Prestige 660R-6xC Series

ADSL/ADSL2/ADSL2+ Router

User's Guide

Version 3.40
November 2004

ZyXEL
Unleash Networking Power

Copyright

Disclaimer

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

Trademarks

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

Federal Communications Commission (FCC) Interference Statement

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

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

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

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

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

Notice 1

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

Certifications

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

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 lightening.

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 LOCATION	SUPPORT E-MAIL SALES E-MAIL	TELEPHONE[A] FAX	WEB SITE FTP SITE	REGULAR MAIL
WORLDWIDE	support@zyxel.com.tw sales@zyxel.com.tw	+886-3-578-3942 +886-3-578-2439	www.zyxel.com www.europe.zyxel.com ftp.zyxel.com ftp.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
NORTH AMERICA	support@zyxel.com sales@zyxel.com	+1-800-255-4101 +1-714-632-0882 +1-714-632-0858	www.us.zyxel.com ftp.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
GERMANY	support@zyxel.de sales@zyxel.de	+49-2405-6909-0 +49-2405-6909-99	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
FRANCE	info@zyxel.fr	+33 (0)4 72 52 97 97 +33 (0)4 72 52 19 20	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
SPAIN	support@zyxel.es sales@zyxel.es	+34 902 195 420 +34 913 005 345	www.zyxel.es	ZyXEL Communications Alejandro Villegas 33 1º, 28043 Madrid Spain
DENMARK	support@zyxel.dk sales@zyxel.dk	+45 39 55 07 00 +45 39 55 07 07	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 5 2860 Soeborg Denmark
NORWAY	support@zyxel.no sales@zyxel.no	+47 22 80 61 80 +47 22 80 61 81	www.zyxel.no	ZyXEL Communications A/S Nils Hansens vei 13 0667 Oslo Norway
SWEDEN	support@zyxel.se sales@zyxel.se	+46 31 744 7700 +46 31 744 7701	www.zyxel.se	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden
FINLAND	support@zyxel.fi sales@zyxel.fi	+358-9-4780-8411 +358-9-4780 8448	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland

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

Table of Contents

List of Figures

List of Tables

Preface

Congratulations on your purchase of the Prestige 660R-6xC ADSL/ADSL2/ADSL2+ Router.

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

Your Prestige is easy to install and configure.

About This User's Guide

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

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

Syntax Conventions

- "Enter" means for you to type one or more characters. "Select" or "Choose" means for you to use one predefined choices.
- The SMT menu titles and labels are in **Bold Times New Roman** font. Predefined field choices are in **Bold Arial** font. Command and arrow keys are enclosed in square brackets. [ENTER] means the Enter, or carriage return key; [ESC] means the Escape key and [SPACE BAR] means the Space Bar.
- Mouse action sequences are denoted using a comma. For example, "click the Apple icon, **Control Panels** and then **Modem**" means first click the Apple icon, then point your mouse pointer to **Control Panels** and then click **Modem**.
- For brevity's sake, we will use "e.g.," as a shorthand for "for instance", and "i.e.," for "that is" or "in other words" throughout this manual.
- The Prestige 660R-6xC series may be referred to as the Prestige in this user's guide. This refers to both models (ADSL over POTS and ADSL over ISDN) unless specifically identified.

Related Documentation

- Supporting Disk

  Refer to the included CD for support documents.

- Quick Start Guide

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

- Web Configurator Online Help

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

- ZyXEL Glossary and Web Site

  Please refer to www.zyxel.com for an online glossary of networking terms and additional support documentation.

User Guide Feedback

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

Graphics Icons Key

Prestige 	Computer 	Notebook computer 
Server 	DSLAM 	Telephone 
Router 	Switch 	

Introduction to DSL

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

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

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

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

Introduction to ADSL

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

CHAPTER 1
Getting To Know Your Prestige

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

1.1 Introducing the Prestige

Your Prestige integrates high-speed 10/100Mbps auto-negotiating LAN interface(s) and a high-speed ADSL port into a single package. The Prestige is ideal for high-speed Internet browsing and making LAN-to-LAN connections to remote networks. The Prestige is an ADSL router compatible with the ADSL/ADSL2/ADSL2+ standards. Maximum data rates attainable by the Prestige for each standard are shown in the next table.

Table 1 ADSL Standards

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

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

By integrating DSL and NAT, the Prestige provides ease of installation and Internet access.

Models ending in "1", for example P660R-61C, denote a device that works over the analog telephone system, POTS (Plain Old Telephone Service). Models ending in "3" denote a device that works over ISDN (Integrated Synchronous Digital System). Models ending in "7" denote a device that works over T-ISDN (UR-2).

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

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

1.1.1 Features of the Prestige

The following sections describe the features of the Prestige.

High Speed Internet Access

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

Traffic Redirect

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

Universal Plug and Play (UPnP)

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

PPPoE Support (RFC2516)

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

Network Address Translation (NAT)

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

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

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

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

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

Dynamic DNS Support

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

Multiple PVC (Permanent Virtual Circuits) Support

Your Prestige supports up to 8 PVC's.

ADSL Standards

- Full-Rate (ANSI T1.413, Issue 2; G.dmt (G.992.1) with line rate support of up to 8 Mbps downstream and 832 Kbps upstream.
- G.lite (G.992.2) with line rate support of up to 1.5Mbps downstream and 512Kbps upstream.
- Supports Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt (G.992.1); G.lite (G992.2)).
- TCP/IP (Transmission Control Protocol/Internet Protocol) network layer protocol.
- ATM Forum UNI 3.1/4.0 PVC.
- Supports up to 8 PVCs (UBR, CBR, VBR).
- Multiple Protocol over AAL5 (RFC 1483).
- PPP over AAL5 (RFC 2364).
- PPP over Ethernet over AAL5 (RFC 2516).
- RFC 1661.
- PPP over PAP (RFC 1334).
- PPP over CHAP (RFC 1994).

Protocol Support

- DHCP Support

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

- IP Alias

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

- IP Policy Routing (IPPR)

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

- PPP (Point-to-Point Protocol) link layer protocol.
- Transparent bridging for unsupported network layer protocols.
- RIP I/RIP II
- IGMP Proxy

- ICMP support
- ATM QoS support
- MIB II support (RFC 1213)

Networking Compatibility

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

Multiplexing

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

Encapsulation

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

Network Management

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

Other PPPoE Features

- PPPoE idle time out
- PPPoE Dial on Demand

Diagnostics Capabilities

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

- FLASH memory
- ADSL circuitry
- RAM

- LAN port

Packet Filters

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

Ease of Installation

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

Housing

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

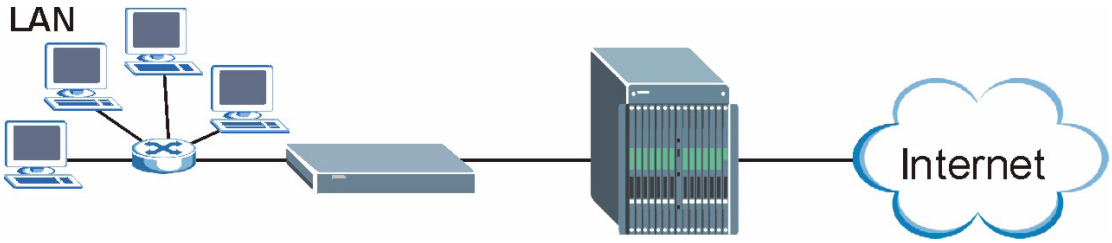
1.1.2 Applications for the Prestige

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

1.1.2.1 Internet Access

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

Figure 1 Prestige Internet Access Application



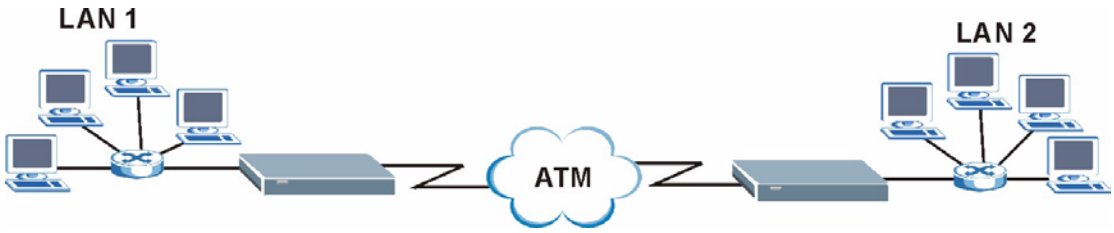
Internet Single User Account

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

1.1.2.2 LAN to LAN Application

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

Figure 2 Prestige LAN-to-LAN Application



1.1.3 Prestige Hardware Installation and Connection

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

CHAPTER 2
Introducing the Web Configurator

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

2.1 Web Configurator Overview

The web configurator is an HTML-based management interface that allows easy Prestige setup and management via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions with JavaScript enabled. Recommended screen resolution is 1024 by 768 pixels.

2.1.1 Accessing the Prestige Web Configurator

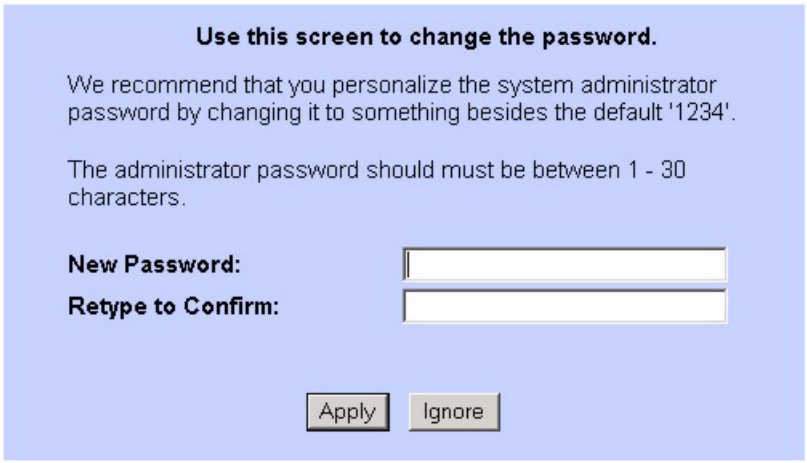
1. Make sure your Prestige hardware is properly connected (refer to the *Quick Start Guide*).
2. Prepare your computer/computer network to connect to the Prestige (refer to the *Quick Start Guide*).
3. Launch your web browser.
4. Type "192.168.1.1" as the URL.
5. An **Enter Network Password** window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

Figure 3 Password Screen

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

Note: If you do not change the password, the following screen appears every time you log in.

