

Prestige 623 Series

Dual-link ADSL Router

User's Guide

Version 1.38

April 2003



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.

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.
- 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 Wuerselen, Germany

Table of Contents

Copyright.....	ii
Federal Communications Commission (FCC) Interference Statement.....	iii
ZyXEL Limited Warranty.....	iv
Customer Support.....	v
List of Figures.....	xi
List of Tables.....	xiii
Preface.....	xv
What is DSL?	xvii
GETTING STARTED.....	I
Chapter 1 Introduction.....	1-1
1.1 Prestige 623 Dual-link ADSL Router.....	1-1
1.2 Features of the Prestige	1-1
1.3 Internet Access Application for The Prestige	1-2
1.4 Additional Requirements.....	1-2
Chapter 2 Hardware Installation and Initial Setup	2-1
2.1 Front Panel	2-1
2.2 Rear Panel and Connections of the Prestige	2-2
2.2.1 DSL Port.....	2-4
2.2.2 10/100M Ethernet Ports.....	2-4
2.2.3 Power Port	2-5
2.2.4 USB Port.....	2-5
2.2.5 Reset Button	2-5
2.3 Prestige with POTS	2-5
2.3.1 Connecting a POTS Splitter	2-5
2.3.2 Telephone Microfilters	2-6
2.4 Prestige With ISDN.....	2-7
2.5 Setting Up Your USB Computer's IP Address.....	2-7
2.6 Configuring the Prestige.....	2-9
2.7 Testing Your Installation	2-11
Chapter 3 Getting Started with the Web Configurator	3-1
3.1 Introduction	3-1
3.2 Accessing the Web Configurator.....	3-1
3.3 Navigating the Web Configurator	3-2
3.3.1 Navigation Tab	3-2
3.3.2 Commonly used buttons	3-3
3.4 Viewing Basic System Information.....	3-3
3.5 Quick Configuration	3-5
3.6 Port Settings	3-8
3.7 System Date and Time.....	3-9

3.8	Managing Prestige User Accounts	3-10
3.8.1	Creating User Accounts	3-10
3.8.2	Changing User Account Password	3-11
3.9	Committing Your Changes and Rebooting the Prestige.....	3-12
3.9.1	Committing Your Changes.....	3-12
3.9.2	Rebooting the Prestige Using the Web Configurator	3-13
Chapter 4 Setting the LAN IP Address		4-1
4.1	What is the LAN IP Address?	4-1
4.2	IGMP	4-1
4.3	Changing the LAN IP Address.....	4-2
Chapter 5 Viewing System IP Information and Performance Statistics		5-1
5.1	Introduction	5-1
5.2	Viewing Your Prestige’s IP Addresses	5-1
5.3	Viewing IP Global Statistics	5-2
ADVANCED APPLICATIONS.....		II
Chapter 6 Configuring IP Routes.....		6-1
6.1	Overview of IP Routes	6-1
6.1.1	Comparing IP Routing to Telephone Switching.....	6-1
6.1.2	Hops and Gateways.....	6-2
6.1.3	Using IP Routes to Define Default Gateways	6-2
6.1.4	Do I Need to Define IP Routes?	6-2
6.2	Viewing the IP Routing Table.....	6-3
6.3	Adding IP Routes	6-4
Chapter 7 Configuring Dynamic Host Configuration Protocol.....		7-1
7.1	Overview of DHCP	7-1
7.1.1	What Is DHCP?	7-1
7.1.2	Why Use DHCP?	7-1
7.1.3	Prestige DHCP modes	7-2
7.2	Configuring DHCP Server	7-2
7.2.1	Creating IP Address Pools.....	7-3
7.2.2	Enabling DHCP Server Mode	7-5
7.2.3	Viewing, Modifying, and Deleting Address Pools.....	7-6
7.2.4	Viewing Current DHCP Address Assignments.....	7-7
7.3	Configuring DHCP Relay	7-8
7.3.1	Defining the DHCP Relay Interface(s).....	7-8
7.3.2	Enabling DHCP relay mode	7-9
Chapter 8 Configuring Network Address Translation		8-1
8.1	Overview of NAT	8-1
8.2	Your Default NAT Setup	8-2
8.3	Viewing Your NAT Configuration	8-3
8.4	Viewing NAT Rules and Rule Statistics	8-5
8.5	Viewing Current NAT Translations	8-6

8.6	Adding NAT Rules.....	8-8
8.6.1	The NATP rule: Translating Between Private and Public IP Addresses	8-8
8.6.2	The RDR Rule: Allowing External Access to a LAN Computer	8-10
8.6.3	The Basic Rule: Performing 1:1 Translations.....	8-13
8.6.4	The Filter Rule: Configuring a Basic Rule with Additional Criteria	8-14
8.6.5	The Bimap Rule: Performing Two-way Translations.....	8-16
8.6.6	The pass rule: Allowing specific addresses to pass through un-translated	8-17
Chapter 9	Configuring the Routing Information Protocol.....	9-1
9.1	RIP Overview	9-1
9.1.1	When Should You Configure RIP?	9-1
9.2	Configuring the Prestige's Interfaces with RIP	9-2
9.3	Viewing RIP Statistics.....	9-4
Chapter 10	System Alarm and Diagnosis.....	10-1
10.1	About the System Alarm	10-1
10.2	Viewing the System Alarm Table	10-1
10.3	Diagnostics	10-2
Chapter 11	Configuring Your PPP Connection	11-1
11.1	Overview of PPP	11-1
11.2	Viewing Your Current PPP Configuration	11-1
11.2.1	Viewing PPP Configuration Details	11-3
11.3	Adding a PPP Interface Definition	11-6
11.4	Modifying PPP Interfaces.....	11-7
11.5	Deleting a PPP interface.....	11-8
Chapter 12	Configuring the ATM.....	12-1
12.1	Introduction	12-1
12.2	Viewing Your ATM Setup	12-1
12.3	Adding and Changing ATM Properties	12-2
Chapter 13	Viewing DSL Parameters.....	13-1
13.1	DSL Parameters.....	13-1
13.2	DSL Performance Statistics.....	13-2
ADVANCED MANAGEMENT	III
Chapter 14	Firewall	14-1
14.1	Overview of IP Firewall	14-1
14.2	Firewall Global Configuration.....	14-1
14.2.1	Black List Hosts	14-3
14.3	Blocking Protocols	14-4
Chapter 15	Configuring IP Filters.....	15-1
15.1	Overview of IP Filters	15-1
15.2	Viewing Your IP Filter Configuration.....	15-1
15.3	Create New IP Filter Rules.....	15-3
15.4	Modify IP Filter Rules.....	15-9
15.5	IP filter rule examples	15-9

15.6	Viewing IP Filter Statistics	15-14
Chapter 16	Configuring EOA Interfaces	16-1
16.1	Overview of EOA	16-1
16.2	PPP vs. EOA	16-1
16.3	Viewing Your EOA Setup.....	16-1
16.4	Adding EOA Interfaces.....	16-3
Chapter 17	Configuring Bridging	17-1
17.1	Introduction.....	17-1
17.2	Overview of Bridges	17-1
17.3	Bridges vs. Routers	17-1
17.4	Using the Prestige’s Bridging Feature.....	17-2
17.5	Defining Bridge Interfaces	17-2
Chapter 18	Configuring IPoA Interfaces.....	18-1
18.1	Introduction.....	18-1
18.2	Viewing Your IPoA Interface Setup	18-1
18.3	Adding IPoA Interfaces.....	18-2
18.4	Creating IPoA Mapping	18-4
18.5	IPoA Mapping Table.....	18-4
Chapter 19	Configuring DNS Relay.....	19-1
19.1	Overview.....	19-1
19.2	Viewing Your DNS Relay Setup.....	19-1
Chapter 20	Firmware Upgrade	20-1
20.1	Filename Convention	20-1
20.2	Firmware UpgradeUsing the Web Configurator	20-1
20.3	Image Upgrade Using FTP.....	20-2
20.4	Recover from Firmware Upload Failure	20-3
20.4.1	TFTP Command Example.....	20-4
20.5	GUI-based TFTP Clients.....	20-4
ADDITIONAL INFORMATION.....		IV
Chapter 20	Troubleshooting	20-1
20.1	Problems Starting Up the Prestige.....	20-1
20.2	Problems with Web Configurator.....	20-2
20.3	Problems with Internet Access	20-3
Appendix A	Diagnosing Problem Using IP Utilities	A
Appendix B	Enable Java Support in Internet Explorer	A
Appendix C	Setting Up Your Computer’s IP Address	A
Appendix D	IP Addresses, Network Masks, and Subnets	M
Appendix E	Binary Numbers.....	Q
Appendix F	PPPoE	S
Appendix G	Virtual Circuit Topology	U
Appendix H	Power Adapter Specifications.....	W
Index		Y

List of Figures

Figure 1-1 Internet Access Application	1-2
Figure 2-1 Prestige Front Panel.....	2-1
Figure 2-2 Prestige Rear Panel.....	2-2
Figure 2-3 Prestige Rear Panel Connection.....	2-4
Figure 2-4 Connecting a POTS Splitter.....	2-6
Figure 2-5 Connecting a Microfilter.....	2-7
Figure 2-6 Prestige with ISDN.....	2-7
Figure 2-7 USB Computer: IP Setup.....	2-8
Figure 2-8 USB Computer: Local Area Connection Properties	2-9
Figure 3-1 Internet Explorer: Enter Address	3-1
Figure 3-2 Web Configurator: Login Screen.....	3-2
Figure 3-3 Web Configurator: Task Bar	3-2
Figure 3-4 Web Configurator: Links	3-2
Figure 3-5 System Information	3-4
Figure 3-6 Quick Configuration	3-6
Figure 3-7 Port Settings.....	3-8
Figure 3-8 System: Modify	3-9
Figure 3-9 User Configuration	3-10
Figure 3-10 User Configuration: Add.....	3-11
Figure 3-11 User Configuration: Modify	3-11
Figure 3-12 Commit & Reboot.....	3-12
Figure 4-1 LAN Configuration.....	4-2
Figure 5-1 IP Address Table	5-1
Figure 5-2 IP Global Statistics.....	5-3
Figure 6-1 IP Route Example	6-3
Figure 6-2 IP Route Table	6-3
Figure 6-3 IP Route: Add	6-5
Figure 7-1 DHCP Server Configuration	7-3
Figure 7-2 DHCP Server Pool: Add	7-4
Figure 7-3 DHCP Configuration: Mode.....	7-6
Figure 7-4 DHCP Server Pool: Modify.....	7-7
Figure 7-5 DHCP Server Address Table.....	7-7
Figure 7-6 DHCP Relay Configuration	7-9
Figure 8-1 NAT Configuration	8-3
Figure 8-2 NAT Rule Global Statistics.....	8-5
Figure 8-3 NAT Rule Configuration.....	8-5
Figure 8-4 NAT Rule Statistics.....	8-6
Figure 8-5 NAT Translation.....	8-7
Figure 8-6 NAT Rule: Add (NAPT flavor).....	8-9

Figure 8-7 NAT Rule: Add (RDR flavor).....	8-11
Figure 8-8 NAT Rule: Add (BASIC flavor).....	8-13
Figure 8-9 NAT Rule: Add (FILTER flavor).....	8-14
Figure 8-10 NAT Rule: Add (BIMAP flavor).....	8-16
Figure 8-11 NAT Rule: Add (PASS flavor).....	8-17
Figure 9-1 RIP Configuration.....	9-2
Figure 9-2 RIP Global Statistics.....	9-4
Figure 10-1 Alarm.....	10-1
Figure 10-2 Diagnostics.....	10-2
Figure 11-1 PPP Interface: Detail.....	11-4
Figure 11-2 PPP Interface: Add.....	11-7
Figure 11-3 PPP Interface: Modify.....	11-8
Figure 12-1 ATM VCC Configuration.....	12-1
Figure 12-2 ATM VC: Add.....	12-2
Figure 13-1 DSL Status.....	13-1
Figure 13-2 DSL Parameters.....	13-2
Figure 13-3 DSL Statistics.....	13-3
Figure 13-4 DSL Interval Statistics.....	13-4
Figure 14-1 Firewall Configuration.....	14-2
Figure 14-2 Firewall Blacklisted Hosts.....	14-4
Figure 14-3 Blocked Protocols.....	14-5
Figure 15-1 IP Filter Configuration.....	15-2
Figure 15-2 IP Filter Rule: Add.....	15-4
Figure 15-3 IP Filter Rule: Modify.....	15-9
Figure 15-4 IP Filter Rule Example 1.....	15-11
Figure 15-5 IP Filter Rule Example 2.....	15-13
Figure 15-6 IP Filter Rule: Statistics.....	15-14
Figure 16-1 EOA.....	16-2
Figure 16-2 EOA Interface: Add.....	16-3
Figure 17-1 Bridge Configuration.....	17-3
Figure 18-1 IPoA.....	18-1
Figure 18-2 IPoA Interface: Add.....	18-3
Figure 18-3 IPoA Interface: Map.....	18-4
Figure 18-4 IPoA Interface: Global Map.....	18-4
Figure 19-1 Dynamic Host Configuration Protocol (DHCP) Relay Configuration.....	19-1
Figure 20-1 Image Upgrade: In Progress.....	20-2
Figure 20-2 Image Upgrade: Successful.....	20-2
Figure 20-3 FTP Session Example.....	20-3

List of Tables

Table 2-1 Front Panel LED Description	2-1
Table 2-2 Rear Panel Description	2-3
Table 2-3 Prestige Default Settings	2-10
Table 3-1 Web Configurator- Button Description	3-3
Table 3-2 System Information	3-5
Table 3-3 Quick Configuration.....	3-7
Table 3-4 System: Modify	3-9
Table 3-5 User Configuration: Add	3-11
Table 3-6 User Configuration: Modify	3-12
Table 3-7 Web Configurator Reboot Options	3-13
Table 4-1 LAN Configuration	4-3
Table 5-1 IP Address Table Field Descriptions.....	5-2
Table 6-1 IP Routing Table.....	6-4
Table 7-1 DHCP Server Pool: Add.....	7-4
Table 7-2 Action Buttons.....	7-6
Table 7-3 DHCP Server Address Table	7-8
Table 8-1 NAPT Rule.....	8-2
Table 8-2 NAT Configuration.....	8-4
Table 8-3 NAT Translation Table Fields.....	8-7
Table 8-4 NAT Translation Details Fields	8-8
Table 11-1 PPP Configuration	11-2
Table 11-2 PPP Interface: Detail	11-4
Table 12-1 ATM VC: Add	12-3
Table 14-1 Firewall Configuration	14-2
Table 14-2 Firewall Blacklisted Hosts.....	14-4
Table 14-3 Blocked Protocols	14-5
Table 15-1 IP Filter Rule: Add	15-5
Table 15-2 IP Filter Rule: Modify	15-9
Table 16-1 EOA	16-2
Table 16-2 EOA Interface: Add.....	16-4
Table 17-1 Bridge Configuration.....	17-3
Table 18-1 IPoA	18-2
Table 18-2 IPoA Interface: Add.....	18-3
Table 18-3 IPoA Interface: Map.....	18-4
Table 18-4 IPoA Interface: Global Map	18-5
Table 19-1 Dynamic Host Configuration Protocol (DHCP) Relay Configuration	19-2
Table 2 General Commands for GUI-based TFTP Clients	20-4
Table 20-1 Troubleshooting the Start-Up of Your Prestige.....	20-1
Table 20-2 Troubleshooting the Web Configurator	20-2

Table 20-3 Troubleshooting the Internet Access 20-3

Preface

Congratulations on your purchase of the Prestige 623 series Dual-link ADSL Router.

There are two Prestige 623 models, one for ADSL over POTS (Plain Old Telephone System) and one for ADSL over ISDN (Integrated Synchronous Digital System). Both models are discussed together in this guide.

About This User's Guide

This user's guide covers all aspects of Prestige's operations and shows you how to get the best out of the multiple advanced features of your Prestige using the web configurator. It is designed to guide you through the correct configuration of your Prestige for various applications.

Related Documentation

- Supporting Disk
More detailed information and examples can be found in the included disk (as well as on the zyxel.com web site).
- 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 Glossary and Web Site
Please refer to www.zyxel.com for an online glossary of networking terms and additional support documentation.

Syntax Conventions

- “Select” or “Choose” means for you to use one predefined choices.
- 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 623 Dual-link ADSL Router may be referred to simply as the Prestige in this user's guide.

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 ADSL?

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

Part I:

GETTING STARTED

This part is structured as a step-by-step guide to help you connect, install and set up your Prestige to operate on your network and to access the Internet. Described are Key Features and Applications, Hardware Installation, Initial Setup and Getting Started with the Web Configurator.

Chapter 1

Introduction

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

1.1 Prestige 623 Dual-link ADSL Router

Your Prestige integrates a high-speed 10/100Mbps auto-negotiating LAN interface, a USB port and one high-speed DSL port into a single package. The Prestige is ideal for high-speed DSL Internet browsing and making LAN-to-LAN connections to remote networks.

1.2 Features of the Prestige

Your Prestige is packed with a number of features that give it the flexibility to provide a complete networking solution for almost anyone.

- Support Multi-Mode standard (ANSI T1.413, Issue 2; G.DMT (G.992.1); G.Lite (G992.2)) with auto detection.
- Supports transparent bridging as specified in IEE 802.1d
- Supports bridged PDU encapsulation(Spanning tree)
- One auto-sensing 10/100M Ethernet interface
- Support Multi-protocol over AAL5 (RFC1483)
- Support PPP over ATM AAL5 (RFC 2364)
- Support PPP over Ethernet (RFC2516)
- DHCP Client, Sever and Relay
- Supports Internet Protocol Configuration Protocol (IPCP)
- RIP I/ RIP II supported.
- PAP or CHAP for user authentication
- Support UBR, CBR, and GFR (Guaranteed Frame Rate) service classes
- Embedded firewall includes NAT, IP filtering and raw filtering
- Supports up to 8 Virtual Channel Connections (VCCs)

- Connection admission control (CAC)--Prevents network users from allocating more bandwidth than the network can provide.
- Support for OAM F5 AIS, RDI and loopback cells
- Management access via SNMP and embedded web configurator.
- Supports most major applications including: FTP, SNMP, ICMP, H.323, L2TP, Quake, ICQ and CUSeeMee
- USB Support Windows98/98SE, Windows 2000, Windows ME and Windows XP.

1.3 Internet Access Application for The Prestige

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

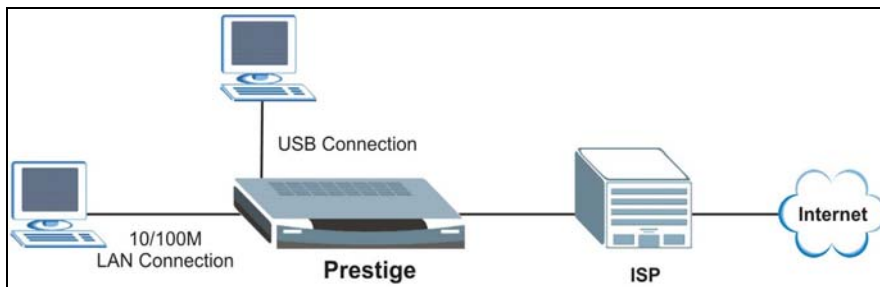


Figure 1-1 Internet Access Application

1.4 Additional Requirements

In order to use your Prestige, you must have the following:

- DSL service up and running on your telephone line.
- A computer with a network card or a USB port.
- An Ethernet hub/switch, if you are connecting the Prestige to more than one computer through the Ethernet ports.
- For web configurator: a web browser such as Internet Explorer v5.0 or later with JavaScript® enabled.

Chapter 2

Hardware Installation and Initial Setup

This chapter describes the physical features of the Prestige and how to make cable connections.

2.1 Front Panel

The LEDs indicate the real-time status of the Prestige.



Figure 2-1 Prestige Front Panel

The following table describes the LEDs on the front panel.

Table 2-1 Front Panel LED Description

LED	COLOR	STATUS	FUNCTION
PWR	Green	On	The Prestige is receiving power.
		Off	The Prestige is not receiving power.
SYS	Green	On	The Prestige is functioning properly.
		Off	The Prestige is not ready or has malfunctioned.
	Orange	On	The Prestige is in reset mode.
USB	Green	On	A computer is connected to the USB port on the Prestige.
		Blinking	The Prestige is sending or receiving data to or from the attached computer through the USB port.
		Off	No computer is connected to the USB port on the Prestige.

Table 2-1 Front Panel LED Description

LED	COLOR	STATUS	FUNCTION
10/100M	Green (10M)	On	The Prestige has a successful LAN connection at 10Mbps.
		Off	The Prestige does not have a LAN connection.
		Blinking	The Prestige is sending or receiving data to or from the attached computer through the LAN port at 10Mps.
	Orange (100M)	On	The Prestige has a successful LAN connection at 100Mbps.
		Off	The Prestige does not have a LAN connection.
		Blinking	The Prestige is sending or receiving data to or from the attached computer through the LAN port at 100 Mbps.
DSL	Green	On	The Prestige is linked successfully to a DSL line.
		Off	The line is down.
		Blinking Slow	The Prestige is waiting for the DSL connection to initialize.
		Blinking Fast	The DSL connection is initializing.
ACT	Green	Off	No data is being transmitted.
		Blinking	The Prestige is receiving or sending data through the DSL line.

2.2 Rear Panel and Connections of the Prestige

The following figure shows the rear panel of your Prestige.

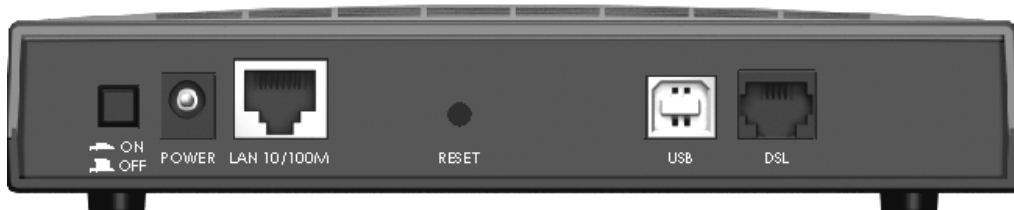
**Figure 2-2 Prestige Rear Panel**

Table 2-2 Rear Panel Description

LABEL	DESCRIPTION
ON/OFF	Switches the unit on and off.
POWER	Connects to the power source using the power adapter for your region.
LAN 10/100M	Connect to a computer using a crossover Ethernet cable or a hub/switch using a straight-through Ethernet cable.
RESET	Resets the Prestige to the manufacturer's default configuration.
USB	Connects to the USB port on your computer.
DSL	Connects to a telephone jack using the telephone wire.

The following figure illustrates the hardware connections.

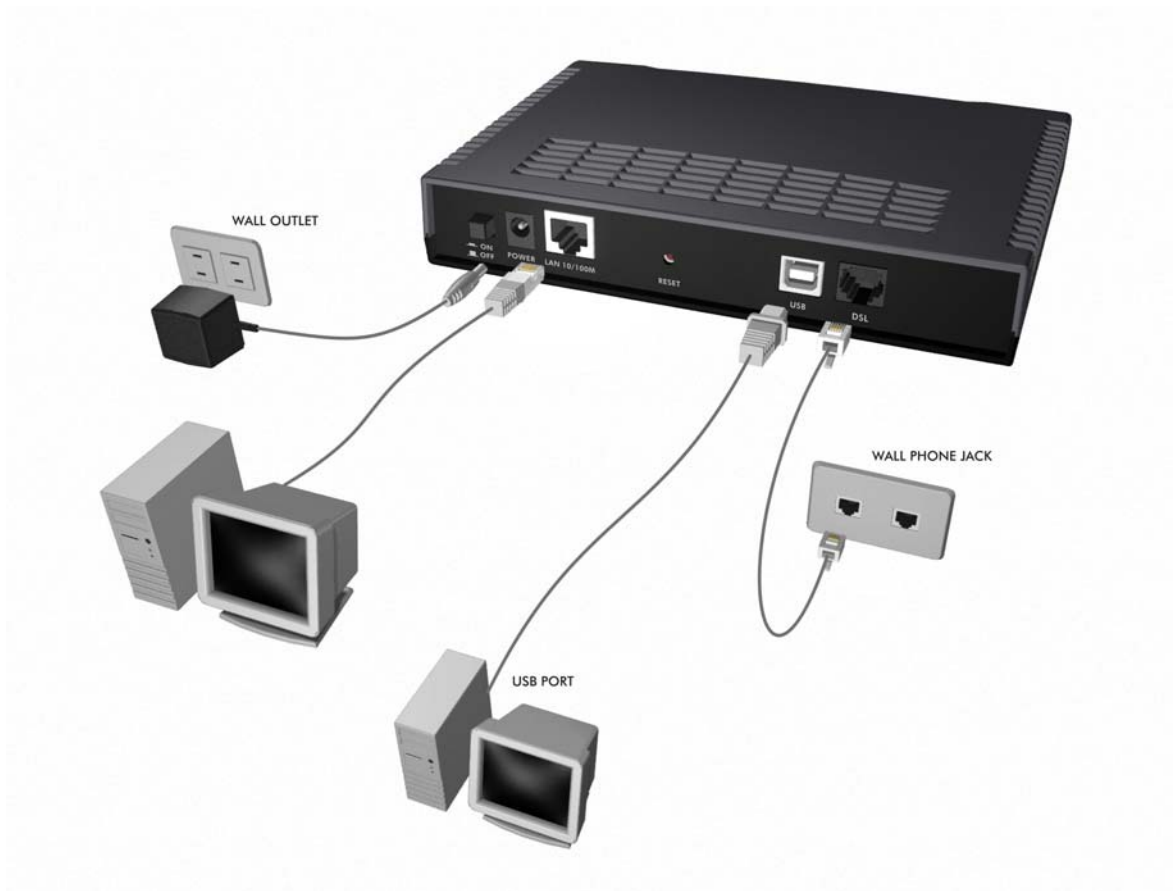


Figure 2-3 Prestige Rear Panel Connection

2.2.1 DSL Port

Connect the Prestige directly to the telephone wall jack using the included telephone wire.

2.2.2 10/100M Ethernet Ports

Connect to a computer using a crossover Ethernet cable or to a hub using a straight-through Ethernet cable.

2.2.3 Power Port

Connect the power adapter to the port labeled **POWER** on the back of your Prestige.

To avoid damage to the Prestige, make sure you use only the included power adapter. Refer to the *Power Adapter Specifications Appendix* for more information.

2.2.4 USB Port

The USB port is useful if you have a USB-enabled computer that does not have a network interface card for attaching to your Ethernet network. The USB driver supports Windows 98/98 SE/Me/2000/XP. Refer to the *Quick Start Guide* for instructions.

2.2.5 Reset Button

If you have forgotten the Prestige's IP address or administrative password, use the **RESET** button to reset the Prestige back to factory default settings. Use a pointed object to press the **RESET** button three times to reset the Prestige. The administrative password will reset to "1234" and the Prestige IP addresses are reset to "192.168.1.1" (LAN port) and "192.168.1.2" (USB port).

Resetting the Prestige erases all your custom configuration.

2.3 Prestige with POTS

Sections 2.3.1 and 2.3.2 relate to people who use the Prestige with ADSL over POTS (analog telephone service) only.

2.3.1 Connecting a POTS Splitter

This is for the Prestige that follows the Full Rate (G.dmt) standard only. One major difference between ADSL and dial-up modems is the optional telephone splitter. This device keeps the telephone and ADSL signals separated, giving them the capability to provide simultaneous Internet access and telephone service on the same line. Splitters also eliminate the destructive interference conditions caused by telephone sets. The purchase of a POTS splitter is optional.

Noise generated from a telephone in the same frequency range as the ADSL signal can be disruptive to the ADSL signal. In addition the impedance of a telephone when off-hook may be so low that it shunts the strength of the ADSL signal. When a POTS splitter is installed at the entry point, where the line comes into the home, it will filter the telephone signals before combining the ADSL and telephone signals transmitted and received. The issues of noise and impedance are eliminated with a single POTS splitter installation.

A telephone splitter is easy to install as shown in the following figure.

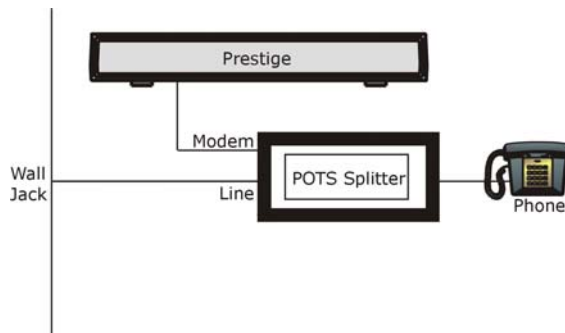


Figure 2-4 Connecting a POTS Splitter

- Step 1.** Connect the side labeled “Phone” to your telephone.
- Step 2.** Connect the side labeled “Modem” to your Prestige.
- Step 3.** Connect the side labeled “Line” to the telephone wall jack.

2.3.2 Telephone Microfilters

Telephone voice transmissions take place in the lower frequency range, 0 - 4KHz, while ADSL transmissions take place in the higher bandwidth range, above 4KHz. A microfilter acts as a low-pass filter, for your telephone, to ensure that ADSL transmissions do not interfere with your telephone voice transmissions. The purchase of a telephone microfilter is optional.

- Step 1.** Connect a phone cable from the wall jack to the single jack end of the Y- Connector.
- Step 2.** Connect a cable from the double jack end of the Y-Connector to the “wall side” of the microfilter.
- Step 3.** Connect another cable from the double jack end of the Y-Connector to the Prestige.
- Step 4.** Connect the “phone side” of the microfilter to your telephone as shown in the following figure.

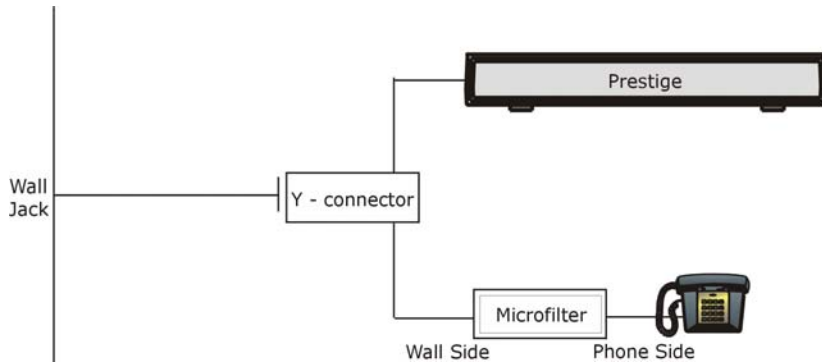


Figure 2-5 Connecting a Microfilter

2.4 Prestige With ISDN

This section relates to people who use their Prestige with ADSL over ISDN (digital telephone service) only. The following is an example installation for the Prestige with ISDN.

