.6 Applying Filters and Factory Defaults

This section shows you where to apply the filter(s) after you design it (them). Sets of factory default filter rules have been configured in menu 21 (but have not been applied) to filter traffic.

Table 12-5 Filter Sets Table

FILTER SETS	DESCRIPTION
Input Filter Sets:	Apply filters for incoming traffic. You may apply protocol or device filter rules. See earlier in this chapter for information on filters.
Output Filter Sets:	Apply filters for traffic leaving the Prestige. You may apply filter rules for protocol or device filters. See earlier in this section for information on types of filters.
Call Filter Sets:	Apply filters to decide if a packet should be allowed to trigger a call.

12.6.1 Ethernet Traffic

You seldom need to filter Ethernet traffic; however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 3.1 (shown next) and type the number(s) of the

filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by typing their numbers separated by commas, for example, 3, 4, 6, 11. The factory default filter set, NetBIOS_LAN, is inserted in the **protocol filters** field under **Input Filter Sets** in menu 3.1 in order to prevent local NetBIOS messages from triggering calls to the DNS server.

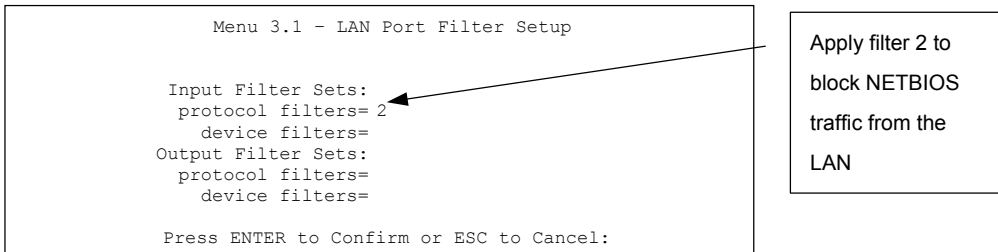


Figure 12-19 Filtering Ethernet Traffic

12.6.2 Remote Node Filters

Go to menu 11.5 (shown next) and type the number(s) of the filter set(s) as appropriate. You can cascade up to four filter sets by typing their numbers separated by commas. The factory default filter set, NetBIOS_WAN, is inserted in the **protocol filters** field under **Call Filter Sets** in menu 11.5 to block local NetBIOS traffic from triggering calls to the ISP.

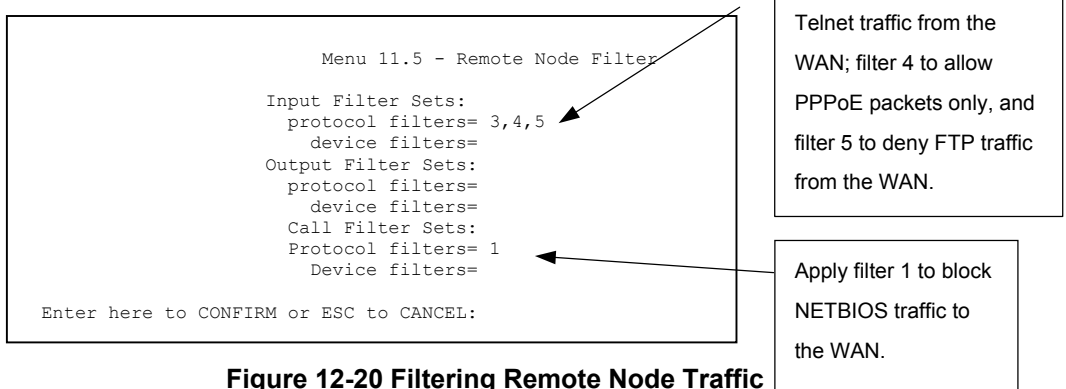


Figure 12-20 Filtering Remote Node Traffic

Note that call filter sets are visible when you select PPPoA or PPPoE encapsulation.

Chapter 13

SNMP Configuration

This chapter explains SNMP Configuration.

SNMP is only available if TCP/IP is configured.

13.1 SNMP Overview

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. SNMP is a member of 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.

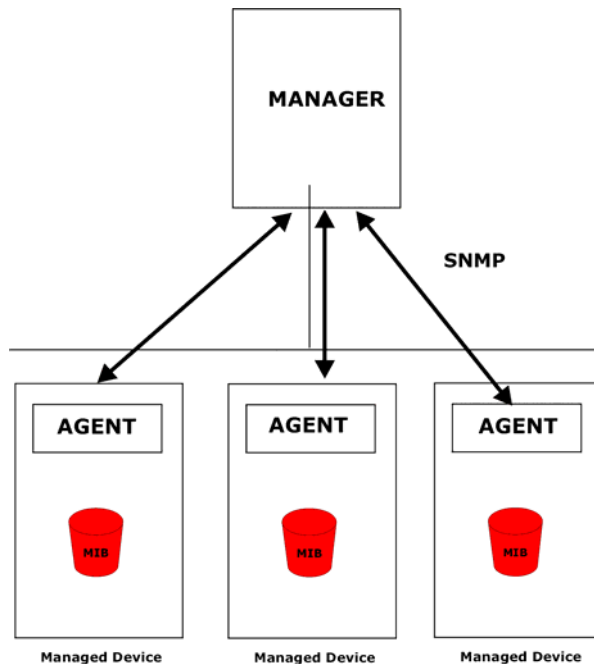


Figure 13-1 SNMP Management Model

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 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.

13.2 Supported MIBs

The Prestige supports MIB II that is defined in RFC-1213 and RFC-1215. The Prestige can also respond with specific data from the ZyXEL private MIB (ZYXEL-MIB). The focus of the MIBs is to let administrators collect statistic data and monitor status and performance.

The only implement MIBs in the Prestige as a SNMP agent. Users must implement their own GUI on SNMP platform (SNMP manager).

13.3 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 Hgst= 0.0.0.0
Trap:
Community= public
Destination= 0.0.0.0

Press ENTER to Confirm or ESC to Cancel:

```

Figure 13-2 SNMP Configuration**Table 13-1 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:		public
Community	Type the trap community, which is the password sent with each trap to the SNMP manager.	
Destination	Type the IP address of the station to send your SNMP traps to.	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.		

13.4 SNMP Traps

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

Table 13-2 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
1	coldStart (<i>defined in RFC-1215</i>)	A trap is sent after booting (power on).

TRAP #	TRAP NAME	DESCRIPTION
2	warmStart (<i>defined in RFC-1215</i>)	A trap is sent after booting (software reboot).
3	linkUp (<i>defined in RFC-1215</i>)	A trap is sent with the port number.
4	authenticationFailure (<i>defined in RFC-1215</i>)	A trap is sent to the manager when receiving any SNMP get or set requirements with wrong community (password).
6	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.

The port number is its interface index under the interface group.

Chapter 14

System Maintenance

This chapter covers the diagnostic tools that help you to maintain your Prestige.

14.1 System Maintenance Overview

These tools include updates on system status, port status, log and trace capabilities and upgrades for the system software. This chapter describes how to use these tools in detail.

Type 24 in the main menu to open **Menu 24 – System Maintenance**, as shown in the following figure.

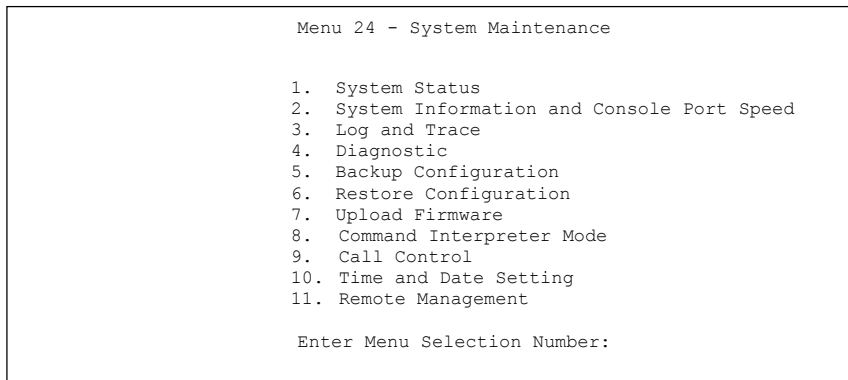


Figure 14-1 System Maintenance

14.2 System Status

The first selection, System Status gives you information on the status and statistics of the ports, as shown next. System Status is a tool that can be used to monitor your Prestige. Specifically, it gives you information on your 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							hh:mm:ss
							Sat. Jan. 01, 2000
Node-Lnk	Status	TxPkts	RxPkts	Errors	Tx B/s	Rx B/s	Up Time
1-ENET	Up	211	0	0	0	0	0:26:20
2	N/A	0	0	0	0	0	0:00:00
3	N/A	0	0	0	0	0	0:00:00
4	N/A	0	0	0	0	0	0:00:00
5	N/A	0	0	0	0	0	0:00:00
6	N/A	0	0	0	0	0	0:00:00
7	N/A	0	0	0	0	0	0:00:00
8	N/A	0	0	0	0	0	0:00:00
My WAN IP (from ISP):0.0.0.0							
Ethernet:				WAN:			
Status: 10M/Half Duplex		Tx Pkts: 53		Line Status: Up			
Collisions: 0		Rx Pkts: 36		Upstream Speed:		0 Kbps	
CPU Load= 3.8%				Downstream Speed:		0 Kbps	
Press Command:							
COMMANDS: 1-Reset Counters				ESC-Exit			

Figure 14-2 System Maintenance — Status

Table 14-1 System Maintenance — Status

FIELD	DESCRIPTION
Node-Lnk	This is the node index number and link type. Link types are: PPP, ENET, 1483.
Status	Shows the status of the remote node.
TxPkts	The number of transmitted packets to this remote node.
RxPkts	The number of received packets from this remote node.
Errors	The number of error packets on this connection.
Tx B/s	Shows the transmission rate in bytes per second.
Rx B/s	Shows the receiving rate in bytes per second.
Up Time	Time this channel has been connected to the current remote node.
My WAN IP (from ISP)	The IP address of the ISP remote node.
Ethernet	Shows statistics for the LAN.

Table 14-1 System Maintenance — Status

FIELD	DESCRIPTION
Status	Shows the current status of the LAN.
Tx Pkts	The number of transmitted packets to the LAN.
Rx Pkts	The number of received packets from the LAN.
Collision	Number of collisions.
WAN	Shows statistics for the WAN.
Line Status	Shows the current status of the xDSL line which can be Up or Down.
Upstream Speed	Shows the upstream transfer rate in kbps.
Downstream Speed	Shows the downstream transfer rate in kbps.
CPU Load	Specifies the percentage of CPU utilization.

14.3 System Information

To get to the System Information:

Step 1. Enter 24 to display **Menu 24 — System Maintenance**.

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
  1. System Information
  2. Console Port Speed

Please enter selection:
```

Figure 14-3 System Information and Console Port Speed

14.3.1 System Information

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

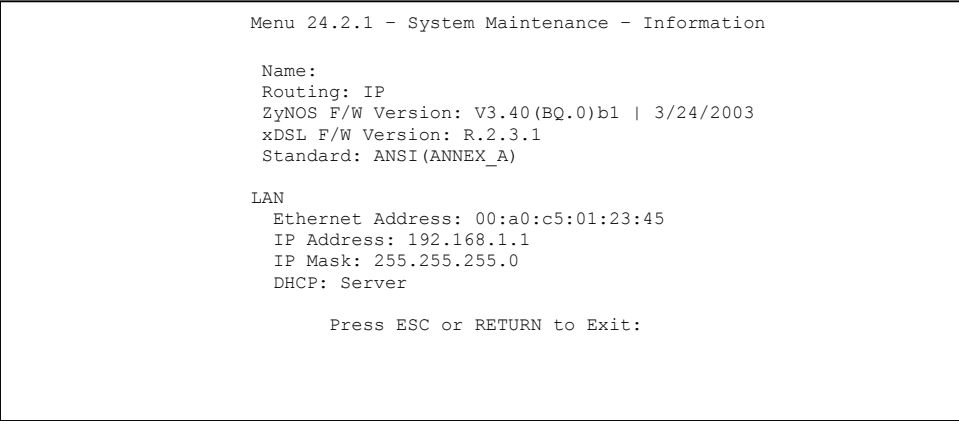


Figure 14-4 System Maintenance — Information

Table 14-2 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.
xDSL F/W Version	Refers to the DSL version.
Standard	This refers to the operational protocol the Prestige and the DSLAM (Digital Subscriber Line Access Multiplexer) are using.
LAN	
Ethernet Address	Refers to the Ethernet MAC (Media Access Control) of your Prestige.
IP Address	This is the IP address of the Prestige in dotted decimal notation.
IP Mask	This shows the subnet mask of the Prestige.
DHCP	This field shows the DHCP setting (None, Relay or Server) of the Prestige.