Figure 4 Change Password at Login



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

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

2.1.2 Resetting the Prestige

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

2.1.2.1 Using the Reset Button

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

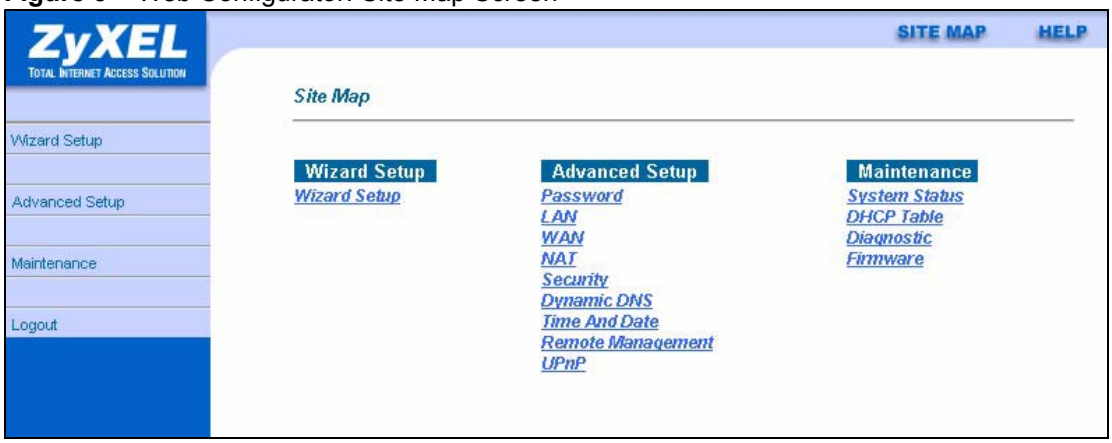
2 Press the **RESET** button for ten seconds or until the **PWR/SYS** LED begins to blink and then release it. When the **PWR/SYS** LED begins to blink, the defaults have been restored and the Prestige restarts.

2.1.3 Navigating the Prestige Web Configurator

The following summarizes how to navigate the web configurator from the **SITE MAP** screen.

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

Figure 5 Web Configurator: Site Map Screen



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

Table 2 Web Configurator Screens Summary

LINK	SUB-LINK	FUNCTION
Wizard Setup	Connection Setup	Use these screens for initial configuration including general setup, ISP parameters for Internet Access and WAN IP/DNS Server/MAC address assignment.
Advanced Setup		
Password		Use this screen to change your password.
LAN		Use this screen to configure LAN DHCP and TCP/IP settings.
WAN	WAN Setup	Use this screen to change the Prestige's WAN remote node settings.
	WAN Backup	Use this screen to configure your traffic redirect properties and WAN backup settings.
NAT	SUA Only	Use this screen to configure servers behind the Prestige.
	Full Feature	Use this screen to configure network address translation mapping rules.
Security		Use this screen to configure Internet security and apply the predefined filter rules.
Dynamic DNS		Use this screen to set up dynamic DNS.
Time and Date		Use this screen to change your Prestige's time and date.

Table 2 Web Configurator Screens Summary (continued)

LINK	SUB-LINK	FUNCTION
Remote Management		Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet/FTP/Web to manage the Prestige.
UPnP		Use this screen to enable UPnP on the Prestige.
Maintenance		
System Status		This screen contains administrative and system-related information.
DHCP Table		This screen displays DHCP (Dynamic Host Configuration Protocol) related information and is READ-ONLY.
Diagnostic	General	These screens display information to help you identify problems with the Prestige general connection.
	DSL Line	These screens display information to help you identify problems with the DSL line.
Firmware		Use this screen to upload firmware to your Prestige
LOGOUT		Click this label to exit the web configurator.

CHAPTER 3
Wizard Setup

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

3.1 Introduction

Use the Wizard Setup screens to configure your system for Internet access with the information (provided by your ISP) that you fill in the *Internet Account Information* table in the *Quick Start Guide*. Your ISP may have already configured some of the fields in the wizard screens for you.

3.1.1 Encapsulation

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

3.1.1.1 ENET ENCAP

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

3.1.1.2 PPP over Ethernet

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

3.1.1.3 PPPoA

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

3.1.1.4 RFC 1483

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

3.1.2 Multiplexing

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

3.1.2.1 VC-based Multiplexing

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

3.1.2.2 LLC-based Multiplexing

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

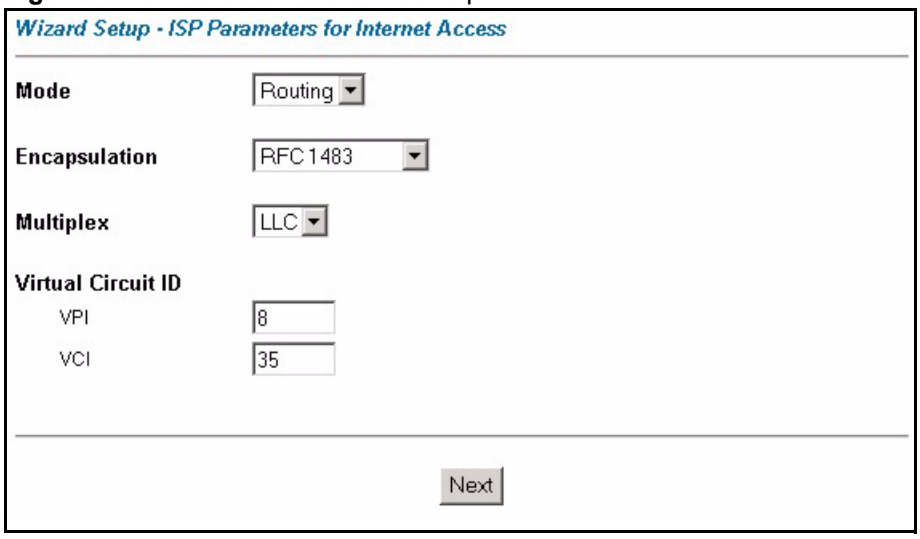
3.1.3 VPI and VCI

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

3.1.4 Internet Access Wizard Setup: First Screen

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

Figure 6 Internet Access Wizard Setup: First Screen



The following table describes the labels in this screen.

Table 3 Internet Access Wizard Setup: First Screen

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

3.2 IP Address and Subnet Mask

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

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

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

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

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

3.2.1 IP Address Assignment

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

3.2.1.1 IP Assignment with PPPoA or PPPoE Encapsulation

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

3.2.1.2 IP Assignment with RFC 1483 Encapsulation

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

3.2.1.3 IP Assignment with ENET ENCAP Encapsulation

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

3.2.1.4 Private IP Addresses

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

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

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

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

3.2.2 Nailed-Up Connection (PPP)

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

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

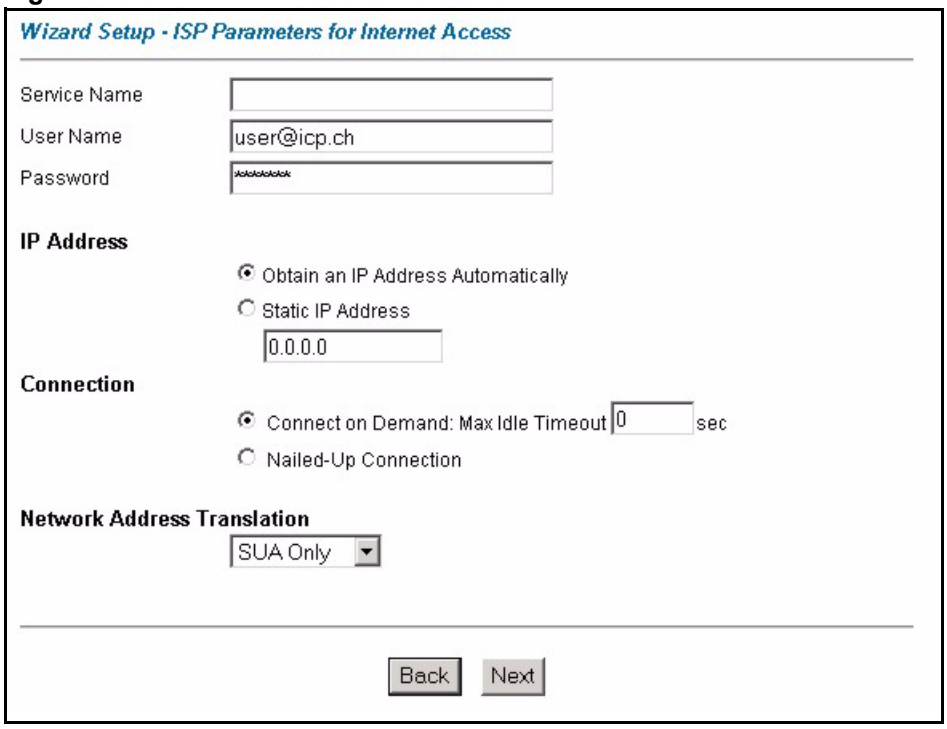
3.2.3 NAT

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

3.2.4 Internet Access Wizard Setup: Second Screen

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

Figure 7 Internet Connection with PPPoE

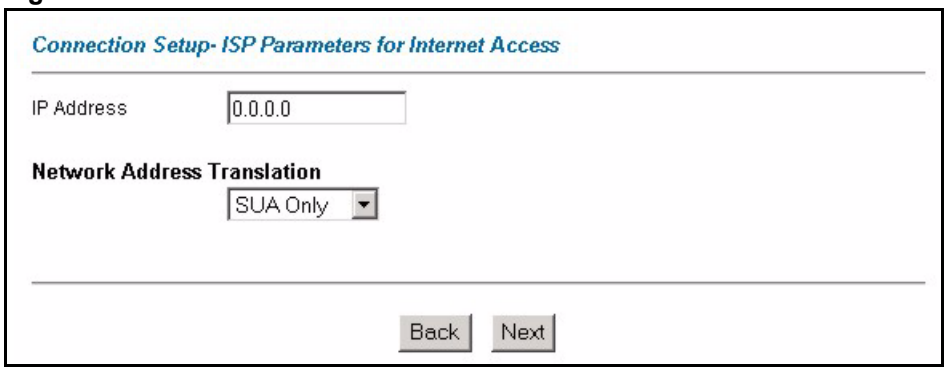


The following table describes the labels in this screen.