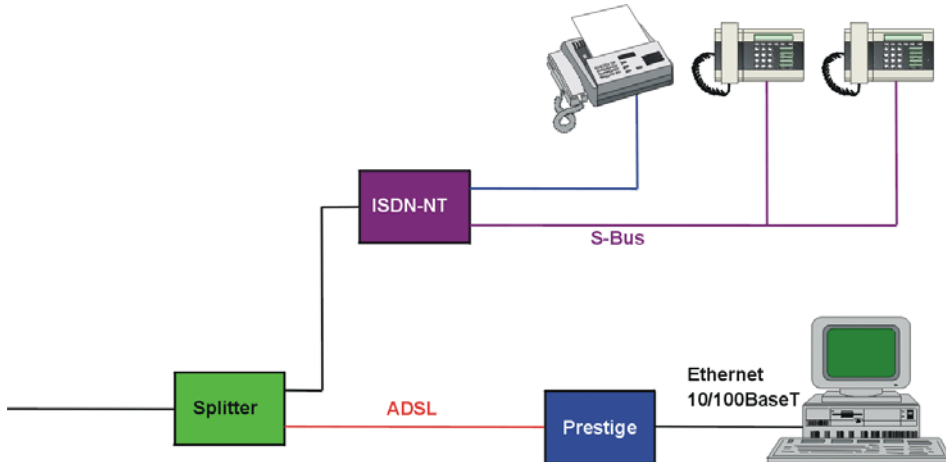


Figure 2-6 Prestige with ISDN

2.5 Setting Up Your USB Computer's IP Address

By default, the Prestige automatically assigns all required Internet settings to your computer(s). You need only to configure the computer(s) to accept the information when it is assigned.

You must configure the USB computer so that its IP properties place it on the same subnet as the Prestige's USB port. There are two ways to do this:

- Use the DHCP Server feature on the Prestige to assign IP address dynamically to your USB computer
- Assign a static IP address to your USB computer.

Follow the steps to set up your USB computer's IP address. Windows 2000 screen shots are shown. Steps and screen shots may vary depending on the version of Windows.

Step 1. Click **Start, Control Panel and Network and Dial-up Connections**. the icon that corresponds to your new USB connection (not the one that corresponds to your Ethernet NIC).

Step 2. Right-click on the icon that corresponds to your new USB connection (not the one that corresponds to your Ethernet NIC) and select **Properties**.

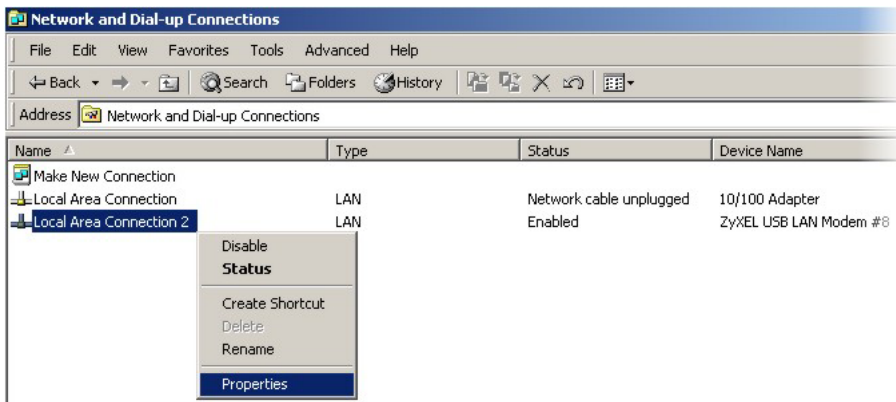


Figure 2-7 USB Computer: IP Setup

Step 3. In the Properties screen, make sure the **Connect Using** field displays “ZyXEL USB LAN Modem #n” (where n is a number).

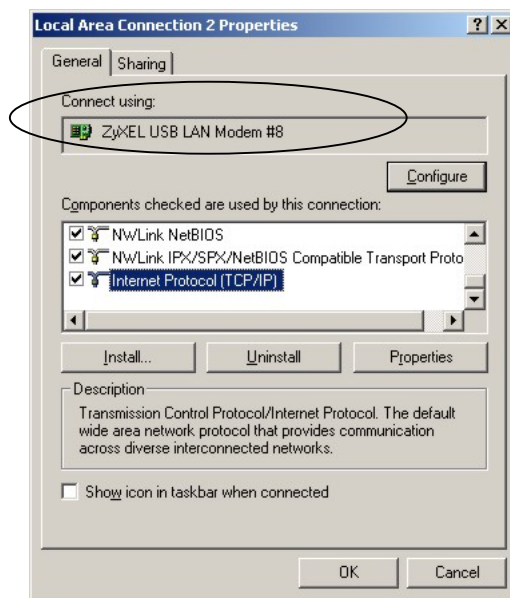


Figure 2-8 USB Computer: Local Area Connection Properties

- Step 4.** Select **Internet Protocol (TCP/IP)** and click **Properties**. Refer to the *Setting Up Your Computer's IP Address* appendix for more information.
- Step 5.** The USB port on the Prestige is pre-configured with these properties (you cannot change these values):

USB port IP address:	192.168.1.2
USB port subnet mask:	255.255.255.0

If you want to assign your USB computer a static (fixed) IP address, your computer must be configured as follows:

IP address:	192.168.1.n where n is a number from 3 to 34.
Subnet mask:	255.255.255.0
Default gateway:	192.168.1.2

2.6 Configuring the Prestige

The Prestige is pre-configured with default settings for use with a typical home or small office network.

The *Prestige Default Settings* table below lists important default settings (others are described in the subsequent chapters). Verify that they meet the needs of your network, or follow the instructions to change them if necessary.

Before modifying any settings, review *Chapter 3* for general information about using the web configurator. You don't need to make changes to the default settings unless your ISP supplies you with additional information.

Table 2-3 Prestige Default Settings

OPTION	DEFAULT SETTING	EXPLANATIONS/INSTRUCTIONS
Web Configurator	Login user name: admin Login password: 1234	The login user name and password allow you to login and configure the embedded web configurator on your Prestige.
ATM Properties	One ATM interface defined with these properties: Supports aal5 VPI = 8 VCI = 35 MUX type: LLC	The VPI and VCI values determine the path of your connection to your ISP. You don't need to change the default settings unless your ISP instructs you with additional information. See chapter on ATM VCC for additional instructions.
DHCP (Dynamic Host Configuration Protocol)	DHCP server enabled with a pool of addresses (for LAN and USB ports): 192.168.1.3 through 192.168.1.34 (subnet mask = 255.255.255.0)	The Prestige maintains a pool of private IP addresses for dynamic assignment to your LAN/USB computers. To use this service, you must have set up your computers to accept IP information dynamically, as described in the <i>Setting Up Your Computer's IP Address</i> appendix. See later chapter for an explanation of the DHCP service.
NAT (Network Address Translation)	napt rule enabled	Your computers' private IP addresses (see DHCP above) will be translated to your public IP address whenever they access the Internet. See chapter on NAT service.
LAN/USB Port IP Address	Assigned static IP address: 192.168.1.1 subnet mask: 255.255.255.0	This is the IP address of the LAN port on the Prestige. The LAN port connects the Prestige to your Ethernet network. Typically, you will not need to change this address. See section on changing the Prestige LAN IP address.

Table 2-3 Prestige Default Settings

OPTION	DEFAULT SETTING	EXPLANATIONS/INSTRUCTIONS
USB Port IP Address	Assigned static IP address: 192.168.1.2 subnet mask: 255.255.255.0	This is the IP address assigned to the USB port on the Prestige.
ISP Connection Properties	Login user name: Login password: (as supplied by your ISP)	The login user name and password are used to authenticate you as a customer of your ISP using the Point-to-Point protocol (PPP). See the chapter on configuring your PPP for instructions on changing these and other PPP values.

2.7 Testing Your Installation

After you have connected the Prestige and set basic configuration as described in the *Quick Start Guide*, test the Internet connection.

To test the connection, turn on the Prestige, wait about 10 seconds, and then verify that its LEDs are illuminated. Refer to the LED descriptions in *Section 2.1*.

If the LEDs illuminate as expected, test your Internet connection from a LAN computer (and from the USB computer, if applicable): Open your web browser, and type the URL of any external website (such as <http://www.zyxel.com>). The **ACT** LED should be blinking rapidly and may appear solid as the Prestige connects to the site.

If the LEDs do not illuminate as expected or the web page does not display:

- Ensure that the default settings are appropriate for your network setup.
- See *Troubleshooting* for tips on correcting a variety of common problems.
- Contact your ISP customer support for assistance.

Chapter 3

Getting Started with the Web Configurator

This chapter describes how to use the web configurator.

3.1 Introduction

The web configurator makes it easy to configure and manage the Prestige. Access the web configurator from any computer connected to the Prestige via the LAN or the USB port.

Your Prestige may already be configured to provide Internet connectivity for your network. If it works properly with the pre-configured settings, then you may not need to use the web configurator. You don't need to change the settings unless your ISP instructs you with additional information.

3.2 Accessing the Web Configurator

To access the web configurator, you need a computer connected to the LAN or USB port on the Prestige and a web browser installed on the computer. The web configurator is designed to work best with Microsoft Internet Explorer® version 5.0, Netscape Navigator® version 4.7, or later versions.

You can access the program from any computer connected to the Prestige via the LAN or USB ports.

- Step 1.** Make sure your Prestige hardware is properly connected.
- Step 2.** Prepare your computer to connect to the Prestige (refer to the *Setting Up Your Computer's IP Address* appendix).
- Step 3.** Launch your web browser.
- Step 4.** Enter either “192.168.1.1” or “192.168.1.2” as the web site address.

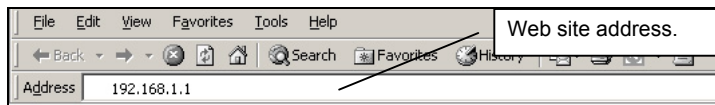


Figure 3-1 Internet Explorer: Enter Address

- Step 6.** Enter the user name (“admin” is the default), password (“1234” is the default) and click **OK**.

Default User Name: **admin**
Default Password: **1234**

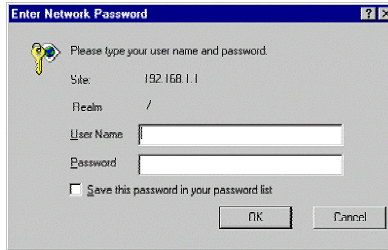


Figure 3-2 Web Configurator: Login Screen

**You can change the password at any time (see *Error! Reference source not found.*).
The default user name cannot be changed.**

3.3 Navigating the Web Configurator

You can use these page elements to navigate through the web configurator:

3.3.1 Navigation Tab

The navigation tab that displays at the top of all web configurator screens provides a consistent way to access all screens.



Figure 3-3 Web Configurator: Task Bar

On certain web configurator screens, you have a selection of links as shown below. There can be more than one way to access some of the web screens.



Figure 3-4 Web Configurator: Links

3.3.2 Commonly used buttons

The commonly used buttons that display at the bottom of each page take action related to the currently displayed task.

Table 3-1 Web Configurator- Button Description

BUTTON	DESCRIPTIONS
Submit	Click this button to store, in temporary system memory, any changes you have made on the current page. See <i>Committing Your Changes</i> discussed later for instructions on storing changes permanently.
Refresh	Click this button to redisplay the current page with updated statistics.
Clear	When accumulated statistics are displaying, click this button to reset the statistics to their initial values.
Help	Click this button to launch the online help for the current topic in a separate browser window. Help is available for any main topic page.

3.4 Viewing Basic System Information

The **System View** screen displays when you first access the web configurator. It is the home page.

The **System View** table provides a snapshot of your system configuration. You can click on the table headings that are highlighted in red to display more details on those settings or the configuration page for that feature. The following table describes the groups of data shown on the **System View** screen and, where appropriate, refers you to the appropriate chapters in this user's guide for more information.

Home | Quick Configuration

System View

Use this page to get the summary on the existing configuration of your device.

Device		DSL			
Model:	P623-43	Operational Status:	Startup Handshake		
H/W Version:	81001a	Last State:	0x0		
S/W Version:	1.38(IR.0)b2	DSL Version:	V1.4.2		
Serial Number:	1	Standard:	Multimode		
Mode:	Routing And Bridging	Up		Down	
Up Time:	2:4:11	Speed	Latency	Speed	Latency
Time:	Thu Jan 01 02:04:11 1970	0 Kbps	-	0 Kbps	-
Time Zone:	GMT				
Daylight Saving Time:	OFF				
Name:	-				
Domain Name:	-				

WAN Interfaces							
Interface	Encapsulation	IP Address	Mask	Gateway	Lower Interface	VPI/VCI	Status
eea-0	Bridged	0.0.0.0	0.0.0.0	0.0.0.0	aal5-0	8/35	

LAN Interface							
Interface	Mac Address	IP Address	Mask	Lower Interface	Speed	Duplex	Status
eth-0	00:A0:C5:41:84:52	192.168.1.1	255.255.255.0	-	Auto	Auto	
usb-0	-	192.168.1.2	255.255.255.0	-	-	-	

Services Summary							
Interface	NAT	IP Filter	RIP	DHCP Relay	DHCP Client	DHCP Server	IGMP
eth-0	✓ inside	✗	✗	✗	✗	✓	✗
eea-0	✓ outside	✗	✗	✗	✗	✗	✗
usb-0	✓ inside	✗	✗	✗	✗	✓	✗

Modify Refresh Help

Figure 3-5 System Information

The following table describes the fields in this screen.

Click on the name in the table heading to display the corresponding configuration screen.

Table 3-2 System Information

FIELD	DESCRIPTION
Device	This table displays basic information about the Prestige hardware and software versions, the system uptime (since the last reboot) and the pre-configured operating mode.
DSL	This table displays performance statistics for the DSL line. Click the DSL in the table header to view additional DSL settings. Refer to the chapter on DSL.
WAN Interfaces	This table displays the various settings for the interfaces on the Prestige that communicate with your ISP via DSL. Although you only have one physical DSL port, multiple software-defined interfaces can be configured to use it. See the <i>PPP</i> , <i>ATM VCC</i> , <i>EOA</i> , and <i>IPoA</i> chapters for more information about the interfaces defined on your system.
LAN Interfaces	This table displays the various settings for the interfaces on the Prestige that communicate directly with your network. These typically include at least one Ethernet interface, named eth-0, and may include a USB interface named usb-0. You can configure some properties of the Ethernet interface. The USB interface properties are not configurable.
Services Summary	<p>This table displays the following service that the Prestige performs to help you manage your network:</p> <ul style="list-style-type: none"> Translating private IP addresses to your public IP address. See the chapter on <i>NAT</i>. Setting up filtering rules that accept or deny incoming or outgoing data. See the chapter on IP filters. Enabling router-to-router communication. See the chapter on <i>RIP</i>. Dynamic assignment or receipt of IP. See the chapter on <i>DHCP</i> and appendix for TCP/IP settings. Message forwarding based on Internet Group assignment (IGMP, not configurable).

You can display the **System View** screen from other locations in the program by clicking the **Home** tab.

3.5 Quick Configuration

The **Quick Configuration** screen displays the settings you are most likely to need to change when you first set up your Prestige for Internet access. Your ISP should have given you most of the information you need to change.

To open the **Quick Configuration** screen, click **Home** on the task bar and then the **Quick Configuration** link.

The screenshot shows the 'Quick Configuration' screen of the Prestige 623 Series Dual-link ADSL Router. The interface has a dark blue header with navigation tabs: Home, LAN, WAN, Bridging, Routing, Services, and Admin. Below the header, the current page is identified as 'Home | Quick Configuration'. The main title is 'Quick Configuration', followed by the instruction: 'Use this page to quickly configure the system.'

The configuration fields are organized into sections:

- ATM Interface:** 0
- Operation Mode:** Enabled
- Encapsulation:** 1483 Bridged IP LLC
- VPI:** 8
- VCI:** 35
- Bridge:** Enabled
- IGMP:** Disabled
- IP Address:** 0 0 0 0
- Subnet Mask:** 0 0 0 0
- Default Route:** Disabled
- Gateway IP Address:** 0 0 0 0

The **PPP** section includes:

- Username:** GSPN
- Password:** (empty)
- Use DNS:** Enable, Disable

The **DNS** section includes:

- Primary DNS Server:** 0 0 0 0
- Secondary DNS Server:** 0 0 0 0

At the bottom of the form are four buttons: Submit, Delete, Cancel, and Help.

Figure 3-6 Quick Configuration

The following table describes the fields in this screen.

Table 3-3 Quick Configuration

FIELD	DESCRIPTION
ATM Interface	Select an ATM interface from the drop-down list menu.
Operation Mode	Select Enabled from the drop-down list menu to set the Prestige to provide routing function and act as an Internet gateway for your LAN. Otherwise select Disabled .
Encapsulation	Select the encapsulation method your ISP uses from the drop-down list menu. See chapter on <i>Configuring the ATM VCC</i> . NOTE: If you select IPoA (starts with 1483) encapsulation types, you must configure the default gateway and default route in the IPoA Configuration page. See chapter on <i>Configuring IPoA Interfaces</i> .
VPI/ VCI	Enter the unique data path your modem uses to communicate with your ISP. See chapter on <i>Configuring the ATM VCC</i> .
Bridge	Select Enabled from the drop-down list menu to activate bridging between your Prestige and ISP. Otherwise select Disabled . Your ISP may also refer to this using "RFC 1483" or "Ethernet over ATM". See chapter on bridging for more information.
IGMP	Depending on your ISP, select Enabled from the drop-down list menu to activate IGMP (Internet Group Management Protocol) which some ISPs may use to perform remote configuration on your Prestige. Otherwise select Disabled .
IP Address and Subnet Mask	If your ISP given a public IP address to you, enter the IP address and the associated subnet mask in the fields provided.
Default Route	Select Enabled from the drop-down list menu to set the IP address specified above as the default route for your LAN. Otherwise select Disabled . This is the default setting.
Gateway IP Address	Enter the IP address of the default gateway (or your ISP server).
PPP	
Username	Enter the username provided by your ISP. (Note: this is not the same as the user name and password you used to log in to Configuration Manager.)
Password	Enter the password associated with the username above.
Use DNS	Select Enable if your ISP provides you with DNS (Domain Name Service) information. Otherwise, select Disable .
DNS	

Table 3-3 Quick Configuration

FIELD	DESCRIPTION
Primary/Secondary DNS	If you select Yes in the Use DNS field, enter the IP address(es) of the DNS server(s) provided by your ISP.
Click Submit to confirm your changes. Refer to the section on <i>Committing Your Changes and Rebooting the Prestige</i> to save your changes to permanent memory and make your changes take effect.	

3.6 Port Settings

Your ISP may also have special circumstances that require changing the HTTP, Telnet or FTP port numbers. You do not have to make the changes unless your ISP informs you with the necessary port information.

To display **Port Settings** screen, click the **Admin** tab and then **Port Settings**.

Figure 3-7 Port Settings

Enter the port number in the corresponding fields.

After you have made the changes, click **Submit** to confirm your changes. Refer to the section on *Committing Your Changes and Rebooting the Prestige* to save your changes to permanent memory and make your changes take effect.

3.7 System Date and Time

The Prestige keeps a record of the current date and time, which it uses to calculate and report various performance data.

Changing the Prestige date and time does not affect the date and time on your computer(s).

To display the **System – Modify** screen, click **Home** and then **Modify** at the bottom of the page

System - Modify

System Parameters

Date: Jan 1 1970

Time: 2 : 12 : 48

Time Zone: GMT +0000 Greenwich Mean

Daylight Saving Time: ON OFF

Name:

Domain Name:

Figure 3-8 System: Modify

Table 3-4 System: Modify

FIELD	DESCRIPTION
Date	Specify a new date from the drop-down list boxes.
Time	Specify a new time from the drop-down list boxes.
Time Zone	Select the time difference between your time zone and the Greenwich Mean Time from the drop-down list menu.
Daylight Saving Time	To use Daylight Saving Time (DST), Select On . Otherwise select Off . Daylight Saving Time is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daylight time in the evenings.
Name	Specify the name of your computer.
Domain Name	Specify the domain name of your ISP.
Click Submit to confirm your changes. Refer to the section on <i>Committing Your Changes and Rebooting the Prestige</i> to save your changes to permanent memory and make your changes take effect.	

3.8 Managing Prestige User Accounts

You can create up to four user accounts to access the web configurator on the Prestige. The first time you log into the web configurator, you use the default user name (**admin**) and password (**1234**). This is the administrator account on the Prestige. You cannot change the administrator account username.

There are two privilege levels: root and user. The privilege levels determine to what extent the user can modify the system configuration on the Prestige.

Root level – full access rights including creating, modifying and deleting Prestige user accounts and changing all Prestige system configuration.

User level – With this account type, no modification of system configuration allowed. You can only view the system settings.

3.8.1 Creating User Accounts

Step 1. Click **Admin** in the task bar. The **User Configuration** screen displays by default. If not, click **User Config**.



Figure 3-9 User Configuration

Step 2. Click **Add** to display the configuration screen as shown.

Figure 3-10 User Configuration: Add

The following table describes the fields in this screen.

Table 3-5 User Configuration: Add

FIELD	DESCRIPTION
User ID	Enter the username for this account.
Privilege	Select the access rights for this account. Choices are Root and User .
Old Password	Enter a password associated with the username specified in this field.
Confirm Password	Enter the password again for confirmation.

Click **Submit** to confirm your changes. Refer to the section on *Committing Your Changes and Rebooting the Prestige* to save your changes to permanent memory and make your changes take effect.

3.8.2 Changing User Account Password


In the **User Configuration** screen, click  in the **Action(s)** column for the user account you wish to change. A screen displays as shown.

Figure 3-11 User Configuration: Modify

The following table describes the fields in this screen.

Table 3-6 User Configuration: Modify

FIELD	DESCRIPTION
User ID	This read-only field displays the username for this account.
New Password	Enter a new password associated with the username specified in this field.
Confirm New Password	Enter the new password again for confirmation.

Click **Submit** to confirm your changes. Refer to the section on *Committing Your Changes and Rebooting the Prestige* to save your changes to permanent memory and make your changes take effect.

3.9 Committing Your Changes and Rebooting the Prestige

Whenever you use the web configurator to change system settings, the changes are initially placed in temporary storage (called random access memory or RAM). Your changes are made effective when you submit them, but will be lost if the Prestige is turned off.

**Submitting changes saves them only until the Prestige is reset or powered down.
Committing changes saves them permanently.**

3.9.1 Committing Your Changes

To save your changes for future use, you can use the commit function. This function saves your changes to permanent storage (called flash memory).

Step 1. Click **Admin** and then click **Commit & Reboot** to display the **Commit & Reboot** screen.

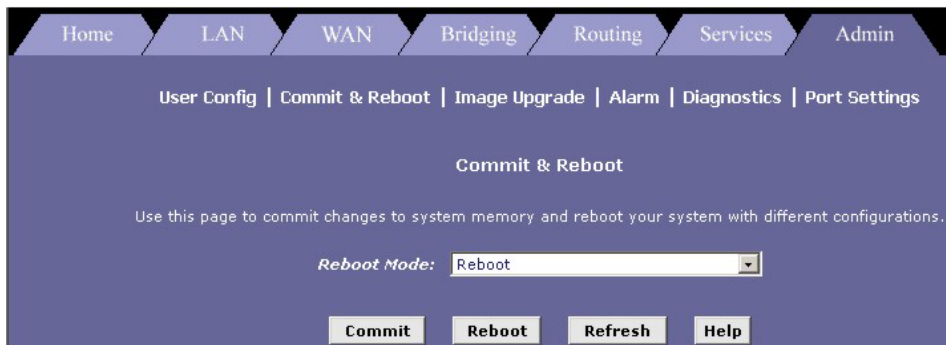


Figure 3-12 Commit & Reboot

Step 2. Click **Commit** to save the changes to permanent storage.

The previous settings are copied to backup storage so that they can be recalled if your new settings do not work properly (see the rebooting instructions next).

3.9.2 Rebooting the Prestige Using the Web Configurator

If you change the LAN IP address information, you must reboot the system after committing the changes in order to activate them. All other changes are activated when you commit them (no reboot is needed).

If, after rebooting the Prestige, you find that it does not operate properly with the new configuration, you can reboot using options that reactivate a previous configuration or the manufacturer's default configuration.

To reboot the Prestige, display the **Commit & Reboot** screen (see *Figure 3-12*), select the appropriate reboot mode from the drop-down menu, and then click **Reboot**.

The following table describes the reboot options available.

Table 3-7 Web Configurator Reboot Options

OPTION	DESCRIPTION
Reboot From Last Configuration	Select this option to reboot the Prestige using the latest saved configuration.
Reboot From Backup Configuration	Select this option to reboot the Prestige using settings stored in backup memory. These are the settings that were in effect before you committed new settings in the current session.
Reboot From Default Configuration	Select this option to reboot the Prestige to default settings provided by your ISP or the manufacturer. Choosing this option erases any custom settings.
Reboot From Clean Configuration	<p style="text-align: center;">This option is reserved for experienced technicians only.</p> <p>Select this option to reboot the Prestige with zero configuration. All configuration is erased including the factory default settings. Your computer <i>cannot</i> communicate with the Prestige through the LAN or USB port. You should have a serial port connection to the Prestige.</p>
Reboot From Minimum Configuration	<p style="text-align: center;">This option is reserved for experienced technicians only.</p> <p>Select this option to reboot the Prestige with minimum configuration. The Ethernet interface and administrative user account are configured for telnet login only.</p>

Do NOT reboot the Prestige using the RESET button on the rear panel of the Prestige to activate new changes. This button resets the Prestige settings to the manufacturer's default values. Any custom settings will be lost.

Chapter 4

Setting the LAN IP Address

This chapter describes how to change the Prestige's LAN IP address, or configure it to be assigned automatically.

4.1 What is the LAN IP Address?

Your Prestige communicates with your network through its LAN port. To allow for Internet communication, the LAN port must be identified by a unique IP address, like your computers. The IP address associated with this port is called the LAN IP address.

The public IP address assigned to you by your ISP is not your LAN IP address. The public IP address identifies the WAN (ADSL) port on your Prestige to the Internet.

Your Prestige is pre-configured with a default LAN IP address of **192.168.1.1**. You can change the default address to reflect the set of IP addresses that you want to use with your network.

You can also configure the Prestige to use a LAN IP address that is assigned dynamically from a DHCP server on your network. When IP information is assigned by another device, the Prestige is said to be acting as a DHCP client of that device.

The Prestige itself can function as a DHCP server for your LAN computers, as described in later chapters, but not for its own LAN port.

4.2 IGMP

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 and version 2 . At start up, the Prestige queries all directly connected networks to gather group membership. After that, the Prestige periodically updates this information.

4.3 Changing the LAN IP Address

Click on the LAN tab to display the LAN Configuration screen as shown next.

LAN Config | DHCP Mode | DHCP Server | DHCP Relay

LAN Configuration

Use this page to set the LAN configuration, which determines how your device is identified on the network.

LAN Configuration	
System Mode:	Routing And Bridging
Get LAN Address:	<input checked="" type="radio"/> Manual <input type="radio"/> External DHCP Server <input type="radio"/> Internal DHCP Server
LAN IP Address:	<input type="text" value="192"/> <input type="text" value="168"/> <input type="text" value="1"/> <input type="text" value="1"/>
LAN Network Mask:	<input type="text" value="255"/> <input type="text" value="255"/> <input type="text" value="255"/> <input type="text" value="0"/>
IGMP:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

USB Configuration	
USB IP Address:	<input type="text" value="192"/> <input type="text" value="168"/> <input type="text" value="1"/> <input type="text" value="2"/>
USB Network Mask:	<input type="text" value="255"/> <input type="text" value="255"/> <input type="text" value="255"/> <input type="text" value="0"/>
IGMP:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Submit Cancel Refresh Help

Figure 4-1 LAN Configuration

The following table describes the fields in this screen.

Table 4-1 LAN Configuration

FIELD	DESCRIPTION
LAN Configuration Set the fields below to configure the LAN port on the Prestige.	
System Mode	This field displays the pre-configured mode for the Prestige. This field is read-only.
Get LAN Address	To specify a static IP address to the LAN port, select Manual and enter an IP address in the IP Address field. To accept a dynamic IP address from your ISP's DHCP server, select External DHCP Server . To accept a dynamic IP address from a DHCP server on your network, select Internal DHCP Server .
LAN IP Address	Enter an IP address if you select Manual in the Get LAN Address field. This is the IP address your computers use to identify the LAN port of the Prestige. The public IP address assigned to you by your ISP is <i>NOT</i> your LAN IP address. The public IP address identifies the WAN (ADSL) port on your ADSL/Ethernet router to the Internet.
LAN Network Mask	Enter the subnet mask that identifies which parts of the LAN IP address refer to your network as a whole and which parts refer to specific nodes on the network.
IGMP	Select Enable to activate IGMP on the LAN port. Otherwise, select Disable .
USB Configuration Set the fields below to configure the USB port on the Prestige.	
USB IP Address	Specify the IP address for the USB port on the Prestige. If you changed the USB IP address through USB connection, then the connection will be terminated.
USB Network Mask	Specify the subnet mask for the USB port on the Prestige. If necessary, change the IP address of the computer's USB port to be in the same subnet of the Prestige's USB port.
IGMP	Select Enable to activate IGMP on the USB port. Otherwise, select Disable .
Click Submit to confirm your changes. Refer to the section on <i>Committing Your Changes and Rebooting the Prestige</i> to save your changes to permanent memory and make your changes take effect.	

Chapter 5

Viewing System IP Information and Performance Statistics

This chapter describes how to view system and network data for your Prestige

5.1 Introduction

The interfaces on your Prestige that communicate with other network and Internet devices are identified by unique Internet Protocol (IP) addresses. You can use the web configurator to view the list of IP addresses that your Prestige uses, and to view other system and network performance data.

See the *IP Addresses, Network Masks and Subnets Appendix* for a description of IP addresses and masks.

5.2 Viewing Your Prestige's IP Addresses

Click **Routing** in the task bar and then click the **IP Addr** link. The **IP Address Table** screen displays.

IP Address	Netmask	IF Name
127.0.0.1	255.0.0.0	lo-0
192.168.1.1	255.255.255.0	eth-0
192.168.1.2	255.255.255.0	usb-0

Figure 5-1 IP Address Table

The following table describes the fields in this screen.

Table 5-1 IP Address Table Field Descriptions

FIELD	DESCRIPTION
IP Address	This field displays the IP address of the ports.
Netmask	This field displays the subnet mask of the ports.
IF Name	This field displays the interface names of the ports. eth-0 : the LAN (Ethernet) port of the Prestige. usb-0 : the USB port. The IP address for the USB port is assigned automatically at start-up. ppp-0 or eoal-0 : the WAN (ADSL line) port of the Prestige. lo-0 : the loopback port. This is a special address that enables the Prestige to keep any data addressed directly to it, rather than route the data through the WAN or LAN port.
Global Stats	Click Global Stats to view global IP statistics. Refer to <i>Section 5.3</i> .
Refresh	Click Refresh to update the screen.
Help	Click Help to display on-line HTML help.

If your Prestige has additional IP-enabled interfaces, the IP addresses of these will be displayed.

5.3 Viewing IP Global Statistics

You can view statistics on the processing of Internet protocol packets (a packet is a collection of data that has been bundled for transmission). You will not typically need to view this data, but you may find it helpful when working with your ISP to diagnose network and Internet data transmission problems.

To view global IP statistics, click **Global Stats** in the **IP Address Table** screen to display the **IP Global Statistics** screen as shown next.