14.3.2 Console Port Speed

You can set up different port speeds for the console port through **Menu 24.2.2 – System Maintenance – Console Port Speed**. Your Prestige supports 9600 (default), 19200 and 38400 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: 115200

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

Figure 14-5 System Maintenance – Change Console Port Speed

Once you change the Prestige console port speed, you must also set the speed parameter for the communication software you are using to connect to the Prestige.

14.4 Log and Trace

There are two logging facilities in the Prestige. The first is the error logs and trace records that are stored locally. The second is the UNIX syslog facility for message logging.

14.4.1 Viewing Error Log

The first place you should look for clues when something goes wrong is the error log. Follow the procedures to view the local error/trace log:

- Step 1.** Type 24 in the main menu to display **Menu 24 – System Maintenance**.
- Step 2.** From menu 24, type 3 to display **Menu 24.3 – System Maintenance – Log and Trace**.

```
Menu 24.3 - System Maintenance - Log and Trace

1. View Error Log
2. UNIX Syslog

Please enter selection
```

Figure 14-6 System Maintenance — Log and Trace

Step 3. Enter 1 from **Menu 24.3 — System Maintenance — Log and Trace** to display the error log in the system.

After the Prestige finishes displaying the error log, you will have the option to clear it. Samples of typical error and information messages are presented in the next figure.

```
59 Thu Jan 01 00:00:03 1970 PP0f INFO LAN promiscuous mode <0>
60 Thu Jan 01 00:00:03 1970 PP00 -WARN SNMP TRAP 0: cold start
61 Thu Jan 01 00:00:03 1970 PP00 INFO main: init completed
62 Thu Jan 01 00:00:19 1970 PP00 INFO SMT Session Begin
63 Thu Jan 01 00:00:24 1970 PP0a WARN MPOA Link Down
Clear Error Log (y/n):
```

Figure 14-7 Sample Error and Information Messages

14.4.2 Syslog

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

```
Menu 24.3.2 - System Maintenance - UNIX Syslog

UNIX Syslog:
Active= No
Syslog IP Address= ?
Log Facility= Local 1

Types:
CDR= No
Packet triggered= No
Filter Log= No
PPP Log= No
```

Figure 14-8 System Maintenance — Syslog and Accounting

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

Table 14-3 System Maintenance Menu — Syslog Parameters

PARAMETER	DESCRIPTION
UNIX Syslog:	
Active	Use [SPACE BAR] and then [ENTER] to turn syslog on or off.
Syslog IP Address	Type the IP address of your syslog server.
Log Facility	Use [SPACE BAR] and then [ENTER] to select one of seven different local options. The log facility lets you log the message in different server files. Refer to your UNIX manual.
Types:	
CDR	Call Detail Record (CDR) logs all data phone line activity if set to Yes .
Packet Triggered	The first 48 bytes or octets and protocol type of the triggering packet is sent to the UNIX syslog server when this field is set to Yes .
Filter Log	No filters are logged when this field is set to No . Filters with the individual filter Log Filter field set to Yes are logged when this field is set to Yes .
PPP Log	PPP events are logged when this field is set to Yes .

The following are examples of the four types of syslog messages sent by the Prestige:

1 - CDR
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.)
C01 Incoming Call xxxxBps xxxxx (L2TP, xxxxx = Remote Call ID)
C01 Incoming Call xxxxx (= connected speed) xxxxx (= Remote Call ID)
L02 Tunnel Connected (L2TP)
C02 OutCall Connected xxxxx (= connected speed) xxxxx (= Remote Call ID)
C02 CLID call refused
L02 Call Terminated
C02 Call Terminated
Jul 19 11:19:27 192.168.102.2 ZYXEL: board 0 line 0 channel 0, call 1, C01 Outgoing Call dev=2 ch=0 40002
Jul 19 11:19:32 192.168.102.2 ZYXEL: board 0 line 0 channel 0, call 1, C02 OutCall Connected 64000 40002
Jul 19 11:20:06 192.168.102.2 ZYXEL: board 0 line 0 channel 0, call 1, C02 Call Terminated
2 - Packet Triggered
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=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a6b6c6d6e6f70717273 74

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
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
Jul 19 14:43:55 192.168.102.2 ZYXEL: IP [Src=202.132.154.123 Dst=255.255.255.255 UDP spo=0208 dpo=0208}] S03>R01mF
Jul 19 14:44:00 192.168.102.2 ZYXEL: IP [Src=192.168.102.20 Dst=202.132.154.1 UDP spo=05d4 dpo=0035}] S03>R01mF
Jul 19 14:44:04 192.168.102.2 ZYXEL: IP [Src=192.168.102.20 Dst=202.132.154.1 UDP spo=05d4 dpo=0035}] S03>R01mF
4 - PPP Log
SdcmSyslogSend (SYSLOG PPPLOG, SYSLOG NOTICE, String);
String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto Shutdown
Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP / IPXCP
Jul 19 11:42:44 192.168.102.2 ZYXEL: ppp:LCP Closing
Jul 19 11:42:49 192.168.102.2 ZYXEL: ppp:IPCP Closing
Jul 19 11:42:54 192.168.102.2 ZYXEL: ppp:CCP Closing

14.5 Diagnostic

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

Menu 24.4 - System Maintenance - Diagnostic	
xDSL	System
1. Reset xDSL	21. Reboot System
	22. Command Mode
TCP/IP	
12. Ping Host	
Enter Menu Selection Number:	
Host IP Address= N/A	

Figure 14-9 System Maintenance — Diagnostic

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. Diagnostic to open **Menu 24.4 – System Maintenance – Diagnostic**.

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

Table 14-4 System Maintenance Menu — Diagnostic

FIELD	DESCRIPTION
Reset xDSL	Re-initialize the xDSL link to the telephone company.
Ping Host	Ping the host to see if the links and TCP/IP protocol on both systems are working.
Reboot System	Reboot the Prestige.
Command Mode	Type the mode to test and diagnose your Prestige using specified commands.
Host IP Address	If you typed 12 to Ping Host, now type the address of the computer you want to ping.

Chapter 15

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.

15.1 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.

```
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 15-1 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

15.2 Backup Configuration

The Prestige displays different messages explaining different ways to backup, restore and upload files in menus 24.5, 24.6, 24. 7.1 and 24.7.2; depending on whether you use the console port or Telnet.

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. You can also perform backup and restore using menu 24 through the console port. Any serial communications program should work fine; however, you must use Xmodem protocol to perform the download/upload and you don’t have to rename the files.

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

15.2.1 Backup Configuration

Follow the instructions as shown in the next screen.

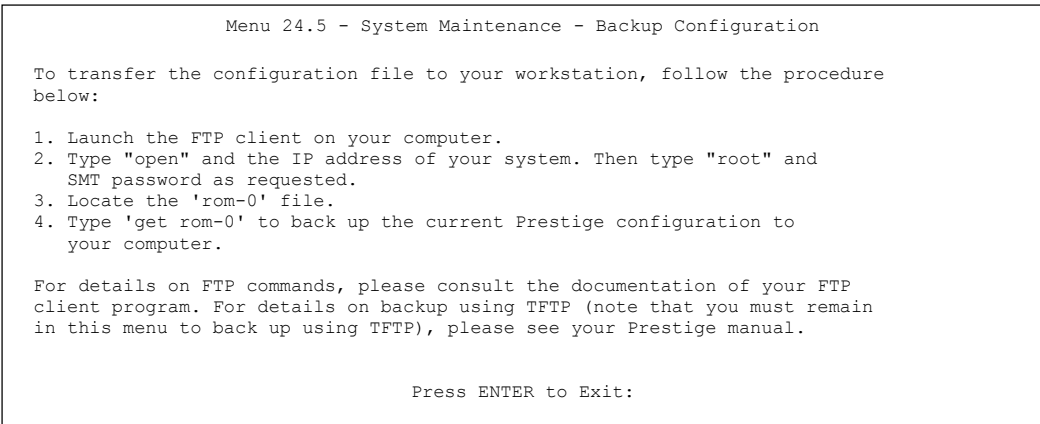


Figure 15-1 System Maintenance - Backup Configuration

15.2.2 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.

15.2.3 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 15-2 FTP Session Example

15.2.4 GUI-based FTP Clients

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

Table 15-2 General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

15.2.5 TFTP and FTP over WAN Will Not Work When

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

- 1. You have disabled Telnet service and remote management.
- 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.

15.2.6 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.

15.2.7 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.

15.2.8 GUI-based TFTP Clients

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

Table 15-3 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 15.2.5* to read about configurations that disallow TFTP and FTP over WAN.

15.2.9 Backup Via Console Port

Back up configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

Step 1. Display menu 24.5 and enter “y” at the following screen.

```
Ready to backup Configuration via Xmodem.  
Do you want to continue (y/n):
```

Figure 15-3 System Maintenance – Backup Configuration

Step 2. The following screen indicates that the Xmodem download has started.

```
You can enter ctrl-x to terminate operation any time.  
Starting XMODEM download...
```

Figure 15-4 System Maintenance – Starting Xmodem Download Screen

Step 3. Run the HyperTerminal program by clicking **Transfer**, then **Receive File** as shown in the following screen.

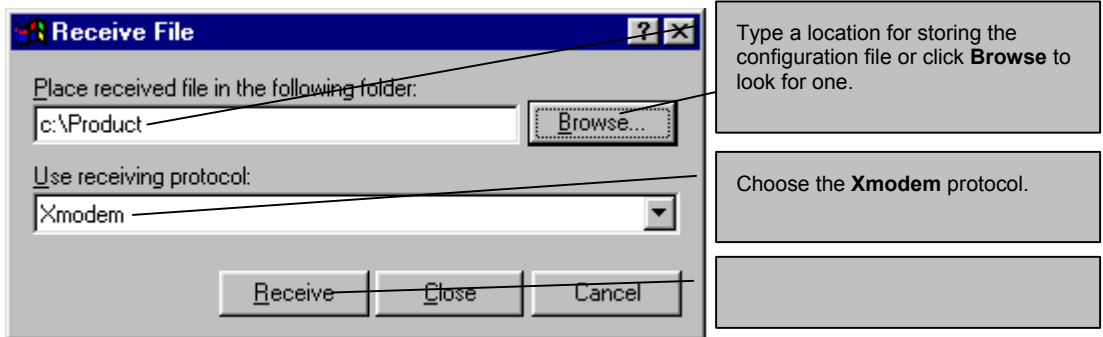


Figure 15-5 Backup Configuration Example

Step 4. After a successful backup you will see the following screen. Press any key to return to the SMT menu.