Table 4 Internet Connection with PPPoE

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

Figure 8 Internet Connection with RFC 1483

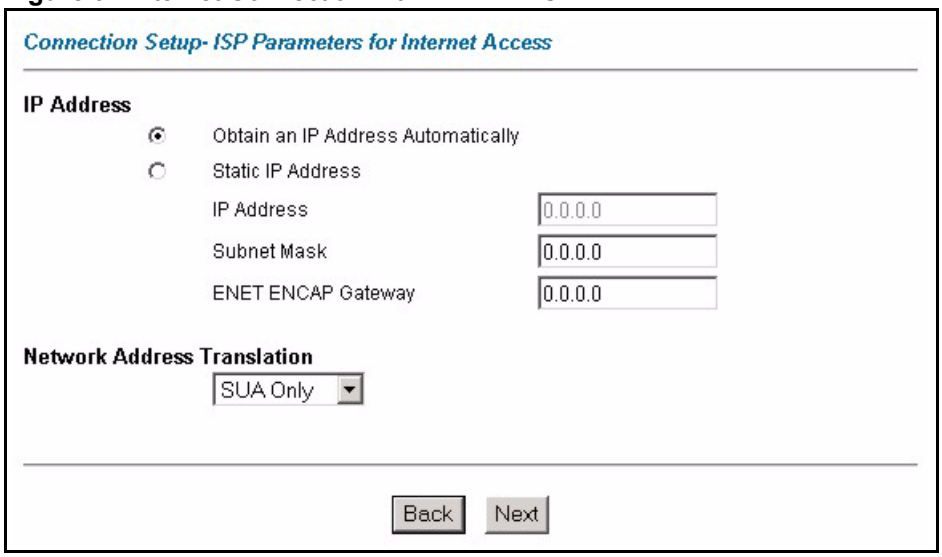


The following table describes the labels in this screen.

Table 5 Internet Connection with RFC 1483

LABEL	DESCRIPTION
IP Address	This field is available if you select **Routing** in the **Mode** field. Type your ISP assigned IP address in this field.
Network Address Translation	Select **None**, **SUA Only** or **Full Feature** from the drop-down list box. Refer to Chapter 7, on page 70 for more details.
Back	Click **Back** to go back to the first wizard screen.
Next	Click **Next** to continue to the next wizard screen.

Figure 9 Internet Connection with ENET ENCAP

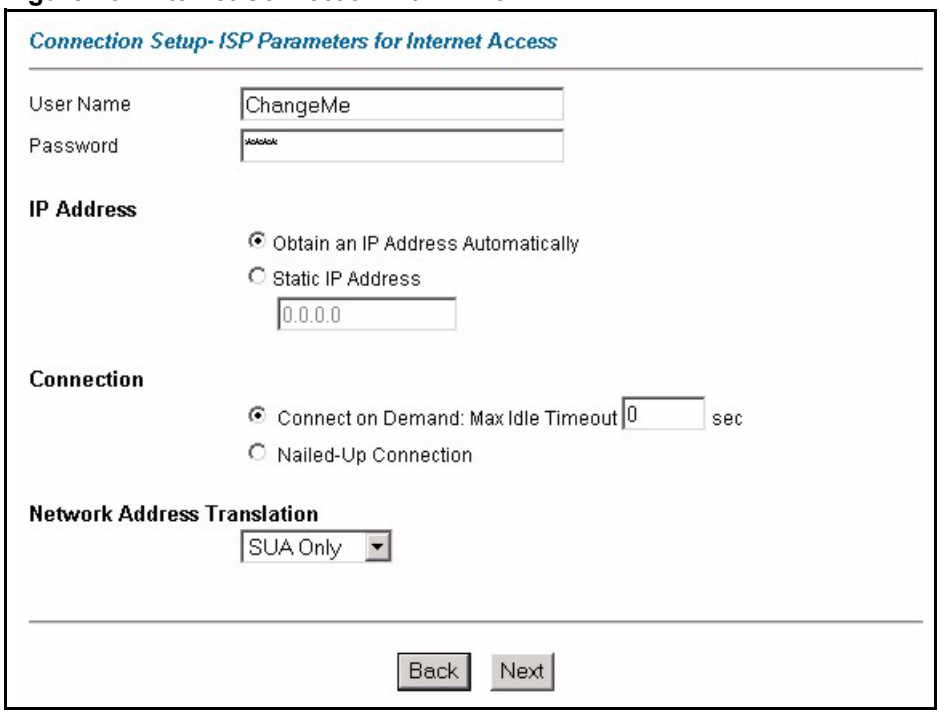


The following table describes the labels in this screen.

Table 6 Internet Connection with ENET ENCAP

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

Figure 10 Internet Connection with PPPoA



The following table describes the labels in this screen.

Table 7 Internet Connection with PPPoA

LABEL	DESCRIPTION
User Name	Enter the login name that your ISP gives you.
Password	Enter the password associated with the user name above.
IP Address	This option is available if you select **Routing** in the **Mode** field. A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. Click **Obtain an IP Address Automatically** if you have a dynamic IP address; otherwise click **Static IP Address** and type your ISP assigned IP address in the IP Address text box below.
Connection	Select **Connect on Demand** when you don't want the connection up all the time and specify an idle time-out (in seconds) in the **Max. Idle Timeout** field. The default setting selects **Connection on Demand** with 0 as the idle time-out, which means the Internet session will not timeout. Select **Nailed-Up Connection** when you want your connection up all the time. The Prestige will try to bring up the connection automatically if it is disconnected. The schedule rule(s) in SMT menu 26 has priority over your **Connection** settings.
Network Address Translation	This option is available if you select **Routing** in the **Mode** field. Select **None**, **SUA Only** or **Full Feature** from the drop-sown list box. Refer to Chapter 7, on page 70 for more details.
Back	Click **Back** to go back to the first wizard screen.
Next	Click **Next** to continue to the next wizard screen.

3.2.5 DHCP Setup

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

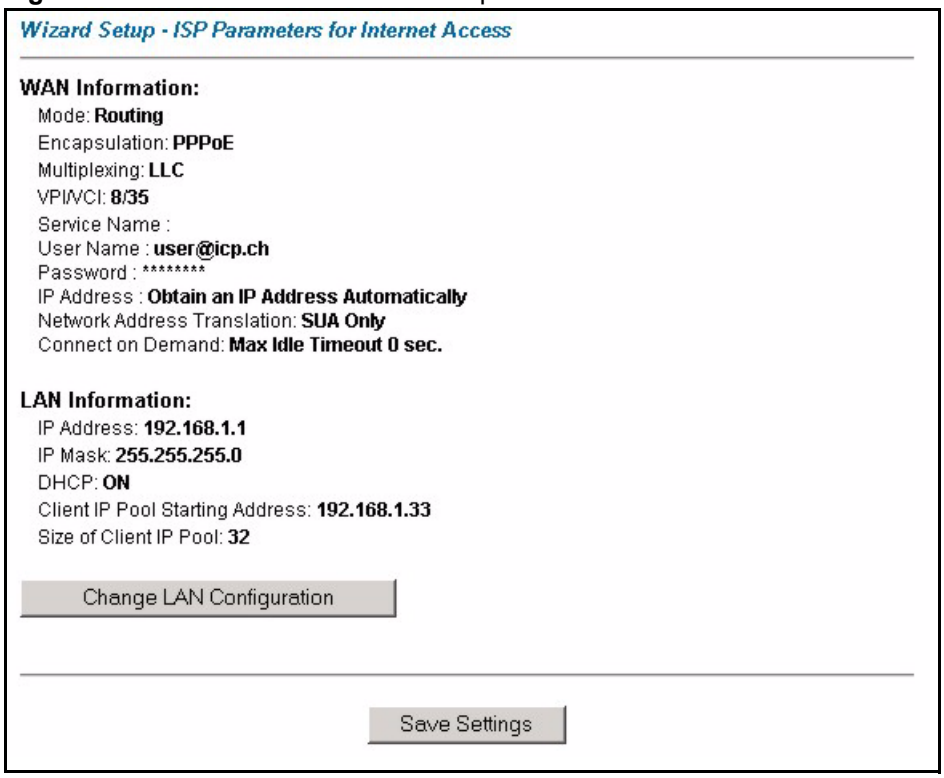
3.2.5.1 IP Pool Setup

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

3.2.6 Internet Access Wizard Setup: Third Screen

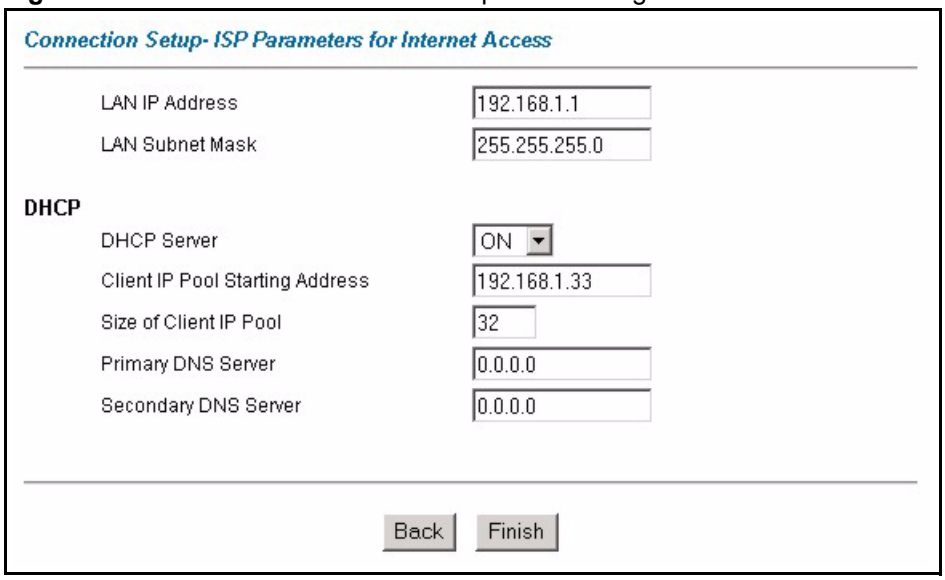
Verify the settings in the screen shown next. To change the LAN information on the Prestige, click **Change LAN Configurations**. Otherwise click **Save Settings** to save the configuration and skip to the section 3.13.

Figure 11 Internet Access Wizard Setup: Third Screen



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

Figure 12 Internet Access Wizard Setup: LAN Configuration



The following table describes the labels in this screen.