IP Global Statistics	
IP Datagrams Statistic	Values
<i>IP Received:</i>	1139 Packets
<i>IP Received w/ Header Error:</i>	0 Packets
<i>IP Received w/ Wrong Address:</i>	0 Packets
<i>IP Received w/ Unknown Protocol:</i>	0 Packets
<i>IP Routing Discarded:</i>	0 Packets
IP Datagrams Forwarded	
<i>Forwarded Datagrams:</i>	218 Packets
Input IP Datagrams	
<i>Input IP Discarded:</i>	0 Packets
<i>Input IP Delivered To User-Protocol:</i>	921 Packets
Output IP Datagrams	
<i>IP Requests For Transmission w/ User-Protocol:</i>	881 Packets
<i>Output IP Discarded:</i>	0 Packets
<i>Output IP Discarded w/ No Route:</i>	218 Packets
IP Datagrams / Reassemble	
<i>Maximum # of Seconds IP Waits For Reassemble:</i>	60 Second(s)
<i>IP Received Which Needed To Be Reassembled:</i>	0 Packets
<i>IP Successfully Re-assembled:</i>	0 Packets
<i>IP Fails To Re-Assemble:</i>	0 Packets
IP Datagrams / Fragment	
<i>IP Successfully Fragmented:</i>	0 Packets
<i>IP Fails To Fragment:</i>	0 Packets
<i>IP Fragments Created:</i>	0 Packets

Figure 5-2 IP Global Statistics

Click **Refresh** to display updated statistics showing any new data since you opened the page. Click **Close** to close the window.

Part II:

ADVANCED APPLICATIONS

This part shows how to set up IP Routes, DHCP, NAT, RIP, PPP Connection, ATM and viewing System Alarm, Diagnostics and DSL Parameters.

Chapter 6

Configuring IP Routes

This chapter describes basic routing concepts and provides instructions for creating routes

6.1 Overview of IP Routes

The essential challenge of a router is: when it receives data intended for a particular destination, which next device should it send that data to? When you define IP routes, you provide the rules that a Prestige uses to make these decisions.

Most users do not need to define IP routes.

6.1.1 Comparing IP Routing to Telephone Switching

IP routing decisions are similar to those made by switchboards that handle telephone calls.

When you dial a long distance telephone number, you are first connected to a switchboard operated by your local phone service carrier. All calls you initiate go first to this main switchboard.

If the phone number you dialed is outside your calling area, the switchboard opens a connection to a higher-level switchboard for long distance calls. That switchboard looks at the area code you dialed and connects you with another switchboard that serves that area. This new switchboard, in turn, may look at the prefix in the number you dialed (the middle set of three numbers) and connect to a more localized switchboard that handles numbers with that prefix. This final switchboard can then look at the last four digits of the phone number to open a connection with the person or company you dialed.

In comparison, when your computer initiates communication over the Internet, such as viewing a web page connecting to a web server, the data it sends out includes the IP address of the destination computer (the “phone number”). All your outgoing requests first go to the same router at your ISP (the first “switchboard”). That router looks at the network ID portion of the destination address (the “area code”) and determines which next router to send the request to. After several such passes, the request arrives at a router for the destination network, which then uses the host ID portion of the destination IP address (the local “phone number”) to route the request to the appropriate computer.

With both the telephone and the computer, all transactions are initially sent to the same switchboard or router, which serves as a gateway to other higher- or lower-level devices. No single device knows at the outset the eventual path the data will take, but each uses a specific part of the destination address/phone number to make a decision about which device to connect to next.

6.1.2 Hops and Gateways

Each time Internet data is passed from one Internet address to another, it is said to take a *hop*. A hop can be a handoff to a different port on the same device, to a different device on the same network, or to a device on an entirely different network.

When a hop passes data from one type of network to another, it uses a gateway. A gateway is an IP address that provides initial access to a network, just as a switchboard serves as a gateway to a specific set of phone numbers. For example, when a computer on your LAN requests access to a company's web site, your ISP serves as a gateway to the Internet. As your request reaches its destination, another gateway provides access to the company's web servers.

6.1.3 Using IP Routes to Define Default Gateways

IP routes are defined on computers, routers, and other IP-enabled devices to instruct them which hop to take, or which gateway to use, to help forward data along to its specified destination.

If no IP route is defined for a destination, then IP data is passed to a predetermined default gateway. The default gateway serves like a higher-level telephone switchboard; it may not be able to connect directly to the destination, but it will know a set of other devices that can help pass the data intelligently. If it cannot determine which of these devices provides a good next hop (because no such route has been defined), then that device will forward the data to *its* default gateway. Eventually, a high level device, using a predefined IP route, will be able to forward the data along a path to its destination.

6.1.4 Do I Need to Define IP Routes?

Most users do not need to define IP routes. On a typical small home or office LAN, the existing routes that set up the default gateways for your LAN computers and for the Prestige provide the most appropriate path for all your Internet traffic.

- On your LAN computers, a default gateway directs all Internet traffic to the LAN port on your Prestige. Your LAN computers know their default gateway either because you assigned it to them when you modified their TCP/IP properties, or because you configured them to receive the information dynamically from a server whenever they access the Internet. (Each of these processes is described in the *Hardware Installation and Initial Setup* chapter.)
- On the Prestige itself, a default gateway is defined to direct all outbound Internet traffic to a router at your ISP. This default gateway is assigned automatically by your ISP whenever the device negotiates an Internet connection. (The process for adding a default route is described later.)

You may need to define routes if your home setup includes two or more networks or subnets, if you connect to two or more ISP services, or if you connect to a remote corporate LAN. For example, the Prestige knows about network **N2** in the following figure through remote node router **R1**. However, the Prestige is unable

to route a packet to network **N3** because it does not know that there is a route through remote node router **R1** (via router **R2**). IP routes allow you to tell the Prestige about the networks beyond the remote nodes.

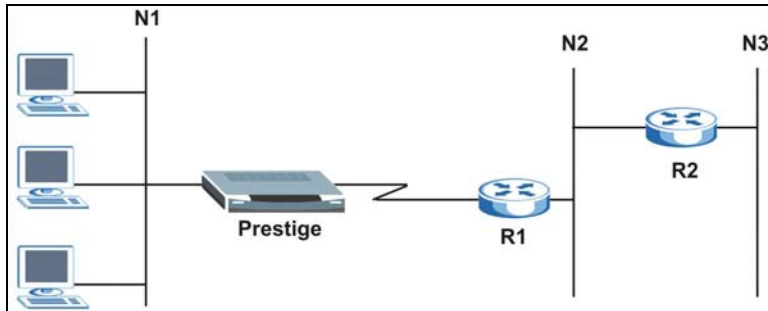


Figure 6-1 IP Route Example

6.2 Viewing the IP Routing Table

All IP-enabled computers and routers maintain a table of IP addresses that are commonly accessed by their users. For each of these destination IP addresses, the table lists the IP address of the first hop the data should take. This table is known as the device's routing table. To view the Prestige's routing table, click **Routing** in the task bar. The **IP Route Table** displays by default.

The screenshot shows the router's web interface. At the top, there is a navigation bar with tabs: Home, LAN, WAN, Bridging, Routing, Services, and Admin. Below this, there is a sub-menu with options: IP Route, IP Addr, LAN Config, DSL, ATM VC, PPP, EOA, and IPOA. The main content area is titled "IP Route Table". Below the title, there is a descriptive paragraph: "This table lists IP addresses of Internet destinations commonly accessed by your network. When a computer requests to send data to a listed destination, the device uses the Next Hop to identify the first Internet router it should contact to route the data most efficiently." Below the text is a table with the following data:

Destination	Netmask	NextHop	IF Name	Route Type	Route Origin	Action
127.0.0.0	255.0.0.0	127.0.0.1	lo-0	Direct	Dynamic	
192.168.1.0	255.255.255.0	192.168.1.1	eth-0	Direct	Dynamic	
192.168.1.1	255.255.255.255	127.0.0.1	lo-0	Direct	Dynamic	
192.168.1.2	255.255.255.255	127.0.0.1	lo-0	Direct	Dynamic	


At the bottom of the table, there are three buttons: Add, Refresh, and Help.

Figure 6-2 IP Route Table

The **IP Route Table** displays a row for each existing route. These include routes that were predefined on the device, routes you may have added, and routes that the device has identified automatically through communication with other devices. The routing table should reflect a default gateway, which directs outbound Internet traffic to your ISP. This default gateway is shown in the row containing destination address 0.0.0.0.

The following table defines the fields in the **IP Route Table**.

Table 6-1 IP Routing Table

FIELD	DESCRIPTION
Destination	This field specifies the IP address of the destination computer. The destination can be specified as the IP address of a specific computer or an entire network. It can also be specified as all zeros to indicate that this route should be used for all destinations for which no other route is defined (this is the route that creates the default gateway).
Netmask	This field indicates which parts of the destination address refer to the network and which parts refer to a computer on the network. Refer to <i>IP Address, Network Masks and Subnets</i> appendix for more information. The default gateway uses a netmask of 0.0.0.0.
NextHop	This field specifies the next IP address to send data to when its final destination is that shown in the destination column.
IFName	This field displays the name of the interface on the device through which data is forwarded to the specified next hop.
Route Type	This field displays whether the route is direct or indirect. In a direct route, the source and destination computers are on the same network, and the router attempts to directly deliver the data to the computer. In an indirect route, the source and destination computers are on different networks, and the router forwards data to a device on another network for further handling.
Route Origin	This field displays how the route was defined. Dynamic indicates that the route was created automatically or predefined by your ISP or the manufacturer. Routes you create are labeled Local. Other routes can be created automatically (using RIP, as described in later chapter), or defined remotely through various network management protocols (LCL or ICMP).
Action	This field displays an icon () you can click on to delete a route.

6.3 Adding IP Routes

Follow these instructions to add an IP route to the routing table.

Step 1. In the **IP Route Table** screen, click **Add**. The **IP Route – Add** page displays.

IP Route Information				
Destination:	0	0	0	0
Netmask:	255	255	255	0
Gateway/NextHop:	0	0	0	0

Submit Cancel Help

Figure 6-3 IP Route: Add

- Step 2.** Specify the destination, network mask, and gateway or next hop for this route.
- To create a route that defines the default gateway for your LAN, enter 0.0.0.0 in both the **Destination** and **Net Mask** fields. Enter your ISP's IP address in the **Gateway/NextHop** field.
- Note that you cannot specify the interface name, route type or route origin. These parameters are used only for routes that are identified automatically as the Prestige communicates with other routing devices. For routes you create, the routing table displays system default values in these fields.
- Step 3.** Click **Submit** to confirm your changes.
- The **IP Routing Table** will now display the new route.
- Step 4.** Follow the instructions in the section on *Committing Your Changes and Rebooting the Prestige* to save your changes to permanent memory and make your changes take effect.

Chapter 7

Configuring Dynamic Host Configuration Protocol

This chapter provides an overview of DHCP and instructions for implementing it on your network.

7.1 Overview of DHCP

7.1.1 What Is DHCP?

DHCP is a protocol that enables network administrators to centrally manage the assignment and distribution of IP information to computers on a network.

When you enable DHCP on a network, you allow a device – such as your Prestige or a router located with your ISP – to assign temporary IP addresses to your computers whenever they want to use the Internet. The assigning device is called a DHCP server, and the receiving device is a DHCP client.

If you follow the instructions in the *Setting Up Your Computer's IP Address* appendix, you either configured each LAN computer with an IP address, or you specified that it will receive IP information dynamically (automatically). If you chose to have the information assigned dynamically, then you configured your computers as DHCP clients that will accept IP addresses assigned from a DHCP server such as the Prestige.

The DHCP server draws from a defined pool of IP addresses and “leases” them for a specified amount of time to your computers when they request an Internet session. It monitors, collects, and redistributes the addresses as needed.

On a DHCP-enabled network, the IP information is assigned dynamically rather than statically. A DHCP client can be assigned a different address from the pool each time it initiates a new Internet connection.

7.1.2 Why Use DHCP?

DHCP allows you to manage and distribute IP addresses throughout your network from a central computer. Without DHCP, you would have to configure each computer separately with IP addresses and related information. DHCP is commonly used with large networks and those that are frequently expanded or otherwise updated.

7.1.3 Prestige DHCP modes

The Prestige can be configured as a DHCP server, DHCP relay agent, or, in some cases, a DHCP client.

- If you configure the Prestige as a DHCP server, it will maintain the pool of addresses and distribute them to your LAN computers. If the pool of addresses includes private IP addresses, you must also configure the Network Address Translation service, so that the private addresses can be translated to your public IP address on the Internet
- If your ISP performs the DHCP server function for your network, then you can configure the Prestige as a DHCP relay agent. When the Prestige receives a request for Internet access from a computer on your network, it contacts your ISP for the necessary IP information, and then relays the assigned information back to the computer.
- If you have another computer or device on your network that is already performing the DHCP server function, then you can configure the LAN port on the device to be a DHCP client of that server (as are your computers). This configuration is not discussed in this chapter. See the chapter on LAN IP settings.

You can input settings for both DHCP server and DHCP relay mode, and then activate either mode at any time. De-activated settings are retained for your future use.

7.2 Configuring DHCP Server

Before you begin, determine the pool of IP addresses you want to make available for distribution to your computers. These addresses can be multiple public addresses that you have purchased from your ISP, but are typically private addresses that you create. (Network administrators often create private IP addresses for use only on their networks. See *Overview of NAT* section.)

By default, the Prestige is configured as a DHCP server, with a predefined IP address pool of 192.168.1.3 through 192.168.1.34 (subnet mask 255.255.255.0). Refer to the *Setting Up Your Computer's IP Address* appendix.

The following sections describe the three steps in configuring DHCP server for you Prestige.

- Create IP pool
- Enable Prestige as DHCP server
- Configure your computer to accept the assigned IP address from the Prestige.

7.2.1 Creating IP Address Pools

Step 1. Click **LAN** in the task bar, then click **DHCP Server**. The **DHCP Server Configuration** screen displays.

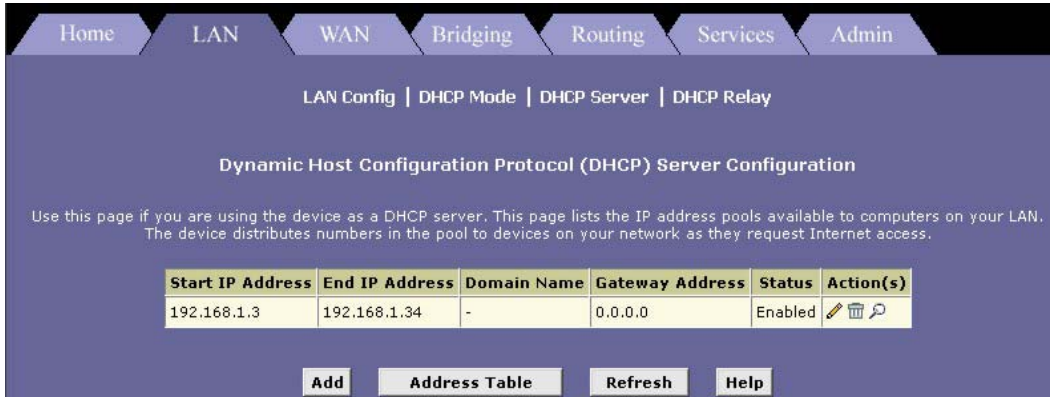


Figure 7-1 DHCP Server Configuration

Each pool you create displays in a row on the table on this screen. You can create up to eight pools. In this example, one pool has been created for the LAN interface and another for the USB interface. Additional pools may be needed when the Prestige is configured with multiple LAN interfaces.

To add an IP address pool, click **Add** to display the **DHCP Server Pool – Add** screen.

Figure 7-2 DHCP Server Pool: Add

Fill in the required **Start IP Address**, **End IP Address**, **Net Mask**, and **Gateway Address**; the others are optional. The following table describes the fields in this screen.

Table 7-1 DHCP Server Pool: Add

FIELD	DESCRIPTION
Start/End IP Addresses	Type the starting and ending addresses in the pool in these fields.
Mac Address	<p>Use this field only if you want to assign a specific IP address to a specific computer (that is, you are creating an exception to the dynamic assignment of addresses). The IP address you specify will be assigned to the computer that corresponds to this MAC address. (A MAC address is a manufacturer-assigned hardware ID that is unique for each device on a network.)</p> <p>If you type a MAC address here, you must have specified the same IP address in both the Start IP Address and End IP Address fields.</p>

Table 7-1 DHCP Server Pool: Add

FIELD	DESCRIPTION
Net Mask	<p>Specifies which portion of each IP address in this range refers to the network and which portion refers to the host (computer).</p> <p>For a description of network masks and LAN network masks, see the appendix. You can use the network mask to distinguish which pool of addresses should be distributed to a particular subset of computers on your LAN (called a subnet).</p>
Domain Name	<p>Enter a user-friendly name that refers to the group of computers (subnet) that will be assigned addresses from this pool.</p>
Gateway Address	<p>Enter the address of the default gateway for computers that receive IP addresses from this pool.</p> <p>The default gateway is the IP address that the computers first contact to communicate with the Internet. Typically, it is the Prestige's LAN port IP address. See previous section for an explanation of gateway addresses.</p>
DNS	<p>Enter the IP address of the Domain Name Server (DNS) to be used by computers that receive IP addresses from this pool.</p> <p>The DNS translates common Internet names that you type into your web browser into their equivalent numeric IP addresses. Typically, this server is located with your ISP.</p>
SDSN...SWINS (optional)	<p>Enter the IP addresses of devices that perform various services for computers that receive IP addresses from this pool. Typically, these devices are servers located with your ISP.</p>
<p>Click Submit to confirm your changes. Refer to the section on <i>Committing Your Changes and Rebooting the Prestige</i> to save your changes to permanent memory and make your changes take effect.</p>	

7.2.2 Enabling DHCP Server Mode

After you have defined a DHCP pool, you set the Prestige to operate in DHCP server mode. (It may already be set, by default.)

- Step 1.** In the **LAN** tab, click **DHCP Mode** to display the **DHCP Configuration** screen. Select **DHCP Server** from the **DHCP Mode** drop-down list and then click **Submit**. A screen displays to confirm the change.

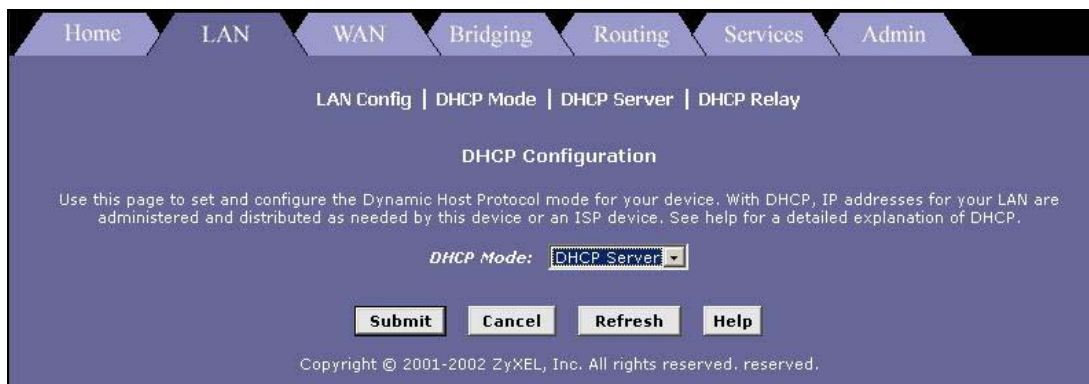


Figure 7-3 DHCP Configuration: Mode




Step 2. Refer to the section on *Committing Your Changes and Rebooting the Prestige* to save your changes to permanent memory and make your changes take effect.

You must configure the computer to obtain IP address dynamically. Refer to the *Setting Up Your Computer's IP Address* appendix.

7.2.3 Viewing, Modifying, and Deleting Address Pools

To view, modify, or delete an existing address pool, display the **DHCP Server Configuration** screen by clicking the **DHCP Server** link, and click the following icons in the corresponding row in the address pool table.

Table 7-2 Action Buttons

TO PERFORM THIS ACTION	...CLICK THIS ICON:
Delete an IP address pool	
Modify an IP address pool	
View details for an IP address pool	

You can modify an address pool to change the domain name associated with the pool or to exclude IP addresses within its range from distribution. You may want to exclude an address if you have already designated it for fixed use with a specific device, or for any other reason you do not want to make it available to your network. To change any other properties of the pool, such as the starting and ending IP addresses, you must delete the pool and create a new one.

DHCP Pool Information							
Start IP Address:	192.168.1.3						
End IP Address:	192.168.1.34						
Netmask:	255.255.255.0						
Domain Name:	<input type="text"/>						
Status:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable						
Excluded IP:	<table border="1"> <thead> <tr> <th>Excluded IP Address</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td colspan="2">No Excluded IP!</td> </tr> <tr> <td> <input type="text" value="192"/> <input type="text" value="168"/> <input type="text" value="1"/> <input type="text" value="3"/> </td> <td><input type="button" value="Add"/></td> </tr> </tbody> </table>	Excluded IP Address	Action	No Excluded IP!		<input type="text" value="192"/> <input type="text" value="168"/> <input type="text" value="1"/> <input type="text" value="3"/>	<input type="button" value="Add"/>
	Excluded IP Address	Action					
No Excluded IP!							
<input type="text" value="192"/> <input type="text" value="168"/> <input type="text" value="1"/> <input type="text" value="3"/>	<input type="button" value="Add"/>						

Figure 7-4 DHCP Server Pool: Modify

To exclude an address from the distribution list, type the address in the **Excluded IP** field and click **Add**.

After you have made the changes, click **Submit** to confirm your changes. Refer to the section on *Committing Your Changes and Rebooting the Prestige* to save your changes to permanent memory and make your changes take effect.

7.2.4 Viewing Current DHCP Address Assignments

When your Prestige functions as a DHCP server for your LAN, it keeps a record of any addresses it has leased to your computers. To view a table of all current IP address assignments, display the **DHCP Server Configuration** screen, and then click **Address Table**.

IP Address	Netmask	Mac Address	Pool Start	Address Type	Time Remaining
192.168.1.3	255.255.255.0	00:A0:C5:41:84:53	192.168.1.3	Dynamic	2582961 Second(s)
192.168.1.4	255.255.255.0	00:00:E8:86:26:5B	192.168.1.3	Dynamic	2583494 Second(s)
192.168.1.5	255.255.255.0	00:A0:C5:FF:01:01	192.168.1.3	Dynamic	2583043 Second(s)
192.168.1.6	255.255.255.0	00:50:BA:24:EA:90	192.168.1.3	Dynamic	0 Second(s)
192.168.1.7	255.255.255.0	00:50:BA:AD:4F:81	192.168.1.3	Dynamic	2589658 Second(s)

Figure 7-5 DHCP Server Address Table

The **DHCP Server Address Table** lists any IP addresses that are currently leased to LAN devices. For each leased address, the table lists the following information:

Table 7-3 DHCP Server Address Table

FIELD	DESCRIPTION
IP Address	This field displays the address that has been leased from the pool.
Netmask	This field displays the network mask associated with the leased address, which identifies the network ID and host ID portions of the address. See <i>IP Addresses, Network Masks and Subnets Appendix</i> for more information.
Mac Address	This field displays a hardware ID for the device to which the number has been assigned.
Pool Start	This field displays the lower boundary of the address pool (provided to identify the pool from which the leased number came).
Address Type	This field displays the type of address, Static or Dynamic , assigned to the specific device. Static indicates that the IP number has been assigned permanently. Dynamic indicates that the number has been leased temporarily for a specified length of time.
Time Remaining	The amount of time left for the device to use the assigned address.

7.3 Configuring DHCP Relay

Some ISPs perform the DHCP server function for their customers' home/small office networks. In this case, you can configure the Prestige as a DHCP relay agent. When a computer on your network requests Internet access, your Prestige contacts your ISP to obtain an IP address (and other information), and then forwards that information to the computer.

Before you begin, be sure to have the IP address and network mask of your ISP's DHCP server.

The following sections describe the three steps in configuring DHCP relay for you Prestige.

- Defining the DHCP relay interface
- Enable Prestige as DHCP relay server
- Configure your computer to accept the assigned IP address from the Prestige.

7.3.1 Defining the DHCP Relay Interface(s)

First, you specify the IP address of the DHCP server and select the interfaces on your network that will be using the relay service.

Step 1. Launch the web configurator, click **LAN** in the task bar, and then click **DHCP Relay** to display the **DHCP Relay Configuration** screen.

Home LAN WAN Bridging Routing Services Admin

LAN Config | DHCP Mode | DHCP Server | DHCP Relay

Dynamic Host Configuration Protocol (DHCP) Relay Configuration

As a DHCP relay agent, when a computer request Internet access, the device requests an IP address from your ISP, and then relays the addresses back to the computers. This table lists each interface on the device that relays data from your ISP. Typically, the LAN port is listed.

DHCP Server Address:

Interfaces Running DHCP Relay	Action
eoa-0	
<input type="text" value="eth-0"/>	<input type="button" value="Add"/>

Figure 7-6 DHCP Relay Configuration

- Step 2.** Type the IP address of your ISP's DHCP server in the **DHCP Server Address** field. If you do not have this number, it is not essential to enter it here. Requests for IP information from your LAN will be passed to the default gateway, which should route the request appropriately.
- Step 3.** If the interface named **eth-0** is not already displayed, select it from the drop-down list and click **Add**. The **eth-0** interface specifies that your default Ethernet (LAN) interface is running DHCP relay for your LAN. Typically, this is the only interface you need to specify here. If your Prestige has additional interfaces that you want to perform DHCP relay, you can select and add them. You can delete an interface from the table by clicking in the **Action** column.
- Step 4.** Click **Submit** to confirm your changes. A page displays to confirm your changes.
- Step 5.** Follow the steps in the section on *Committing Your Changes and Rebooting the Prestige* to save your changes to permanent memory and make your changes take effect.

7.3.2 Enabling DHCP relay mode

- Step 1.** Click **DHCP Mode** to display the **DHCP Mode** screen (see *Figure 7-3*). From the **DHCP Mode** drop-down list menu, select **DHCP Relay** and click **Submit**. A page displays to confirm the change.

Step 2. Refer to the section on *Committing Your Changes and Rebooting the Prestige* to save your changes to permanent memory and make your changes take effect.

You must configure the computer to obtain IP address dynamically. Refer to the *Setting Up Your Computer's IP Address* appendix.

Chapter 8

Configuring Network Address Translation

This chapter provides an overview of Network Address Translation (NAT) and instructions for modifying the default configuration on your device.

8.1 Overview of NAT

Network Address Translation is a method for disguising the private IP addresses you use on your LAN as the public IP address you use on the Internet. You define NAT rules that specify exactly how and when to translate between public and private IP addresses.

In a typical NAT setup, your ISP provides you with a single public IP address to use for your entire network. Then, you assign each computer on your LAN a unique private IP address. (Or, you define a pool of private IP addresses for dynamic assignment to your computers, as described in the chapter on *Configuring Dynamic Host Configuration Protocol*.) On the Prestige, you set up a NAT rule to specify that whenever one of your computers communicates with the Internet, (that is, it sends and receives IP data packets) its private IP address – which is referenced in each packet – will be replaced by the LAN's public IP address.

An IP data packet contains bits of data bundled together in a specific format for efficient transmission over the Internet. Such packets are the building blocks of all Internet communication. Each packet contains header information that identifies the IP address of the computer that initiates the communication (the source IP address), the port number that the router associates with that computer (the source port number), the IP address of the targeted Internet computer (the destination IP address), and other information.

When the NAT rule is applied, because the source IP address is swapped out, it appears to other Internet computers as if the data packets are coming from the computer assigned your public IP address (in this case, the Prestige).

The NAT rule could further be defined to disguise the source port in the data packet (i.e., change it to another number), so that outside computers will not be able to determine the actual port from which the packet originated. Data packets that arrive in response contain the public IP address as the destination IP address and the disguised source port number. The Prestige changes the IP address and source port number back to the original values (having kept track of the changes it made earlier), and then routes the packet to the originating computer.

NAT rules such as these provide several benefits:

- They eliminate the need for purchasing multiple public IP addresses for computers on your LAN. You can make up your own private IP addresses at no cost. These addresses are not useful on the Internet, however.
- They provide a measure of security for your LAN by enabling you to assign private IP addresses. The Prestige prevents external access to your privately addressed computers (except when using an rdr rule discussed later). In addition, the private addresses are replaced in all outbound data packets, so external computers never see the private addresses anyway.

The type of NAT function described above is called network address port translation (napt). You can use other types, called flavors, of NAT for other purposes; for example, providing outside access to your LAN or translating multiple private addresses to multiple public addresses.

8.2 Your Default NAT Setup

By default, NAT is enabled, with an **napt** rule configured to perform the following translation:

Table 8-1 NAPT Rule

THESE PRIVATE IP ADDRESSES:	...ARE TRANSLATED TO:
192.168.1.3 192.168.1.4 . . . 192.168.1.34	Your ISP-assigned public IP address

This default NAT setup assumes that, on each LAN computer, you configured TCP/IP properties as follows:

- You selected the check box that enables them to receive their IP addresses automatically (that is, to use a DHCP server);
- or,
- You assigned static IP addresses to your computers in the range 192.168.1.3 through 192.168.1.34.

If your computers are not configured in one of these ways, you can either change the IP addresses on your computers to match the NAT setup, or delete this NAT rule and add a new one that matches the addresses you assigned to your computers (see *Adding NAT Rules* section).

8.3 Viewing Your NAT Configuration

To view your NAT settings, click **Services** in the task bar, and then click **NAT**. The **Network Address Translation (NAT) Configuration** screen displays as shown.

NAT | RIP | FireWall | IP Filter | DNS | Blocked Protocols

Network Address Translation (NAT) Configuration

Use this page to configure Network Address Translation, a security protocol in which the device translates the IP addresses of your LAN computers to new addresses before sending data out on the Internet.

NAT Options: NAT Global Info

Enable Disable

NAT Global Information	
TCP Idle Timeout(sec):	86400
TCP Close Wait(sec):	60
TCP Def Timeout(sec):	60
UDP Timeout(sec):	300
ICMP Timeout(sec):	5
GRE Timeout(sec):	300
Default Nat Age(sec):	240
NAPT Port Start:	50000
NAPT Port End:	51023

Submit Global Stats Cancel Refresh Help

Figure 8-1 NAT Configuration

The **Network Address Translation (NAT) Configuration** page contains the following elements:

- The **NAT Options** drop-down list, which provides access to the **Global Information** page (shown by default), the **Network Address Translation (NAT) Rule Configuration** page, and the **NAT Translations** page, which shows current translations.
- **Enable/Disable** buttons allow you to turn the NAT feature on or off.
- The **NAT Global Information** table displays settings that apply to all NAT rule translations.

- Buttons you use to submit or cancel changes, display global statistics, and access help.

Table 8-2 NAT Configuration

FIELD	DESCRIPTION
TCP Idle Timeout (sec)	Enter the number of seconds. For a NAT translation session on data that uses the TCP protocol, the translation will no longer be performed if no matching data packets are received after the specified time has elapsed.
TCP Close Wait (sec)	Enter the number of seconds. For a NAT translation on data using the TCP protocol, after a communication session has been closed, the translation will no longer be performed if no matching data packets are received after the specified time has elapsed.
TCP Def Timeout (sec)	Enter the number of seconds. For a NAT translation session on data that uses the TCP protocol, the translation will no longer be performed if no matching data packets are received after the specified time has elapsed.
UDP Timeout (sec)	Same as TCP Idle Timeout, but for UDP packets.
ICMP Timeout (sec)	Same as TCP Idle Timeout, but for ICMP packets.
GRE Timeout (sec)	Same as TCP Idle Timeout, but for GRE packets.
Default Nat Age (sec)	For all other NAT translation sessions, the number of seconds after which a translation session will no longer be valid.
NAPT Port Start/End	When an napt rule is defined, the source ports will be translated to sequential numbers in this range.
Click Submit to confirm your changes. Refer to the section on <i>Committing Your Changes and Rebooting the Prestige</i> to save your changes to permanent memory and make your changes take effect.	