```

** Backup Configuration completed. OK.
### Hit any key to continue.###

```

Figure 15-6 Successful Backup Confirmation Screen

15.3 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. WHEN THE RESTORE CONFIGURATION PROCESS IS COMPLETE, THE PRESTIGE WILL AUTOMATICALLY RESTART.

15.3.1 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, follow the procedure below:

1. Launch the FTP client on your computer.
2. Type "open" and the IP address of your system. 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 computer and rom-0 is the
   remote file name on your system. This restores the configuration to
   your system.
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 15-7 System Maintenance - Restore Configuration

- 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.

15.3.2 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 15-8 Restore Using FTP Session Example

Refer to *section 15.2.5* to read about configurations that disallow TFTP and FTP over WAN.

15.3.3 Restore Via Console Port

Restore configuration via console port by following the HyperTerminal procedure shown next. Procedures using other serial communications programs should be similar.

Step 1. Display menu 24.6 and enter “y” at the following screen.

```
Ready to restore Configuration via Xmodem.
Do you want to continue (y/n):
```

Figure 15-9 System Maintenance – Restore Configuration

Step 2. The following screen indicates that the Xmodem download has started.

```
Starting XMODEM download (CRC mode) ...
CCCCCCCC
```

Figure 15-10 System Maintenance – Starting Xmodem Download Screen

Step 3. Run the HyperTerminal program by clicking **Transfer**, then **Send File** as shown in the following screen.

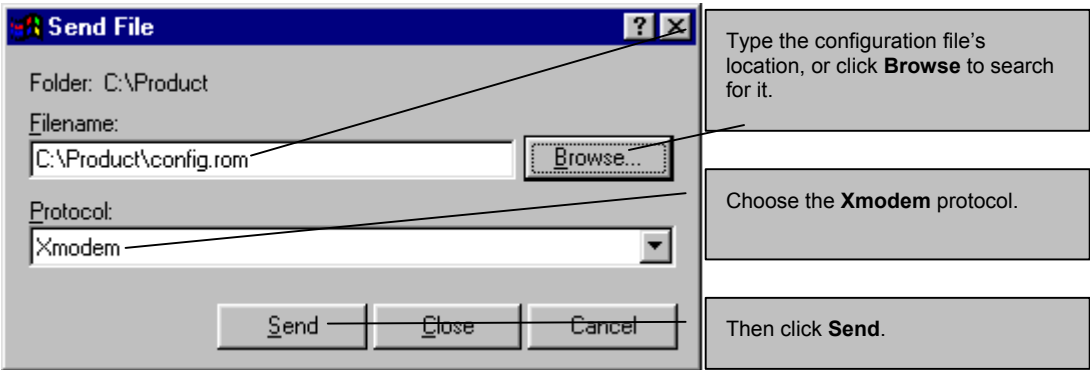


Figure 15-11 Restore Configuration Example

Step 4. After a successful restoration you will see the following screen. Press any key to restart the Prestige and return to the SMT menu.

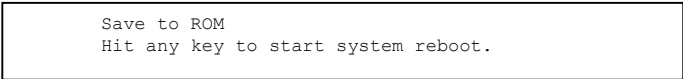


Figure 15-12 Successful Restoration Confirmation Screen

15.4 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** (for console port).

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

15.4.1 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 firmwarefilename 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 15-13 System Maintenance - Upload System Firmware

15.4.2 Configuration File Upload

You will 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 configurationfilename 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 15-14 Telnet Into Menu 24.7.2 – System Maintenance

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

15.4.3 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.

15.4.4 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 15-15 FTP Session Example of Firmware File Upload

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

Refer to *section 15.2.5* to read about configurations that disallow TFTP and FTP over WAN.

15.4.5 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.

15.4.6 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.

15.4.7 Uploading Via Console Port

FTP or TFTP are the preferred methods for uploading firmware to your Prestige. However, in the event of your network being down, uploading files is only possible with a direct connection to your Prestige via the console port. Uploading files via the console port under normal conditions is not recommended since FTP or TFTP is faster. Any serial communications program should work fine; however, you must use the Xmodem protocol to perform the download/upload.

15.4.8 Uploading Firmware File Via Console Port

Step 1. Select 1 from **Menu 24.7 – System Maintenance – Upload Firmware** to display **Menu 24.7.1 – System Maintenance – Upload System Firmware**, then follow the instructions as shown in the following screen.

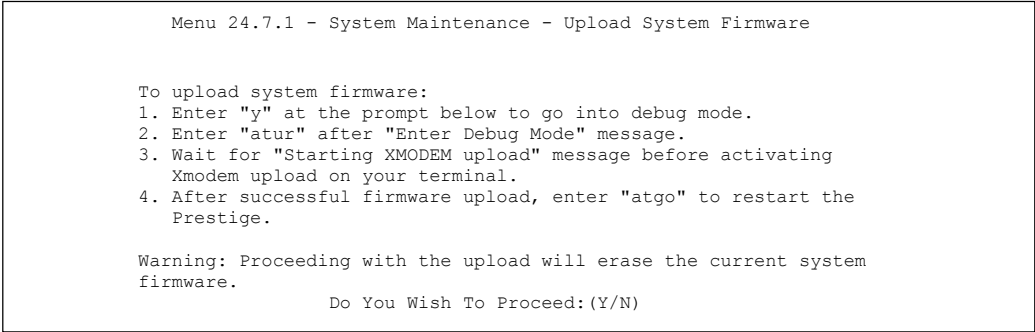


Figure 15-16 Menu 24.7.1 as seen using the Console Port

Step 2. After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

15.4.9 Example Xmodem Firmware Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

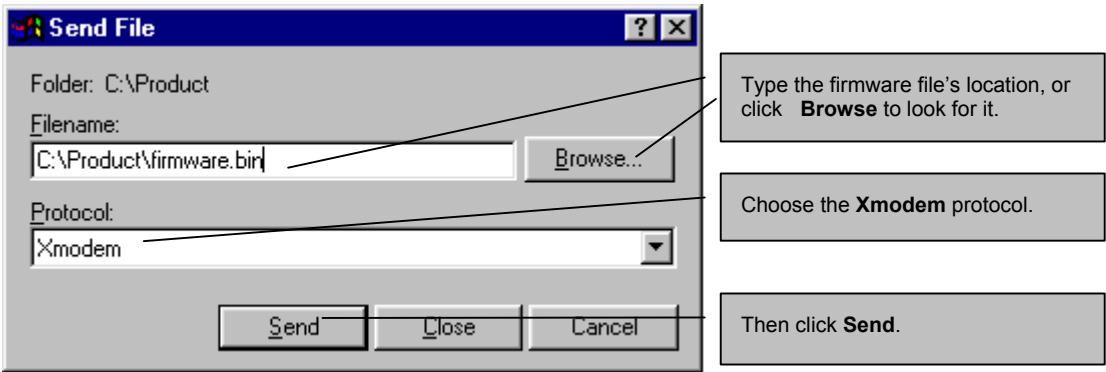


Figure 15-17 Example Xmodem Upload

After the configuration upload process has completed, restart the Prestige by entering "atgo".

15.4.10 Uploading Configuration File Via Console Port

- Step 1.** Select 2 from **Menu 24.7 – System Maintenance – Upload Firmware** to display **Menu 24.7.2 – System Maintenance – Upload System Configuration File**. Follow the instructions as shown in the next screen.

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

To upload system configuration file:
1. Enter "y" at the prompt below to go into debug mode.
2. Enter "atlc" after "Enter Debug Mode" message.
3. Wait for "Starting XMODEM upload" message before activating
   Xmodem upload on your terminal.
4. After successful firmware upload, enter "atgo" to restart the
   system.

Warning:
1. Proceeding with the upload will erase the current
   configuration file.
2. The system's console port speed (Menu 24.2.2) may change
   when it is restarted; please adjust your terminal's speed
   accordingly. The password may change (menu 23), also.
3. When uploading the DEFAULT configuration file, the console
   port speed will be reset to 9600 bps and the password to
   "1234".

Do You Wish To Proceed:(Y/N)
```

Figure 15-18 Menu 24.7.2 as seen using the Console Port

- Step 2.** After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.
- Step 3.** Enter "atgo" to restart the Prestige.

15.4.11 Example Xmodem Configuration Upload Using HyperTerminal

Click **Transfer**, then **Send File** to display the following screen.

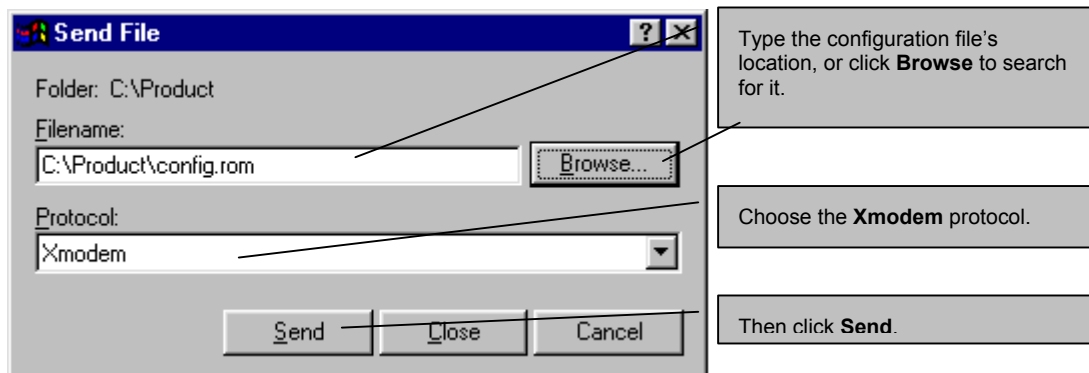


Figure 15-19 Example Xmodem Upload

After the configuration upload process has completed, restart the Prestige by entering “atgo”.

Chapter 16

System Maintenance and Information

This chapter leads you through SMT menus 24.8 to 24.10.

16.1 Command Interpreter Mode

The Command Interpreter (CI) is a part of the main system firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. Enter the CI from the SMT by selecting menu 24.8. See the included disk or the zyxel.com web site for more detailed information on CI commands. Enter 8 from **Menu 24 — System Maintenance**. A list of valid commands can be found by typing `help` or `?` at the command prompt. Type “exit” to return to the SMT main menu when finished.