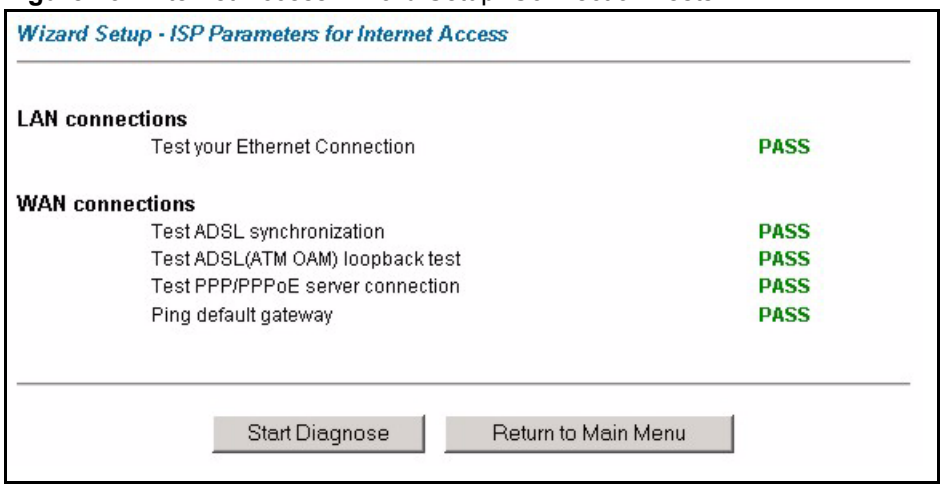
Table 8 Internet Access Wizard Setup: LAN Configuration

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

3.2.7 Internet Access Wizard Setup: Connection Test

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

Figure 13 Internet Access Wizard Setup: Connection Tests



3.2.7.1 Test Your Internet Connection

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

CHAPTER 4
Password Setup

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

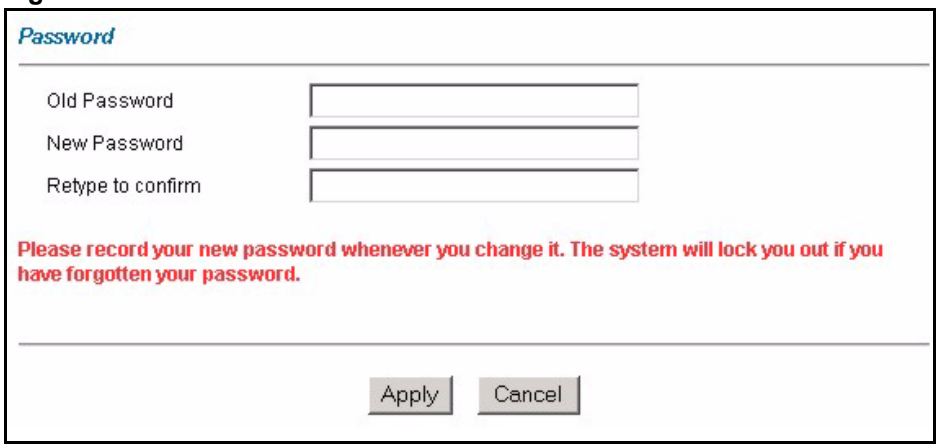
4.1 Password Overview

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

4.1.1 Configuring Password

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

Figure 14 Password



The following table describes the fields in this screen.

Table 9 Password

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

CHAPTER 5
LAN Setup

This chapter describes how to configure LAN settings.

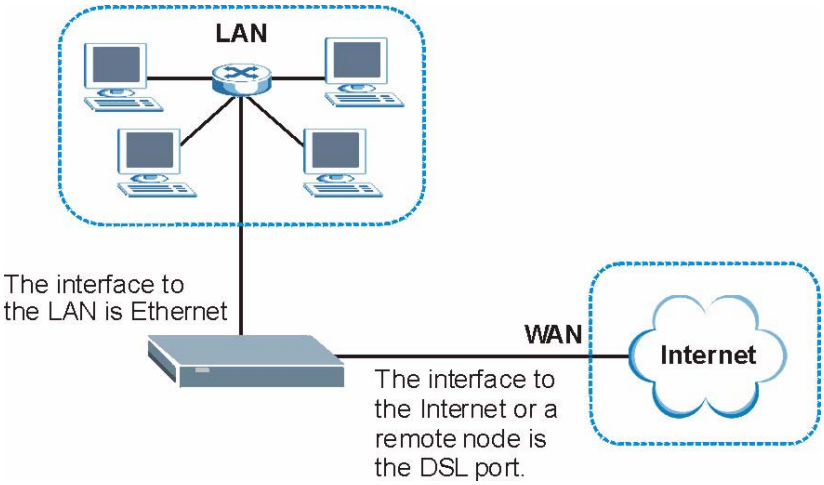
5.1 LAN Overview

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building. The LAN screens can help you configure a LAN DHCP server and manage IP addresses.

5.1.1 LANs, WANs and the Prestige

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

Figure 15 LAN and WAN IP Addresses



5.2 DNS Server Address

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

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

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

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

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

5.3 DNS Server Address Assignment

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

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

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

5.4 LAN TCP/IP

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

5.4.1 Factory LAN Defaults

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

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

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

5.4.2 IP Address and Subnet Mask

Refer to the IP Address and Subnet Mask section in Chapter 3 Wizard Setupfor this information.

5.4.3 RIP Setup

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

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

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

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

5.4.4 Multicast

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

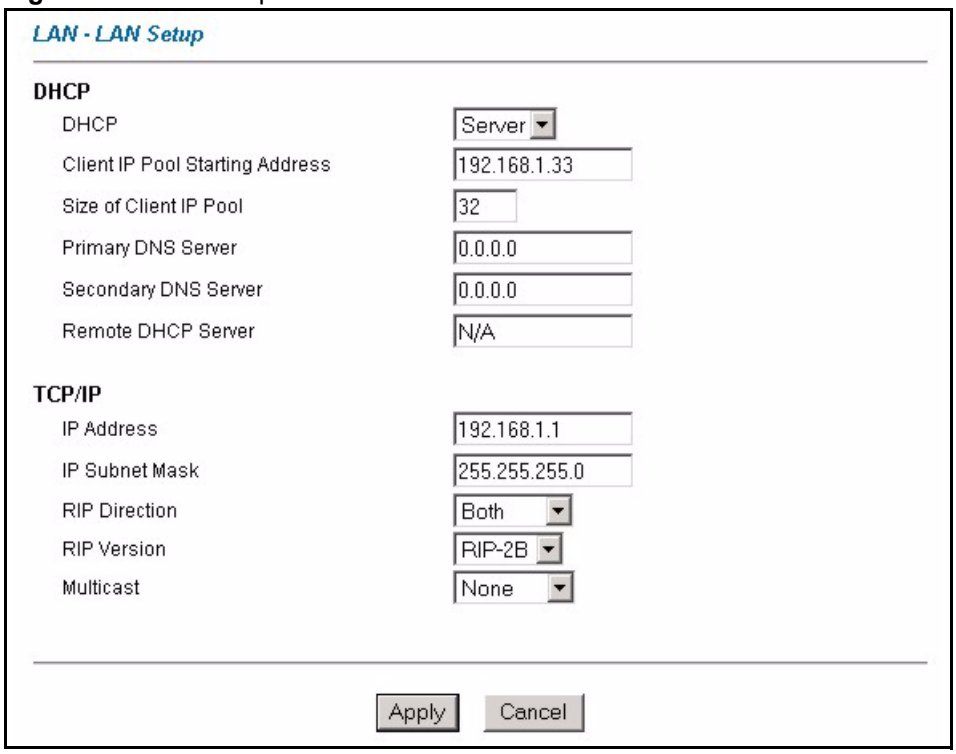
IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group - it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you would like to read more detailed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

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

5.5 Configuring LAN

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

Figure 16 LAN Setup



The following table describes the labels in this screen.

Table 10 LAN Setup

LABEL	DESCRIPTION
DHCP	
DHCP	If set to **Server**, your Prestige can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client. If set to **None**, the DHCP server will be disabled. If set to **Relay**, the Prestige acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the **Remote DHCP Server** field in this case. When DHCP is used, the following items need to be set:
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Size of Client IP Pool	This field specifies the size or count of the IP address pool.
Primary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Secondary DNS Server	As above.
Remote DHCP Server	If **Relay** is selected in the **DHCP** field above then enter the IP address of the actual remote DHCP server here.
TCP/IP	

Table 10 LAN Setup (continued)

LABEL	DESCRIPTION
IP Address	Enter the IP address of your Prestige in dotted decimal notation, for example, 192.168.1.1 (factory default).
IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
RIP Direction	Select the RIP direction from **None**, **Both**, **In Only** and **Out Only**.
RIP Version	Select the RIP version from **RIP-1**, **RIP-2B** and **RIP-2M**.
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a multicast group. The Prestige supports both IGMP version 1 (**IGMP-v1**) and **IGMP-v2**. Select **None** to disable it.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to begin configuring this screen afresh.

CHAPTER 6
WAN Setup

This chapter describes how to configure WAN settings.

6.1 WAN Overview

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

See Chapter 3 Wizard Setupfor more information on the fields in the WAN screens.

6.2 Metric

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

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

- Normal route: designated by the ISP (see the Configuring WAN Setup section)
- Traffic-redirect route (see the Traffic Redirect section)
- WAN-backup route, also called dial-backup (see the Configuring WAN Backup section)

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

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

Note: IP Policy Routing overrides the default routing behavior and takes priority over all of the routes mentioned above (see Chapter 28 IP Policy Routing).

6.3 PPPoE Encapsulation

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

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

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

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

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

6.4 Traffic Shaping

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

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

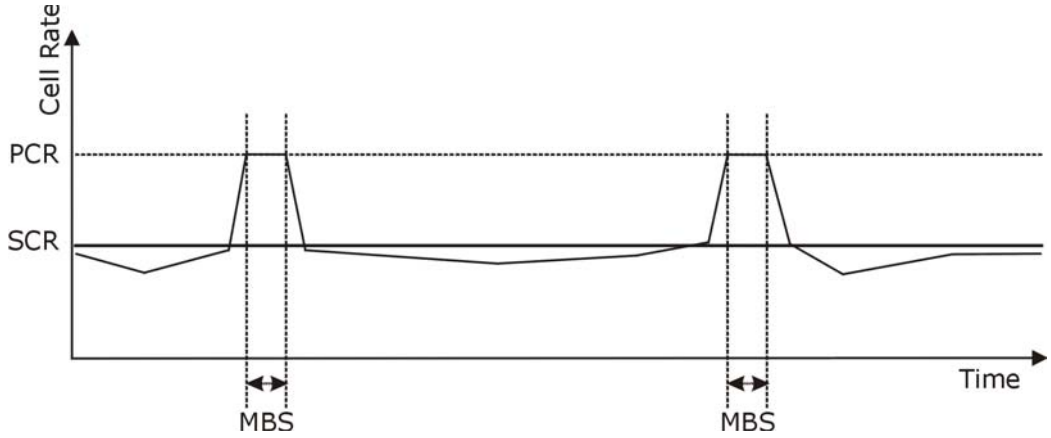
Sustained Cell Rate (SCR) is the mean cell rate of each bursty traffic source. It specifies the maximum average rate at which cells can be sent over the virtual connection. SCR may not be greater than the PCR.