Click **Global Stats** to view accumulated data on how many NAT rules have been invoked and how much data has been translated.

NAT Rule Global Statistics	
Total NAT Sessions	
<i>Total Translation Sessions:</i>	0 Sessions
<i>Number of FTP ALG Sessions:</i>	0 Sessions
<i>Number of SNMP ALG Sessions:</i>	0 Sessions
<i>Number of Real Audio ALG Sessions:</i>	0 Sessions
<i>Number of Remote-Command Sessions:</i>	0 Sessions
<i>Number Of L2TP ALG Sessions:</i>	0 Sessions
<i>Number Of MIRC ALG Sessions:</i>	0 Sessions
<i>Number Of ICQ ALG Sessions:</i>	0 Sessions
<i>Number Of CUCME ALG Sessions:</i>	0 Sessions
<i>Number Of H323 Q931 ALG Sessions:</i>	0 Sessions
<i>Number Of H323 RAS ALG Sessions:</i>	0 Sessions
<i>Number Of H323 H245 ALG Sessions:</i>	0 Sessions

Figure 8-2 NAT Rule Global Statistics

The table provides basic information for each NAT rule you have set up. You can click **Clear** to restart the accumulation of the statistics at their initial values.

8.4 Viewing NAT Rules and Rule Statistics

To view the NAT rules currently defined on the Prestige, select **NAT Rule Entry** from the **NAT Options** drop-down list menu. The **Network Address Translation (NAT) Rule Configuration** screen displays as shown.

Home LAN WAN Bridging Routing Services Admin

NAT | RIP | FireWall | IP Filter | DNS | Blocked Protocols

Network Address Translation (NAT) Rule Configuration

Each row in the table lists a rule for translating addresses. See Help for instructions on creating NAT rules.

NAT Options: NAT Rule Entry

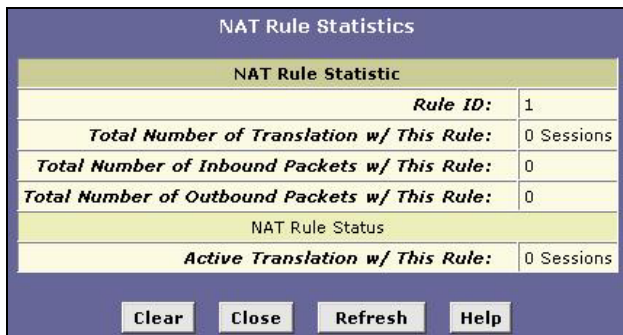
Rule ID	IF Name	Rule Flavor	Protocol	Local IP From	Local IP To	Action
1	ALL	NAPT	ANY	0.0.0.0	255.255.255.255	Stats

Add Refresh Help

Figure 8-3 NAT Rule Configuration

The **Network Address Translation (NAT) Rule Configuration** screen displays a row containing basic information for each rule. For a description of these fields, refer to *section 8.6*.

Click **Add** to add a new rule, or use the icons in the **Action** column to delete (🗑️) or view details on (🔍) a rule. To view often a specific NAT rule has been used, click **Stats** in the **Action** column.



NAT Rule Statistic	
<i>Rule ID:</i>	1
<i>Total Number of Translation w/ This Rule:</i>	0 Sessions
<i>Total Number of Inbound Packets w/ This Rule:</i>	0
<i>Total Number of Outbound Packets w/ This Rule:</i>	0
NAT Rule Status	
<i>Active Translation w/ This Rule:</i>	0 Sessions

Clear Close Refresh Help

Figure 8-4 NAT Rule Statistics

The statistics show how many times this rule has been invoked and how many currently active sessions are using this rule. You can click **Clear** to reset the statistics to zeros and **Refresh** to update the screen.

8.5 Viewing Current NAT Translations

To view a list of NAT translations that have recently been performed and which remain in effect (for any of the defined rules), select **NAT Translations** from the **NAT Options** drop-down list. The **NAT Translations** screen displays as shown.

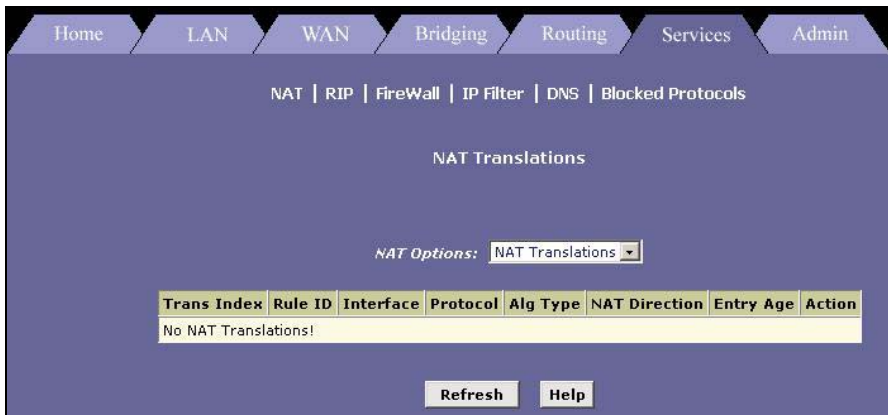



Figure 8-5 NAT Translation

The following table describes the fields in this screen.

Table 8-3 NAT Translation Table Fields

FIELD	DESCRIPTION
Trans Index	This field displays the sequential number assigned to the IP session used by this NAT translation session.
Rule ID	This field displays the number of the NAT rule invoked.
Interface	This field displays the device interface on which the NAT rule was invoked (from the rule definition).
Protocol	This field displays the IP protocol used by the data packets that are undergoing translations (from the rule definition) Example: TCP, UDP, ICMP.
Alg Type	This field displays the Application Level Gateway (ALG), if any, that was used to enable this NAT translation (ALGs are special settings that certain applications require in order to work while NAT is enabled).
NAT Direction	This field displays the direction (incoming or outgoing) of the translation (from the port definition).
Entry Age	This field displays the elapsed time, in seconds, of the NAT translation session.

Click  in the **Action** column to view additional details about a NAT translation session.

The following table describes the NAT translation related fields in the **NAT Translation -Details** screen. For other fields, refer to *Table 8-3*.

Table 8-4 NAT Translation Details Fields

FIELD	DESCRIPTION
Translated InAddress	This field shows the public IP address to which the private IP address was translated.
In Address	This field shows the private IP address that was translated.
Out Address	This field shows the IP address of the outside destination (web, ftp site, etc.)
In/Out Packets	This field indicates the number of incoming and outgoing IP packets that have been translated in this translation session.
In Ports	This field indicates the actual port number corresponding to the LAN computer.
Out Ports	This field indicates the port number associated with the destination address.
Translated In Ports	This field shows the port number to which the LAN computer's actual port number was translated.

8.6 Adding NAT Rules

This section explains how to create rules for the various NAT flavors.

You cannot edit existing NAT rules. To change a rule setup, delete it and add a new rule with the modified settings.

Depending on the flavor you choose, the screen may look different.

8.6.1 The NAPT rule: Translating Between Private and Public IP Addresses

Follow these instructions to create a rule for translating the private IP addresses on your LAN to your public IP address. This type of rule uses the NAT flavor napt, which was used in your Prestige's default configuration. The napt flavor translates private source IP addresses to a single public IP address. The napt rule also translates the source port numbers to port numbers that are defined on the **NAT Global Configuration** screen. The *Introduction to NAT* section describes how the napt rule works.

By default, the device is configured with a napt rule that translates all LAN-side IP addresses to a public address assigned to the WAN port.

Step 1. From the **Network Address Translation (NAT) Configuration** page, click **Add**. The **NAT Rule – Add** screen displays.

NAT Rule Information				
Rule Flavor:	NAPT			
Rule ID:				
IF Name:	ALL			
Local Address From:	0	0	0	0
Local Address To:	255	255	255	255
Global Address:	0	0	0	0

Submit Cancel Help

Figure 8-6 NAT Rule: Add (NAPT flavor)

Step 2. Select **NAPT** from the **Rule Flavor** drop-down list menu.

Step 3. Enter a unique number to the rule in the **Rule ID** field for identification purposes.

The **Rule ID** determines the order in which rules are invoked (the lowest numbered rule is invoked first, and so on). In some cases, two or more rules may be defined to act on the same set of IP addresses. Be sure to assign the **Rule ID** so that the higher priority rules are invoked before lower-priority rules. Once a data packet matches a rule, the data is acted upon according to that rule and is not subjected to higher-numbered rules.

Step 4. From the **IFName** drop-down list, select the interface on the Prestige to which this rule applies.

Typically, NAT rules apply to communication between your LAN and the Internet. Because the device uses the WAN interface (which may be named *ppp-0* or *eoal-0* in the Web Configurator) to connect your LAN to your ISP, it is the usual IF Name selection.

Step 5. In the **IFName** drop-down list, select a protocol to which this rule applies, or choose **ALL**.

This selection specifies which type of Internet communication will be subject to this translation rule. You can select **ALL** if the rule applies to all data.

By associating a protocol with this type of NAT rule, you ensure that all data using that protocol is sent to the Internet referencing the public Internet address as the source computer. However, data packets that use protocols not specified here will not undergo translation; their packet headers will reflect the true source address of the LAN computer (and, because they contain private IP addresses, these packets will not be routable on the Internet).

Step 6. In the **Local Address From** field and **Local Address To** fields, type the starting and ending IP addresses, respectively, of the range of private addresses you want to be translated. Or type the same address in both fields to specify a single value.

To specify that data from all LAN addresses should be translated, type 0 (zero) in each **From** field and 255 in each **To** field.

If you use non-sequential private addresses, you can create an additional napt rule for each separate range of addresses.

These addresses should correspond to private addresses already in use on your network (either assigned statically to your computers, or assigned dynamically using DHCP, as discussed in chapter on DHCP).

- Step 7.** When you have completed entering all information, click **Submit**. A page displays to confirm the change.
- Step 8.** Click **Close** to return to the **NAT Configuration** page. The new rule should display in the **NAT Rule** table.
- Step 9.** On the **NAT Configuration** page, ensure that the **Enable** radio button is turned on and click **Submit**. A page displays to confirm your changes. Refer to the section on *Committing Your Changes and Rebooting the Prestige* to save your changes to permanent memory and make your changes take effect.

8.6.2 The RDR Rule: Allowing External Access to a LAN Computer

You can create an rdr rule to make a computer on your LAN, such as a Web or FTP server, available to Internet users without requiring you to obtain a public IP address for that computer. The computer's private IP address is translated to your public IP address in all incoming and outgoing data packets.

Without an rdr rule (or bimap rule described on page 8-16), the Prestige blocks attempts by external computers to access your LAN computers.

The following example illustrates using the rdr rule to provide external access to your web server:

Your Prestige receives a packet from the Internet containing a request for access to your Web server. The packet header contains your public IP address (which is assigned to the Prestige's WAN port) as the destination IP address, and 80 as the destination port number. Port 80 is commonly used for web servers. Because you have set up an rdr rule for incoming packets with destination port 80, the Prestige recognizes the data as a request for Web server access. The Prestige changes the destination IP address in the packet to the private IP address assigned to your Web server and forwards the data packet to it.

Your Web server sends data packets in response. Before the Prestige forwards these packets to the Internet, it changes the source IP address in the data packets from the Web server's private address to your LAN's public address. To an external Internet user, then, it appears as if your Web server uses your public IP address.

Follow these instructions to add an rdr rule:

Step 1. In the NAT Rule – Add Page, type in a unique **Rule ID**, and select **RDR** as the **Rule Flavor**.

The screenshot shows the 'NAT Rule - Add' configuration window. It contains the following fields and values:

NAT Rule Information	
Rule Flavor:	RDR
Rule ID:	
IF Name:	ALL
Protocol:	ANY
Local Address From:	
Local Address To:	
Global Address From:	0 0 0 0
Global Address To:	0 0 0 0
Destination Port From:	Any other port 0
Destination Port To:	Any other port 65535
Local Port:	Any other port 0

At the bottom of the window are three buttons: Submit, Cancel, and Help.

Figure 8-7 NAT Rule: Add (RDR flavor)

Step 2. Select the interface and, if desired, a protocol that this rule applies to.

Step 3. In the **Local Address From** and **Local Address To** fields, type the same private IP address, or the lowest and highest addresses in a range:

- If you type the same IP address in both fields, incoming traffic that matches the criteria you specify in steps 4 and 5 will be redirected to that IP address.
- If you type a range of addresses, incoming traffic will be redirected to any available computer in that range. This option would typically be used for load balancing, whereby traffic is distributed among several redundant servers to help ensure efficient network performance.

These addresses should correspond to private addresses already in use on your network (either assigned statically to your computers or assigned dynamically using DHCP, as discussed in *Configuring Dynamic Host Configuration Protocol* chapter).

Step 4. In the **Global Address From** and **Global Address To** fields, type the public IP address assigned to you by your ISP.

If you have multiple WAN interfaces, in both fields type the IP address of the interface to which this rule applies. This rule will not be enforced for data that arrives on WAN interfaces not specified here.

If you have multiple WAN interfaces and want the rule to be enforced on a range of them, type the starting and ending IP addresses of the range.

Step 5. Enter a destination address (or a range) and port ID (or a range) as criteria for incoming traffic.

Depending on which other fields you define in this step, incoming traffic that meets this criteria will be redirected to the address(es) specified in step 3 (assuming it comes through the interface specified in step 2).

- Enter a starting and ending IP address in the **Destination Address From** and **Destination Address To** fields if incoming traffic destined for these addresses should be redirected.

You can also enter a single address in both fields.

When your Prestige receives a data packet intended for these destination addresses, it replaces the destination IP addresses with the private IP address(es) you specified in step 3. The edited packet can then be forwarded to the new destination address—the LAN computer(s).

- Enter a starting and ending port number in the **Destination Port From** and **Destination Port To** fields if incoming traffic destined for these port types should be redirected to the address(es) specified in step 3. Or enter the same address in both fields.

For example, if you grant public access to a Web server on your LAN, you would expect that incoming packets destined for that computer would contain the port number 80. This setting serves as a filter; data packets not containing this port number would not be forwarded internally.

Step 6. If the LAN computer that you are making publicly available is configured to use a non-standard port number for the type of traffic it receives, type the non-standard port number in the **Local Port** field.

This option translates the standard port number in packets destined for your LAN computer to the non-standard number you specify. For example, if your Web server uses (non-standard) port 2000, but you expect incoming data packets to refer to (standard) port 80, you would enter 2000 in the **Local Port** field and 80 in the **Destination Port** fields. The headers of incoming packets destined for port 80 will be modified to refer to port 2000. The packet can then be routed appropriately to the web server.

After making the changes, click **Submit** to confirm your changes. Refer to the section on *Committing Your Changes and Rebooting the Prestige* to save your changes to permanent memory and make your changes take effect.

8.6.3 The Basic Rule: Performing 1:1 Translations

The basic flavor translates the private (LAN-side) IP address to a public (WAN-side) address, like napt rules. However, unlike napt rules, basic rules do not also translate the port numbers in the packet header; they are passed through un-translated. Therefore, the basic rule does not provide the same level of security as the napt rule.

Step 1. In the **NAT Rule – Add** page, type in a **Rule ID**, and select **BASIC** from the **Rule Flavor** drop-down list menu.

NAT Rule Information	
Rule Flavor:	BASIC
Rule ID:	
IF Name:	ALL
Protocol:	ANY
Local Address From:	0 0 0 0
Local Address To:	255 255 255 255
Global Address From:	0 0 0 0
Global Address To:	0 0 0 0

Submit Cancel Help

Figure 8-8 NAT Rule: Add (BASIC flavor)

Step 2. Select the interface and, if desired, a protocol that this rule applies to, as explained previously.

Step 3. In the **Local Address From** and **Local Address To** fields, type the starting and ending IP addresses that identify the range of private addresses you want to be translated. Or type the same address in both fields.

If you specify a range, each address will be translated in sequence to a corresponding address in a range of global addresses (which you specify in step 4).

The address (or range of addresses) should correspond to a private address (or addresses) already in use on your network. These may be assigned statically to your computers, or assigned dynamically using DHCP, as discussed in previous chapter on *Configuring DHCP*.

Step 4. In the **Global Address From** and **Global Address To** fields, type the starting and ending address that identify the pool of public IP addresses to which to translate your private addresses. Or, type the same address in both fields (if you also specified a single address in step 3).

After making the changes, click **Submit** to confirm your changes. Refer to the section on *Committing Your Changes and Rebooting the Prestige* to save your changes to permanent memory and make your changes take effect.

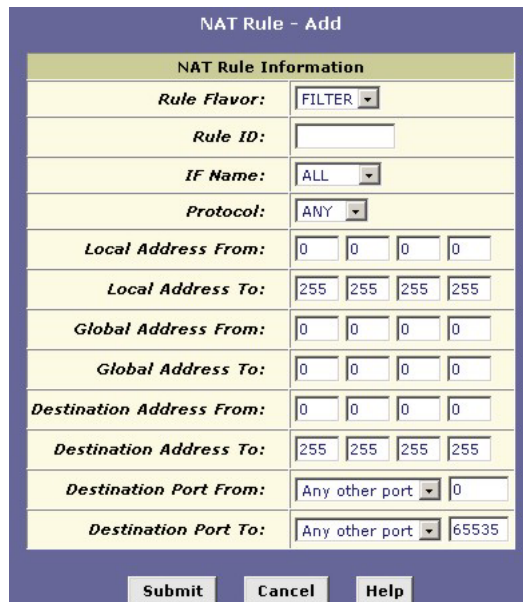
8.6.4 The Filter Rule: Configuring a Basic Rule with Additional Criteria

Like the basic flavor, the filter flavor translates public and private IP addresses on a one-to-one basis. The filter flavor extends the capability of the basic rule. Refer to **The Basic Rule** in the previous section for a general description.

You can use the filter rule if you want an address translation to occur only when your LAN computers initiate access to specific destinations. The destinations can be identified by their IP addresses, server type (such as FTP or Web server), or both.

Follow these instructions to add a filter rule:

- Step 1.** In the **NAT Rule – Add** page, type a Rule ID, and select **FILTER** from the **Rule Flavor** drop-down list menu.



The screenshot shows the 'NAT Rule - Add' configuration page. The 'Rule Flavor' is set to 'FILTER'. The 'Rule ID' field is empty. The 'IF Name' is set to 'ALL' and the 'Protocol' is set to 'ANY'. The 'Local Address From' and 'Global Address From' fields are both set to '0.0.0.0'. The 'Local Address To' and 'Global Address To' fields are both set to '255.255.255.255'. The 'Destination Address From' field is set to '0.0.0.0'. The 'Destination Address To' field is set to '255.255.255.255'. The 'Destination Port From' is set to 'Any other port' and '0'. The 'Destination Port To' is set to 'Any other port' and '65535'. At the bottom, there are 'Submit', 'Cancel', and 'Help' buttons.

NAT Rule Information	
Rule Flavor:	FILTER
Rule ID:	
IF Name:	ALL
Protocol:	ANY
Local Address From:	0 0 0 0
Local Address To:	255 255 255 255
Global Address From:	0 0 0 0
Global Address To:	0 0 0 0
Destination Address From:	0 0 0 0
Destination Address To:	255 255 255 255
Destination Port From:	Any other port 0
Destination Port To:	Any other port 65535

Figure 8-9 NAT Rule: Add (FILTER flavor)

- Step 2.** Select the interface in the **IF Name** drop-down list and, if desired, a protocol that this rule applies to.

Step 3. In the **Local Address From** and **Local Address To** fields, type the starting and ending IP addresses that identify the range of private addresses you want to be translated. Or, type the same address in both fields.

If you specify a range, each address will be translated in sequence to a corresponding address in a range of global addresses (which you specify in step 4).

The address (or range of addresses) should correspond to a private addresses (or addresses) already in use on your network. These may be assigned statically to your computers or assigned dynamically using DHCP, as discussed in the previous chapter.

Step 4. In the **Global Address From** and **Global Address To** fields, type the starting and ending addresses that identify the range of public IP addresses to translate your private addresses to. Or, type the same address in both fields (if you also specified a single address in step 3).

Step 5. Specify a destination address or addresses, destination port (or ports), or both. You can specify a single value by entering that value in both fields.

- Specify a destination address (or range) if you want this rule to apply only to outbound traffic to the address (or range).

If you enter only the network ID portion of the destination address, then the rule will apply to outbound traffic to all computers on the network.

- Specify a destination port (or range) if you want this rule to apply to any outbound traffic to the types of servers identified by that port number.

For example, if you do not specify a destination address, but specify a destination port from/to of 21, then this translation will occur on all accesses by your LAN to all external FTP servers (that is, when one of your LAN computers communicates with an external FTP server, the source IP address in the packet headers is changed to the public address, not the initiator's private IP address).

Common port numbers include:

20, 21—FTP (file transfer protocol) server

25—SMTP (simple mail transfer protocol) server

80—HTTP (World Wide Web) server

- Specify both a destination address (or range) and a destination port (or range) if you want this translation rule to apply to accesses to the specified server type at the specified location.

After making the changes, click **Submit** to confirm your changes. Refer to the section on *Committing Your Changes and Rebooting the Prestige* to save your changes to permanent memory and make your changes take effect.

8.6.5 The Bimap Rule: Performing Two-way Translations

Unlike the other NAT flavors, the bimap flavor performs address translations in both the outgoing and incoming directions.

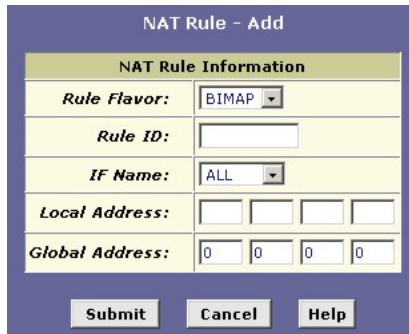
In the incoming direction, when the specified Prestige interface receives a packet with your public IP address as the destination address, this address is translated to the private IP address of a computer on your LAN. To the external computer, it appears as if the access is being made to the public IP address, when, in fact, it is communicating with a LAN computer.

In the outgoing direction, the private source IP address in a data packet is translated to the LAN's public IP address. To the rest of the Internet, it appears as if the data packet originated from the public IP address.

Bimap rules can be used to provide external access to a LAN device. They do not provide the same level of security as rdr rules, because rdr rules also reroute incoming packets based on the port ID. Bimap rules do not account for the port number, and therefore allow external access regardless of the destination port type specified in the incoming packet.

To add a bimap rule, follow these instructions:

- Step 1.** Display the **NAT Rule – Add Page**, choose a **Rule ID**, and select **BIMAP** from the **Rule Flavor** drop-down list menu.



The screenshot shows a web-based configuration page titled "NAT Rule - Add". It features a "NAT Rule Information" section with the following fields:

- Rule Flavor:** A dropdown menu with "BIMAP" selected.
- Rule ID:** An empty text input field.
- IF Name:** A dropdown menu with "ALL" selected.
- Local Address:** Four empty text input fields for IP address octets.
- Global Address:** Four text input fields, each containing the digit "0".

At the bottom of the form are three buttons: "Submit", "Cancel", and "Help".

Figure 8-10 NAT Rule: Add (BIMAP flavor)

- Step 2.** Select the interface and, if desired, a protocol that this rule applies to.
- Step 3.** In the **Local Address** field, type the private IP address of the computer to which you are granting external access.
- Step 4.** In the **Global Address** field, type the address that you want to serve as the publicly known address for the LAN computer.

After making the changes, click **Submit** to confirm your changes. Refer to the section on *Committing Your Changes and Rebooting the Prestige* to save your changes to permanent memory and make your changes take effect.

8.6.6 The pass rule: Allowing specific addresses to pass through un-translated

You can create a pass rule to allow a range of IP addresses to remain un-translated when another rule would otherwise do so.

The pass rule must be assigned a rule ID that is a lower number than the ID assigned to the rule it is intended to pass. In you want a specific IP address or range of addresses to not be subject to an existing rule, say rule ID #5, then you can create a pass rule with ID #1 through 4.

To add a pass rule, follow these instructions:

Step 1. In the NAT Rule – Add page, type a **Rule ID**, and select **Pass** from the **Rule Flavor** drop-down list menu.

The screenshot shows the 'NAT Rule - Add' configuration window. It features a title bar 'NAT Rule - Add' and a section titled 'NAT Rule Information'. The 'Rule Flavor' dropdown is set to 'PASS'. The 'Rule ID' field is empty. The 'IF Name' dropdown is set to 'ALL'. The 'Local Address From' field is set to '0.0.0.0' and the 'Local Address To' field is set to '255.255.255.255'. At the bottom, there are three buttons: 'Submit', 'Cancel', and 'Help'.

Figure 8-11 NAT Rule: Add (PASS flavor)

Step 2. Select the interface and, if desired, a protocol that this rule applies to.

Step 3. In the **Local Address From** and **Local Address To** fields, type the lowest and highest IP addresses that define the range of private address you want to be passed without translation.

If you want the pass rule to act on only one address, type that address in both fields.

After making the changes, click **Submit** to confirm your changes. Refer to the section on *Committing Your Changes and Rebooting the Prestige* to save your changes to permanent memory and make your changes take effect.

Chapter 9

Configuring the Routing Information Protocol

This chapter describes how to configure the Routing Information Protocol (RIP) on your Prestige.

9.1 RIP Overview

RIP is an Internet protocol you can set up to share routing table information with other routing devices on your LAN, at your ISP's location, or on remote networks connected to your network via the ADSL line. Generally, RIP is used to enable communication on autonomous networks. An autonomous network is one in which all of the computers are administered by the same entity. An autonomous network may be a single network, or a grouping of several networks under the same administration. An example of an autonomous network is a corporate LAN, including devices that can access it from remote locations, such as the computers telecommuters use.

Using RIP, each device sends its routing table to its closest neighbor every 30 seconds. The neighboring device in turn passes the information on to its next neighbor and so on until all devices in the autonomous network have the same set of routes.

9.1.1 When Should You Configure RIP?

Most small home or office networks do not need to use RIP; they have only one router, such as the Prestige, and one path to an ISP. In these cases, there is no need to share routes, because all Internet data from the network is sent to the same ISP gateway.

You may want to configure RIP if any of the following circumstances apply to your network:

- Your home network setup includes an additional router or RIP-enabled computer (other than the Prestige). The Prestige and the router will need to communicate via RIP to share their routing tables.
- Your network connects via the ADSL line to a remote network, such as a corporate network. In order for your LAN to learn the routes used within your corporate network, they should *both* be configured with RIP.
- Your ISP requests that you run RIP for communication with devices on their network.

9.2 Configuring the Prestige's Interfaces with RIP

The following instructions describe how to enable RIP on your Prestige.

In order for the Prestige to communicate with other devices using RIP, you must also enable the other devices to use the same protocol. See the product documentation for those devices.

Click **Services** in the task bar, and then click **RIP**.

NAT | RIP | FireWall | IP Filter | DNS | Blocked Protocols

Routing Information Protocol (RIP) Configuration

Routers on your LAN communicate with one another using the Routing Information Protocol. This table lists any interfaces on your device that use RIP (typically the LAN interface), and the version of the protocol used.

Enable Disable

Age(seconds):

Update Time(seconds):

IF Name	Metric	Send Mode	Receive Mode	Action
ppp-0	1	RIP1	RIP1	
<input type="text" value="eth-0"/>	<input type="text" value="1"/>	<input type="text" value="RIP1COMPAT"/>	<input type="text" value="RIP1"/>	<input type="button" value="Add"/>

Figure 9-1 RIP Configuration

The page contains option buttons for enabling or disabling the RIP feature and a table listing interfaces on which the protocol is currently running. The first time you open this page, the table may be empty.

Step 1. If necessary, change the **Age** and **Update Time**. These are global settings for all interfaces that use RIP.

- **Age** is the amount of time in seconds that the device's RIP table will retain each route that it learns from adjacent computers.
- **Update Time** specifies how frequently the Prestige will send out its routing table its neighbors.

- Step 2.** In the **IFName** column, select the name of the interface on which you want to enable RIP.
For communication with RIP-enabled devices on your LAN, select eth-0 or the name of the appropriate virtual Ethernet interface. For communication with your ISP or a remote LAN, select the corresponding ppp, eoa, or other WAN interface.
- Step 3.** Select a metric value for the interface.
RIP uses a “hop count” as a way to determine the best path to a given destination in the network. The hop count is the sum of the metric values assigned to each port through which data is passed before reaching the destination. Among several alternative routes, the one with the lowest hop count is considered the fastest path.
For example, if you assign this port a metric of 1, then RIP will add 1 to the hop count when calculating a route that passes through this port. If you know that communication via this interface is slower than through other interfaces on your network, you can assign it a higher metric value than the others.
You can select any integer from 1 to 15.
- Step 4.** Select a send and receive modes.
The **Send Mode** setting indicates the RIP version this interface will use when it sends its route information to other devices.
The **Receive Mode** setting indicates the RIP version(s) in which information must be passed to the Prestige in order for it to be accepted into its routing table.
RIP version 1 is the original RIP protocol. Select RIP1 if you have devices that communicate with this interface that understand RIP version 1 only.
RIP version 2 is the preferred selection because it supports “classless” IP addresses (which are used to create subnets) and other features. Select RIP2 if all other routing devices on the autonomous network support this version of the protocol.
- Step 5.** Click **Add**. The new RIP entry will display in the table.
- Step 6.** Click the **Enable** option button to enable the RIP feature.

If you disable the RIP feature, the interface settings you have configured will remain available for future activation.

- Step 7.** When you are finished defining RIP interfaces, click **Submit**. A page displays to confirm your changes.
- Step 8.** Follow the instructions in the section on *Committing Your Changes and Rebooting the Prestige* to save your changes to permanent memory and make your changes take effect.

9.3 Viewing RIP Statistics

From the **RIP Configuration** page, you can click **Global Stats** to view statistics on attempts to send and receive route table data over RIP-enabled interfaces on your Prestige.

RIP Global Statistics	
RIP Active Sessions	
<i>Request Sent:</i>	0 Packets
<i>Response Sent:</i>	0 Packets
<i>Request Received:</i>	0 Packets
RIP Packets w/ Error	
<i>Packets Received w/ Bad Version:</i>	0 Packets
<i>Packets Received w/ Bad Address Family:</i>	0 Packets
<i>Packets Received w/ Bad Request Format:</i>	0 Packets
<i>Packets Received w/ Bad Metrics:</i>	0 Packets
<i>Packets Received w/ Bad Response Format:</i>	0 Packets
<i>Packets Received w/ Invalid Port:</i>	0 Packets
<i>Packets Rejected:</i>	0 Packets
<i>Response Received:</i>	0 Packets
<i>Unknown Packets Received:</i>	0 Packets
<i>Packets Received from Non-Neighbor Router:</i>	0 Packets
<i>Packets Rejected for Authentication Failure:</i>	0 Packets
<i>Packets w/ Route Changed:</i>	0 Packets
Clear	Close
Refresh	Help

Figure 9-2 RIP Global Statistics

Click **Clear** to reset all statistics to 0 and **Refresh** to display any newly accumulated data.

Chapter 10

System Alarm and Diagnosis

This chapter shows you the alarm and diagnostics features in the Prestige.

10.1 About the System Alarm

System alarms, also called traps, are caused by a variety of system events, including connection attempts, resets, and configuration changes.

Although you will not typically need to view this information, it may be helpful in working with your ISP to troubleshoot problems you encounter with the Prestige. (Despite their name, not all alarms indicate problems in the functioning of the system.)