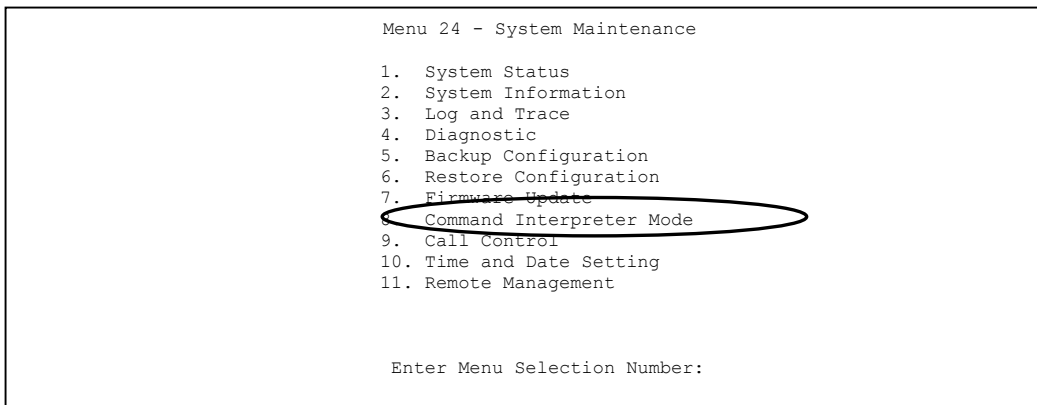


Figure 16-1 Command Mode in Menu 24

```
Copyright (c) 1994 - 2003 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys          exit          device      ether
wan          poe           xdsl        ip
ppp          bridge       hdap
ras>
```

Figure 16-2 Valid Commands

16.2 Call Control Support

Call Control Support is only applicable when **Encapsulation** is set to **PPPoE** in menu 4 or menu 11.1.

The budget management function allows you to set a limit on the total outgoing call time of the Prestige within certain times. When the total outgoing call time exceeds the limit, the current call will be dropped and any future outgoing calls will be blocked.

To access the call control menu, select option 9 in menu 24 to go to **Menu 24.9 — System Maintenance — Call Control**, as shown in the next table.

```
Menu 24.9 - System Maintenance - Call Control

1. Budget Management

Enter Menu Selection Number:
```

Figure 16-3 Call Control

16.2.1 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 - System Maintenance - Budget Management		
Remote Node	Connection Time/Total Budget	Elapsed Time/Total Period
1.MyISP	No Budget	No Budget
2.-----	---	---
3.-----	---	---
4.-----	---	---
5.-----	---	---
6.-----	---	---
7.-----	---	---
8.-----	---	---
Reset Node (0 to update screen):		

Figure 16-4 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 when PPPoE encapsulation is selected.

Table 16-1 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.		

16.3 Time and Date Setting

The Prestige keeps track of the time and date. There is also a software mechanism to set the time manually or get the current time and date from an external server when you turn on your Prestige. Menu 24.10 allows you to update the time and date settings of your Prestige. The real time is then displayed in the Prestige error logs and firewall logs.

Select menu 24 in the main menu to open **Menu 24 — System Maintenance**, as shown next.

```
Menu 24 - System Maintenance

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

Enter Menu Selection Number:
```

Figure 16-5 System Maintenance

Then enter 10 to go to **Menu 24.10 — System Maintenance — Time and Date Setting** to update the time and date settings of your Prestige as shown in the following screen.

```
Menu 24.10 - System Maintenance - Time and Date Setting

Use Time Server when Bootup= None
Time Server Address= N/A

Current Time:                00 : 00 : 00
New Time (hh:mm:ss):        11 : 23 : 16

Current Date:                2000 - 01 - 01
New Date (yyyy-mm-dd):      2001 - 03 - 01

Time Zone= GMT

Daylight Saving= No
Start Date (mm-dd):          01 - 00
End Date (mm_dd):            01 - 00

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 16-6 System Maintenance — Time and Date Setting

Table 16-2 Time and Date Setting Fields

FIELD	DESCRIPTION
Use Time Server when Bootup	Enter the time service protocol that your time server sends when you turn on the Prestige. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main differences between them are the format. Daytime (RFC 867) format is day/month/year/time zone of the server. Time (RFC-868) format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. NTP (RFC-1305) is similar to Time (RFC-868). None. The default, enter the time manually.
Time Server Address	Enter the IP address or domain name of your time server. Check with your ISP/network administrator if you are unsure of this information.
Current Time	This field displays an updated time only when you reenter this menu.
New Time	Enter the new time in hour, minute and second format.
Current Date	This field displays an updated date only when you re-enter this menu.
New Date	Enter the new date in year, month and day format.
Time Zone	Press [SPACE BAR] and then [ENTER] to set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Saving	If you use daylight savings time, then choose Yes .
Start Date	If using daylight savings time, enter the month and day that it starts on.
End Date	If using daylight savings time, enter the month and day that it ends on
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.	

16.3.1 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 time server configured in menu 24.10.
- iii. 24-hour intervals after starting.

Chapter 17

IP Policy Routing

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

17.1 IP Policy Routing Overview

Traditionally, routing is based on the destination address only and the IAD takes the shortest path to forward a packet. IP Routing Policy (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing.

17.1.1 IP Policy Routing Benefits

- Source-Based Routing – Network administrators can use policy-based routing to direct traffic from different users through different connections.
- Quality of Service (QoS) – Organizations can differentiate traffic by setting the precedence or TOS (Type of Service) values in the IP header at the periphery of the network to enable the backbone to prioritize traffic.
- Cost Savings – IPPR allows organizations to distribute interactive traffic on high-bandwidth, high-cost paths while using low-cost paths for batch traffic.
- Load Sharing – Network administrators can use IPPR to distribute traffic among multiple paths.

17.1.2 Routing Policy

Individual routing policies are used as part of the overall IPPR process. A policy defines the matching criteria and the action to take when a packet meets the criteria. The action is taken only when all the criteria are met. The criteria include the source address and port, IP protocol (ICMP, UDP, TCP, etc.), destination address and port, TOS and precedence (fields in the IP header) and length. The inclusion of length criterion is to differentiate between interactive and bulk traffic. Interactive applications, for example, telnet, tend to have short packets, while bulk traffic, for example, file transfer, tends to have large packets.

The actions that can be taken include:

- Routing the packet to a different gateway (and hence the outgoing interface).
- Setting the TOS and precedence fields in the IP header.

IPPR follows the existing packet filtering facility of RAS in style and in implementation. The policies are divided into sets, where related policies are grouped together. A user defines the policies before applying them to an interface or a remote node, in the same fashion as the filters. There are 12 policy sets with six policies in each set.

17.2 IP Routing Policy Setup

Menu 25 shows all the policies defined.

Menu 25 - IP Routing Policy Setup

Policy Set #	Name	Policy Set #	Name
1	test	7	
2		8	
3		9	
4		10	
5		11	
6		12	

Enter Policy Set Number to Configure= 0

Edit Name= N/A

Press ENTER to Confirm or ESC to Cancel:

Figure 17-1 IP Routing Policy Setup

To setup a routing policy, perform the following procedures:

- Step 1. Type 25 in the main menu to open **Menu 25 – IP Routing Policy Setup**.
- Step 2. Type the index of the policy set you want to configure to open **Menu 25.1 – IP Routing Policy Setup**.

Menu 25.1 shows the summary of a policy set, including the criteria and the action of a single policy, and whether a policy is active or not. Each policy contains two lines. The former part is the criteria of the incoming packet and the latter is the action. Between these two parts, separator “|” means the action is taken on criteria matched and separator “=” means the action is taken on criteria not matched.

```

Menu 25.1 - IP Routing Policy Setup

# A Criteria/Action
- - - - -
1 Y SA=1.1.1.1-1.1.1.1, DA=2.2.2.2-2.2.2.5
   SP=20-25, DP=20-25, P=6, T=NM, PR=0 | GW=192.168.1.1, T=MT, PR=0
2 N
3 N
4 N
5 N
6 N