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

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

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

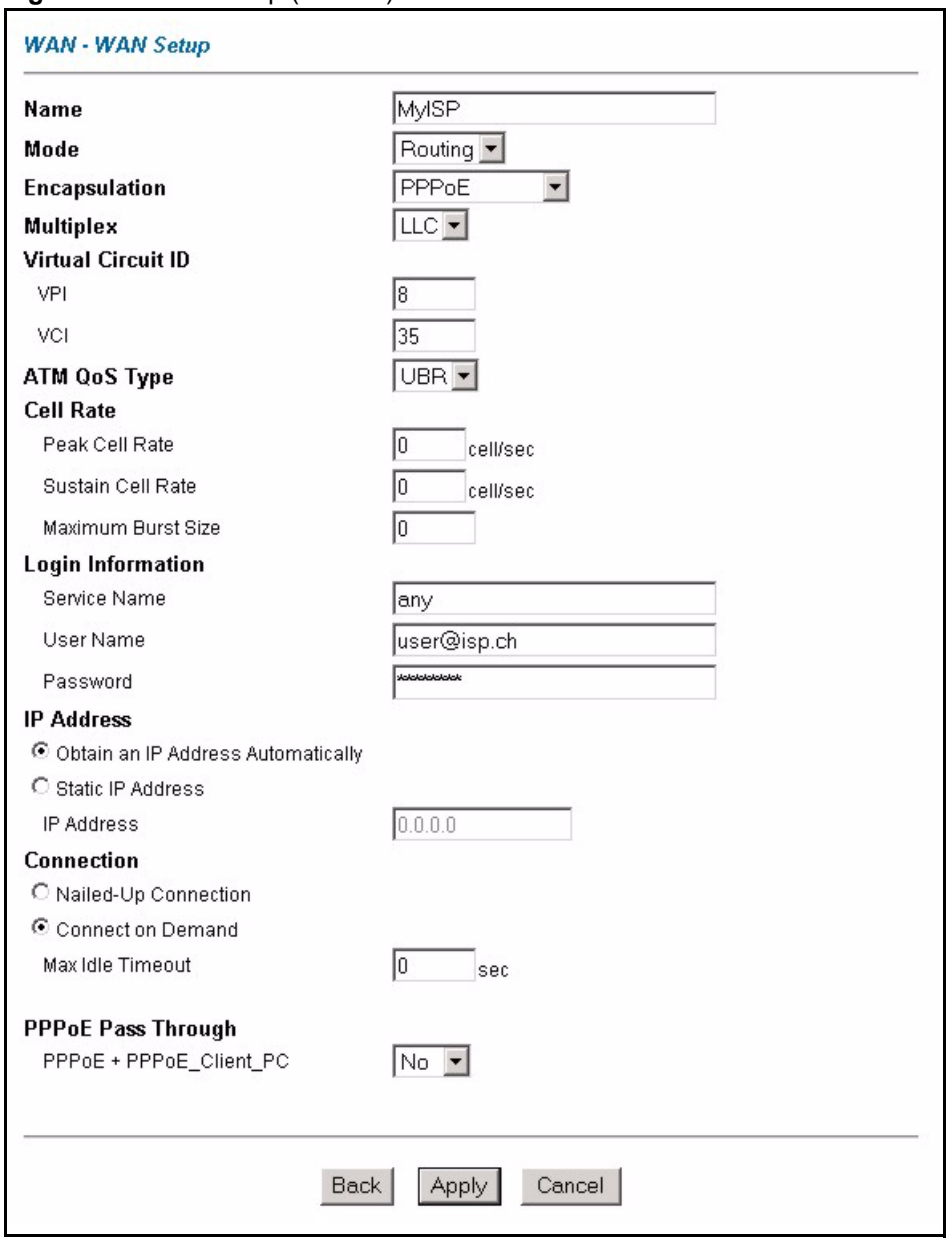
Figure 17 Example of Traffic Shaping



6.5 Configuring WAN Setup

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

Figure 18 WAN Setup (PPPoE)



The following table describes the labels in this screen.

Table 11 WAN Setup

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

Table 11 WAN Setup (continued)

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

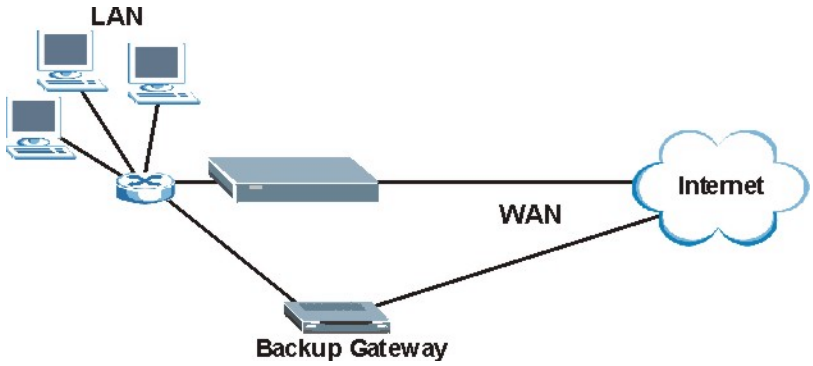
Table 11 WAN Setup (continued)

LABEL	DESCRIPTION
Max Idle Timeout	Specify an idle time-out in the **Max Idle Timeout** field when you select **Connect on Demand**. The default setting is 0, which means the Internet session will not timeout.
PPPoE Passthrough	This field is available when you select **PPPoE** encapsulation.
PPPoE + PPPoE_Client_PC (PPPoE encapsulation only)	In addition to the Prestige's built-in PPPoE client, you can enable PPPoE pass through to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the Prestige. Each host can have a separate account and a public WAN IP address. PPPoE pass through is an alternative to NAT for application where NAT is not appropriate. Disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.
Subnet Mask (ENET ENCAP encapsulation only)	Enter a subnet mask in dotted decimal notation. Refer to Appendix C IP Subnetting in the to calculate a subnet mask If you are implementing subnetting.
ENET ENCAP Gateway (ENET ENCAP encapsulation only)	You must specify a gateway IP address (supplied by your ISP) when you select **ENET ENCAP** in the **Encapsulation** field
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

6.6 Traffic Redirect

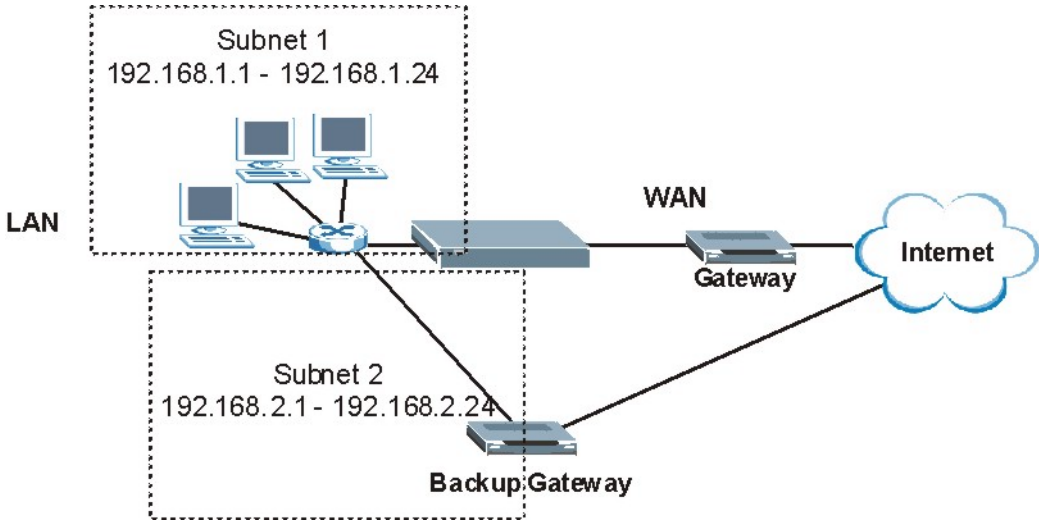
Traffic redirect forwards traffic to a backup gateway when the Prestige cannot connect to the Internet. An example is shown in the figure below.

Figure 19 Traffic Redirect Example



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

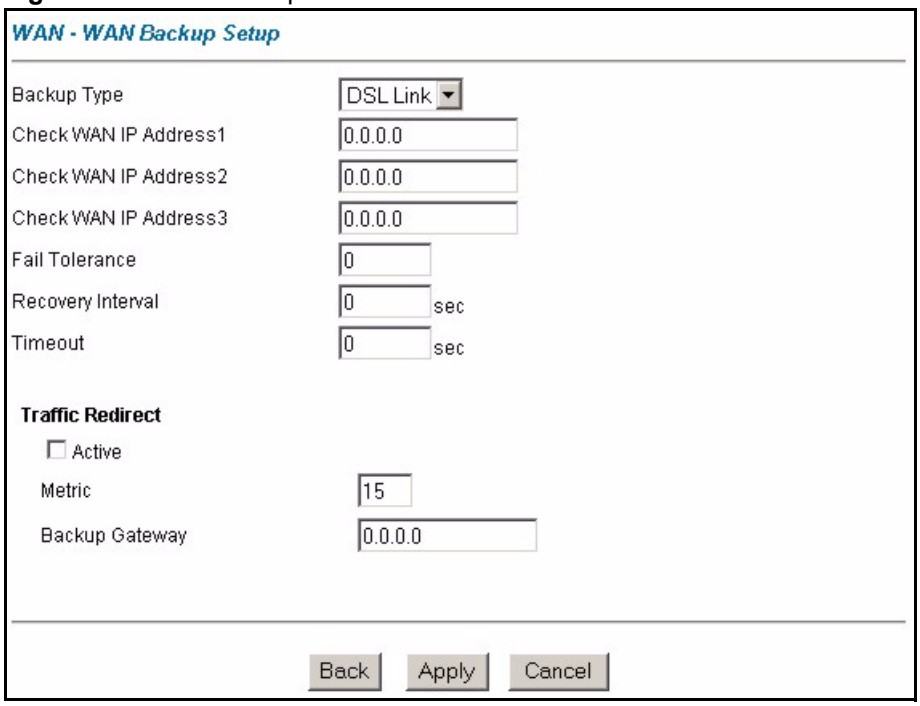
Figure 20 Traffic Redirect LAN Setup



6.7 Configuring WAN Backup

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

Figure 21 WAN Backup



The following table describes the labels in this screen.