10.2 Viewing the System Alarm Table

To display the **Alarm** page, log into the web configurator, click **Admin**, and then click **Alarm**.



Figure 10-1 Alarm

Each row in the table displays the time and date that an alarm occurred, the type of alarm, and a brief statement indicating its cause. To remove all entries from the list, click **Clear**. New entries will begin accumulating and will display when you click **Refresh**.

10.3 Diagnostics

The diagnostics feature executes a series of test of your system software and hardware connections. Use this feature to troubleshoot connection problems to your ISP. Follow the steps below to begin the diagnostics program.

- Step 1.** To open the **Diagnostics** page, click the **Admin** tab and then click **Diagnostics**.
- Step 2.** From the **Virtual Circuits** drop-down list, select the name of your ATM interface (see chapter on *ATM*).
- Step 3.** Click **Submit** to start the diagnostic test. The test result is displayed as shown.

Home LAN WAN Bridging Routing Services Admin

User Config | Commit & Reboot | Image Upgrade | Alarm | Diagnostics | Port Settings

Diagnostics

This page is used for performing diagnostics on the system.

ATM VC:

Testing Connectivity to modem		
Testing Ethernet connection	PASS	Help
Testing ADSL line for sync	PASS	Help
Testing Ethernet connection to ATM	PASS	Help
Testing Telco Connectivity		
Testing ATM OAM segment ping	PASS	Help
Testing ATM OAM end to end ping	PASS	Help
Testing ISP Connectivity		
Testing PPPoE server connectivity	PASS	Help
Testing PPPoE server session	PASS	Help
Testing authentication with server	PASS	Help
Validating assigned IP address 0.0.0.0	PASS	Help
Testing Internet Connectivity		
Ping default gateway 0.0.0.0	PASS	Help
Ping Primary Domain Name Server	PASS	Help
Query DNS for www.globespanvirata.com	PASS	Help
Ping www.globespanvirata.com	PASS	Help

Submit Help

Figure 10-2 Diagnostics

The diagnostics utility will run a series of test to check whether the device's connections are up and working. This will take only a few seconds. The program will report whether the test passed, failed, or was skipped. A test may be skipped if the program determines that no suitable interface is configured on which to run the test. You can click **Help** in the right column of the output table to display an explanation of each test.

Chapter 11

Configuring Your PPP Connection

This chapter describes how to configure the PPP protocol. Contact your ISP to determine if you will need to change the default settings in order to connect to their server.

When the Prestige is turned on, it initiates a connection through your DSL line to your ISP. The Prestige communicates with your ISP's server using the *Point-to-Point Protocol (PPP)*.

11.1 Overview of PPP

The PPP protocol is commonly used between ISPs and their customers to identify and control various communication properties, including:

- Identifying the type of service the ISP provides to a given customer
- Identifying the customer to the ISP through a username and password
- Enabling the ISP to assign Internet information to the customer's computers

11.2 Viewing Your Current PPP Configuration

To view your current PPP setup, click **WAN** or **Routing** in the task bar, then click **PPP**. The **Point to Point Protocol (PPP) Configuration** screen displays as shown.

Figure 11-2 PPP Configuration

PPP is configured as a group of software settings associated with the ADSL port. Although the device has only one physical ADSL port, the Prestige can be defined with more than one group of PPP settings. Each group of settings is called a *PPP interface* and is given a name.


Table 11-1 PPP Configuration

FIELD	DESCRIPTION
Inactivity TimeOut (mins) for starondata PPP Interface.	Enter the number of minutes of inactivity on the PPP interface after which the link will need to be reestablished. After timing out, you will need to log in to your ISP again to re-establish service. 0 timeout means the internet connection will not be disconnected.
Ignore WAN to LAN traffic while monitoring inactivity.	When enabled, data traffic traveling in the incoming direction - from the WAN port to the LAN port - will not count as activity on the WAN port. That is, it will not prevent the connection from being terminated if inactive for the specified time.
Interface	This field displays the predefined name of the PPP interface.
VC	The Virtual Channel (VC) connection over which this PPP data is sent. The VCC identifies the physical path the data takes to reach your ISP. See the chapter on <i>Configuring ATM VCC</i> for more information.

Table 11-1 PPP Configuration

FIELD	DESCRIPTION
Interface Sec Type	This field displays the interface that the IP firewall is effective on. A public interface connects to the Internet. A private interface connects to your LAN, such as the Ethernet interface. The term DMZ (de-militarized zone), in Internet networking terms, refers to computers that are available for both public and in-network accesses (such as a company's public Web server).
Protocol	The type of PPP protocol used. Your ISP may use PPP-over-Ethernet (PPPoE) or PPP-over-ATM (PPPoA).
WAN IP	This field displays the IP address currently assigned to your WAN (DSL) port by your ISP.
Gateway IP	This field displays the IP address of the server at your ISP that provides you access to the Internet. See the chapter on ATM VCC for a description of gateway addresses.
Default Route	This field displays Enabled when the Prestige is set to use the default route configured. Otherwise this field displays Disabled . (Refer to the chapter on IP routes for more information).
Use DHCP	This field displays Enabled when the Prestige gets IP information from the ISP's DHCP server. Otherwise it is Disabled .
Use DNS	This field displays Enabled when the Prestige is set to distribute DNS address learned from the PPP connection to the connected computer(s) on the LAN. This feature is useful when the Prestige is acting as a DHCP server on the LAN.
Oper. Status	This field indicates whether the link is currently up or down.
Actions	You can use these icons to edit (✎), delete (🗑), and view (🔍) details on a PPP interface.
Click Submit to confirm your changes. Refer to the section on <i>Committing Your Changes and Rebooting the Prestige</i> to save your changes to permanent memory and make your changes take effect.	

11.2.1 Viewing PPP Configuration Details

In the **Point to Point Protocol (PPP) Configuration** screen, click  to display the **PPP Interface - Detail** screen as shown next.

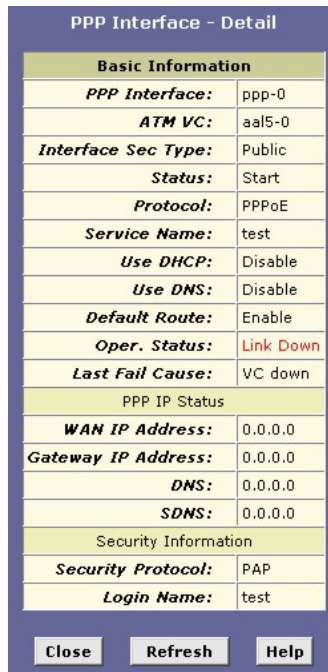


Figure 11-1 PPP Interface: Detail

The following table describes the fields in this screen.

Table 11-2 PPP Interface: Detail

FIELD	DESCRIPTION
PPP IP Status	
PPP Interface	The field displays the name of the PPP interface.
ATM VC	This field displays the name of the virtual channel.
Interface Sec Type	This field displays the name of the interface on which the firewall is effective.
Status	Indicates whether the interface has been specified in the system as: Start: A connection will be established for use when the device is turned on or rebooted. Stop: The PPP interface cannot currently be used. StartOnData: The PPP connection will be made only when data is sent to the interface.

Table 11-2 PPP Interface: Detail

FIELD	DESCRIPTION
Protocol	This field displays the type of PPP protocols used.
Service Name	This field displays the name of the ISP service you are using with this PPP connection. ISPs may offer different types of services (for example, for online gaming or business communications), each requiring a different login and other connection properties.
Default Route	This field indicates whether the Prestige should use the IP address assigned to this connection as its default route. It can be either Enable or Disable . See the chapter on IP Routes for an explanation of default routes.
Last Fail Cause	<p>This field indicates the cause of the last failed operation.</p> <p>No Valid PADO Recvd: The Prestige has initiated a PPPoE handshake but did not receive a reply from the ISP.</p> <p>No Valid PADS Recvd: After the initial handshake, the Prestige did not receive a confirmation from the ISP.</p> <p>Stopped by User: The user stopped the connection (for example, by changing the settings for the PPP interface in the web configurator.)</p> <p>No Activity: The PPP communication timed out, in accordance with the timeout period specified in the Point to Point Protocol (PPP) Configuration screen.</p> <p>Auth Failure: The ISP could not authorize the connection based on the user name and/or password provided.</p> <p>PADT recvd: The ISP issued a special packet type to terminate the PPP connection.</p> <p>VC down: The virtual circuit between the Prestige and the ISP is down.</p> <p>Internal failure: A system software failure occurred.</p>
PPP IP Status	
WAN IP Address	This field displays the WAN IP address of the Prestige. This is different from the LAN or USB IP addresses.
Gateway IP Address	This field displays the IP address of the gateway device.
DNS	This field displays the IP address of the DNS server (located with your ISP) used on this PPP connection.
SDNS	This field displays the IP address of the secondary DNS server (located with your ISP) used on this PPP connection.

Table 11-2 PPP Interface: Detail

FIELD	DESCRIPTION
Security Information	
Security Protocol	This field displays the type of PPP security your ISP uses: PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol).
Login Name	This field displays the name you use to log in to your ISP each time this PPP connection is established.

11.3 Adding a PPP Interface Definition

If you intend to use more than one type of service from your ISP, the device may be configured with multiple PPP interfaces, each with unique logon and other properties. Follow this procedure to define properties for a PPP interface:

Step 1. Click **Add** in the **Point to Point Protocol (PPP) Configuration** screen.

Basic Information	
PPP Interface:	ppp-0
ATM VC:	aal5-0
Interface Sec Type:	Public
Status:	Start
Protocol:	<input type="radio"/> PPPoA <input checked="" type="radio"/> PPPoE
Service Name:	
Use DHCP:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Use DNS:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Default Route:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Security Information	
Security Protocol:	<input checked="" type="radio"/> PAP <input type="radio"/> CHAP
Login Name:	
Password:	

Submit Cancel Help


Figure 11-2 PPP Interface: Add

- Step 2.** Select a PPP interface name from the **PPP Interface** drop-down list. Refer to *Table 11-2* to configure the other fields.

You can create multiple PPP interfaces only if you are using the PPPoA protocol. You can define only one PPP interface if you are using PPPoE. Check with your ISP about which version of the protocol they require.

- Step 3.** Click **Submit**. A screen displays to confirm your changes.
- Step 4.** Follow the instructions in the section on *Committing Your Changes and Rebooting the Prestige* to save your changes to permanent memory and make your changes take effect.

11.4 Modifying PPP Interfaces

To modify a PPP interface, click  for the interface you want to modify in the **Point to Point Protocol (PPP) Configuration** screen. The **PPP Interface – Modify** screen displays as shown next.

Basic Information	
PPP Interface:	ppp-0
ATM VC:	aal5-0
Protocol:	PPPoE
Service Name:	test
Default Route:	Enabled
Status:	Start

Security Information	
Security Protocol:	<input checked="" type="radio"/> PAP <input type="radio"/> CHAP
Login Name:	test
Password:	****

Submit Cancel Help

Figure 11-3 PPP Interface: Modify

You can change the status, security protocol, your login name, and your password only. To modify the other settings, you must delete the interface and create a new one. Refer to *Table 11-1* for field descriptions.

After making the changes, click **Submit** to confirm your changes. Refer to the section on *Committing Your Changes and Rebooting the Prestige* to save your changes to permanent memory and make your changes take effect.

11.5 Deleting a PPP interface

Do not delete a PPP interface unless you have received instructions to do so from your ISP. Without an appropriately defined PPP interface, you will not be able to connect to your ISP.

To delete a PPP interface, click  in the **Action** column for the interface you want to delete.

After making the changes, click **Submit** to confirm your changes. Refer to the section on *Committing Your Changes and Rebooting the Prestige* to save your changes to permanent memory and make your changes take effect.

Chapter 12

Configuring the ATM

This chapter describes how to configure the ATM virtual channel (VC) connection, which defines the path the Prestige uses to communicate with your ISP over the ATM network.

12.1 Introduction

As your LAN computers access the Internet via the Prestige, data is exchanged with your ISP through a complex network of telephone switches, Internet routers, servers, and other specialized hardware. These various devices communicate using a common language, or protocol, called Asynchronous Transfer Mode (ATM). On the Wide Area Network (WAN) that connects you to your ISP, the ATM protocol performs functions like those that the Ethernet protocol performs on your LAN.

12.2 Viewing Your ATM Setup

To view your current configuration, click **WAN** and then **ATM VC** to display the **ATM VC Configuration** screen.

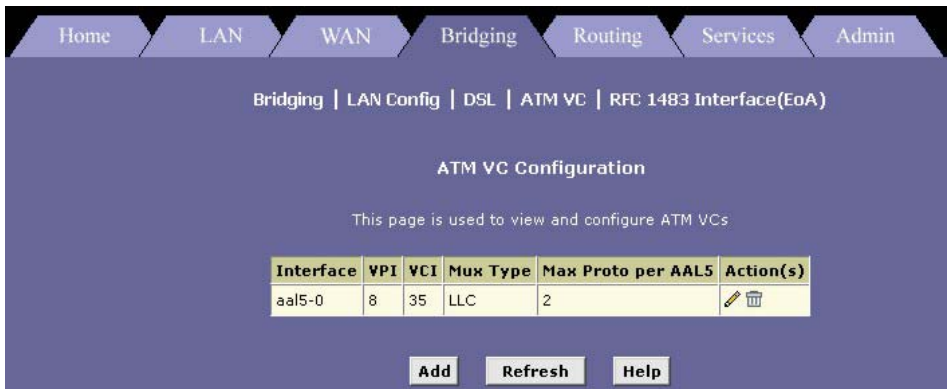



Figure 12-1 ATM VCC Configuration

The **ATM VC Configuration** screen displays a row for each VC interface currently configured (usually only one). Each set of VC properties is considered as an interface because it defines a data path to the Prestige over the ATM network. VC interfaces are completely defined in the Prestige firmware, and then associated with the DSL (WAN) port.

Your Prestige may already be pre-configured with the necessary ATM VC interface properties, or the screen may contain placeholder values that you must change before using the Prestige. Only change these values if your ISP gives you different ones.

To delete an ATM interface, click  in the **Action** column.

12.3 Adding and Changing ATM Properties

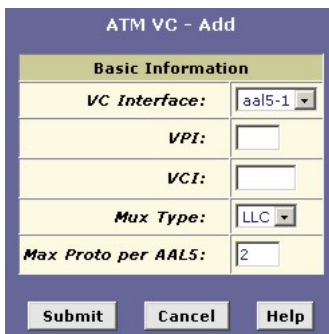
You may need to change the ATM VC properties if your ISP provides settings that differ from those that were pre-configured. To change the properties associated with a VCC interface, you must delete the VC interface, and then add a new interface of the same name with new settings.

You may need to create more than one VC interface if you use multiple services with your ISP.

Before creating a new VC interface, make sure you have the following information from your ISP or telephone company:

- VPI
- VCI
- Mux Type: (LLC or VC)

In the **ATM VCC Configuration** screen, click **Add**. The **ATM VC – Add** screen displays.



Basic Information	
VC Interface:	aal5-1
VPI:	
VCI:	
Mux Type:	LLC
Max Proto per AAL5:	2

Submit Cancel Help

Figure 12-2 ATM VC: Add

The following table describes the fields in this screen.

Table 12-1 ATM VC: Add

FIELD	DESCRIPTION
VC Interface	Select an interface name from the drop-down list menu.
VPI/VCI	Enter the VPI and VCI number provided by your ISP.
Mux. Type	Select LLC or VC from the drop-down list menu.
Max Proto per AAL5	If you are using an AAL5-type of interface, enter number of higher level interfaces that the VC can support (the higher level interfaces can be PPP, EoA, or IPoA interfaces).
Click Submit to confirm your changes. Refer to the section on <i>Committing Your Changes and Rebooting the Prestige</i> to save your changes to permanent memory and make your changes take effect.	

The new interface should now display in the **ATM VC Configuration** table. Verify that the new settings work by accessing the Internet from a LAN/USB computer.

Chapter 13

Viewing DSL Parameters

13.1 DSL Parameters

To view displays current information on the DSL line performance, click **WAN** and **DSL** to display the **DSL Status** screen. You can also get the same screen in **Bridging** or **Routing**

Home LAN WAN Bridging Routing Services Admin

Bridging | LAN Config | DSL | ATM VC | RFC 1483 Interface(EoA)

DSL Status

This page displays DSL Status Information

Refresh Rate: 10 Seconds

Counters	Local		Remote	
	Intrlvd	Fast	Intrlvd	Fast
FEC:	0	0	0	0
CRC:	0	0	0	0
NCD:	0	0	0	0
OCD:	0	0	-	-
HEC:	0	0	0	0
SEF:	0	0	0	0
LOS:	0	0	0	0
LOS:	0	0	0	0
Failures	Local		Remote	
NCD:	0	0	0	0
SEF:	0	0	0	0
LOS:	0	0	0	0
LCD:	0	0	0	0

DSL Status	
Operational Status:	Startup Handshake <input type="button" value="Loop Stop"/>
Last Failed Status:	0x0
Last Failed Status:	0x0
Startup Progress:	0xA0

Clear DSL Param Stats Refresh Help

Figure 13-1 DSL Status

The screen refreshes about every 10 seconds. You can click **Clear** to reset all counters to zero, and **Refresh** to redisplay the screen with newly accumulated values.

Although you generally will not need to view this data, it may be helpful when troubleshooting connection or performance problems with your ISP.

Click **DSL Param** to display the configuration of the DSL line.

DSL Parameter							
DSL Parameters and Status							
<i>Vendor ID:</i>	00B5GSPN						
<i>Revision Number:</i>	V1.4.2						
<i>Serial Number:</i>	1						
<i>Local Tx Power:</i>	0.0 dB	Config Data	Up		Down		
<i>Remote Tx Power:</i>	0.0 dB		Intrlvd	Fast	Intrlvd	Fast	
<i>Local Line Atten.:</i>	0.5 dB		<i>AS0(kbps):</i>	-	-	0	0
<i>Remote Line Atten.:</i>	0.5 dB		<i>AS1(kbps):</i>	-	-	0	0
<i>Local SNR Margin:</i>	0.0 dB		<i>LS0(kbps):</i>	0	0	-	-
<i>Remote SNR Margin:</i>	0.0 dB		<i>LS1(kbps):</i>	0	0	-	-
<i>Self Test:</i>	Passed		<i>RValue:</i>	0	0	0	0
<i>DSL Standard:</i>	T1.413		<i>SValue:</i>	0		0	
<i>Trellis Coding:</i>	Disable		<i>DValue:</i>	0		0	
<i>Framing Structure:</i>	Framing-0						
<input type="button" value="Close"/> <input type="button" value="Refresh"/> <input type="button" value="Help"/>							

Figure 13-2 DSL Parameters

The **DSL Parameters and Status** table displays pre-configured settings.

The **Config Data** table lists various types of error and defect measurements on the DSL line.

13.2 DSL Performance Statistics

In the **DSL Status** screen, click **Stats** to display DSL line performance statistics.

DSL Statistics					
<i>No. of 15 Min. Valid Data Intervals: 0</i>					
<i>No. of 15 Min. Invalid Data Intervals: 0</i>					
Current 15-Min Interval Statistics					
<i>Elapsed Time(MM:SS):</i>	0:0				
<i>Errored Seconds:</i>	0				
<i>Severely Errored Seconds:</i>	0				
<i>Unavailable Seconds:</i>	0				
Current Day Statistics					
<i>Elapsed Time(HH:MM:SS):</i>	0:0:0				
<i>Errored Seconds:</i>	0				
<i>Severely Errored Seconds:</i>	0				
<i>Unavailable Seconds:</i>	0				
Previous Day Statistics					
<i>Monitored Time(HH:MM:SS):</i>	0:0:0				
<i>Errored Seconds:</i>	0				
<i>Severely Errored Seconds:</i>	0				
<i>Unavailable Seconds:</i>	0				
Detailed Interval Statistic (Past 24 hrs)					
1-4	5-8	9-12	13-16	17-20	21-24
Close		Refresh		Help	

Figure 13-3 DSL Statistics

The **DSL Statistics** screen displays error data for the last 15-minute interval, the current day, and the previous day.

Click on the link in the **Detailed Interval Statistic (Past 24 Hrs)** table to display detailed statistics for each 15-minute interval in the past 24 hours. For example, when you click **1-4**, a screen displays to show statistics for the 15-minute intervals (there are 16 of these) that make up the previous 4 hours as shown next.

DSL Interval Statistics				
15-Min Interval No.	Errored Seconds	Severely Errored Seconds	Unavailable Seconds	Valid Data
1	0	0	0	No
2	0	0	0	No
3	0	0	0	No
4	0	0	0	No
5	0	0	0	No
6	0	0	0	No
7	0	0	0	No
8	0	0	0	No
9	0	0	0	No
10	0	0	0	No
11	0	0	0	No
12	0	0	0	No
13	0	0	0	No
14	0	0	0	No
15	0	0	0	No
16	0	0	0	No

Detailed Interval Statistic (Past 24 hrs)					
1-4	5-8	9-12	13-16	17-20	21-24

Close Refresh Help

Figure 13-4 DSL Interval Statistics

Part III:

ADVANCED MANAGEMENT

This part shows how to configure Firewall, IP Filters, EOA, IPoA, DNS Relay and Bridging.

Chapter 14

Firewall

This chapter describes the firewall feature and instructions for configuring the feature on your Prestige.

14.1 Overview of IP Firewall

IP firewall protects the computers and other network device behind the router (your Prestige) from malicious attacks originating from WAN hosts. Various attacks are known to cause disruption to regular service for hosts behind the router, or cause damage to computers on the LAN. The firewall feature detects and protects against such common attacks and reports to network administrators for appropriate actions.

The Prestige firewall offers the following types of protection:

- **Attack Protection** against use of malicious IP address, network packet flooding or OS vulnerabilities.
- **Denial of Service (DOS) Protection** against the flooding of the modem with large number of packets denying service to genuine connections.
- **Service Protection** by blocking certain services or protocols that may be misused by hackers.
- **Router Protection** prevents common attacks on routers such as the Ping of Death, IP Spooling, Tear Drop, Smurf and Fraggle or the Land Attack.

14.2 Firewall Global Configuration

To configure general firewall settings, click **Service** and then **FireWall** to display the **FireWall Configuration** screen.

The screenshot shows the 'FireWall Configuration' page. At the top, there is a navigation menu with tabs for Home, LAN, WAN, Bridging, Routing, Services, and Admin. Below the menu, there are links for NAT, RIP, FireWall, IP Filter, DNS, and Blocked Protocols. The main title is 'FireWall Configuration', followed by the text 'This Page is used to view FireWall Configuration.' The configuration area is titled 'Firewall Global Configuration' and contains the following fields:

- Blacklist Status:** Radio buttons for Enable and Disable (Disable is selected).
- Blacklist Period(min):** A text input field containing the value '10'.
- Attack Protection:** Radio buttons for Enable and Disable (Disable is selected).
- Dos Protection:** Radio buttons for Enable and Disable (Disable is selected).
- Max Half open TCP Conn.:** A text input field containing the value '25'.
- Max ICMP Conn.:** A text input field containing the value '25'.
- Max Single Host Conn.:** A text input field containing the value '75'.
- Log Destination:** Checkboxes for Email and Trace (Trace is checked).
- E-Mail ID of Admin 1:** An empty text input field.
- E-Mail ID of Admin 2:** An empty text input field.
- E-Mail ID of Admin 3:** An empty text input field.

At the bottom of the configuration area, there are five buttons: Submit, Cancel, Black List, Refresh, and Help.

Figure 14-1 Firewall Configuration

The following table describes the fields in this screen.

Table 14-1 Firewall Configuration

FIELD	DESCRIPTION
Blacklist Status	The blacklist feature adds the IP address of a malicious host to the blacklist table. Select Enable (default) to turn on the blacklisting function. Otherwise select Disable .

Table 14-1 Firewall Configuration

FIELD	DESCRIPTION
Blacklist Period (min)	Enter the time duration (in minutes) after which the external host IP address will be removed from the blacklist.
Attack Protection	Select Enable to protect against the use of malicious IP address hijacked by hackers, network packet flooding or OS vulnerabilities. Otherwise select Disable .
Dos Protection	Select Enable to protect against Denial of Service (DoS) attacks. Otherwise select Disable .
Max Half open TCP conn.	Sets the percentage of concurrent IP sessions that can be in the half-open state. In ordinary TCP communication, packets are in the half-open state only briefly as a connection is being initiated; the state changes to active when packets are being exchanged, or closed when the exchange is complete. TCP connections in the half-open state can use up the available IP sessions. If the percentage is exceeded, then the half-open sessions will be closed and replaced with new sessions as they are initiated.
Max ICMP conn.	Specifies a maximum number of ICMP connections allowed. Newer ICMP packets are allowed by removing older ICMP sessions.
Max Single Host conn.	Specifies a maximum number of connection sessions allowed. All further connection requests are dropped until the older sessions time-out.
Log Destination	Specifies how attempted violations of the firewall settings will be tracked. Select Trace to send records of such events via Ethernet to a system utility. Select Email to e-mail the logs to the administrators) specified below.
E-Mail ID of Admin 1 - 3	If you select Email in the Log Destination field, enter the e-mail address(es) to which the logs are sent.
Click Submit to confirm your changes. Refer to the section on <i>Committing Your Changes and Rebooting the Prestige</i> to save your changes to permanent memory and make your changes take effect.	

14.2.1 Black List Hosts

In the **Firewall Configuration** screen, click **Black List** to view the list of malicious hosts.

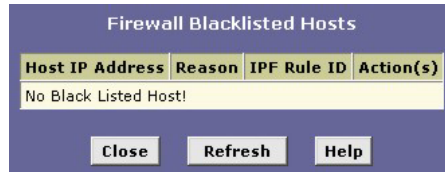



Figure 14-2 Firewall Blacklisted Hosts

The following table describes the fields in this screen.

Table 14-2 Firewall Blacklisted Hosts

FIELD	DESCRIPTION
Host IP Address	This field displays the IP address of the computer that sent the packet(s) which caused the violation
Reason	This field displays a short description of the type of violation. If the packet violated a rule, the custom text from the Log Tag field of the IP filter will be displayed (refer to <i>Table 15-1</i>).
IPF Rule ID	If the packet violated an IP Filter rule, this field displays the ID assigned to the rule.
Action(s)	Click  to remove the entry from the list prior to its automatic timed expiration.

14.3 Blocking Protocols

Your Prestige is capable of sending and receiving information in a variety of protocol formats. The **Blocked Protocols** feature prevents the Prestige from passing any data that uses a particular protocol. Unlike IP filtering, you cannot specify additional criteria for blocked protocols, such as particular users or destinations. However, when you are certain that a particular protocol is not needed or wanted on your network, this feature provides a convenient way to discard such data before it is passed.

Blocking certain protocols may disrupt or disable your network communication or Internet access. If you are unfamiliar with how your network or Internet connection uses these protocols, contact your ISP before doing so.

Click the **Service** tab and then click **Blocked Protocols**.

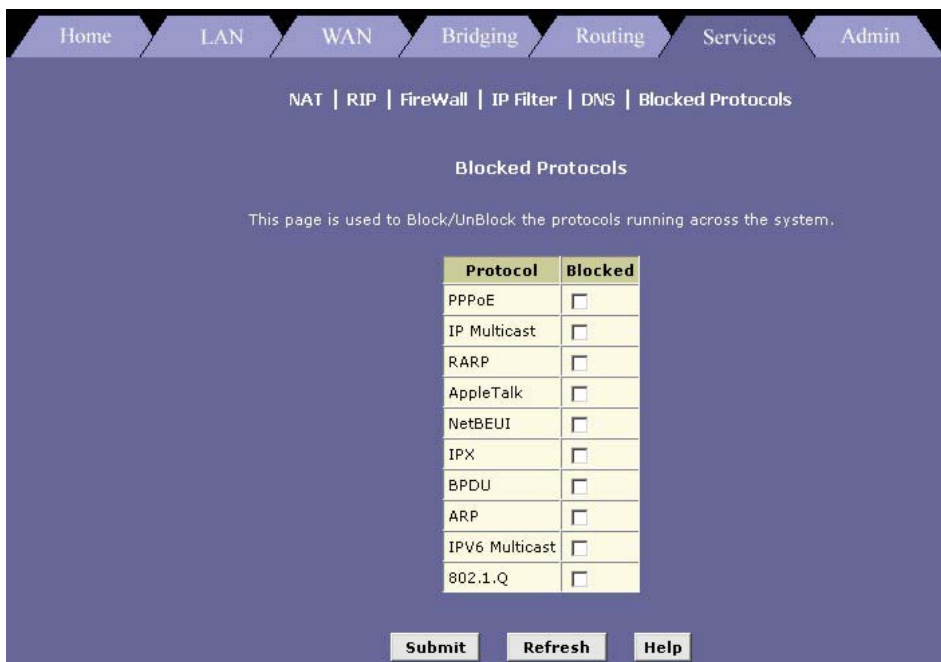


Figure 14-3 Blocked Protocols

The following table describes the protocol options in this screen.

Table 14-3 Blocked Protocols

PROTOCOL	DESCRIPTION
PPPoE	Many DSL modems use Point-to-Point Protocol over Ethernet (PPPoE) to establish and maintain a connection with an ISP. PPPoE provides a means of logging in to the ISP's server so that they can authenticate you as a customer and provide you access to the Internet. Check with your ISP before blocking this protocol.
IP Multicast	IP Multicast is an extension to the IP protocol. It enables individual packets to be sent to multiple hosts on the Internet, and is often used for handling e-mail mailing lists and teleconferencing/videoconferencing.
RARP	Reverse Address Resolution Protocol (RARP) is an IP protocol that provides a way for computers to determine their own IP addresses when they only know their hardware address (i.e., MAC addresses). Certain types of computers, such as diskless workstations, must use RARP to determine their IP address before communicating with other network devices.

Table 14-3 Blocked Protocols

PROTOCOL	DESCRIPTION
AppleTalk	A networking protocol used in for Apple Macintosh® networks.
NetBEUI	On many LAN operating systems, the NetBIOS Enhanced User Interface (NetBEUI) protocol provides the method by which computers identify themselves to and communicate with each other.
IPX	Internetwork Packet Exchange (IPX) is a networking protocol used on Novell Netware®-based LANs.
BPDU	Bridge Protocol Data Units (BPDUs) are data messages that are exchanged across the switches between LANs that are connected by a bridge. BPDU packets contain information on ports, addresses, priorities and costs, and are exchanged across bridges to detect and eliminate loops in a network.
ARP	Computers on a LAN use Address Resolution Protocol (ARP) to learn the hardware addresses (i.e., MAC addresses) of other computers when they know only their IP addresses.
IPV6 Multicast	IP Multicasting under IP Protocol version 6. See <i>IP Multicast</i> above.
802.1.Q	This IEEE specification defines a protocol for virtual LANs on Ethernet networks. A virtual LAN is a group of PCs that function as a local area network, even though the PCs may not be physically connected. They are commonly used to facilitate administration of large networks.
Click Submit to confirm your changes. Refer to the section on <i>Committing Your Changes and Rebooting the Prestige</i> to save your changes to permanent memory and make your changes take effect.	

Chapter 15

Configuring IP Filters

The IP filter feature enables you to create rules that control the forwarding of incoming and outgoing data between your LAN and the Internet. This chapter explains how to create IP filter rules.

15.1 Overview of IP Filters

IP filters enable you to control the types of data that pass to and from your network. You can create IP filter rules to block certain computers on your LAN from accessing certain types of data or Internet locations. You can also block incoming access to computers on your LAN.