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

```

Figure 17-2 Sample IP Routing Policy Setup

Table 17-1 IP Routing Policy Setup Abbreviations

ABBREVIATION		MEANING
Criterion	SA	Source IP Address
	SP	Source Port
	DA	Destination IP Address
	DP	Destination Port
	P	IP layer 4 protocol number (TCP=6, UDP=17...)
	T	Type of service of incoming packet
	PR	Precedence of incoming packet
Action	GW	Gateway IP address
	T	Outgoing Type of service
	P	Outgoing Precedence
Service	NM	Normal
	MD	Minimum Delay
	MT	Maximum Throughput
	MR	Maximum Reliability
	MC	Minimum Cost

Type a number from 1 to 6 to display **Menu 25.1.1 – IP Routing Policy** (see the next figure). This menu allows you to configure a policy rule.

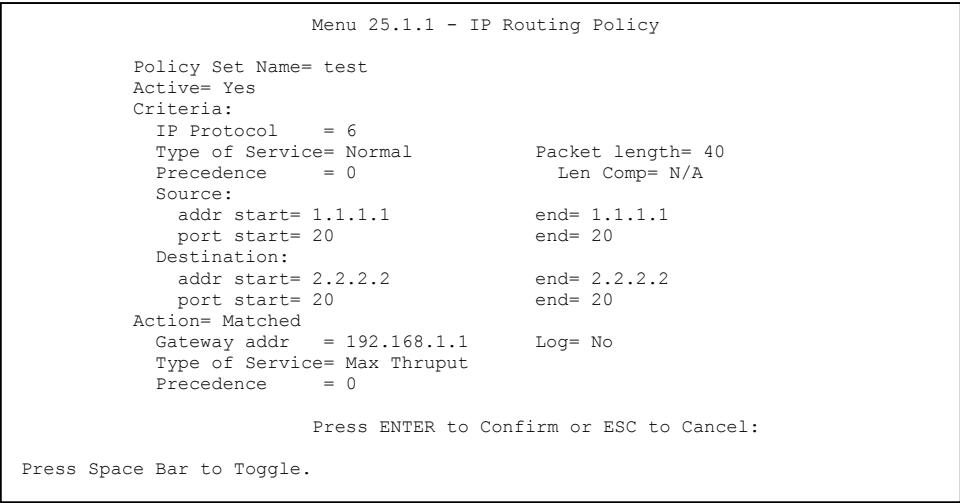


Figure 17-3 IP Routing Policy

Table 17-2 IP Routing Policy

FIELD	DESCRIPTION
Policy Set Name	This is the policy set name assigned in Menu 25 – IP Routing Policy Setup .
Active	Press [SPACE BAR] and then [ENTER] to select Yes to activate or No to deactivate the policy. Inactive policies are displayed with a minus sign “-“ in SMT menu 25.
Criteria	
IP Protocol	IP layer 4 protocol, for example, UDP, TCP, ICMP , etc.
Type of Service	Prioritize incoming network traffic by choosing from Don’t Care, Normal, Min Delay, Max Thruput, Min Cost or Max Reliable .
Precedence	Precedence value of the incoming packet. Press [SPACE BAR] and then [ENTER] to select a value from 0 to 7 or Don’t Care .
Packet Length	Type the length of incoming packets (in bytes). The operators in the Len Comp (next field) apply to packets of this length.
Len Comp	Press [SPACE BAR] and then [ENTER] to choose from Equal, Not Equal ,

Table 17-2 IP Routing Policy

FIELD	DESCRIPTION
Len Comp	Press [SPACE BAR] and then [ENTER] to choose from Equal , Not Equal , Less , Greater , Less or Equal or Greater or Equal .
Source:	
addr start / end	Source IP address range from start to end.
port start / end	Source port number range from start to end; applicable only for TCP/UDP.
Destination:	
addr start / end	Destination IP address range from start to end.
port start / end	Destination port number range from start to end; applicable only for TCP/UDP.
Action	Specifies whether action should be taken on criteria Matched or Not Matched .
Gateway addr	Defines the outgoing gateway address. The gateway must be on the same subnet as the Prestige if it is on the LAN, otherwise, the gateway must be the IP address of a remote node. The default gateway is specified as 0.0.0.0.
Type of Service	Set the new TOS value of the outgoing packet. Prioritize incoming network traffic by choosing No Change , Normal , Min Delay , Max Thruput , Max Reliable or Min Cost .
Precedence	Set the new outgoing packet precedence value. Values are 0 to 7 or No Change .
Log	Press [SPACE BAR] and then [ENTER] to select Yes to make an entry in the system log when a policy is executed.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

17.3 Applying an IP Policy

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

17.3.1 Ethernet IP Policies

From **Menu 3 — Ethernet Setup**, type 2 to go to **Menu 3.2 — TCP/IP and DHCP Ethernet Setup**.

You can choose up to four IP policy sets (from 12) by typing their numbers separated by commas, for example, 2, 4, 7, 9.

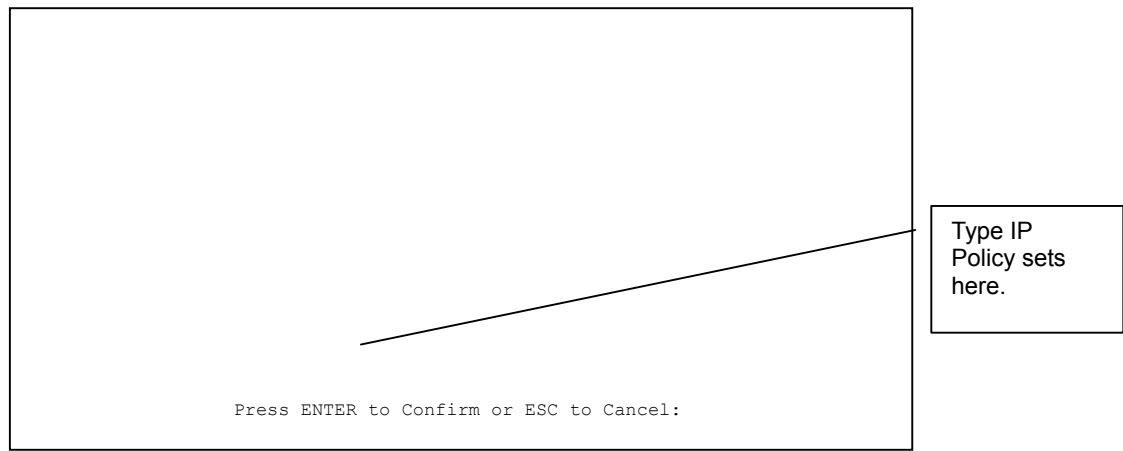


Figure 17-4 TCP/IP and DHCP Ethernet Setup

Go to menu 11.3 (shown next) and type the number(s) of the IP Routing Policy set(s) as appropriate. You can cascade up to four policy sets by typing their numbers separated by commas.

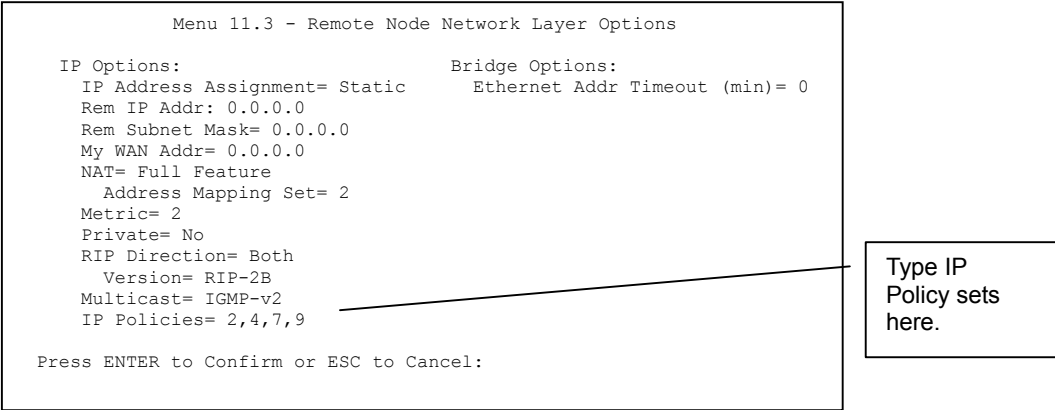


Figure 17-5 Remote Node Network Layer Options

17.4 IP Policy Routing Example

If a network has both Internet and remote node connections, you can route Web packets to the Internet using one policy and route FTP packets to a remote network using another policy. See the next figure.

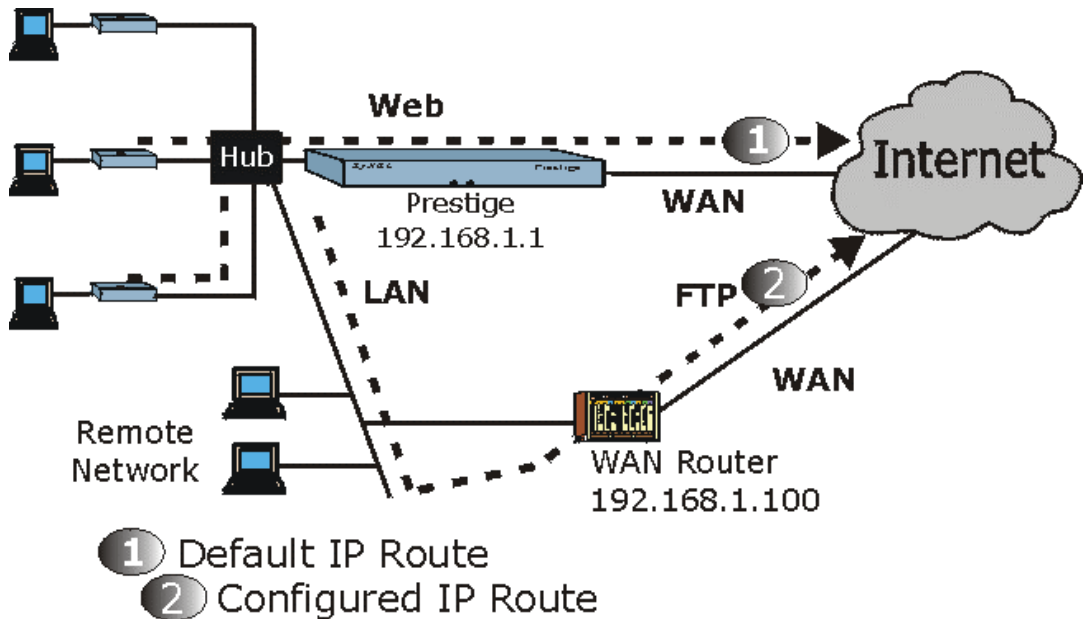


Figure 17-6 Example of IP Policy Routing

To force Web packets coming from clients with IP addresses of 192.168.1.33 to 192.168.1.64 to be routed to the Internet via the WAN port of the Prestige, follow the steps as shown next.

- Step 1.** Create a routing policy set in menu 25.
- Step 2.** Create a rule for this set in **Menu 25.1.1 — IP Routing Policy** as shown next.

```
Menu 25.1.1 - IP Routing Policy

Policy Set Name= set1
Active= Yes
Criteria:
  IP Protocol      = 6
  Type of Service= Don't Care
  Precedence       = Don't Care
  Source:
    addr start= 192.168.1.2
    port start= 0
  Destination:
    addr start= 0.0.0.0
    port start= 80
  Action= Matched
  Gateway addr    = 192.168.1.1
  Type of Service= No Change
  Precedence      = No Change
  Packet length= 10
  Len Comp= N/A
  end= 192.168.1.64
  end= N/A
  end= N/A
  end= 80
  Log= No

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

Figure 17-7 IP Routing Policy Example

- Step 3.** Check **Menu 25.1 — IP Routing Policy Setup** to see if the rule is added correctly.
- Step 4.** Create another policy set in menu 25.
- Step 5.** Create a rule in menu 25.1 for this set to route packets from any host (IP=0.0.0.0 means any host) with protocol TCP and port FTP access through another gateway (192.168.1.100).

```

Menu 25.1.1 - IP Routing Policy

Policy Set Name= set2

Active= Yes
Criteria:
  IP Protocol      = 6
  Type of Service= Don't Care      Packet length= 10
  Precedence       = Don't Care      Len Comp= N/A
Source:
  addr start= 0.0.0.0              end= N/A
  port start= 0                    end= N/A
Destination:
  addr start= 0.0.0.0              end= N/A
  port start= 20                   end= 21
Action= Matched
Gateway addr =192.168.1.100        Log= No
Type of Service= No Change
Precedence   = No Change

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

```

Figure 17-8 IP Routing Policy

Step 6. Check **Menu 25.1 — IP Routing Policy Setup** to see if the rule is added correctly.

Step 7. Apply both policy sets in menu 3.2 as shown next.

```

Menu 3.2 - TCP/IP and DHCP Ethernet Setup

DHCP Setup
  DHCP= Server
  Client IP Pool Starting Address= 192.168.1.33
  Size of Client IP Pool= 64
  Primary DNS Server= 0.0.0.0
  Secondary DNS Server= 0.0.0.0
  Remote DHCP Server= N/A
TCP/IP Setup:
  IP Address= 192.168.1.1
  IP Subnet Mask= 255.255.255.0
  RIP Direction= Both
  Version= RIP-1
  Multicast= None
  IP Policies= 1,2
  Edit IP Alias= No

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

```

Figure 17-9 Applying IP Policies

Chapter 18

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.

18.1 Call Scheduling Overview

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 video cassette 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**.

18.2 Schedule Setup

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=

Edit Name=

Press ENTER to Confirm or ESC to Cancel:

Figure 18-1 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(yy/yy/mm/dd) = 2000 - 01 - 01
How Often= Once
Once:
  Date(yy/yy/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 18-2 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 18-1 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

Table 18-1 Schedule Set Setup

FIELD	DESCRIPTION	EXAMPLE
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
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	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. Forced Down means that the connection is blocked whether or not there is a demand call on the line. 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.	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.

Menu 11.1 - Remote Node Profile

Rem Node Name= ?
Active= Yes

Encapsulation= PPPoE
Multiplexing=VC-based
Service Name=
Incoming
 Rem Login=
 Rem Password= *****
Outgoing=
 My Login=?
 My Password= *****
 Authen= CHAP/PAP

Route= IP
Bridge= No

Edit IP/Bridge= No
Edit ATM Options= No
Telco Option:
 Allocated Budget (min)= 0
 Period(hr)= 0
 Schedules= 1,2,3,4
 Nailed-Up Connection= No

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

Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.

Apply your
schedule
sets here.

Figure 18-3 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).

Chapter 19

Remote Management

This chapter covers remote management (SMT menu 24.11).

19.1 Remote Management Overview

Remote management setup is for managing Telnet, FTP and Web services. You can customize the service port, access interface and the secured client IP address to enhance security and flexibility.

You may manage your Prestige from a remote location via:

the Internet (**WAN only**), the **LAN only**, **All** (LAN and WAN) or **Disable** (neither).

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

If you enable remote management of a service, but have applied a filter to block the service, then you will not be able to remotely manage the service.