Table 12 WAN Backup

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

Table 12 WAN Backup (continued)

LABEL	DESCRIPTION
Traffic Redirect	
Active	Select this check box to have the Prestige use traffic redirect if the normal WAN connection goes down. **Note:** If you activate traffic redirect, you must configure at least one **Check WAN IP Address**.
Metric	This field sets this route's priority among the routes the Prestige uses. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".
Backup Gateway	Type the IP address of your backup gateway in dotted decimal notation. The Prestige automatically forwards traffic to this IP address if the Prestige's Internet connection terminates.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save the changes.
Cancel	Click **Cancel** to begin configuring this screen afresh.

CHAPTER 7
Network Address Translation (NAT) Screens

This chapter discusses how to configure NAT on the Prestige.

7.1 NAT Overview

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

7.1.1 NAT Definitions

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

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

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

Table 13 NAT Definitions

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

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

7.1.2 What NAT Does

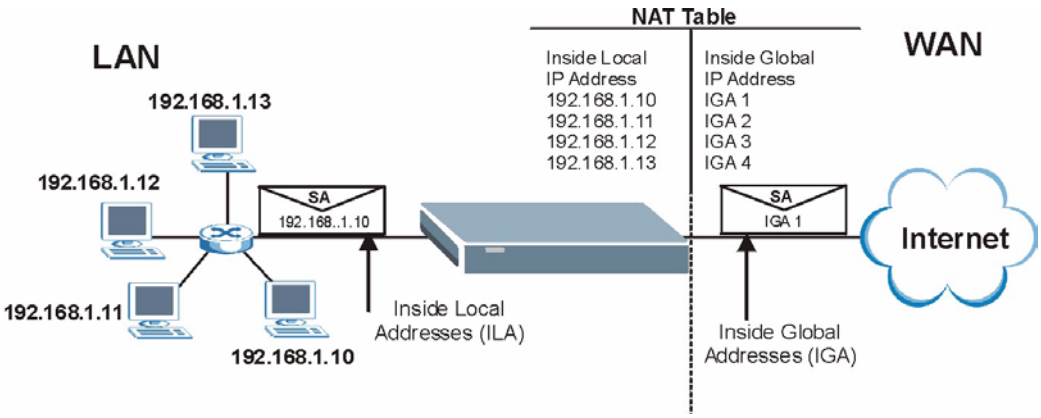
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address)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

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping – see *Table 14*), NAT offers the additional benefit of firewall protection. With no servers defined, your Prestige filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631*, *The IP Network Address Translator (NAT)*.

7.1.3 How NAT Works

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

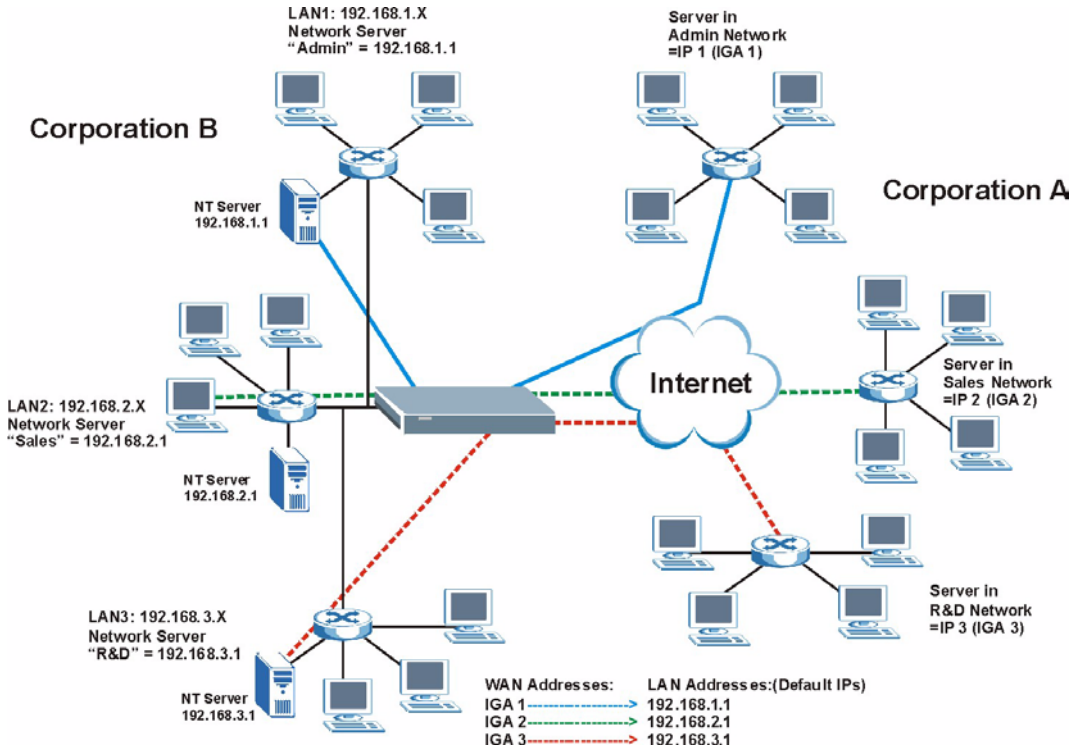
Figure 22 How NAT Works



7.1.4 NAT Application

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

Figure 23 NAT Application With IP Alias



7.1.5 NAT Mapping Types

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

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

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

The following table summarizes these types.

Table 14 NAT Mapping Types

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

7.2 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. The Prestige also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types as outlined in Table 14.

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

7.3 SUA Server

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

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

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

7.3.1 Default Server IP Address

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

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

7.3.2 Port Forwarding: Services and Port Numbers

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

Table 15 Services and Port Numbers

SERVICES	PORT NUMBER
ECHO	7
FTP (File Transfer Protocol)	21

Table 15 Services and Port Numbers (continued)

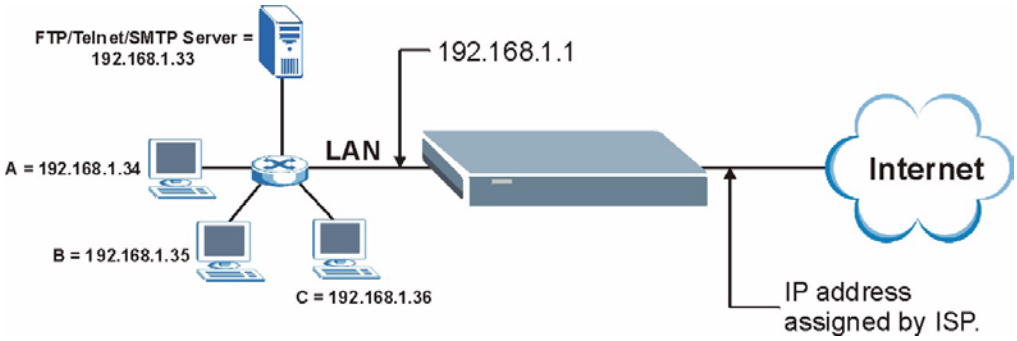
SERVICES	PORT NUMBER
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point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

7.3.3 Configuring Servers Behind SUA (Example)

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

IP address assigned by ISP.

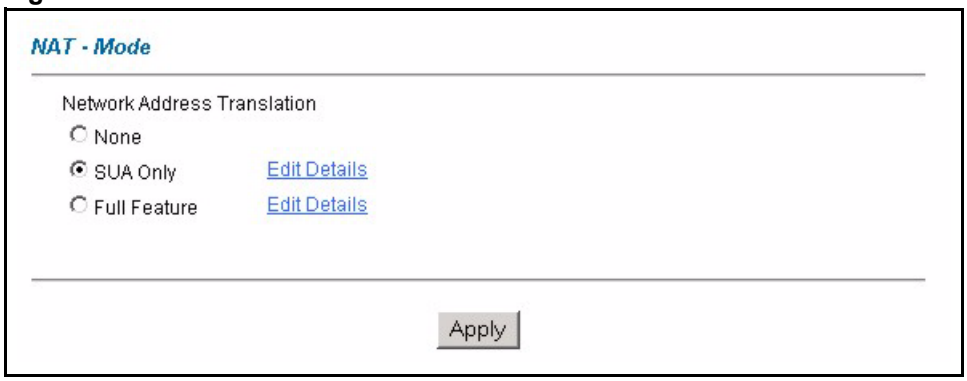
Figure 24 Multiple Servers Behind NAT Example



7.4 Selecting the NAT Mode

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

Figure 25 NAT Mode



The following table describes the labels in this screen.

Table 16 NAT Mode

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

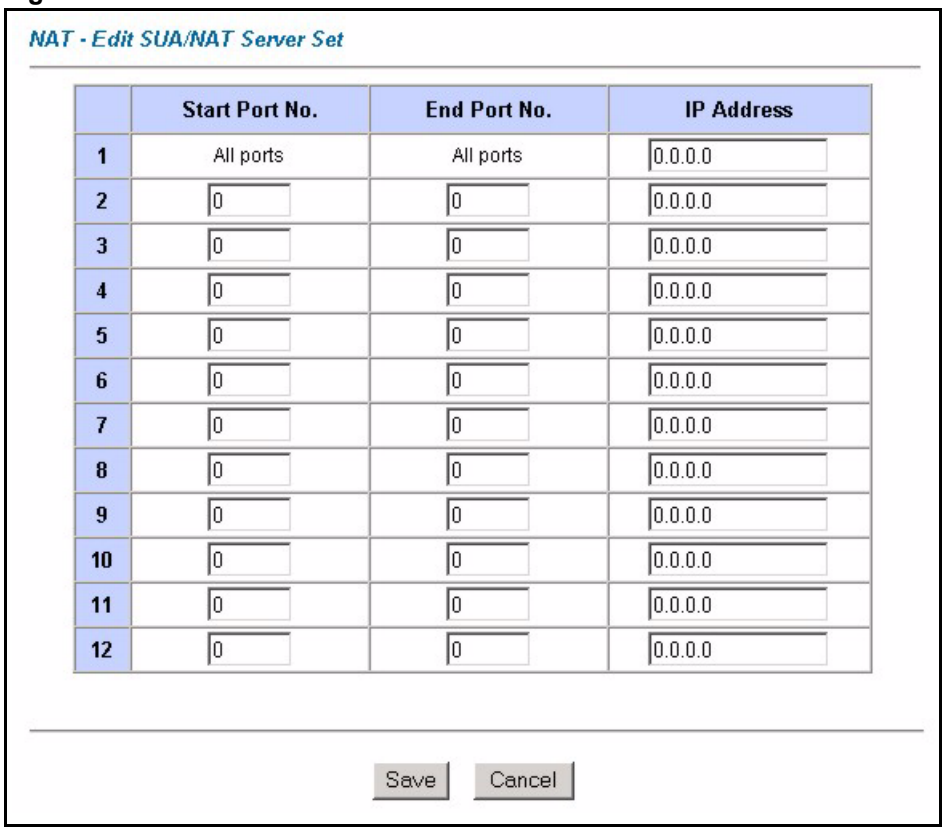
7.5 Configuring SUA Server

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

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

Refer to Table 15 for port numbers commonly used for particular services.