When you define an IP filter rule and enable the feature, you instruct the Prestige to examine each data packet it receives to determine whether it meets criteria set forth in the rule. The criteria can include the size of the packet, the network or internet protocol it is carrying, the direction in which it is traveling (for example, from the LAN to the Internet or vice versa), the IP address of the sending computer, the destination IP address, and other characteristics of the packet data.

If the packet matches the criteria established in a rule, the packet can be either accepted (forwarded towards its destination), or denied (discarded), depending on the action specified in the rule.

No IP filter rules are predefined and the feature is disabled by default on the Prestige. All valid data packets are accepted and forwarded to their destination.

15.2 Viewing Your IP Filter Configuration

To view your current IP filter configuration, click **Services** in the task bar and **IP Filter**. The **IP Filter Configuration** screen displays.

Home | LAN | WAN | Bridging | Routing | Services | Admin

NAT | RIP | FireWall | IP Filter | DNS | Blocked Protocols

IP Filter Configuration

This Page is used to View and Modify IP Filter Global and Rule Configuration.

Security Level: Public Default Action:
 Private Default Action: DMZ Default Action:

Rule ID	I/F	Apply Stateful Inspection	Direction	Rule Action	In I/F	Log Option	Rule Description	Oper. Status	Action(s)
10	ALL	Disable	Incoming	Deny	N/A	Disable	-		
20	ALL	Disable	Incoming	Deny	N/A	Disable	1.Dest IP equal to 255.255.255.255		
30	Private	Enable	Incoming	Accept	N/A	Disable	-		
40	Private	Enable	Outgoing	Accept	ALL	Disable	-		
350	Public	Disable	Incoming	Deny	N/A	Disable	-		
360	DMZ	Disable	Incoming	Deny	N/A	Disable	1.Protocol eq TCP 2.TCP Flag All 3.Dest Port equal to 80		
370	DMZ	Disable	Incoming	Deny	N/A	Disable	1.Protocol eq TCP 2.TCP Flag All 3.Dest Port equal to 21		
380	DMZ	Disable	Incoming	Deny	N/A	Disable	1.Protocol eq TCP 2.TCP Flag All 3.Dest Port equal to 23		
390	DMZ	Enable	Incoming	Accept	N/A	Disable	-		

Figure 15-1 IP Filter Configuration:

This screen displays the pre-configure IP filter rules, security level options and actions for each interface.

- **Security Level:** This setting determines which IP Filter rules take effect, based on the security level specified in each rule. For example, when **High** is selected, only those rules that are assigned a security value of **High** will be in effect. The same is true for the **Medium** and **Low** options. Select **None** to disable IP filtering.

- **Private/Public/DMZ Default Action:** This setting specifies a default action to be taken (**Accept** or **Deny**) on private, public, or DMZ-type device interfaces when they receive packets that *do not* match any of the filtering rules. You can specify a different default action for each interface type. (You specify an interface's type when you create the interface; see the **Point to Point Protocol (PPP) Configuration** screen.)

A public interface typically connects to the Internet. PPP, EoA, and IPoA interfaces are typically public. Packets received on a public interface are subject to the most restrictive set of firewall protections defined in the software. Typically, the global setting for public interfaces is **Deny**, so that all accesses to your LAN initiated from external computers are denied (discarded at the public interface), except for those allowed by a specific IP filter rule.

A private interface connects to your LAN, such as the Ethernet interface. Packets received on a private interface are subject to a less restrictive set of protections because they originate within the network. Typically, the global setting for private interfaces is **Accept**, so that LAN computers have access to the ADSL/Ethernet routers' Internet connection.

The term DMZ (De-Militarized Zone), in Internet networking terms, refers to computers that are available for both public and in-network accesses (such as a company's public Web server). Packets received on a DMZ interface - whether from a LAN or external source - are subject to a set of protections that is in between public and private interfaces in terms of restrictiveness. The global setting for DMZ-type interfaces may be set to **Deny** so that all attempts to access these servers are denied by default; the administrator may then configure IP Filter rules to allow accesses of certain types.

15.3 Create New IP Filter Rules

To create an IP filter rule, you set the criteria that must be met in order for the rule to be invoked. Use these instructions to add a new IP filter rule, and refer to the examples described later for assistance:

in the main **IP Filter Configuration** screen, click **Add** to display the **IP Filter Rule – Add** screen.

IP Filter Rule - Add			
<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Basic Information			
Rule ID:	<input type="text"/>	Action:	<input type="radio"/> Accept <input checked="" type="radio"/> Deny
Direction:	<input type="radio"/> Incoming <input checked="" type="radio"/> Outgoing	Interface:	ALL <input type="button" value="v"/>
In Interface:	ALL <input type="button" value="v"/>	Log Option:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Security Level:	<input type="checkbox"/> High <input type="checkbox"/> Medium <input checked="" type="checkbox"/> Low	Blacklist Status:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Log Tag:	<input type="text"/>		
Start Time (HH MM SS):	00 00 00	End Time (HH MM SS):	23 59 59
Src IP Address:	any <input type="button" value="v"/> 0 0 0 0 0 0 0 0 0 0 <input type="text"/>		
Dest IP Address:	any <input type="button" value="v"/> 0 0 0 0 0 0 0 0 0 0 <input type="text"/>		
Protocol:	any <input type="button" value="v"/> TCP <input type="button" value="v"/>		
Apply Stateful Inspection:	<input type="checkbox"/>		
Source Port:	any <input type="button" value="v"/> 0	Any other port <input type="button" value="v"/> 0	Any other port <input type="button" value="v"/> 0
Dest Port:	any <input type="button" value="v"/> 0	Any other port <input type="button" value="v"/> 0	Any other port <input type="button" value="v"/> 0
TCP Flag:	All <input type="button" value="v"/>		
ICMP Type:	any <input type="button" value="v"/> Echo Reply <input type="button" value="v"/>		
ICMP Code:	any <input type="button" value="v"/> 0		
IP Frag Pkt:	<input type="radio"/> Yes <input type="radio"/> No <input checked="" type="radio"/> Ignore	IP Option Pkt:	<input type="radio"/> Yes <input type="radio"/> No <input checked="" type="radio"/> Ignore
Packet Size:	any <input type="button" value="v"/> 0		
TOD Rule Status :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
<input type="button" value="Submit"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>			

Figure 15-2 IP Filter Rule: Add

The following table describes the fields in this screen.

Table 15-1 IP Filter Rule: Add

FIELD	DESCRIPTION
Enable/Disable	<p>Select Enable to activate IP filtering. This is the default setting.</p> <p>Select Disable de-activate IP filtering. If you disabled the feature, existing rules are retained for future use.</p>
Rule ID	<p>Enter a unique number for identification and prioritization purposes.</p> <p>Rules are processed from lowest to highest on each data packet, until a match is found. It is recommended that you assign rule IDs in multiples of 5 or 10 (e.g., 10, 20, 30) so that you leave enough room between them for inserting a new rule if necessary.</p>
Action	<p>Select Accept to forward a packet to a destination when the packet matches the rule criteria.</p> <p>Select Deny to discard the packet that match the rule criteria.</p>
Direction	<p>Specify whether the rule should apply to incoming or outgoing data packets on the selected interface.</p> <p>Incoming refers to packets coming from the LAN, and Outgoing refers to packets going to the Internet.</p> <p>You can use rules that specify the incoming direction to prevent outside accesses to your LAN. You can use rules that specify the outgoing direction to block LAN accesses to the Internet.</p>
Interface	<p>Specifies the interface on the Prestige on which the rule will take effect.</p>
In Interface	<p>Specifies the interface from which packets must have been forwarded to the interface specified in the previous selection. This option is valid only for the outgoing direction and is useful only when the Prestige is configured with both a LAN and a USB interface, or with multiple LAN or WAN interfaces.</p> <p>For example, if your Prestige connects to two subnets (that is, it has two LAN interfaces, eth-0 and eth-1) and you want to block one of the subnets (say, eth-1) from accessing the web, you would create an outgoing rule on the WAN interface that denies HTTP accesses. You would specify the eth-1 as the incoming interface.</p>
Log Option	<p>Select Enable to create a log for any packets that match the criteria. The log entry will include the time of the violation, the source address of the computer responsible for the violation, the destination IP address, the protocol used, the source and destination ports, and the number violations occurred in the previous x minutes. (Logging may be helpful when troubleshooting.) This information can also be e-mailed to designated administrators. Otherwise select Disable.</p>

Table 15-1 IP Filter Rule: Add

FIELD	DESCRIPTION
Security Level	<p>Specify the security level that must be enabled globally for this rule to take affect. A rule will be active only if its security level is the same as the globally configured setting (shown on the main IP Filter Configuration screen).</p> <p>For example, if the rule is set to Medium and the global firewall level is set to Medium, then the rule will be active; but if the global firewall level is set to High or Low, then the rule will be inactive.</p>
Blacklist Status	<p>Specify whether or not a violation of this rule will result in the offending computer's IP address being added to the black list, which blocks the ADSL/Ethernet router from forwarding packets from that source for a specified period of time.</p>
Log Tag	<p>Type a description (up to 16 characters) to be recorded in the log in the event that a packet violates this rule.</p> <p>Note: You must select Enable in the Log Option field if you enter a tag in this field.</p>
Src IP Address	<p>Enter the IP address (or a range of IP addresses) of the source computer(s) from which the packet originates. Then in the drop-down list, select the rule to be invoked on packets containing:</p> <p>any: any source IP address.</p> <p>lt: any source IP address that is numerically less than the specified address.</p> <p>lteq: any source IP address that is numerically less than or equal to the specified address.</p> <p>gt: any source IP address that is numerically greater than the specified address.</p> <p>eq: any source IP address that is numerically equal to the specified address.</p> <p>neq: any source IP address that is not equal to the specified address.</p> <p>range: any source IP address that is within the specified range, inclusive.</p> <p>out of range: any source IP address that is outside the specified range.</p>
Dest IP Address	<p>Enter the IP address (or a range of IP addresses) of the destination computer(s) to which the packet is being sent.</p> <p>Then select the rule option from the drop-down list menu. Refer to Src IP Address field for the description of the options.</p>

Table 15-1 IP Filter Rule: Add


FIELD	DESCRIPTION
Protocol	Specify the basic IP protocol criteria that must be met for a rule to be invoked. Using the options in the drop-down list, you can specify that packets must contain the selected protocol (eq), that they must not contain the specified protocol (neq), or that the rule can be invoked regardless of the protocol (any). TCP, UDP, and ICMP are commonly IP protocols; others can be identified by number from 0-255, as defined by the Internet Assigned Numbers Authority (IANA).
Store State	If this option is enabled, then stateful filtering is performed and the rule is also applied in the other direction on the given interface during an IP session.
Source Port	Specify the port number of the source computer(s) from which the packet originates. You may either select the port number from the drop-down list menu or enter the port number in the field provided. These two fields will be dimmed (unavailable for entry) if you have not specified a protocol criteria. See the description of Src IP Address for the selection options. The fields are only available if you specified that the protocol be equal to TCP or UDP in the Protocol field.
Dest Port	Specify the port number of the type of computer to which the packet is being sent. In addition to the options described for the Src IP Address field, the following option is available: bcast : specifies that the rule will be invoked for any packets sent to the broadcast address for the receiving interface. (The broadcast address is used to send packets to all hosts on the LAN or subnet connected to the specified interface.) When you select this option, you do not need to specify the address, so the address fields are dimmed. You may either select the port number from the drop-down list menu or enter the port number in the field provided. The fields are only available if you specified that the protocol be equal to TCP or UDP in the Protocol field.
TCP Flag	Specify whether the type of TCP protocol should be restricted to only those packets containing synchronous (SYN) TCP or only those that do not use synchronous (NON-SYN) TCP. You can also select ALL to apply all restrictions. This field is only available if you specified that the protocol must equal TCP in the Protocol field.
ICMP Code	Specify whether the value in the code field in ICMP packet headers will be used as a criterion. The code value can be any decimal value from 0-255. You can specify that the value must equal (eq), or not equal the specified value, or you can select any to enable the rule to be invoked regardless of the ICMP code field. This field is only available if you specified that the protocol must equal ICMP in the Protocol field.

Table 15-1 IP Filter Rule: Add

FIELD	DESCRIPTION
ICMP Type	<p>Specifies whether the value in the type field in ICMP packet headers will be used as a criteria. The code value can be any decimal value from 0-255. You can specify that the value must equal (eq) or not equal (neq) to the specified value, or you can select any to enable the rule to be invoked regardless of the ICMP type field.</p> <p>This field is only available if you specified that the protocol must equal ICMP in the Protocol field.</p>
IP Frag. Pkt	<p>Specify how the rule should apply to IP packets that contain fragments. Select from the following options:</p> <p>Yes: The rule will be applied only to packets that contain fragments.</p> <p>No: The rule will be applied only to packets that do not contain fragments.</p> <p>Ignore: (Default) The rule will be applied to packets whether or not they contain fragments, assuming that they match the other criteria.</p>
IP Option Pkt	<p>Specify whether the rule should apply to IP packets that have options specified in their packet headers.</p> <p>Yes: The rule will be applied only to packets that contain header options.</p> <p>No: The rule will be applied only to packets that do not contain header options.</p> <p>Ignore: (Default) The rule will be applied to packets whether or not they contain header options, assuming that they match the other criteria.</p>
Packet Size	<p>Specify that the IP filter rule will take affect only on packets whose size in bytes matches this criteria. (lt = less than, gt = greater than, lteq = less than or equal to, etc.)</p>
TOD Rule Status	<p>The TOD (Time Of Day) Rule Status determines how the Start Time and End Time settings are used.</p> <p>Enable: (Default) The rule is in effect for the specified time period.</p> <p>Disable: The rule is not in effect for the specified time period, but is effective at all other times.</p>
<p>Click Submit to confirm your changes. Refer to the section on <i>Committing Your Changes and Rebooting the Prestige</i> to save your changes to permanent memory and make your changes take effect.</p>	

15.4 Modify IP Filter Rules

A red dot displays in the **Oper. Status** column indicates that the rule is currently disabled. You can modify the rule to enable it.

In the **IP Filter Rule** table, click  in the **Actions** column to display the **IP Filter Rule – Modify** screen.

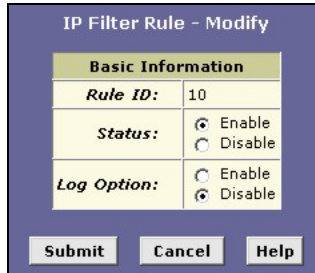


Figure 15-3 IP Filter Rule: Modify

The following table describes the fields in this screen.


Table 15-2 IP Filter Rule: Modify

FIELD	DESCRIPTION
Rule ID	This field displays the index of the IP filter rule.
Status	Select Enable to activate the filter rule. When the filter rule is enabled, a green bullet will be displayed in the Status column in the IP Filter Configuration screen.
Log Option	Select Enable to create a log entry when the filter rule is violated.
Click Submit to confirm your changes. Refer to the section on <i>Committing Your Changes and Rebooting the Prestige</i> to save your changes to permanent memory and make your changes take effect.	

Do not enable the IP filter feature unless you have defined rules and specified a default action. Doing so may result in filtering out content that you intend to let pass.

15.5 IP filter rule examples


Example 1. Blocking a specific computer on your LAN from using accessing web servers on the Internet. The specified computer will not be able to access the Web, but will be able to access FTP Internet sites (and any others that use destination port numbers other than 80).

- Step 1.** Define a rule for outgoing packets on the ppp-0 interface from any incoming interface (this would include the eth-0 and usb-0 interfaces, for example).
- Step 2.** Specify that the packets must contain the source port associated with the computer you want to block. Alternatively, if the computer is assigned a static IP address, you could specify that value as the criteria.
- Step 3.** Specify that the packet must be destined for port 80, which is the well-known port number for web servers.
- Step 4.** Click **Submit** to save the changes to your Prestige, and then click  to modify the rule and enable it.
- Step 5.** Choose a default action, enable the IP filtering feature.
- Step 6.** Follow the instructions in the section on *Committing Your Changes and Rebooting the Prestige* to commit your changes to permanent memory and make your changes take effect.

IP Filter Rule - Add			
<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Basic Information			
Rule ID:	<input type="text" value="21"/>	Action:	<input type="radio"/> Accept <input checked="" type="radio"/> Deny
Direction:	<input type="radio"/> Incoming <input checked="" type="radio"/> Outgoing	Interface:	<input type="text" value="ppp-0"/>
In Interface:	<input type="text" value="ALL"/>	Log Option:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Security Level:	<input type="checkbox"/> High <input type="checkbox"/> Medium <input checked="" type="checkbox"/> Low	Blacklist Status:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Log Tag:	<input type="text"/>		
Start Time (HH MM SS):	<input type="text" value="00"/> <input type="text" value="00"/> <input type="text" value="00"/>	End Time (HH MM SS):	<input type="text" value="23"/> <input type="text" value="59"/> <input type="text" value="59"/>
Src IP Address:	<input type="text" value="any"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>		
Dest IP Address:	<input type="text" value="any"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>		
Protocol:	<input type="text" value="eq"/> <input type="text" value="TCP"/>		
Apply Stateful Inspection:	<input type="checkbox"/>		
Source Port:	<input type="text" value="eq"/>	<input type="text" value="Any other port"/> <input type="text" value="3"/>	<input type="text" value="Any other port"/>
Dest Port:	<input type="text" value="eq"/>	<input type="text" value="HTTP (80)"/>	<input type="text" value="Any other port"/>
TCP Flag:	<input type="text" value="NOT-SYN"/>		
ICMP Type:	<input type="text" value="any"/> <input type="text" value="Echo Reply"/>		
ICMP Code:	<input type="text" value="any"/> <input type="text" value="0"/>		
IP Frag Pkt:	<input type="radio"/> Yes <input type="radio"/> No <input checked="" type="radio"/> Ignore	IP Option Pkt:	<input type="radio"/> Yes <input type="radio"/> No <input checked="" type="radio"/> Ignore
Packet Size:	<input type="text" value="any"/> <input type="text" value="0"/>		
TOD Rule Status :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
<input type="button" value="Submit"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>			

Figure 15-4 IP Filter Rule Example 1

Example 2. Blocking Telnet accesses to the Prestige:

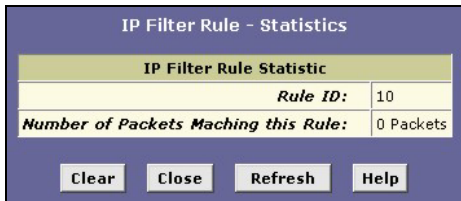
- Step 1.** Define a new rule for incoming packets incoming on the ppp-0 interface.
- Step 2.** Specify that the packet must contain the TCP protocol, and must be destined for port 23, the well-known port number for Telnet communication.
- Step 3.** Click **Submit** to confirm the changes to your Prestige, and then click  to modify the rule and enable it.
- Step 4.** Choose a default action, enable the IP filtering feature.
- Step 5.** Follow the steps in the section on *Committing Your Changes and Rebooting the Prestige* to save your changes to permanent memory and make your changes take effect.

IP Filter Rule - Add			
<input checked="" type="radio"/> Enable <input type="radio"/> Disable			
Basic Information			
Rule ID:	<input type="text" value="31"/>	Action:	<input type="radio"/> Accept <input checked="" type="radio"/> Deny
Direction:	<input type="radio"/> Incoming <input checked="" type="radio"/> Outgoing	Interface:	<input type="text" value="ppp-2"/>
In Interface:	<input type="text" value="ALL"/>	Log Option:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Security Level:	<input type="checkbox"/> High <input type="checkbox"/> Medium <input checked="" type="checkbox"/> Low	Blacklist Status:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Log Tag:	<input type="text"/>		
Start Time (HH MM SS):	<input type="text" value="00"/> <input type="text" value="00"/> <input type="text" value="00"/>	End Time (HH MM SS):	<input type="text" value="23"/> <input type="text" value="59"/> <input type="text" value="59"/>
Src IP Address:	<input type="text" value="any"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>		
Dest IP Address:	<input type="text" value="any"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>		
Protocol:	<input type="text" value="eq"/> <input type="text" value="TCP"/>		
Apply Stateful Inspection:	<input type="checkbox"/>		
Source Port:	<input type="text" value="any"/>	<input type="text" value="Any other port"/>	<input type="text" value="Any other port"/>
Dest Port:	<input type="text" value="eq"/>	<input type="text" value="TELNET (23)"/>	<input type="text" value="Any other port"/>
TCP Flag:	<input type="text" value="NOT-SYN"/>		
ICMP Type:	<input type="text" value="any"/> <input type="text" value="Echo Reply"/>		
ICMP Code:	<input type="text" value="any"/> <input type="text" value="0"/>		
IP Frag Pkt:	<input type="radio"/> Yes <input type="radio"/> No <input checked="" type="radio"/> Ignore	IP Option Pkt:	<input type="radio"/> Yes <input type="radio"/> No <input checked="" type="radio"/> Ignore
Packet Size:	<input type="text" value="any"/> <input type="text" value="0"/>		
TOD Rule Status :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
<input type="button" value="Submit"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>			

Figure 15-5 IP Filter Rule Example 2

15.6 Viewing IP Filter Statistics

For each rule, you can view statistics on how many packets were accepted or denied. Click **Stats** in the corresponding row in the **IP Filter Rule** table.



IP Filter Rule - Statistics	
IP Filter Rule Statistic	
<i>Rule ID:</i>	10
<i>Number of Packets Matching this Rule:</i>	0 Packets

Clear Close Refresh Help

Figure 15-6 IP Filter Rule: Statistics

Click **Clear** to reset the count to zero or click **Refresh** to update the screen.

Chapter 16

Configuring EOA Interfaces

This chapter describes how to configure an EOA (Ethernet over ATM) interface on the Prestige, if one is needed to communicate with your ISP.

16.1 Overview of EOA

The EOA protocol is commonly used to carry data between local area networks that use the Ethernet protocol and wide-area networks that use the ATM protocol. Many telecommunications industry networks use the ATM protocol. ISPs who provide DSL services often use the EOA protocol for data transfer with their customers' DSL modems.

EOA can be implemented to provide a bridged connection between a DSL modem and the ISP. In a bridged connection, data is shared between the ISP's network and their customer's as if the networks were on the same physical LAN. Bridged connections do not use the IP protocol. EOA can also be configured to provide a routed connection with the ISP, which uses the IP protocol to exchange data.

Before creating an EOA interface or modifying the default settings, make sure you know the type of protocol your ISP uses.

16.2 PPP vs. EOA

Your ISP may use a protocol other than EOA for communication with your Prestige, such as the point-to-point protocol (PPP). One type of PPP, named PPP over Ethernet (PPPoE), actually works "on top" of the EOA protocol. The other type, PPP over ATM (PPPoA), does not. However, if your ISP uses either type of PPP, you do not need to create an EOA interface. See the chapter on *Configuring PPP Connection* for instructions on configuring a PPP interface.

16.3 Viewing Your EOA Setup

To view your current EOA configuration, click **WAN** in the task bar and **EOA**. You can also get this same screen through **Bridging** or **Routing**.

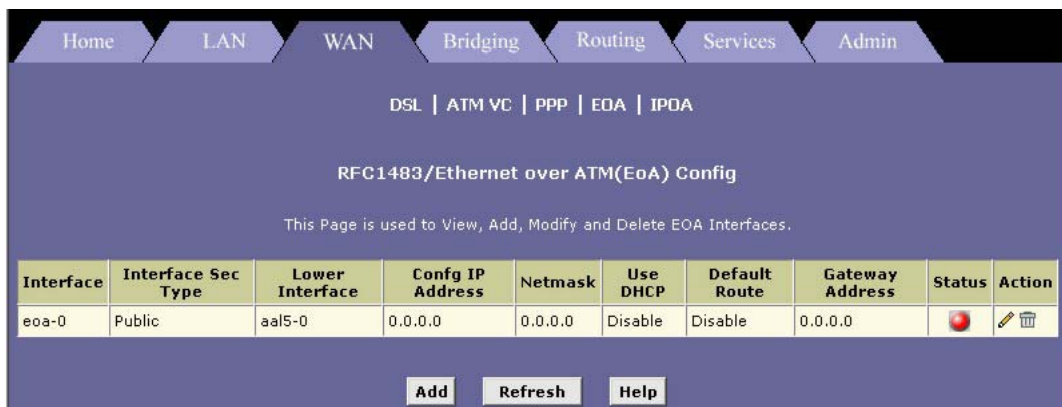


Figure 16-1 EOA

The following table describes the fields in this screen.

Table 16-1 EOA

FIELD	DESCRIPTION
Interface	The name the software uses to identify the EOA interface.
Interface Sec Type	This field displays the interface that the IP firewall is effective on. A public interface connects to the Internet. A private interface connects to your LAN, such as the Ethernet interface. The term DMZ (De-Militarized Zone), in Internet networking terms, refers to computers that are available for both public and in-network accesses (such as a company's public web server).
Lower interface	EOA interfaces are defined in software, and then associated with lower-level software and hardware structures (at the lowest level, they are associated with a physical port – the WAN port). This field should reflect an interface name defined in the next lower level of software over which the EOA interface will operate. This will be an ATM VCC interface, such as aal5-0, as described in the ATM VCC chapter.
Config IP Address and Net Mask	The IP address and network mask you want to assign to the interface. If the interface will be used for bridging with your ISP and you will not be using the Prestige as a router on your LAN, then you do not need to specify IP information. If you enable DHCP for this interface, then the Configured IP address will serve only as a request to the DHCP server. The actual address that is assigned by the ISP may differ if this address is not available.

Table 16-1 EOA

FIELD	DESCRIPTION
Use DHCP	When this option is Enable in the Add screen, this setting instructs the device to accept IP information assigned dynamically by your ISP's DHCP server. If the interface will be used for bridging with your ISP and you will not be routing data through it, select Disable for this option.
Default Route	Indicates whether the Prestige should use the IP address assigned to this interface, if any, as its default route for your LAN. This can be Enable or Disable. See the chapter on IP Routes for an explanation of default routes.
Gateway Address	This field displays the IP address of the gateway device.
Status	A green or red dot will display to indicate that the interface is currently enabled or disabled, respectively. You cannot manually enable or disable the interface; a disabled interface may indicate a problem with the DSL connection.
Action	Icons you can click on to edit (✎) or delete (🗑) the associated EOA interface.

16.4 Adding EOA Interfaces

In the RFC 1483/ Ethernet over ATM (EoA) Config screen click **Add** to display the **EOA Interface – Add** screen as shown next.

The screenshot shows the 'EOA Interface - Add' configuration window. It contains the following fields and options:

- EOA Interface:** A dropdown menu with 'eoa-1' selected.
- Interface Sec Type:** A dropdown menu with 'Public' selected.
- Lower Interface:** A dropdown menu with 'aal5-0' selected.
- Conf. IP Address:** Four input boxes, each containing the digit '0'.
- Netmask:** Four input boxes, each containing the digit '0'.
- Use DHCP:** Two radio buttons; 'Disable' is selected.
- Default Route:** Two radio buttons; 'Enable' is selected.
- Gateway IP Address:** Four empty input boxes.

At the bottom of the window are three buttons: 'Submit', 'Cancel', and 'Help'.

Figure 16-2 EOA Interface: Add

The following table describes the fields in this screen.

Table 16-2 EOA Interface: Add

FIELD	DESCRIPTION
EOA Interface	Select a predefined interface name from the drop-down list.
Interface Sec Type	Select the level of IP filter rule to be applied to from the drop-down list.
Lower Interface	Select the interface name over which this protocol is being configured from the drop-down list. Typically, an EOA interface is configured to operate over an aal5 interface, such as <i>aal5-0</i> .
Conf. IP Address	If you are using the Prestige as a router on your LAN, enter the IP address for the interface. You do not have to enter the IP address if you are using the Prestige as a bridge or when your Prestige gets the IP address from your ISP automatically.
Netmask	If you are using the Prestige as a router on your LAN, enter the network mask for the interface. You do not have to enter the network mask if you are using the Prestige as a bridge.
Use DHCP	Select Enable to get an IP address from a DHCP server.
Default Route	Select Enable to set a default route through your Prestige for your LAN to access the Internet.
Gateway Address	Enter the IP address of the gateway device.
Click Submit to confirm your changes. Refer to the section on <i>Committing Your Changes and Rebooting the Prestige</i> to save your changes to permanent memory and make your changes take effect.	

Chapter 17

Configuring Bridging

This chapter describes how to configure the Prestige to operate as a bridge.

17.1 Introduction

You can configure your Prestige to act as a bridging device between your LAN and your ISP. Bridges are devices that enable two or more networks to communicate as if they are two segments of the same physical LAN.

Before changing your bridge configuration, make sure you know which of connection your ISP uses to exchange data with their customer's DSL modems (such as Ethernet bridging or IP routing).

17.2 Overview of Bridges

A bridge is a device used to connect two or more networks so they can exchange data. A bridge learns the unique manufacturer-assigned hardware IDs of each computer or device on both (or all) networks. It learns that some of the IDs represent computers attached via one of the device's interfaces and others represent computers connected via other interfaces. It stores the ID list and the interfaces associated with each in its bridge forwarding table.

When the bridge receives a data packet, it compares its destination hardware ID to the entries in the bridge forwarding table. When the packet's ID matches one of the entries, it forwards the packet through the interface that connects to the network where that device resides. Note that the bridge does not send the data directly to the receiving computer, but broadcasts it to the receiving network, making it available to any node on the network. On the receiving network, a LAN protocol such as Ethernet takes over, helping the packet reach its destination.

When the bridge does not recognize a packet's destination hardware ID, it broadcasts the packet through all of its interfaces – to each network it is attached to.

17.3 Bridges vs. Routers

The essential difference between a bridge and a router is that a router uses a higher-level protocol (such as the IP) to determine how to pass data. IP data packets contain IP addresses that specifically identify the

destination computer. Routers can read this information and pass the data to the destination computer, or determine which next router to send the data to if the destination is not on a connected network.

Bridges cannot read or use IP information, but instead use the manufacturer-assigned hardware IDs to determine the port through which it should send the data packet.

Routers are considered more intelligent and flexible devices than bridges, and often provide a variety of security and network administration services.

17.4 Using the Prestige's Bridging Feature

Although the Prestige is pre-configured to serve as a router to provide Internet connectivity to your LAN, there are several instances in which you may also want to configure bridging:

- Your ISP may use protocols that require bridging with your LAN. The Prestige can be configured to appear as a bridge when communicating with your ISP, while continuing to provide router functionality for your LAN.
- Your LAN may include computers that communicate using “layer-3” protocols other than the Internet Protocol. These include IPX[®] and AppleTalk[®]. In this case, the Prestige can be configured to act as a bridge for packets that use these protocols while continuing to serve as a router for IP data.

In both cases, you need to specify the Prestige's interfaces as bridge interfaces.

17.5 Defining Bridge Interfaces

To enable bridging, specify the Prestige interfaces on which you want to bridge data and then enable bridging mode.

- Step 1.** Click **Bridging** to display the **Bridge Configuration** screen. The table may be empty if bridging has not yet been established.