19.1.1 Remote Management and Telnet Services

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

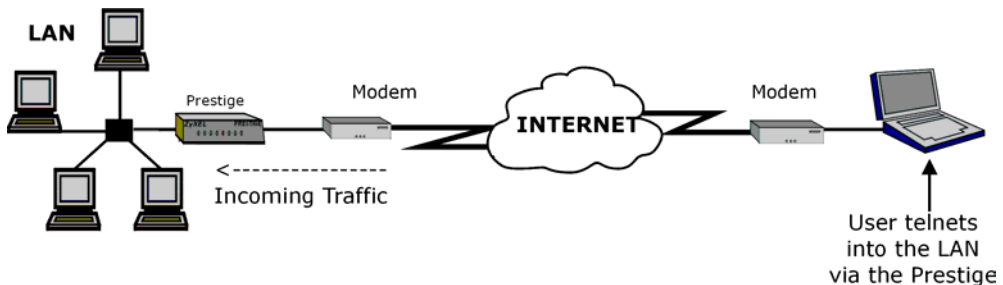


Figure 19-1 Telnet Configuration on a TCP/IP Network

19.1.2 Remote Management and FTP Services

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

19.1.3 Remote Management and Web Services

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

19.1.4 Disabling Remote Management

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

19.2 Remote Management Setup

Enter 11 in menu 24 to display **Menu 24.11 — Remote Management Control** (shown next).

Menu 24.11 - Remote Management Control

TELNET Server:

Server Port = 23

Secured Client IP = 0.0.0.0

Server Access = LAN only

FTP Server:

Server Port = 21

Secured Client IP = 0.0.0.0

Server Access = LAN only

Web Server:

Server Port = 80

Secured Client IP = 0.0.0.0

Server Access = LAN only

Press ENTER to Confirm or ESC to Cancel:

Figure 19-2 Remote Management Control

Table 19-1 Remote Management Control

FIELD	DESCRIPTION	EXAMPLE
Telnet Server FTP Server Web Server	Each of these read-only labels denotes a service that you may use to remotely manage the Prestige.	
Server Port	This field shows the port number for the remote management service. You may change the port number for a service if needed, but you must use the same port number to use that service for remote management.	23
Server Access	Select the access interface (if any) by pressing the [SPACE BAR]. Choices are: LAN only , WAN only , All or Disable . The default is LAN only .	LAN only

Table 19-1 Remote Management Control

FIELD	DESCRIPTION	EXAMPLE
Secured Client IP	The default 0.0.0.0 allows any client to use this service to remotely manage 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.		

19.2.1 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 **Secured Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the Prestige will disconnect the session immediately.
4. There is already another remote management session of the same type (Telnet, FTP or Web) running. You may only have one remote management session of the same type running at one time.
5. There is a web remote management session running with a Telnet session. A Telnet session will be disconnected if you begin a web session; it will not begin if there already is a web session.

19.3 Remote Management and NAT

When NAT is enabled:

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

19.4 System Timeout

There is a system timeout of five minutes (300 seconds) for Telnet/web/FTP connections. Your Prestige will automatically log you out if you do nothing in this timeout period, except when it is continuously updating the status in menu 24.1 or when `sys stdio` has been changed on the command line.

Part: IV

ADDITIONAL INFORMATION

This part contains UPnP, Troubleshooting, the Appendices and the Index.

Chapter 20

Universal Plug-and-Play (UPnP)

This chapter introduces the UPnP feature in the web configurator.

20.1 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.

20.1.1 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.

20.1.2 NAT Transversal

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 Transversal and UPnP.

See the Network Address Translation (NAT) chapter in your User's Guide for further information about NAT.

20.1.3 Cautions with UPnP

The automated nature of NAT Transversal 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.

20.1.4 UPnP and ZyXEL

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

UPnP broadcasts are only allowed on the LAN.

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

20.2 Accessing the Prestige Web Configurator to Configure UPnP

- Step 1.** Make sure your Prestige hardware is properly connected (refer to instructions in *Chapter 2*).
- Step 2.** Prepare your computer/computer network to connect to the Internet (refer to the *Preparing Your Network* portion of the *Quick Start Guide*).
- Step 3.** Launch your web browser.
- Step 4.** Type "192.168.1.1" as the URL.
- Step 5.** Type "admin" as the user name and "1234" (default) as the password and click **OK**. The main menu screen displays.

20.2.1 Configuring UPnP

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

UPnP

☐ Enable the Universal Plug and Play(UPnP) Service

☐ Allow users to make configuration changes through UPnP

Apply

Reset

Figure 20-1 Configuring UPnP

Table 20-1 Configuring UPnP

FIELD	DESCRIPTION
Enable the Universal Plug and Play (UPnP) Service	Select this checkbox to activate UPnP. Be aware that anyone could use a UPnP application to open the web configurator's login screen without entering the Prestige's IP address (although you must still enter the password to access the web configurator).
Allow users to make configuration changes through UPnP	Select this check box to allow UPnP-enabled applications to automatically configure the Prestige so that they can communicate through the Prestige, for example by using NAT Transversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.
Apply	Click Apply to save the setting to the Prestige.
Reset	Click Reset to begin configuring this screen afresh.

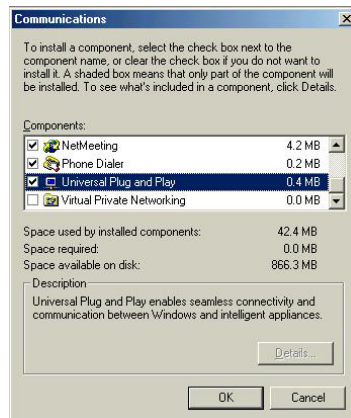
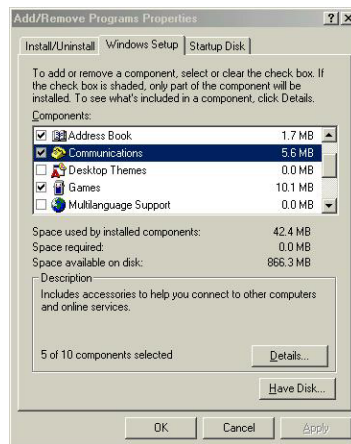
20.3 Installing UPnP in Windows Example

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

Installing UPnP in Windows Me

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

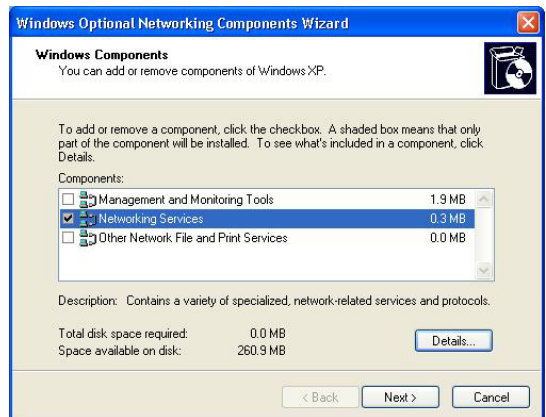
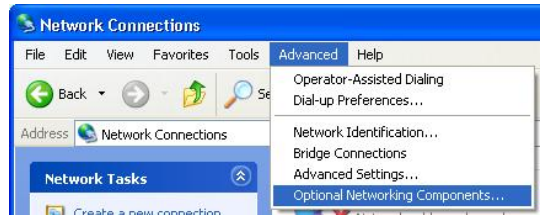
- Step 1.** Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.
- Step 2.** Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.
- Step 3.** In the **Communications** window, select the **Universal Plug and Play** 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.



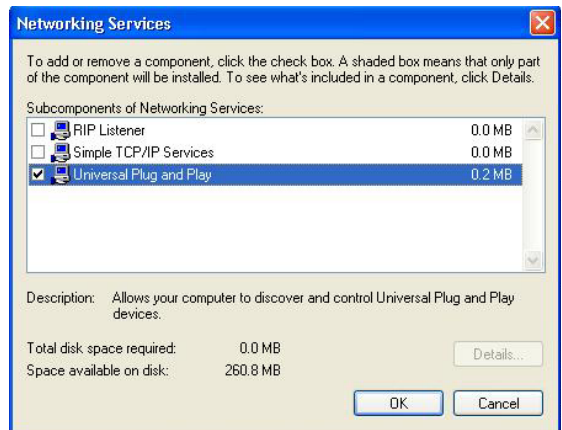
Installing UPnP in Windows XP

Follow the steps below to install the 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**.



20.4 Using UPnP in Windows XP Example

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

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

Auto-discover Your UPnP-enabled Network Device

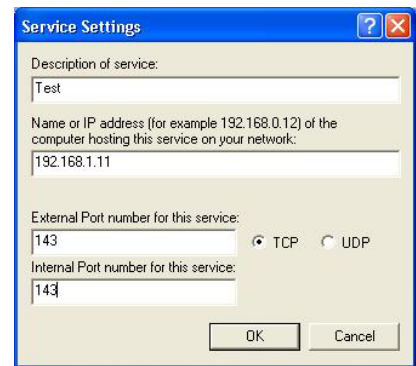
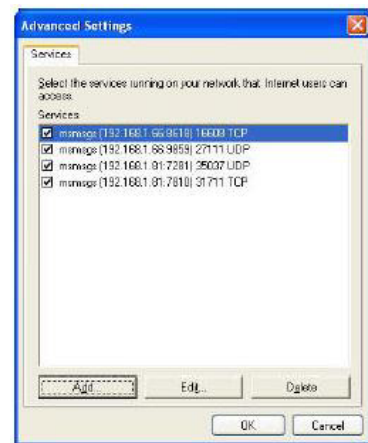
- Step 1.** Click **start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.
- Step 2.** Right-click the icon and select **Properties**.



Step 3. In the **Internet Connection Properties** window, click **Settings** to see the port mappings there 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 **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray



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

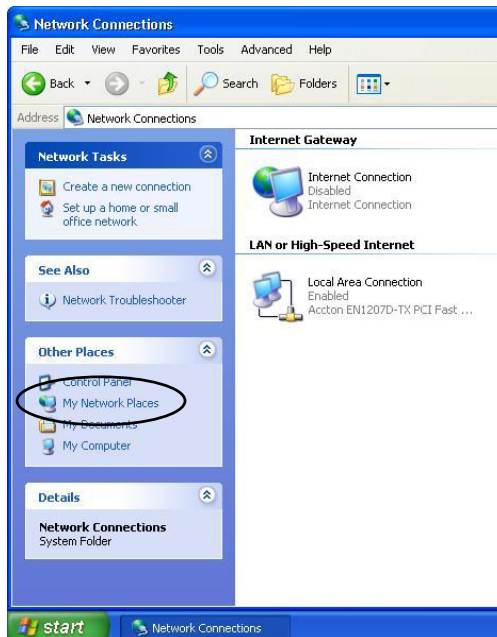


Web Configurator Easy Access

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

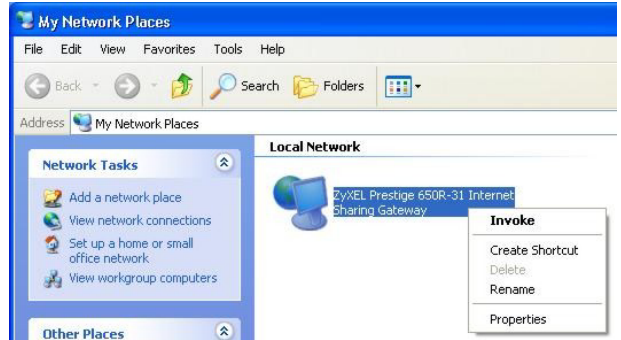
Follow the steps below to access the web configurator.