Figure 26 Edit SUA/NAT Server Set



The following table describes the labels in this screen.

Table 17 Edit SUA/NAT Server Set

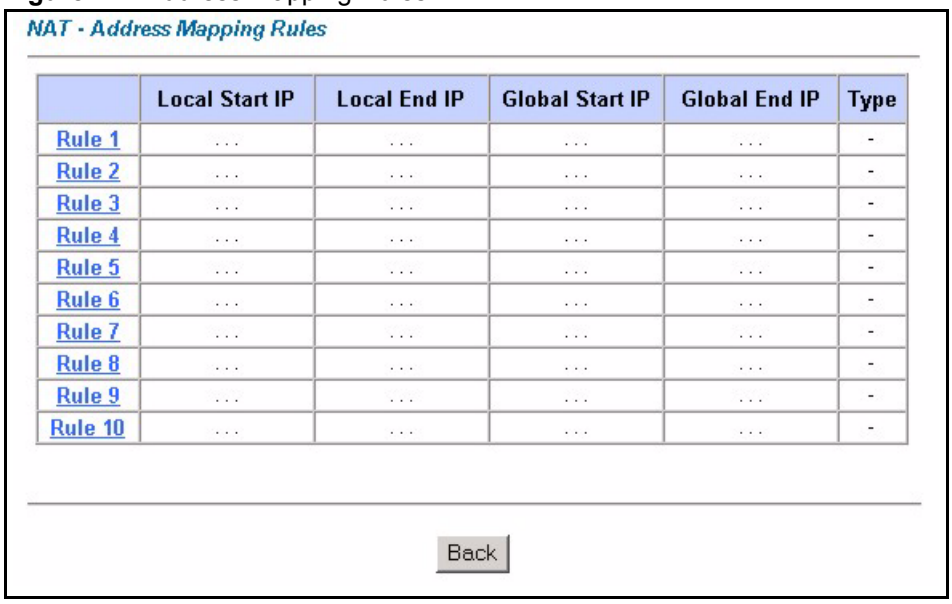
LABEL	DESCRIPTION
Start Port No.	Enter a port number in this field. To forward only one port, enter the port number again in the **End Port No.** field. To forward a series of ports, enter the start port number here and the end port number in the **End Port No.** field.
End Port No.	Enter a port number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

7.6 Configuring Address Mapping

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

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

Figure 27 Address Mapping Rules



The following table describes the labels in this screen.

Table 18 Address Mapping Rules

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

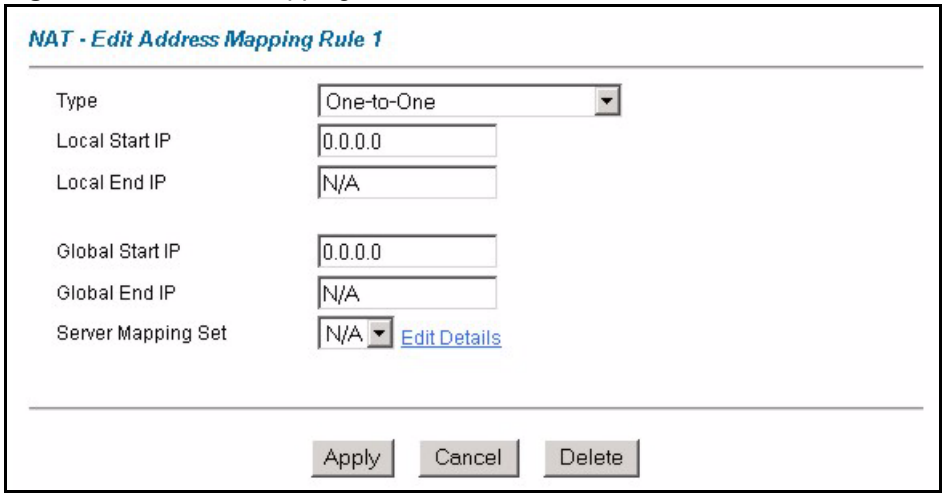
Table 18 Address Mapping Rules (continued)

LABEL	DESCRIPTION
Type	**1-1**: One-to-one mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type. **M-1**: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only. **M-M Ov** (Overload): Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. **MM No** (No Overload): Many-to-Many No Overload mode maps each local IP address to unique global IP addresses. **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Back	Click **Back** to return to the **NAT Mode** screen.

7.7 Editing an Address Mapping Rule

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

Figure 28 Address Mapping Rule Edit



The following table describes the labels in this screen.

Table 19 Address Mapping Rule Edit

LABEL	DESCRIPTION
Type	Choose the port mapping type from one of the following. • **One-to-One**: One-to-One mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-one NAT mapping type. • **Many-to-One**: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only. • **Many-to-Many Overload**: Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. • **Many-to-Many No Overload**: Many-to-Many No Overload mode maps each local IP address to unique global IP addresses. • **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Local Start IP	This is the starting local IP address (ILA). Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end local IP address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the **Local Start IP** address and 255.255.255.255 as the **Local End IP** address. This field is **N/A** for **One-to-One** and **Server** mapping types.
Global Start IP	This is the starting global IP address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP.
Global End IP	This is the ending global IP address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server** mapping types.
Server Mapping Set	Only available when **Type** is set to **Server**. Select a number from the drop-down menu to choose a server set from the **NAT - Address Mapping Rules** screen.
Edit Details	Click this link to go to the **NAT - Edit SUA/NAT Server Set** screen to edit a server set that you have selected in the **Server Mapping Set** field.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to return to the previously saved settings.
Delete	Click **Delete** to exit this screen without saving.

CHAPTER 8
Dynamic DNS Setup

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

8.1 Dynamic DNS

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

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

8.1.1 DYNDNS Wildcard

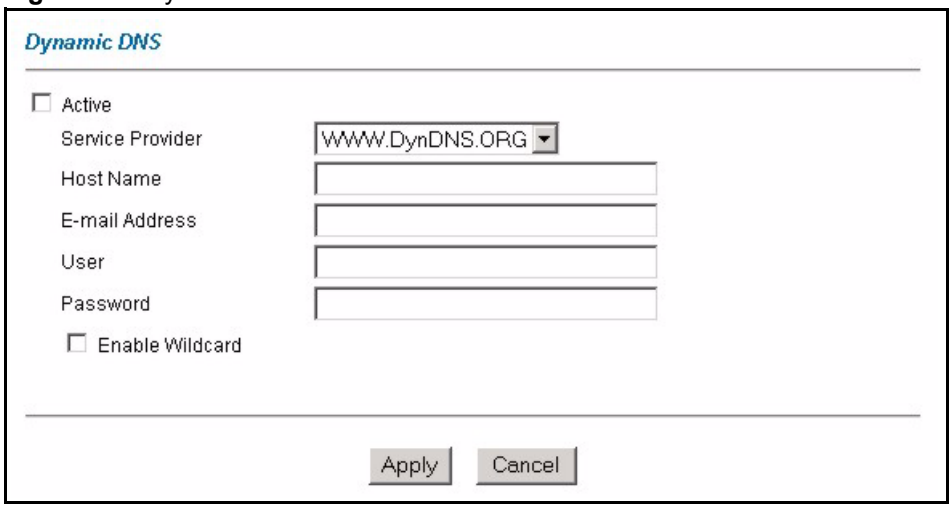
Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

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

8.2 Configuring Dynamic DNS

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

Figure 29 Dynamic DNS



The following table describes the labels in this screen.

Table 20 Dynamic DNS

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

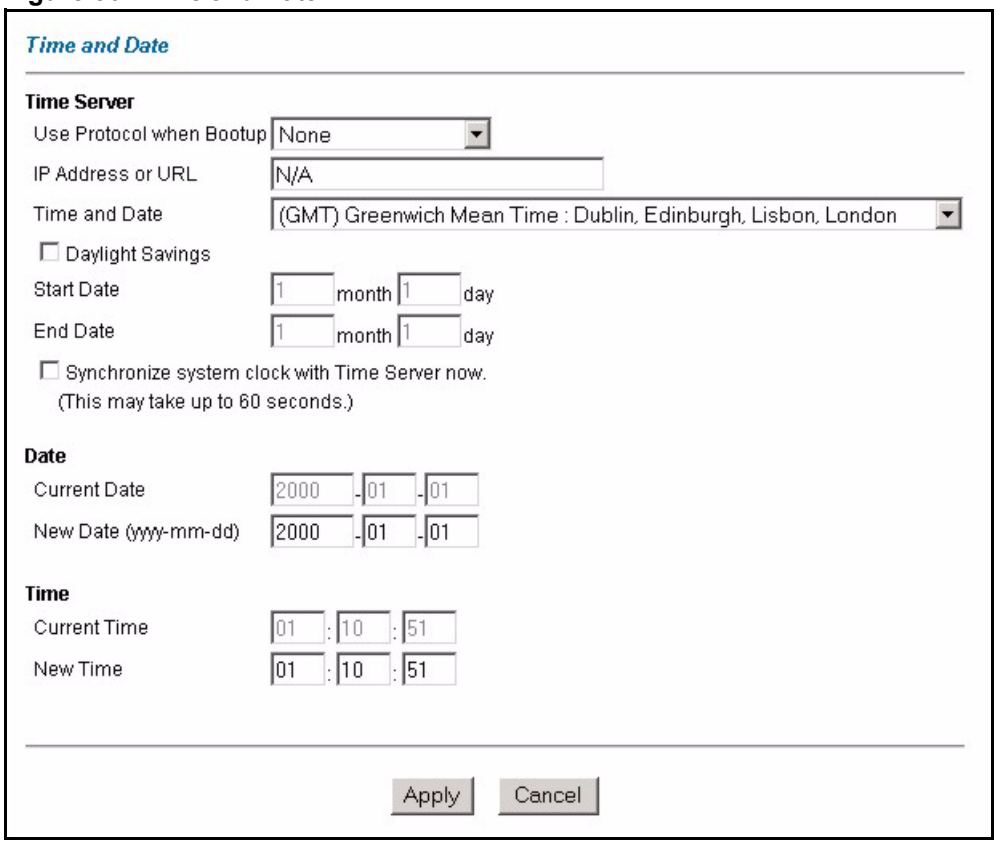
CHAPTER 9
Time and Date

This screen is not available on all models. Use this screen to configure the Prestige's time and date settings.