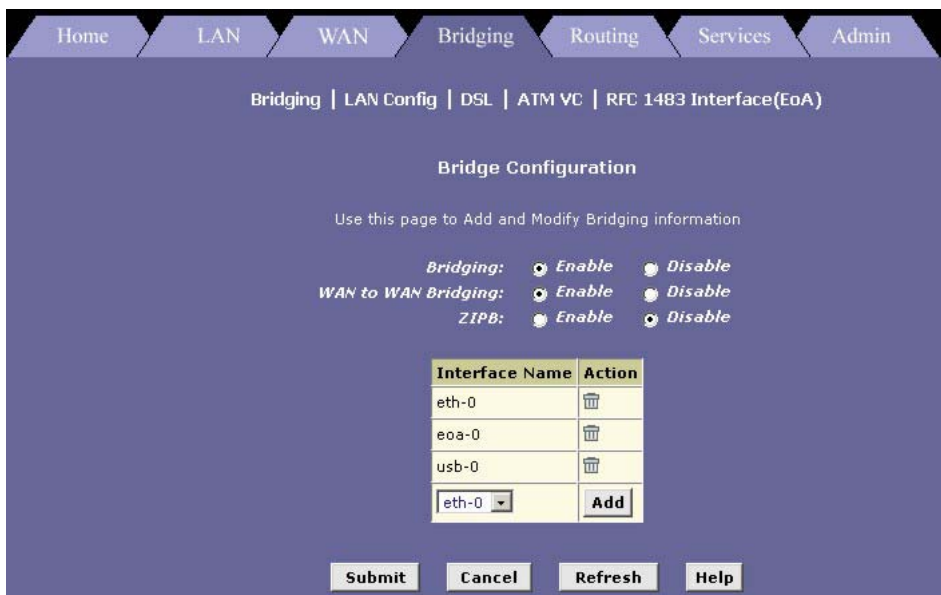



Figure 17-1 Bridge Configuration

The following table describes the fields in this screen.

Table 17-1 Bridge Configuration

FIELD	DESCRIPTION
Bridging	Select Enable to activate bridge mode on the Prestige.
WAN to WAN Bridging	Select Enable to allow WAN to WAN bridging. This is the default setting. Activating WAN to WAN bridging may not be desirable in situations where security or bandwidth is a major concern.
ZIPB	Select Enable to activate the Zero Installation PPPoE Bridge (ZIPB) mode so your ISP does not have to install a PPPoE client on your computer(s). Further more, you don't have to set up NAT (Network Address Translation) on the Prestige. ZIPB combines the advantages of routing and bridging modes.

Table 17-1 Bridge Configuration

FIELD	DESCRIPTION
Interface Name	<p>From the drop-down list menu, select the interface name on which you want to perform bridging and click Add.</p> <p>For example, select eth-0 (LAN) and eo-a-0 (WAN) interfaces. If you use such protocols on a USB-connected computer, you can also select usb-0.</p> <p>If you do not have an eo-a-0 interface, but instead have an interface named ppp-0 or ipo-a-0, your Prestige is not currently configured with a WAN interface that allows bridging with your ISP. You may want to check with your ISP to determine whether they use this protocol. See the chapter on <i>Configuring EOA</i> for instructions on creating an EOA interface.</p> <p>If you enable bridging on an interface that has already been assigned an IP address, then it is considered IP-enabled and will route (rather than bridge) IP packets received on the interface. The interface will bridge non-IP data it receives, however.</p> <p>You can determine whether the Ethernet (eth-0) and USB (usb-0) interfaces have been assigned IP addresses by displaying the IP Address Table (click Routing in the task bar and then click IP Addr). These interfaces will display in the table only if they have been assigned IP addresses.</p> <p>You can check whether the eo-a-0 interface has been assigned an IP address by displaying the EOA configuration table (in the advanced task bar, click EOA). If the Config IP Address field is empty and the Use DHCP field contains the word Disable, then no IP address has been assigned.</p>
Action	<p>Click  to remove the selected interface from the list. This prevents the selected interface from performing bridging.</p> <p>Click Add to include the selected interface in the list. This allows bridging on the selected interface.</p>
<p>Click Submit to confirm your changes. Refer to the section on <i>Committing Your Changes and Rebooting the Prestige</i> to save your changes to permanent memory and make your changes take effect.</p>	

Chapter 18

Configuring IPoA Interfaces

This chapter describes how to configure an IPoA (Internet Protocol over ATM) interface on the Prestige.

18.1 Introduction

An IPoA interface can be used to exchange IP packets over the ATM network, without using an underlying Ethernet over ATM (EOA) connection. You may use this type of interface in product development environments to eliminate unneeded variables when testing IP layer processing.

18.2 Viewing Your IPoA Interface Setup



To configure an IPoA interface, click the **WAN** tab and then **IPoA**.

Interface	Interface Sec Type	RFC 1577	Lower Interface	Peer IP Address	Config IP Address	Netmask	Gateway Address	Status	Action
ipoa-0	Public	No	-	-	192.168.20.20	255.255.0.0	192.168.10.10		

Figure 18-1 IPoA

The following table describes the fields in this screen.

Table 18-1 IPoA

FIELD	DESCRIPTION
Interface	This field displays the name the Prestige uses to identify the IPoA interface
Interface Sec Type	This field displays the interface that the IP firewall is effective on. A public interface connects to the Internet. A private interface connects to your LAN, such as the Ethernet interface. The term DMZ (De-Militarized Zone), in Internet networking terms, refers to computers that are available for both public and in-network accesses (such as a company's public web server).
RFC 1577	This field displays Yes if the IPoA interface is of type 1577. This means that one IPOA interface can have multiple VC mappings.
Lower Interface	IPoA interfaces are defined in software, and then associated with lower-level software and hardware structures (at the lowest level, they are associated with a physical port – the WAN port). This field should reflect an interface name defined in the next lower level of software over which the IPoA interface will operate. This will be an ATM VCC interface, such as aal5-0, as described in the ATM VCC chapter.
Peer IP Address	This field displays the IP address of the remote computer that the Prestige is connected to via the WAN connection.
Config IP Address and Net Mask	The two fields display the IP address and network mask you want to assign to the interface.
Gateway Address	This field displays the IP address of the gateway for this interface.
Status	A green or red dot will display to indicate that the interface is currently enabled or disabled, respectively. You cannot manually enable or disable the interface; a disabled interface may indicate a problem with the DSL connection.
Action	Click  to delete the selected IPoA interface, Click  to delete the selected IPoA interface. Click Map to specify the mapping of the IPoA interface with a VC.

18.3 Adding IPoA Interfaces

- Step 1.** Click **Add** in the **IP over ATM (IPoA) Configuration** screen. The **IPoA Interface – Add** screen displays.

Figure 18-2 IPoA Interface: Add

The following table describes the fields in this screen.

Table 18-2 IPoA Interface: Add

FIELD	DESCRIPTION
IPoA Interface	Select a pre-defined interface from the drop—down list menu.
Conf. IP Address	Enter the IP address to assign to the IPoA interface.
Interface Sec Type	Select the security type from the drop-down list menu to assign to the IPoA interface.
Netmask	Enter the subnet mask for the IPoA interface.
RFC 1577	Select Yes to configure the IPoA interface as type RFC 1577 to support multiple VC.
Use DHCP	Select Enable to use the DHCP server from the ISP.
Default Route	Select Enable to use a default route.
Gateway IP Address	Enter the IP address of the gateway device.
Click Submit to confirm your changes. Refer to the section on <i>Committing Your Changes and Rebooting the Prestige</i> to save your changes to permanent memory and make your changes take effect.	

18.4 Creating IPoA Mapping

To create IPoA mapping on the selected interface, click **Map** in the **Action** column in the **IP over ATM (IPoA) Configuration** screen.

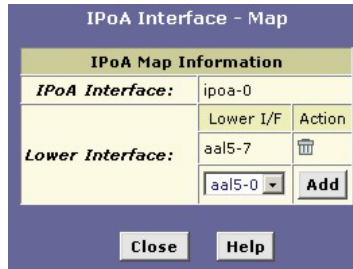



Figure 18-3 IPoA Interface: Map

The following table describes the fields in this screen.

Table 18-3 IPoA Interface: Map

FIELD	DESCRIPTION
IPoA Interface	This read-only field displays the interface name.
Lower Interface	
Lower I/F	This field displays the ATM VC to which this interface is associated (or mapped).
Action	Click  to delete existing mapping. Click Add to map the interface to the selected VC.

18.5 IPoA Mapping Table

To display the global mapping table, click the **Map** button in the **IP over ATM (IPoA) Configuration** screen.

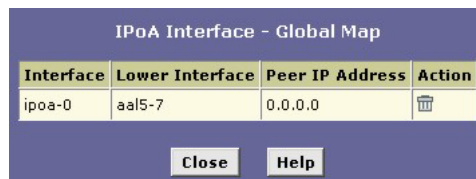



Figure 18-4 IPoA Interface: Global Map

The following table describes the fields in this screen.

Table 18-4 IPoA Interface: Global Map

FIELD	DESCRIPTION
Interface	This field displays the interface name.
Lower Interface	This field displays the lower interface (or VC) to which the interface is associated.
Peer IP Address	This field displays the IP address of the remote computer that the Prestige is connected to via the WAN connection through this interface.
Action	Click  to delete existing mapping.

Chapter 19

Configuring DNS Relay

This chapter describes how to configure DNS (Domain Name System) Relay on your Prestige.

19.1 Overview

An IP address uniquely identifies a host on the Internet. Since IP addresses are difficult to remember, a user-friendly domain name is used often instead. A domain name is a unique name that identifies an Internet site. The Domain Name System (DNS) maps a domain name to an IP address. When you access a web site, you can type either the IP address or the domain name. As your LAN computers access the Internet, domain names are converted to IP addresses on the DNS server.

With your Prestige configured as a DNS relay server, Internet access requests received from the LAN computers will be forwarded to the actual DNS servers at your ISP.

19.2 Viewing Your DNS Relay Setup

To view your current DNS relay configuration, launch the web configurator, click **Services** and **DNS** to display the **DNS Configuration** screen. DNS relay is enabled by default.

Home LAN WAN Bridging Routing Services Admin

LAN Config | DHCP Mode | DHCP Server | DHCP Relay

Dynamic Host Configuration Protocol (DHCP) Relay Configuration

As a DHCP relay agent, when a computer request Internet access, the device requests an IP address from your ISP, and then relays the addresses back to the computers. This table lists each interface on the device that relays data from your ISP. Typically, the LAN port is listed.


DHCP Server Address:

Interfaces Running DHCP Relay	Action
eo0-0	<input type="button" value=""/>
<input type="text" value="eth-0"/>	<input type="button" value="Add"/>

Figure 19-1 Dynamic Host Configuration Protocol (DHCP) Relay Configuration

The following table describes the fields in this screen.

Table 19-1 Dynamic Host Configuration Protocol (DHCP) Relay Configuration

FIELD	DESCRIPTION
DHCP Server Address	Enter the IP address of the ISP's DHCP server. If this field is 0.0.0.0 , request for IP information from your LAN will pass through the default gateway which will route the request appropriately.
Interfaces Running DHCP Relay	This field displays the interfaces that are currently configured with DHCP relay. To set an interface to use DHCP relay, select the interface from the drop-down list menu and click Add .
Action	Click  to disable DHCP relay on the select interface and remove the entry from the table. Click Add to set the selected interface to use DHCP relay.

Chapter 20

Firmware Upgrade

This chapter shows you how to upgrade the system firmware on the Prestige.

20.1 Filename Convention

Download the latest firmware from www.zyxel.com. The system firmware is contained in a single file, also known as an image. The firmware is composed of several distinct parts, each of which implements a different set of functions. You can use either the web configurator or FTP to upgrade the firmware.

Rename the firmware file to “TEPatch.bin” before uploading to your Prestige.

DO NOT turn off the Prestige during the file transfer. See section on *Recover from Firmware Upload Failure*, in case the file transfer is interrupted.

The Prestige automatically restarts after a successful firmware upgrade.

20.2 Firmware Upgrade Using the Web Configurator

- Step 1.** Download the latest firmware and rename it to “TEPatch.bin”.
- Step 2.** In the web configurator, click **Admin** on the task bar and then **Image Upgrade**.



Diagram 1 Image Upgrade

Step 2. Click **Browse** to specify the location of the firmware.

Step 3. Click **Upload** to start the file transfer process. The following screen displays during the firmware upload process.



Figure 20-1 Image Upgrade: In Progress

Step 4. If the file is transferred successfully, the following screen displays.



Figure 20-2 Image Upgrade: Successful

Step 5. The Prestige automatically reboots after a successful firmware upload.

20.3 Image Upgrade Using FTP

Follow the steps below to upgrade the firmware using FTP.

Step 1. Rename the new firmware file name to “TEPatch.bin”.

- Step 2.** Launch an FTP client on your computer.
- Step 3.** Enter “open” and the IP address of your Prestige. The default for LAN IP address is 192.168.1.1 and for USB port is 192.168.1.2.
- Step 4.** Enter “admin” as the username and then enter the password. The default password is “1234”.
- Step 5.** Enter “bin” to set the transfer mode to be binary.
- Step 6.** Enter “put TEPatch.bin” to transfer the file from the computer to the Prestige. Waite for a moment for the file transfer process to complete.
- Step 7.** Enter “quit” or “bye” to exit the ftp prompt.

```
D:\>ftp
ftp> open 192.168.1.1
Connected to 192.168.1.1.
220 FTP Server (Version 1.0) ready.
User (192.168.1.1:(none)): admin
331 User name okay, need password.
Password:
230 User logged in, proceed.
ftp> bin
200 Command okay.
ftp> hash
Hash mark printing On  ftp: (2048 bytes/hash mark) .
ftp> put TEPatch.bin
200 Command okay.
150 File status okay; about to open data connection.
226 Closing data connection. Requested file action successful.
ftp: 1462032 bytes sent in 43.71Seconds 33.45Kbytes/sec.
ftp> quit
~::~
```

Figure 20-3 FTP Session Example

- Step 8.** The Prestige automatically reboots after a successful firmware upload. Waite until the **SYS** LED turns off and on again. The new image will now be in effect.

20.4 Recover from Firmware Upload Failure

When the image file transfer process is interrupted, the **SYS**, **USB**, **DSL** and **ACT** LEDs blink after the Prestige is restarted. At this point, the Prestige is inaccessible. You *must* use TFTP to upload the firmware to the Prestige.

Since TFTP does not have any security checks, no username or password is required. To upload the image file using TFTP, follow the steps below.

- Step 1.** Launch the TFTP client on your computer and connect to the Prestige. Set the transfer mode to binary before starting data transfer.

Step 2. The file name for the image file must be renamed to “TEPatch.bin”. Use the TFTP client to transfer files between the Prestige and the computer.

For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use "put" to transfer from the Prestige to the computer and "binary" to set binary transfer mode.

20.4.1 TFTP Command Example

The following is an example TFTP command:

```
tftp [-i] host put image.bin TEPatch.bin
```

where "i" specifies binary image transfer mode (use this mode when transferring binary files), "host" is the Prestige's IP address, "put" transfers the file source on the computer (image.bin – name of the image file on the computer) to the file destination on the Prestige (TEPatch.bin – name of the image file on the Prestige).

20.5 GUI-based TFTP Clients

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

Table 2 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 image file (*.bin extension) on your computer.
Remote File	This is the filename on the Prestige. The filename for the image must be "TEPatch.bin".
Binary	Transfer the file in binary mode.
Abort	Stop file transfer.

Part: IV

ADDITIONAL INFORMATION

This part contains Troubleshooting, Appendices and the Index.

Chapter 20

Troubleshooting

This chapter suggests solutions for problems you may encounter in installing or using your Prestige, and provides instructions for using several IP utilities to diagnose problems.

Contact Customer Support if these suggestions do not resolve the problem.

20.1 Problems Starting Up the Prestige

Table 20-1 Troubleshooting the Start-Up of Your Prestige

PROBLEM	CORRECTIVE ACTIONS
The PWR LED is off.	Verify that you use the included power adapter and that it is securely connected to the Prestige and a wall socket/power strip. Make sure that the wall socket or the power strip is turned on and is receiving power.
The SYS LED is off.	Make sure you are using the correct power adapter and that it is connected to an adequate power supply. Turn the Prestige off and on. If the SYS LED is still not on after 5 ~10 seconds, you may have a hardware problem. Contact your local vender.
The USB LED is off.	Check the USB connect between the computer and the Prestige. Turn the Prestige off and on. Reinstall the USB driver. Refer to the <i>Quick Start Guide</i> .
The 10/100M LED is off.	Verify that the Ethernet cable is securely connected to your LAN hub or computer and to the Prestige. Make sure the computer and/or hub is turned on. Verify that your cable is sufficient for your network requirements. A 100 Mbit/sec network (10BaseTx) should use cables labeled Cat 5. 10Mbit/sec cables may tolerate lower quality cables.
The DSL LED is off.	Check the connection between the Prestige and the wall telephone jack. Wait for about 30 seconds to allow the Prestige to negotiate a connection with your ISP.

20.2 Problems with Web Configurator

Table 20-2 Troubleshooting the Web Configurator

PROBLEM	CORRECTIVE ACTIONS
<p>You have forgotten the administrator's login password.</p>	<p>If you have not changed the password from the default, try using "1234" as the password. The username by default is "admin" which you can't change.</p> <p>If you have created another account with administrative rights, login using that account.</p> <p>Otherwise, you can reset the Prestige to the default configuration by pressing the RESET button three times (using a pointed object such as a pen tip). Then login using the default username and password shown above.</p> <div style="text-align: center; border: 1px solid black; padding: 5px; background-color: #e0e0e0;"> <p>Resetting the Prestige removes any custom settings and returns all settings to their default values.</p> </div>
<p>Cannot access the web configurator program from your browser.</p>	<p>Use the <i>ping</i> utility (refer to the appendix) to check whether your computer can communicate with the Prestige. If it cannot, check the LAN or USB connection or restart the Prestige.</p> <p>The web configurator is best viewed with Internet Explorer version 5.0 or later. Support for Java® and JavaScript® should be enabled in your browser.</p> <p>Verify that the computer's IP address is defined as being on the same subnet as the IP address assigned to the LAN or USB port on the Prestige.</p>
<p>Changes to web configurator are not being retained.</p>	<p>Be sure to use the Commit function after any changes. Refer to the section on the commit function.</p>

20.3 Problems with Internet Access

Table 20-3 Troubleshooting the Internet Access

PROBLEM	CORRECTIVE ACTIONS
Computer(s) cannot access Internet.	<p>Use the <i>ping</i> utility (refer to the appendix) to check whether your computer can communicate with the Prestige. If it cannot, check the LAN or USB connection or restart the Prestige.</p> <p>If you assigned a fixed (static), private IP address to the computer, (not a registered public address), verify the following:</p> <p>Check that the gateway IP address on the computer is your public IP address (see the appendix on TCP/IP for instructions on viewing the IP information.) If it is not, correct the address or configure the computer to receive IP information. Verify with your ISP that the DNS server specified for the computer is valid. Correct the address or configure the computer to receive this information automatically.</p> <p>Verify that a Network Address Translation (NAT) rule has been defined on the Prestige to translate the private address to your public IP address. The assigned IP address must be within the range specified in the NAT rules (see the chapter on NAT). Or configure the computer to accept an address assigned by another device (see the chapter on NAT or the appendix on TCP/IP). The default configuration includes a NAT rule for all dynamically assigned addresses within a predefined pool (see the instructions in chapter on NAT to view the address pool).</p>
computers cannot display web pages on the Internet.	<p>Verify that the DNS server specified on the computers is correct for your ISP, as discussed in the item above. You can use the ping utility, discussed in the following section, to test connectivity with your ISP's DNS server.</p>

Appendix A

Diagnosing Problem Using IP Utilities

ping

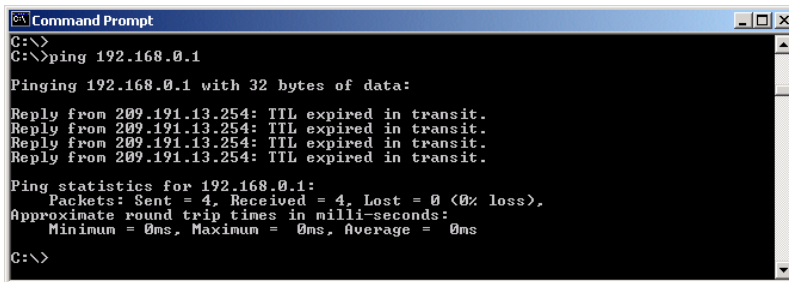
Ping is a command you can use to check whether your computer can recognize other computers on your network and the Internet. A ping command sends a message to the computer you specify. If the computer receives the message, it sends messages in reply. To use it, you must know the IP address of the computer you are trying to communicate with.

On Windows-based computers, you can execute a ping command from the **Start** menu. Click the **Start** button, and then click **Run**. In the **Open** text box, type a statement such as the following:

```
ping 192.168.1.1
```

Click **OK**. You can substitute any private IP address on your LAN or a public IP address for an Internet site, if known.

If the target computer receives the message, a Command Prompt window displays like that shown.



```
Command Prompt
C:\>
C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 209.191.13.254: TTL expired in transit.
Reply from 209.191.13.254: TTL expired in transit.
Reply from 209.191.13.254: TTL expired in transit.
Reply from 209.191.13.254: TTL expired in transit.

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Diagram 1 Using the ping Utility

If the target computer cannot be located, you will receive the message **Request timed out**.

Using the ping command, you can test whether the path to your Prestige is working (using the preconfigured default LAN IP address 192.168.1.1) or another address you assigned.

You can also test whether access to the Internet is working by typing an external address, such as that for www.yahoo.com (216.115.108.243). If you do not know the IP address of a particular Internet location, you can use the **nslookup** command, as explained in the following section.

From most other IP-enabled operating systems, you can execute the same command at a command prompt or through a system administration utility.

nslookup

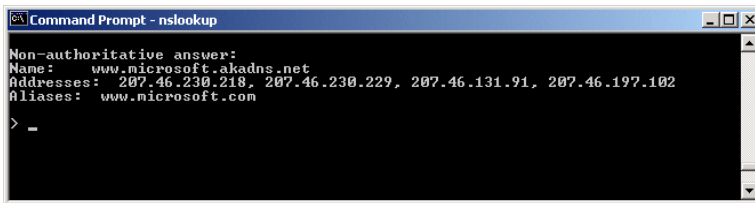
You can use the nslookup command to determine the IP address associated with an Internet site name. You specify the common name, and the nslookup command looks up the name on your DNS server (usually located with your ISP). If that name is not an entry in your ISP's DNS table, the request is then referred to another higher-level server, and so on, until the entry is found. The server then returns the associated IP address.

On Windows-based computers, you can execute the nslookup command from the **Start** menu. Click the **Start** button, and then click **Run**. In the **Open** text box, type the following:

nslookup

Click **OK**. A Command Prompt window displays with a bracket prompt (>). At the prompt, type the name of the Internet address you are interested in, such as www.zyxel.com.

The window will display the associate IP address.