- 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 on the icon for your Prestige and select **Invoke**. The web configurator login screen displays.



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



Chapter 21

Troubleshooting

This chapter covers potential problems and the corresponding remedies.

21.1 Problems Starting Up the Prestige

Table 21-1 Troubleshooting the Start-Up of Your Prestige

PROBLEM	CORRECTIVE ACTION	
None of the LEDs turn on when I turn on the Prestige.	Make sure that the Prestige's power adapter is connected to the Prestige and plugged in to an appropriate power source. Check that the Prestige and the power source are both turned on. If the error persists, you may have a hardware problem. In this case, you should contact your vendor.	
I cannot access the Prestige via the console port.	1. Make sure the Prestige is connected to your computer's serial port.	
	2. Make sure the communications program is configured correctly. The communications software should be configured as follows:	VT100 terminal emulation.
		9600 bps is the default speed on leaving the factory. Try other speeds in case the speed has been changed.
		No parity, 8 data bits, 1 stop bit, data flow set to none.

21.2 Problems with the LAN Interface

Table 21-2 Troubleshooting the LAN Interface

PROBLEM	CORRECTIVE ACTION
Cannot access the Prestige from the LAN.	If the 10M/100M LEDs on the front panel is off, check the Ethernet cable connections between your Prestige and computer. Check for faulty Ethernet cables.
	Make sure your NIC (Network Interface Card) is installed and functioning properly.
	Check the TCP/IP configuration on your computer. Make sure that the IP address and the subnet mask of the Prestige and your computer(s) are on the same subnet.

21.3 Problems with the WAN Interface

Table 21-3 Troubleshooting the WAN Interface

PROBLEM	CORRECTIVE ACTION
I cannot get a WAN IP address from the ISP.	The WAN IP is provided when the ISP recognizes the user as an authorized user after verifying the MAC address, Host Name or User ID. Find out the verification method used by your ISP.
	If the ISP checks the host name, enter your computer's name in the System Name field in Menu 1 — General Setup .
	If the ISP checks the User ID, make sure that you have entered the correct user name (in the My Login field) and password (in the My Password field) in Menu 4 — Internet Access Setup .
I cannot connect to a remote node or ISP.	Check menu 4 or menu 11.1 to verify the Encapsulation for the remote node.

21.4 Problems with Internet Access

Table 21-4 Troubleshooting Internet Access

PROBLEM	CORRECTIVE ACTION
I cannot access the Internet	Verify your settings in menu LAN and Internet settings.
	Make sure the Prestige is turned on and connected to the network. If the Prestige's DSL LED is off, check the cable between the Prestige and the telephone wall jack. Make sure you entered your user name and password correctly. Your username and password may be case-sensitive.
	Internet connection disconnects Check the schedule rules in SMT menu 26. If you use PPPoA or PPPoE encapsulation, check the idle time-out setting in SMT menu 11.5. If the problem persists, contact your ISP.

21.5 Problems with the Password

Table 21-5 Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
I cannot access the Prestige.	The Password and Username fields are case-sensitive. Make sure that you enter the correct password and username using the proper casing. Restore the factory default configuration file. This will restore all of the factory defaults including the password. Refer to the <i>Reset Button</i> section in the <i>User's Guide</i> for details.

21.6 Problems with Telnet

Table 21-6 Troubleshooting Telnet

PROBLEM	CORRECTIVE ACTION
I cannot access the Prestige from the LAN or WAN.	Refer to the <i>Remote Management Limitations</i> section for scenarios when remote management may not be possible.
	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.
	Refer to the <i>Problems with the LAN Interface</i> section in Troubleshooting for instructions on checking your LAN connection.
	Refer to the <i>Problems with the WAN Interface</i> section in Troubleshooting for instructions on checking your WAN connection.

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) which connects to a 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 and 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.

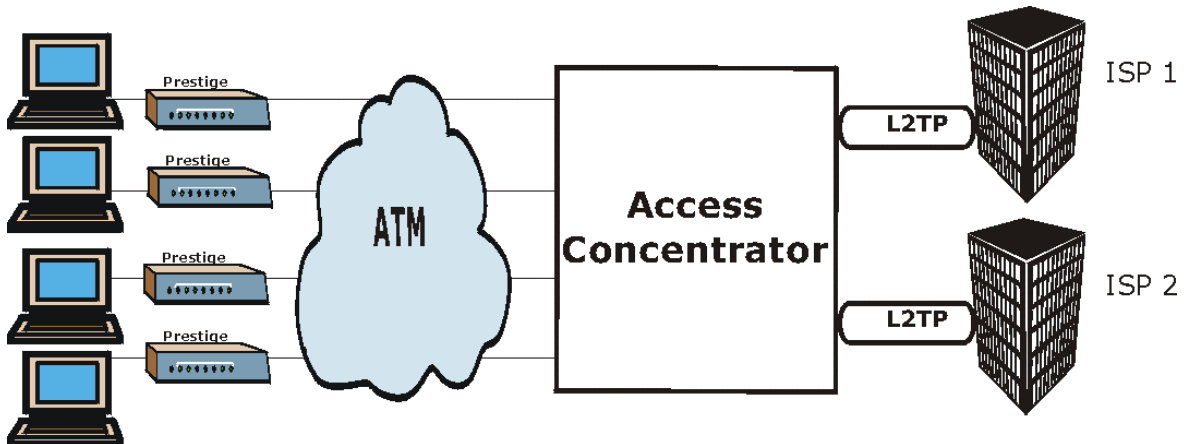


Diagram 1 Single-PC per Router Hardware Configuration

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.

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.

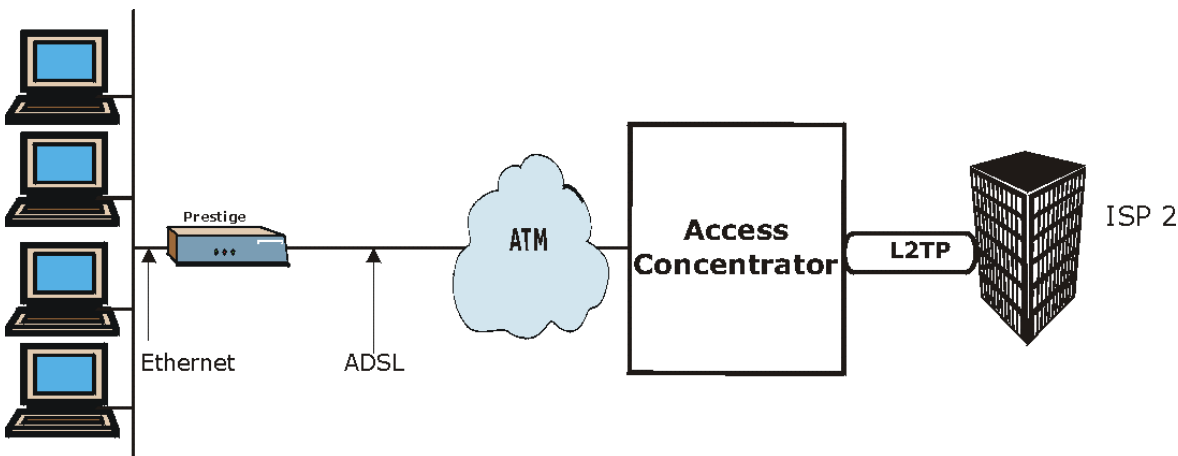


Diagram 2 Prestige as a PPPoE Client

Appendix B

Virtual Circuit Topology

ATM is a connection-oriented technology, meaning that it sets up virtual circuits over which end systems communicate. The terminology for virtual circuits is as follows:

- Virtual Channel Logical connections between ATM switches
- Virtual Path A bundle of virtual channels
- Virtual Circuit A series of virtual paths between circuit end points

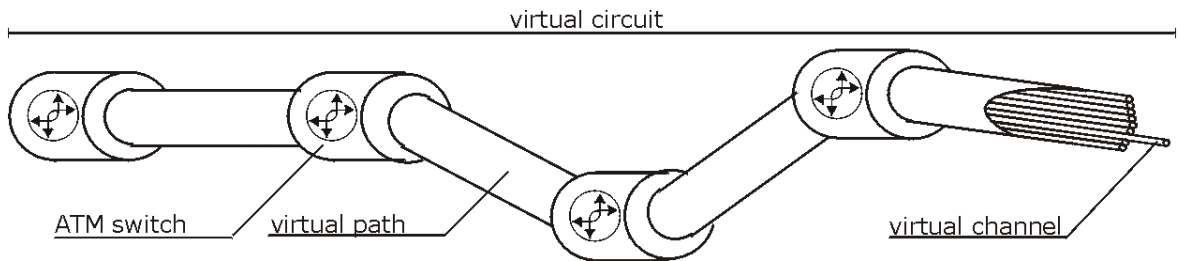


Diagram 3 Virtual Circuit Topology

Think of a virtual path as a cable that contains a bundle of wires. The cable connects two points and wires within the cable provide individual circuits between the two points. In an ATM cell header, a VPI (Virtual Path Identifier) identifies a link formed by a virtual path; a VCI (Virtual Channel Identifier) identifies a channel within a virtual path.

The VPI and VCI identify a virtual path, that is, termination points between ATM switches. A series of virtual paths make up a virtual circuit.

Your service provider should supply you with VPI/VCI numbers.

Appendix C

Power Adapter Specifications

NORTH AMERICAN PLUG STANDARDS	
AC Power Adapter Model	DV-121AACS
Input Power	AC120Volts/60Hz/23W max
Output Power	AC12Volts/1.0A
Power Consumption	8 W
Safety Standards	UL, CUL (UL 1310, CSA C22.2 No.223)
NORTH AMERICAN PLUG STANDARDS	
AC Power Adapter Model	AA-121A
Input Power	AC120Volts/60Hz/18W max
Output Power	AC12Volts/1.0A
Power Consumption	8 W
Safety Standards	UL, CUL (UL 1310, CSA C22.2 No.223)
UNITED KINGDOM PLUG STANDARDS	
AC Power Adapter Model	AA-121AD
Input Power	AC230Volts/50Hz/140mA
Output Power	AC12Volts/1.0A
Power Consumption	8 W
Safety Standards	ITS-GS, CE (EN 60950, BS 7002)
AUSTRALIA AND NEW ZELAND PLUG STANDARDS	
AC Power Adapter Model	AA-121AE
Input Power	AC240Volts/50Hz/140mA
Output Power	AC12Volts/1.0A
Power Consumption	8 W
Safety Standards	NATA (AS/NZS 60950)

EUROPEAN PLUG STANDARDS	
AC Power Adapter Model	DV-121AACCP-5716
Input Power	AC230Volts/50Hz/100mA
Output Power	AC12Volts/1.0A
Power Consumption	8W
Safety Standards	TUV-GS, CE (EN 60950)
EUROPEAN PLUG STANDARDS	
AC Power Adapter Model	AA-121ABN
Input Power	AC230Volts/50Hz/140mA
Output Power	AC12Volts/1.0A
Power Consumption	8 W
Safety Standards	ITS-GS, CE (EN 60950)
UNITED KINGDOM PLUG STANDARDS	
AC Power Adapter Model	AA-121A3D
Input Power	AC230Volts/50Hz/140mA
Output Power	AC12Volts/1.3A
Power Consumption	15W
Safety Standards	ITS-GS, CE (EN 60950)
China Standards	
AC Power Adapter Model	DV-121AACCP-5720
Input Power	AC220Volts/50Hz/18W
Output Power	AC12Volts/1.0A
Power Consumption	8 W
Safety Standards	CCEE (GB8898)
China Standards	
AC Power Adapter Model	BH-48 (AA-121AP)
Input Power	AC220Volts/50Hz
Output Power	AC12Volts/1.0A