```
Command Prompt - nslookup
Non-authoritative answer:
Name:    www.microsoft.akadns.net
Addresses: 207.46.230.218, 207.46.230.229, 207.46.131.91, 207.46.197.102
Aliases: www.microsoft.com
> -
```

Diagram 2 Using the nslookup Utility

There may be several addresses associated with an Internet name. This is common for web sites that receive heavy traffic; they use multiple, redundant servers to carry the same information.

To exit from the nslookup utility, type “exit” and press <Enter> at the command prompt.

Appendix B

Enable Java Support in Internet Explorer

If the pages of the web configurator does not display properly in Internet Explorer, follow the steps below to enable the Java security option. Screen shots for Internet Explorer 5 are shown. Steps may vary depending on your version of Internet Explorer.

Step 1. From Internet Explorer, click **Tools** and then **Internet Options** .

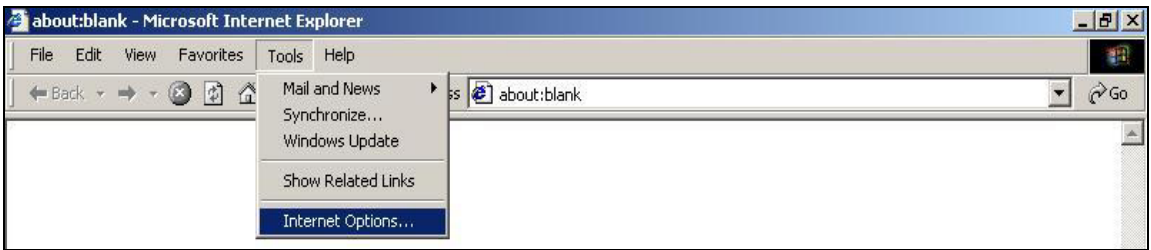


Diagram 3 Internet Explorer 5.0

Step 2. Select the **Security** tab in the **Internet Options** window. Then click **Trusted Sites**.

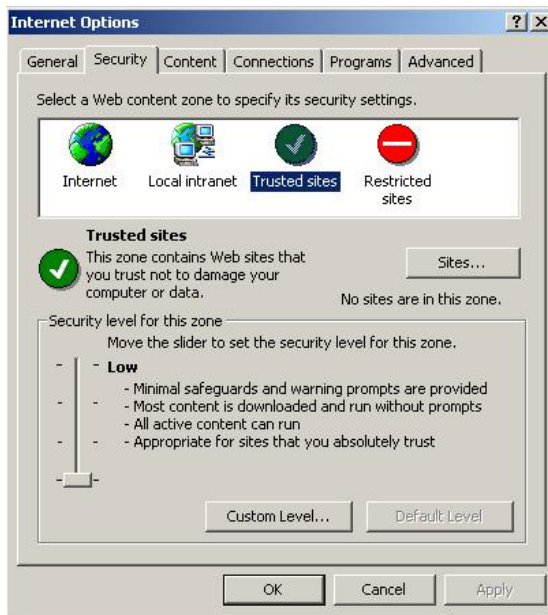


Diagram 4 IE 5.0: Internet Options

Step 3. Click **Sites** and type the IP address of the Prestige with the prefix “**https://**”. For example, **https://190.168.1.1**. Click **Add** and then **OK** to return to the **Internet Options** window.

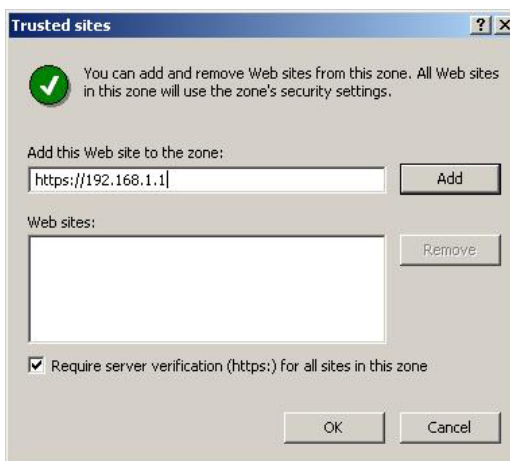


Diagram 5 IE 5.0: Add Trusted Site IP Address

- Step 4.** In the **Internet Options** window, click **Custom Level**.
- Step 5.** Scroll down to the **Microsoft VM** option. Under **Java Permissions** select **Custom**. Then click the **Java Custom Settings** button that displays.

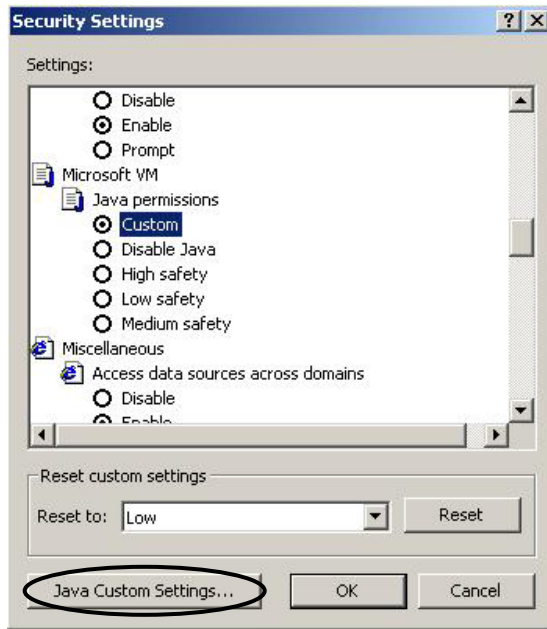


Diagram 6 IE 5.0: Security Settings

- Step 6.** Click the **Edit Permission** tab.
- Step 7.** Select **Enable** under the **Run Unsigned Content** option. Then click **OK**.

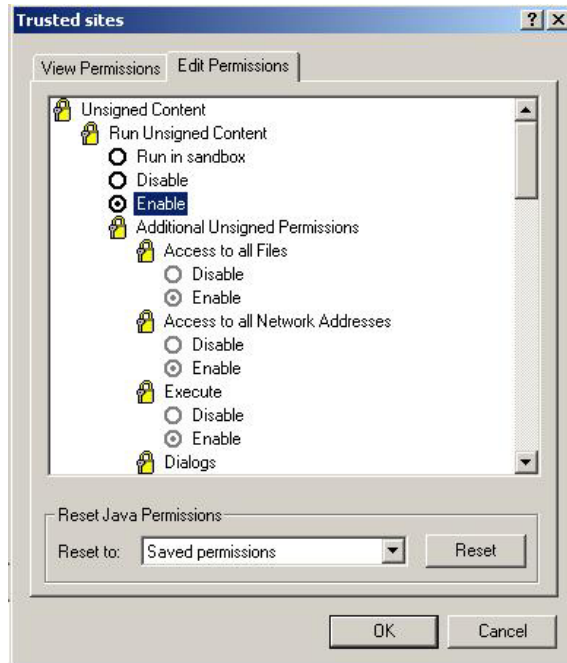


Diagram 7 IE 5.0: Edit Permissions

Step 8. Click **Yes** to change the security settings then click **OK** to close all settings windows.

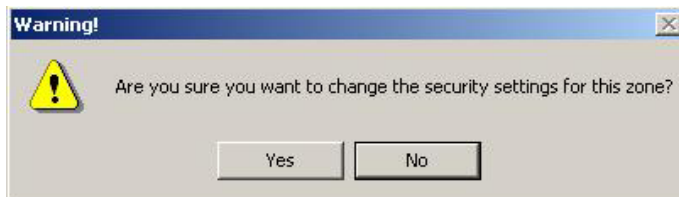


Diagram 8 IE 5.0: Internet Security Change Verification

Appendix C

Setting Up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

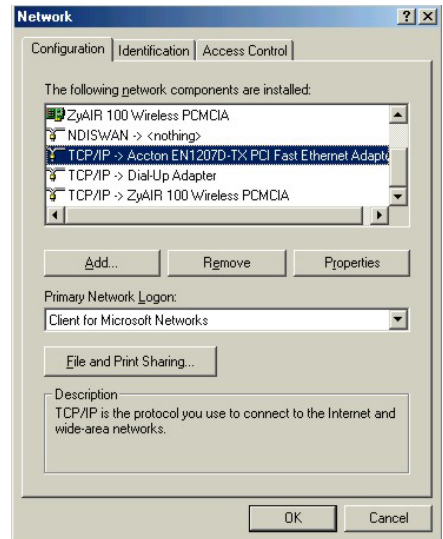
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the Prestige's LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.



Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

- a. In the **Network** window, click **Add**.
- b. Select **Adapter** and then click **Add**.
- c. Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

- a. In the **Network** window, click **Add**.
- b. Select **Protocol** and then click **Add**.
- c. Select **Microsoft** from the list of **manufacturers**.
- d. Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

- a. Click **Add**.
- b. Select **Client** and then click **Add**.
- c. Select **Microsoft** from the list of manufacturers.
- d. Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
- e. Restart your computer so the changes you made take effect.

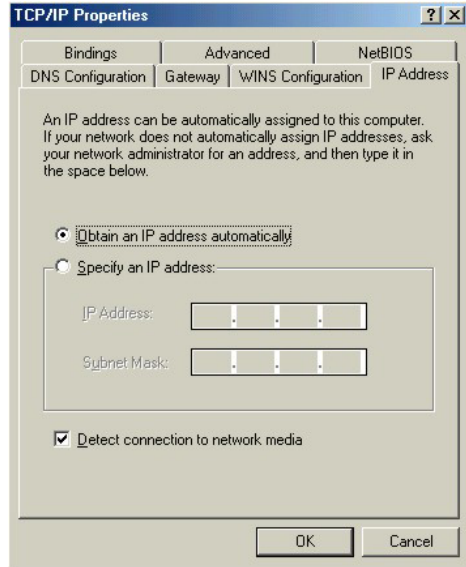
Configuring IP Address

1. In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**.

2. Click the **IP Address** tab.

-If your IP address is dynamic, select **Obtain an IP address automatically**.

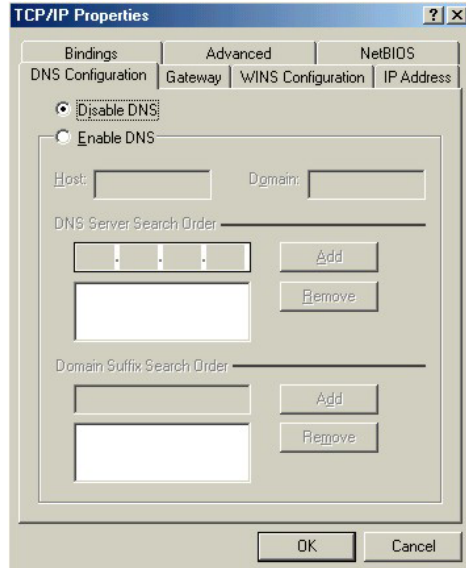
-If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.



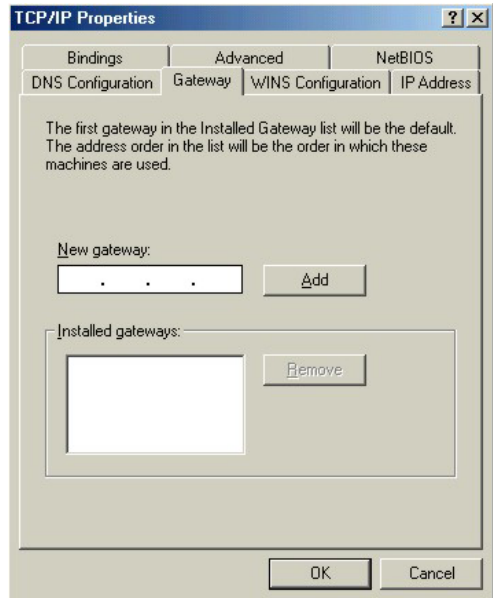
3. Click the **DNS Configuration** tab.

-If you do not know your DNS information, select **Disable DNS**.

-If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).



4. Click the **Gateway** tab.
-If you do not know your gateway's IP address, remove previously installed gateways.
-If you have a gateway IP address, type it in the **New gateway field** and click **Add**.



5. Click **OK** to save and close the **TCP/IP Properties** window.
6. Click **OK** to close the **Network** window. Insert the Windows CD if prompted.
7. Turn on your Prestige and restart your computer when prompted.

Verifying Settings

1. Click **Start** and then **Run**.
2. In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.
3. Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

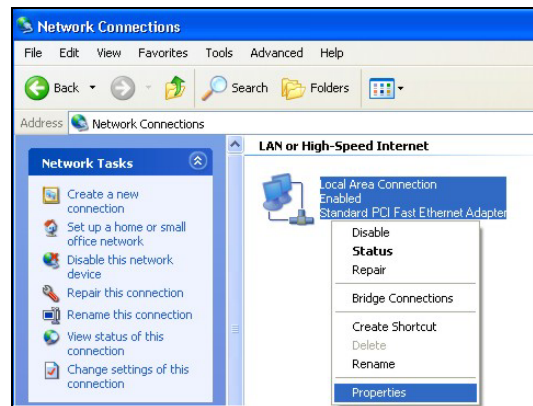
1. For Windows XP, click **start, Control Panel**. In Windows 2000/NT, click **Start, Settings, Control Panel**.



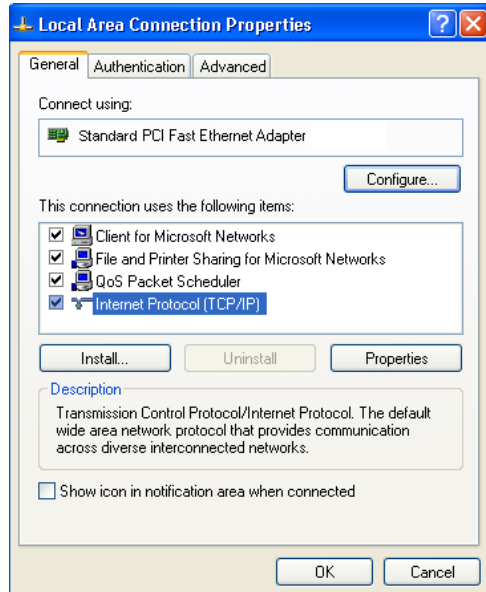
2. For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.



3. Right-click **Local Area Connection** and then click **Properties**.



4. Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and click **Properties**.

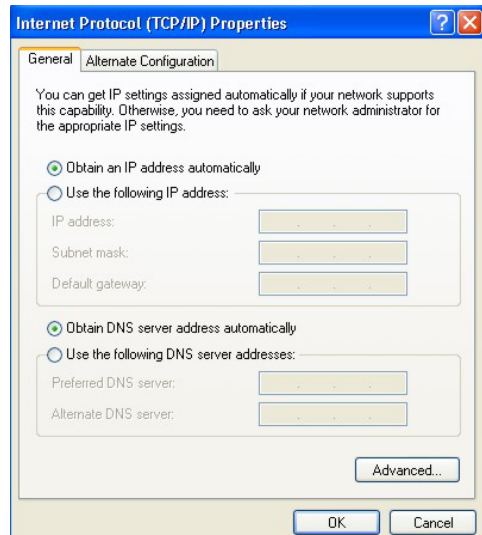


5. The **Internet Protocol TCP/IP Properties** window opens (the **General** tab in Windows XP).

-If you have a dynamic IP address click **Obtain an IP address automatically**.

-If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.

Click **Advanced**.



6. -If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

-In the **IP Settings** tab, in IP addresses, click **Add**.

-In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.

-Repeat the above two steps for each IP address you want to add.

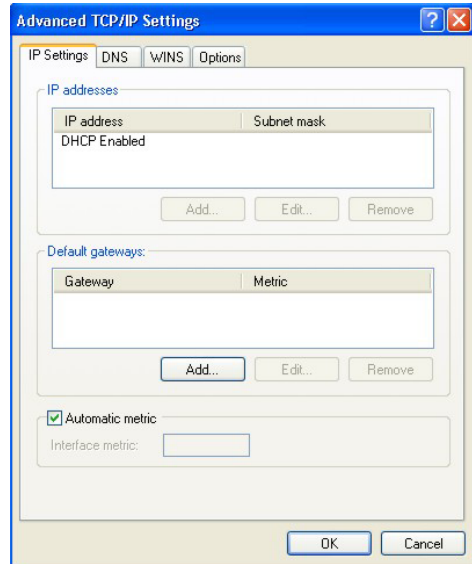
-Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.

-In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.

-Click **Add**.

-Repeat the previous three steps for each default gateway you want to add.

-Click **OK** when finished.

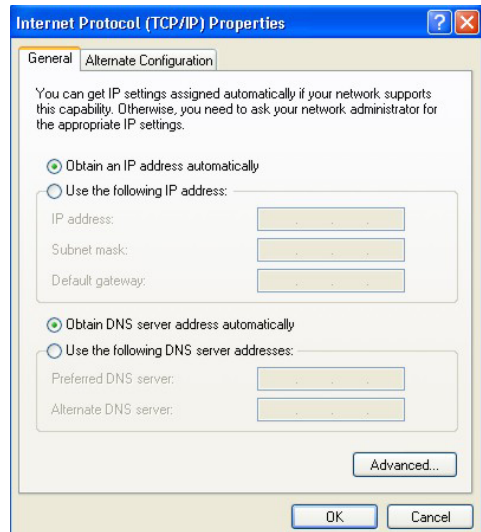


7. In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):

-Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).

-If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.



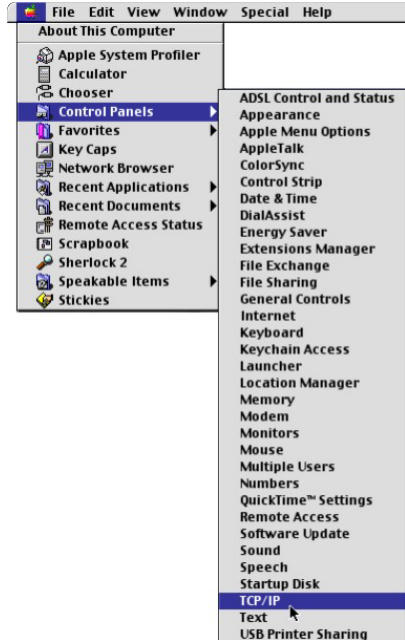
8. Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
9. Click **OK** to close the **Local Area Connection Properties** window.
10. Turn on your Prestige and restart your computer (if prompted).

Verifying Settings

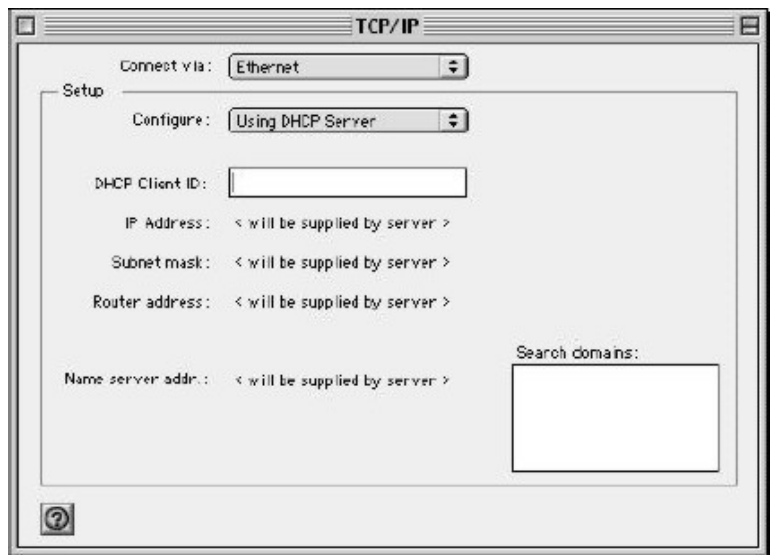
1. Click **Start, All Programs, Accessories** and then **Command Prompt**.
2. In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

1. Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.



2. Select **Ethernet built-in** from the **Connect via** list.



3. For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

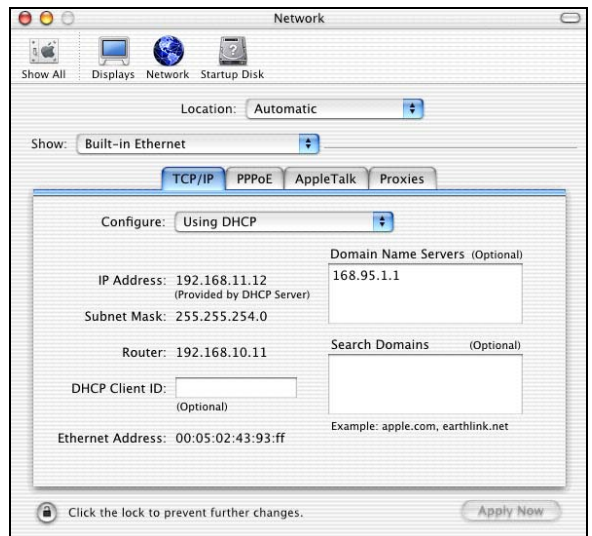
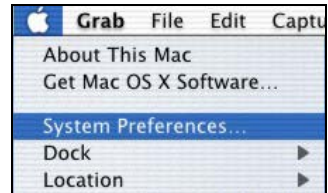
- For statically assigned settings, do the following:
 - From the **Configure** box, select **Manually**.
 - Type your IP address in the **IP Address** box.
 - Type your subnet mask in the **Subnet mask** box.
 - Type the IP address of your Prestige in the **Router address** box.
- Close the **TCP/IP Control Panel**.
- Click **Save** if prompted, to save changes to your configuration.
- Turn on your Prestige and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

Macintosh OS X

- Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.
- Click **Network** in the icon bar.
 - Select **Automatic** from the **Location** list.
 - Select **Built-in Ethernet** from the **Show** list.
 - Click the **TCP/IP** tab.



3. For dynamically assigned settings, select **Using DHCP** from the **Configure** list.
4. For statically assigned settings, do the following:
 - From the **Configure** box, select **Manually**.
 - Type your IP address in the **IP Address** box.
 - Type your subnet mask in the **Subnet mask** box.
 - Type the IP address of your Prestige in the **Router address** box.
5. Click **Apply Now** and close the window.
6. Turn on your Prestige and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

Appendix D

IP Addresses, Network Masks, and Subnets

This section pertains only to IP addresses for IPv4 (version 4 of the Internet Protocol). IPv6 addresses are not covered. This section assumes basic knowledge of binary numbers, bits and bytes.

IP Addresses

IP addresses, the Internet's version of telephone numbers, are used to identify individual nodes (computers or devices) on the Internet. Every IP address contains four numbers, each from 0 to 255 and separated by dots (periods), e.g. 20.56.0.211. These numbers are called, from left to right, field1, field2, field3, and field4.

This style of writing IP addresses as decimal numbers separated by dots is called *dotted decimal notation*. The IP address 20.56.0.211 is read "twenty dot fifty-six dot zero dot two-eleven."

Structure of an IP address

IP addresses have a hierarchical design similar to that of telephone numbers. For example, a 7-digit telephone number starts with a 3-digit prefix that identifies a group of thousands of telephone lines, and ends with four digits that identify one specific line in that group.

Similarly, IP addresses contain two kinds of information.

- **Network ID** Identifies a particular network within the Internet or intranet
- **Host ID** Identifies a particular computer or device on the network

The first part of every IP address contains the network ID, and the rest of the address contains the host ID. The length of the network ID depends on the network's *class* (see following section).

Diagram 9 IP Address structure

	Field1	Field2	Field3	Field4
Class A	Network ID	Host ID		
Class B	Network ID		Host ID	
Class C	Network ID			Host ID

Here are some examples of valid IP addresses:

Class A: 10.30.6.125 (network = 10, host = 30.6.125)

Class B: 129.88.16.49 (network = 129.88, host = 16.49)

Class C: 192.60.201.11 (network = 192.60.201, host = 11)

Network classes

The three commonly used network classes are A, B, and C. (There is also a class D but it has a special use beyond the scope of this discussion.) These classes have different uses and characteristics.

Class A networks are the Internet's largest networks, each with room for over 16 million hosts. Up to 126 of these huge networks can exist, for a total of over 2 billion hosts. Because of their huge size, these networks are used for WANs and by organizations at the infrastructure level of the Internet, such as your ISP.

Class B networks are smaller but still quite large, each able to hold over 65,000 hosts. There can be up to 16,384 class B networks in existence. A class B network might be appropriate for a large organization such as a business or government agency.

Class C networks are the smallest, only able to hold 254 hosts at most, but the total possible number of class C networks exceeds 2 million (2,097,152 to be exact). LANs connected to the Internet are usually class C networks.

Some important notes regarding IP addresses:

- The class can be determined easily from field1:
field1 = 1-126: Class A
field1 = 128-191: Class B
field1 = 192-223: Class C
(field1 values not shown are reserved for special uses)
- A host ID can have any value except all fields set to 0 or all fields set to 255, as those values are reserved for special uses.

Subnet masks

A *mask* looks like a regular IP address, but contains a pattern of bits that tells what parts of an IP address are the network ID and what parts are the host ID: bits set to 1 mean "this bit is part of the network ID" and bits set to 0 mean "this bit is part of the host ID."

Subnet masks are used to define *subnets* (what you get after dividing a network into smaller pieces). A subnet's network ID is created by "borrowing" one or more bits from the host ID portion of the address. The subnet mask identifies these host ID bits.

For example, consider a class C network 192.168.1. To split this into two subnets, you would use the subnet mask:

255.255.255.128

It's easier to see what's happening if we write this in binary:

11111111. 11111111. 11111111.10000000

As with any class C address, all of the bits in field1 through field 3 are part of the network ID, but note how the mask specifies that the first bit in field 4 is also included. Since this extra bit has only two values (0 and 1), this means there are two subnets. Each subnet uses the remaining 7 bits in field4 for its host IDs, which range from 0 to 127 (instead of the usual 0 to 255 for a class C address).

Similarly, to split a class C network into four subnets, the mask is:

255.255.255.192 or 11111111. 11111111. 11111111.11000000

The two extra bits in field4 can have four values (00, 01, 10, 11), so there are four subnets. Each subnet uses the remaining six bits in field4 for its host IDs, ranging from 0 to 63.

Sometimes a subnet mask does not specify any additional network ID bits, and thus no subnets. Such a mask is called a *default subnet mask*. These masks are:

Class A: 255.0.0.0

Class B: 255.255.0.0

Class C: 255.255.255.0

These are called *default* because they are used when a network is initially configured, at which time it has no subnets.

Appendix E

Binary Numbers

Binary Numbers

Binary numbers are numbers written using only the two digits 0 and 1, e.g., 110100.

In everyday life, we use the decimal system of numbers. In decimal, numbers are written using the ten digits 0, 1, 2, 3, 4, 5, 6, 7, 8, and 9. Computers, however, do not use decimal. Instead, they use *binary*.

Just as each digit in a decimal number represents a multiple of 10 (1, 10, 100, 1000, 10,000, etc.), each digit in a binary number represents a multiple of 2 (1, 2, 4, 8, 16, etc.). For example:

Decimal Binary

$$\begin{array}{cccccccc} \text{1,000's} & \text{100's} & \text{10's} & \text{1's} & = & \text{8's} & \text{4's} & \text{2's} & \text{1's} \\ - & - & \mathbf{1} & \mathbf{3} & & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} \end{array}$$

Also, since binary uses only two digits to represent all numbers, a binary number has more digits than the same number in decimal. In the example above, you can see that the decimal number 13 is the same as the binary number 1101 ($8 + 4 + 1 = 13$).

Bits and bytes

Computers handle binary numbers by grouping them into units of distinct sizes. The smallest unit is called a *bit*, (a *bit* is a single binary digit, i.e., 0 or 1) and the most commonly used unit is called a *byte*.

A *byte* is a group of eight consecutive bits (the number of bits can vary with computers, but is almost always eight), e.g., 11011001. The value of a byte ranges from 0 (00000000) to 255 (11111111). The following shows the values of the eight digits in a byte along with a sample value:

$$\begin{array}{cccccccc} \text{128's} & \text{64's} & \text{32's} & \text{16's} & \text{8's} & \text{4's} & \text{2's} & \text{1's} \\ \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} \end{array}$$

The decimal value of this byte is 173 ($128 + 32 + 8 + 4 + 1 = 173$).

Appendix F

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.

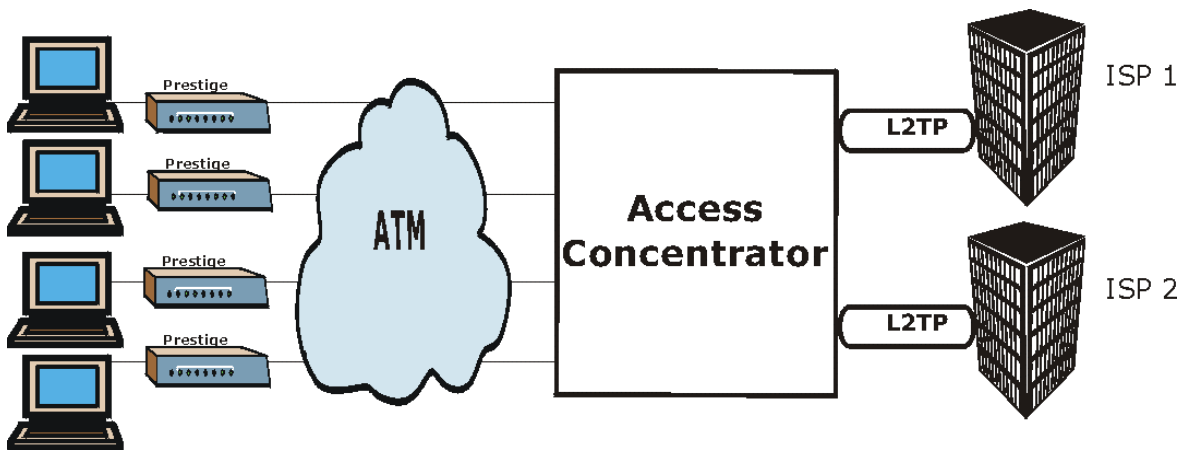


Diagram 10 Single-PC per Router Hardware Configuration

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.

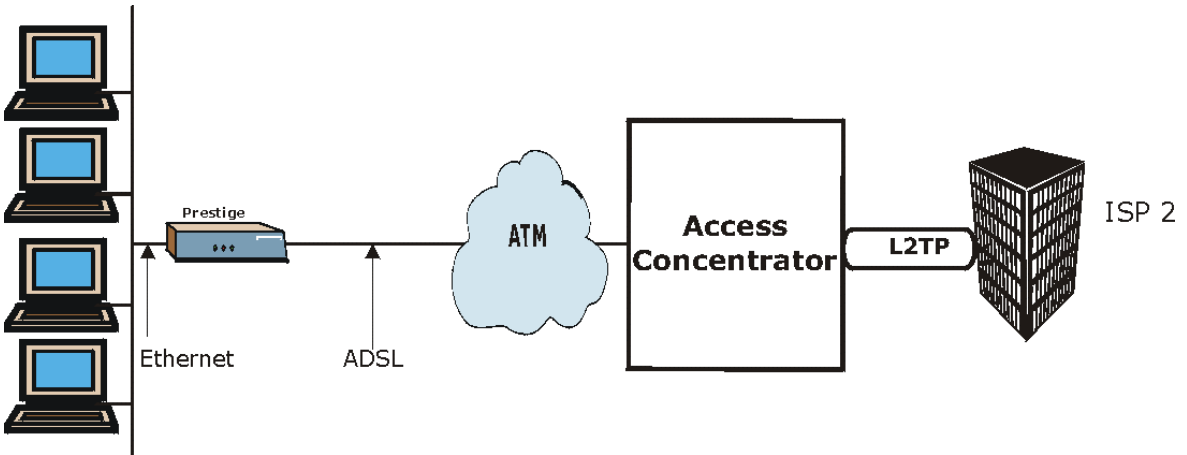


Diagram 11 Prestige as a PPPoE Client

Appendix G

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

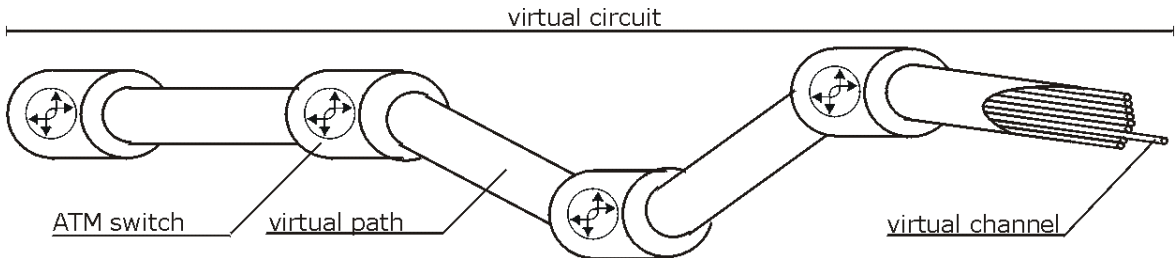


Diagram 12 Virtual Circuit Topology

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 H

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)
EUROPEAN PLUG STANDARDS	
AC Power Adapter Model	DV-121AACCP-5716
Input Power	AC230Volts/50Hz/100mA
Output Power	AC12Volts/1.0A
Power Consumption	8 W
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-121AD
Input Power	AC230Volts/50Hz/140mA
Output Power	AC12Volts/1.0A
Power Consumption	8 W
Safety Standards	ITS-GS, CE (EN 60950, BS 7002)
CHINESE PLUG 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)
CHINESE PLUG 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

- A**
- ADSL, what is it?..... xvii
- Alarm page..... 10-1
- Alarms
- defined 10-1
- Asynchronous Transfer Mode..... See ATM
- ATM
- viewing configuration 12-1
- ATM VCC – Add page..... 12-3
- B**
- BASIC NAT flavor 8-13
- BIMAP NAT flavor 8-16
- Binary numbers..... Q
- Bits Q
- Bridge Configuration page..... 17-2
- Bytes Q
- C**
- Configuration Manager
- troubleshooting 20-2
- Copyright ii
- Customer Support v
- D**
- Date and time
- changing in the system..... 3-9
- Default configuration 2-9
- Default gateway 6-2
- DHCP
- defined 7-1
 - device modes..... 7-2
- DHCP Address Table page 7-7
- DHCP client
- defined 7-1
- DHCP relay
- configuring device as..... 7-2
 - Configuring the device as 7-8
- DHCP Relay Configuration page 7-8, 7-9
- DHCP server
- configuring the device as 7-2
 - using a LAN device as 7-2
 - using the device as 7-2
 - viewing assigned addresses 7-7
- DHCP Server
- defined 7-1
- DHCP Server Pool—Add page 7-3
- Diagnostics 10-2
- Digital Subscriber Line Access Multiplexer..... 1-2
- DSL (Digital Subscriber Line)..... xvii
- DSL Interval Statistics page 13-4
- DSL Parameters page 13-2
- DSL Statistics page..... 13-3
- DSL Status page 13-1
- DSL, What Is It?..... xvii
- DSLAM..... See Digital Subscriber Line Access Multiplexer
- Dynamically assigned IP addresses 7-1
- E**
- EOA Interface – Add page 16-4
- EOA page 16-2
- Eth-0 interface
- defined 2-10
- F**
- FCC iii
- FILTER NAT flavor..... 8-14
- Firmware Uload
- GUI-based TFTP Clients 20-4
- Firmware Upgrade..... 20-1
- Web Configurator 20-1

Firmware Upload 20-1
 Filename Convention 20-1
 FTP 20-2
 recover from failure 20-3
 TFTP Command Example 20-4
 Frame Relay 1-2
 Front panel 2-1
 Full Rate 2-5

G

Gateway
 defined 6-2
 General Commands for GUI-based TFTP Clients
 20-4

H

Hop
 defined 6-2
 Hop count 9-3
 Host ID M

I

Internet Access 1-1, 1-2
 IP address
 in device's routing table 6-4
 IP address pools
 creating 7-3
 excluding addresses 7-7
 IP Address Table page 5-1
 IP addresses
 explained M
 viewing device's 5-1
 IP filter
 overview 15-1
 IP Filter Configuration page 15-2
 IP Filter Rule – Modify Page 15-9
 IP Filter Rule – Statistics page 15-14
 IP Filter Rule – Add Page 15-4
 IP filter rules
 adding 15-3

 examples 15-9
 IP filters
 viewing statistics 15-14
 IP Global Statistics page 5-3
 IP Route Table page 6-3
 IP routes
 adding 6-4
 manually configuring 6-2
 IP Routes
 defined 6-1
 IP Static Route 6-3
 IP Utilities A
 IPoA Interface – Add page 18-4
 IPoA page 18-1
 ISDN 2-7
 ISP
 as DHCP server 7-2

L

LAN interface 7-9
 configuring multiple 5-2
 LAN IP address 4-1
 default 4-1
 LAN port 4-1
 LEDs
 troubleshooting 20-1
 Login
 to Configuration Manager 3-1

N

NAT
 Adding rules - overview 8-8
 BASIC flavor 8-13
 BIMAP flavor 8-16
 defined 8-1
 FILTER flavor 8-14
 PASS flavor 8-17
 RDR flavor 8-10
 NAT Configuration page 8-3
 NAT Rule Configuration page 8-5
 NAT Rule Global Statistics page 8-5

NAT Rule—Add page - bimap	8-16
NAT Rule—Add page - filter	8-14
NAT Rule—Add page - pass	8-17
NAT Translations page	8-7
Navigating	3-2
Network Address Translation	<i>See</i> NAT
Network classes	N
Network ID	M
Network mask	N
nslookup	C

P

Packets	
filtering	15-1
Pages	
Alarm	10-1
ATM VCC - Add	12-3
Bridge Configuration	17-2
DHCP Address Table	7-7
DHCP Relay Configuration	7-8, 7-9
DHCP Server Pool - Add	7-3
DHCP Server Pool- Modify	7-7
DSL Interval Statistics	13-4
DSL Parameters	13-2
DSL Statistics	13-3
DSL Status	13-1
EOA	16-2
EOA Interface - Add	16-4
IP Address Table	5-1
IP Filter Configuration	15-2
IP Filter Rule - Add	15-4
IP Filter Rule - Modify	15-9
IP Filter Rule - Statistics	15-14
IP Global Statistics	5-3
IP Route Table	6-3
IPoA	18-1
IPoA Interface	18-4
NAT Configuration	8-3
NAT Rule Add - bimap	8-16
NAT Rule Add - filter	8-14
NAT Rule Add - pass	8-17

NAT Rule Configuration	8-5
NAT Rule Global Statistics	8-5
NAT Translations	8-7
PPP Configuration	11-2
PPP Interface - Add	11-7
PPP Interface - Modify	11-8
RIP Global Statistics	9-4
PASS - NAT flavor	8-17
Password	
changing	3-10
default	3-2
Performance statistics	5-2
Ping	A
Point to Point Protocol	<i>See</i> PPP
Point-to-Point	xvii
Port numbers	
using non-standard	8-12
POTS Splitter	2-6
PPP Configuration page	11-2
<i>PPP interface</i>	
<i>with NAT</i>	8-9
PPP Interface – Add page	11-7
PPP Interface – Modify page	11-8
Protocols	
IP <i>See</i> IP	
PPP	<i>See</i> PPP
selecting for NAT rules	8-9

Q

Quick Start Guide	3-1
-------------------------	-----

R

RDR (NAT flavor)	8-10
Read Me First	xv
Rear Panel	2-2
Rebooting	3-13
Recover from Firmware Upload Failure	20-3
Related Documentation	xv
Reset button	3-14
Reset Button	2-5
RIP	

configuring on device 9-2
overview 9-1
viewing statistics 9-4
Routing Information Protocol *See* RIP

S

Serviceiv
Splitters 2-5
Statically assigned IP addresses 7-1
Submitting vs committing 3-12
Subnet masksN
Supporting Diskxv
Syntax Conventionsxv
System requirements
 for Configuration Manager 3-1
System requirements: 1-2

T

Task bar 3-2
Telephone Microfilters 2-6
Testing installation 2-11
Time and date
 changing in the system 3-9
Traps *See* Alarms
Troubleshooting 20-1

Internet Access20-3
Start-Up of Your Prestige20-1
Web Configurator20-2

U

USB
 configuring IP on PC2-8
Username
 default3-2

W

WAN interface
 configuring multiple5-2
Web browser
 requirements1-2
 version requirements3-1
Web browsers
 compatible versions3-1

Z

ZyXEL Limited Warranty
 Noteiv