Power Consumption	8 W
Safety Standards	CCEE (GB8898)

Index

10/100 MB Auto-negotiation	1-2	Maximum Number of Schedule Sets	18-1
Active	5-5, 5-7	PPPoE	18-3
Allocated Budget	5-6	Precedence	18-1
Application Scenario	1-3	Precedence Example	See precedence
AT command	5-2, 5-3, 15-1	CDR	14-7
Authen	5-5	CDR (Call Detail Record)	14-6
Authentication	5-5, 8-4, 8-5	CHAP	5-5, 8-4
auto-negotiation	1-2	CHAP (Challenge Handshake Authentication Protocol)	1-2
Back Panel		Collision	14-3
connections description	2-3	Command Interpreter Mode	16-1
Backup	15-2	Community	13-2
Bridging		Computer Name	3-8
Ether Address	10-3	Conditions that prevent TFTP and FTP from working over WAN	15-4
Ethernet	10-1	Connecting the Prestige	2-3
Ethernet Addr Timeout	10-2	Connections	
Remote Node	10-1	ADSL Line	2-3
Static Route Setup	10-2	Power Adapter	2-4
Budget Management	16-2, 16-3	Cost Of Transmission	8-7, 9-3
Call Back Delay	5-4	Country Code	14-4
Call Filtering	12-1	CPU Load	14-3
Call Filters		Data Filtering	12-1
Built-In	12-1	Device Filter rules	12-16
User-Defined	12-1	DHCP	1-2, 14-4
Call Scheduling	18-1		

Diagnostic	14-8	Filter	5-11, 12-1
Diagnostic Tools	14-1	Applying Filters	12-20
Dial Timeout	5-4	Ethernet Setup	6-6
DNS	6-10	Ethernet traffic	12-21
Domain Name	11-14	Ethernet Traffic	12-20
Domain Name System	6-3	Filter Rules	12-8
Drop Timeout	5-4	Filter Structure	12-4
DTR	5-3	Generic Filter Rule	12-14
Dynamic DNS	3-8, 3-10	Remote Node	8-8
Dynamic Host Configuration Protocol	6-3	Remote Node Filter	8-8
DYNDNS Wildcard	3-9	Remote Node Filters	12-21
Edit IP	5-6	SUA	12-16
Encapsulation	1-2, 7-1, 7-7, 8-2	TCP/IP Filter Rule	12-10
ENET ENCAP	7-1	Filter Log	14-7, 14-8
PPP over Ethernet	7-1	Filter Rule Process	12-3
PPPoA	7-2	Filter Rule Setup	12-9
RFC 1483	7-2	Filter Rules Summary	
ENET ENCAP	1-2	Sample	12-18, 12-19, 12-20
Error Log	14-5	Filter Set	
Error/Information Messages		Class	12-9
Sample	14-6	Filter Set Configuration	12-4
Ethernet	6-6	Filtering	12-1, 12-9
Ethernet Encapsulation	11-14	Filtering Process	
Ethernet Traffic	12-21	Outgoing Packets	12-2
Ethernet/802.3 bridged	1-4	Firmware Upgrade	1-3
Features	1-1	Front Panel	2-1
Filename Conventions	15-1	FTP	19-3

Restrictions	19-3	Internet Assigned Numbers Authority .. See IANA
FTP File Transfer	15-10	IP address.....
FTP Restrictions.....	15-4	5-6, 5-8
FTP Server	11-22	IP Address 6-10, 9-3, 10-3, 12-11, 14-4, 14-9, 17-3
G.SHDSL	1-1	Remote
Gateway	9-3	5-8
Gateway Node.....	10-3	IP Address Assignment.....
General Setup	3-8	7-2
Hardware Installation	2-1	ENET ENCAP.....
Hidden Menus	3-5	7-2
Hop Count.....	8-7, 9-3	PPPoA or PPPoE
HTTP	11-15	7-2
HyperTerminal program	15-6, 15-9	RFC 1483
IANA	6-1, 6-2	7-2
Idle Timeout.....	5-6, 5-7	IP Alias Setup
IGMP support.....	8-7	6-6
Initial Setup.....	2-1	IP Filter
Install UPnP	20-3	Logic Flow
Windows Me.....	20-3	12-12
Windows XP.....	20-5	IP mask
Installation		12-11
Ease.....	1-3	IP Multicast.....
Installation Requirements	2-1	1-1
Interactive Applications	17-1	Internet Group Management Protocol (IGMP)
Internet Access.....	1-1, 3-6, 4-1, 5-1, 6-1, 7-5, 7-6	
Internet Access Application	1-4	1-1
Internet Access Setup.....	11-6	IP network number
		6-1
		IP Packet
		12-14
		IP Policies.....
		17-5
		IP Policy Routing.....
		1-2
		IP Policy Routing (IPPR).....
		6-5
		Applying an IP Policy
		17-5
		Ethernet IP Policies
		17-5
		Gateway.....
		17-5
		IP Pool
		6-3
		IP Protocol
		17-4
		IP Routing Policy (IPPR).....
		17-1
		Benefits.....
		17-1
		Cost Savings
		17-1

Criteria.....	17-1	VC-based.....	7-3
Load Sharing	17-1	Multiplexing	7-3, 7-7, 8-2
Setup.....	17-2	Multiprotocol Encapsulation	7-2
IP Routing Policy Setup.....	17-3	My Login.....	5-5
IP Static Route	9-1	My Password	5-5
IP Static Route Setup	9-2	My WAN Address.....	5-8, 8-6
IP Subnet Mask	5-8	Nailed-Up Connection.....	5-6
Remote	5-8	NAT.....	5-8, 12-16
LAN	14-3	Application.....	11-3
LED indicators.....	2-1	Applying NAT in the SMT Menus.....	11-6
Link type.....	14-2	Configuring	11-7
LLC-based Multiplexing.....	8-13	Definitions.....	11-1
Log and Trace	14-6	Examples	11-17
Log Facility.....	14-7	How NAT Works	11-2
Logging Option.....	12-12, 12-15	Mapping Types	11-4
Login.....	8-3	Non NAT Friendly Application Programs.....	11-24
MAC address	10-3	Ordering Rules	11-11
Main Menu	3-5	What NAT does.....	11-2
Management Information Base (MIB).....	13-2	NAT Traversal.....	20-1
MBS.....	See Maximum Burst Size	Network Address Translation.....	7-8
Media Access Control.....	10-1	Network Address Translation (NAT)	11-1
Message Logging	14-5	Network Management	1-3
Metric.....	5-8, 8-7, 9-3	NIC (Network Interface Card).....	2-1
Multicast.....	5-9, 8-7	Packet	
Multiple Protocol over ATM	1-2	Error	14-2
Multiplexing		Received.....	14-3
LLC-based.....	7-3	Transmitted	14-3

Packet Triggered	14-7	Remote DHCP Server.....	6-10
Packets	14-2	Remote Management Limitations.....	19-3
PAP	5-5, 8-4	Remote Management Setup	19-2
PAP (Password Authentication Protocol)	1-2	Remote Node	8-1, 14-2
Password	3-2, 3-7, 8-4, 13-2	Remote Node Setup.....	8-1, 8-2
Period(hr)	5-6	Remote Node Filter.....	5-11
Ping	14-9	Remote Node Index Number	14-2
policy-based routing.....	17-1	Remote Node Traffic	12-21
PPP	5-7	Required fields.....	3-5
PPP Encapsulation	8-13	Restore Configuration.....	15-7
PPP Log	14-7, 14-8	retry count.....	5-4
PPP over ATM.....	1-2	retry interval	5-4
PPPoA	8-2	RFC-1483	1-2, 1-4, 8-2
Precedence	17-1, 17-4	RFC-2364	1-2, 8-2, 8-3
Private	5-9, 8-7, 9-3	RIP.....	5-9, 6-10, 8-7. See Routing Information Protocol
Protocol.....	12-11	Routing Information Protocol.....	6-2
Protocol Filter Rules	12-16	Direction.....	6-2
Protocols Supported	1-2	Version	6-3
Quality of Service	17-1	Routing Policy	17-1
Quick Start Guide	20-2	Sample IP Addresses	8-8
RAS.....	14-4, 17-2	Scalability	1-1
Rate		Schedule Sets	
Receiving.....	14-2	Duration.....	18-2
Transmission.....	14-2	SCR.....	See Sustain Cell Rate
Rear Panel	2-3	Script.....	5-9
Rem IP Address	5-8	Security.....	1-2
Rem Node Name.....	5-5, 5-7		

Server	11-5, 11-8, 11-10, 11-13, 11-14, 11-15, 11-16, 11-19, 11-20, 16-5	System Information.....	14-3
Service Type	4-4	System Status	14-1
setup a schedule	18-2	System Information	14-3
SMT Menu Overview	3-3	System Maintenance....	14-1, 14-3, 15-2, 15-5, 15-13, 15-14, 16-1, 16-2, 16-4
SNMP	1-1	System Management Terminal	3-4
Community	13-3	System Status	14-2
Configuration.....	13-2	System Timeout.....	19-3
Get	13-2	TCP/IP	5-8, 12-16, 14-9, 19-1
Manager.....	13-2	TCP/IP Options	8-12
MIBs.....	13-2	Telnet.....	19-1
Trap	13-2	Telnet Configuration	19-1
Trusted Host	13-3	Telnet Under NAT.....	19-1
Source-Based Routing	17-1	TFTP	
Speed	1-1	And FTP Over WAN}.....	19-3
Static Routing Topology	9-1	Restrictions.....	19-3
STP	2-3	TFTP and FTP over WAN Will Not Work	
SUA	1-2	When.....	15-4
SUA (Single User Account)	See NAT	TFTP File Transfer	15-12
Subnet Mask	5-8, 6-1, 6-10, 8-6, 9-3, 14-4	TFTP Restrictions.....	15-4
Syslog	14-6	Time and Date Setting.....	16-4, 16-5
Syslog IP Address.....	14-7	Time Zone	16-5
Syslog Server.....	14-6	Timeout	5-6, 5-7
System		To avoid damage to the Prestige.....	2-4
Console Port Speed	14-5	TOS (Type of Service)	17-1
Diagnostic.....	14-8	Trace Records.....	14-5
Log and Trace.....	14-5	Type of Service	17-1, 17-3, 17-4, 17-5
Syslog and Accounting.....	14-6	Universal Plug and Play	20-1

Application	20-1	VC-based Multiplexing	8-2, 8-12
Security issues	20-1	VPI & VCI.....	7-3
Universal Plug and Play Forum	20-2	WAN Setup.....	4-2, 4-4
UNIX Syslog.....	14-5, 14-7	Web Configurator	20-2
UNIX syslog parameters	14-6	XMODEM protocol.....	15-2
Upload Firmware	15-10	ZyNOS.....	15-1, 15-2
UPnP	See Universal Plug and Play	ZyNOS F/W Version	15-1