9.1 Configuring Time and Date

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

Figure 30 Time and Date



The following table describes the labels in this screen.

Table 21 Time and Date

LABEL	DESCRIPTION
Time Server	
Use Protocol when Bootup	Select the time service protocol that your time server sends when you turn on the Prestige. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main difference between them is the format. **Daytime (RFC 867)** format is day/month/year/time zone of the server. **Time (RFC 868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. **NTP (RFC 1305)** is similar to **Time (RFC 868)**. Select **None** to enter the time and date manually.
IP Address or URL	Enter the IP address or URL of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time and Date	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Select this option if you use daylight savings time. Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
Start Date	Enter the month and day that your daylight-savings time starts on if you selected **Daylight Savings**.
End Date	Enter the month and day that your daylight-savings time ends on if you selected **Daylight Savings**.
Synchronize system clock with Time Server now.	Select this option to have your Prestige use the time server (that you configured above) to set its internal system clock. Please wait for up to 60 seconds while the Prestige locates the time server. If the Prestige cannot find the time server, please check the time server protocol and its IP address. If the IP address was entered correctly, try pinging it for example to test the connection.
Date	
Current Date	This field displays the date of your Prestige. Each time you reload this page, the Prestige synchronizes the time with the time server.
New Date (yyyy-mm-dd)	This field displays the last updated date from the time server. When you select **None** in the **Use Protocol when Bootup** field, enter the new date in this field and then click **Apply**.
Time	
Current Time	This field displays the time of your Prestige. Each time you reload this page, the Prestige synchronizes the time with the time server.
New Time	This field displays the last updated time from the time server. When you select **None** in the **Use Protocol when Bootup** field, enter the new time in this field and then click **Apply**.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to begin configuring this screen afresh.

CHAPTER 10
Remote Management Configuration

This chapter provides information on configuring remote management.

10.1 Remote Management Overview

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

You may manage your Prestige from a remote location via:

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

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

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

1. Telnet
2. HTTP

10.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

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

10.1.2 Remote Management and NAT

When NAT is enabled:

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

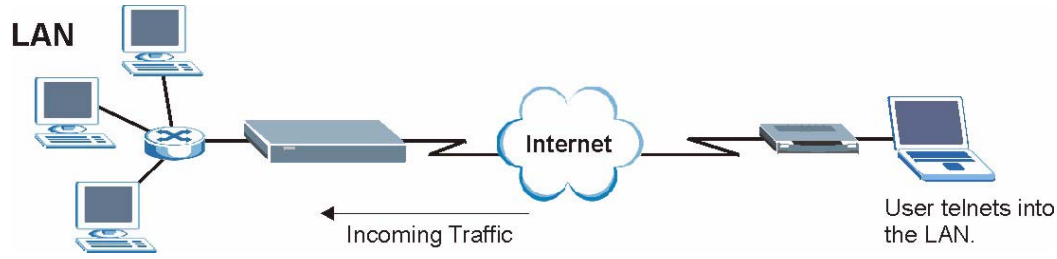
10.1.3 System Timeout

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

10.2 Telnet

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

Figure 31 Telnet Configuration on a TCP/IP Network



10.3 FTP

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

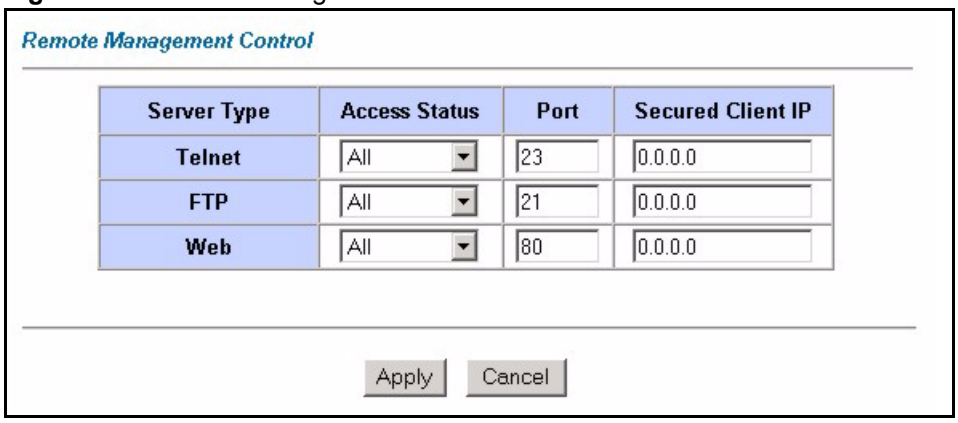
10.4 Web

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

10.5 Configuring Remote Management

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

Figure 32 Remote Management



The following table describes the labels in this screen.

Table 22 Remote Management

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

CHAPTER 11
Universal Plug-and-Play (UPnP)

This chapter introduces the UPnP feature in the web configurator.

11.1 Introducing Universal Plug and Play

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

11.1.1 How do I know if I'm using UPnP?

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

11.1.2 NAT Traversal

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

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

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

See the Network Address Translation (NAT) Screens chapter for further information about NAT.

11.1.3 Cautions with UPnP

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

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

11.2 UPnP and ZyXEL

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

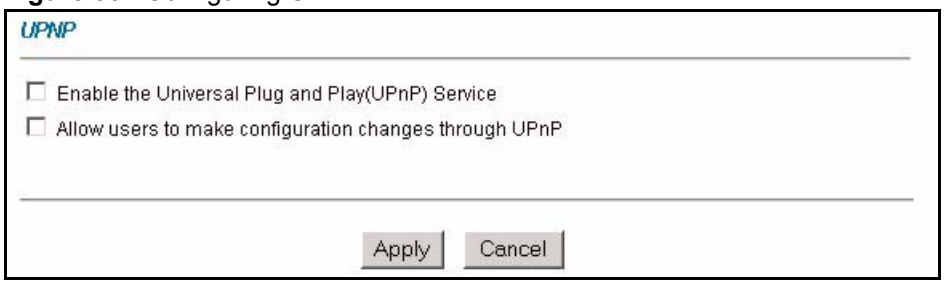
UPnP broadcasts are only allowed on the LAN.

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

11.2.1 Configuring UPnP

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

Figure 33 Configuring UPnP



The following table describes the labels in this screen.

Table 23 Configuring UPnP

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

11.3 Installing UPnP in Windows Example

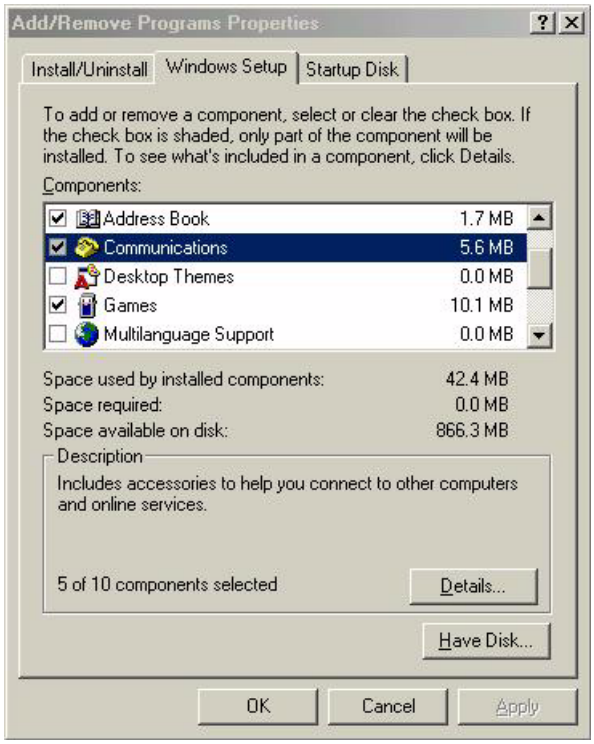
This section shows how to install UPnP in Windows Me and Windows XP.

Installing UPnP in Windows Me

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

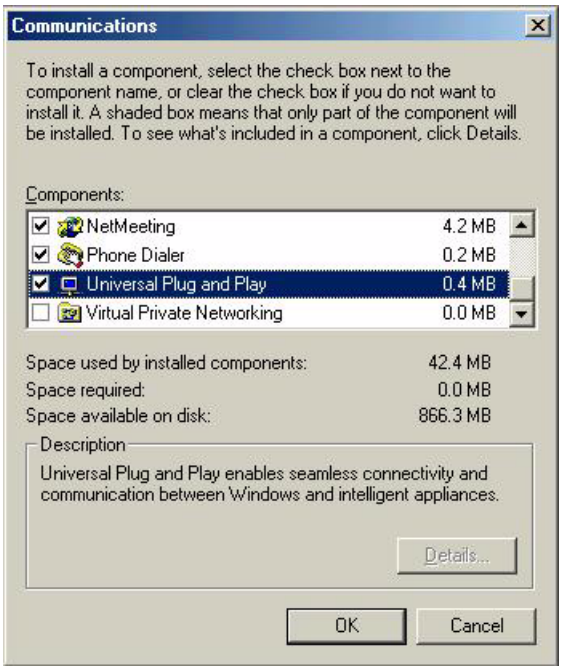
1. Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.
2. Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.

Figure 34 Add/Remove Programs: Windows Setup: Communication



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

Figure 35 Add/Remove Programs: Windows Setup: Communication: Components



4 Click **OK** to go back to the **Add/Remove Programs Properties** window and click **Next**.

5 Restart the computer when prompted.

Installing UPnP in Windows XP

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

1 Click **Start** and **Control Panel**.

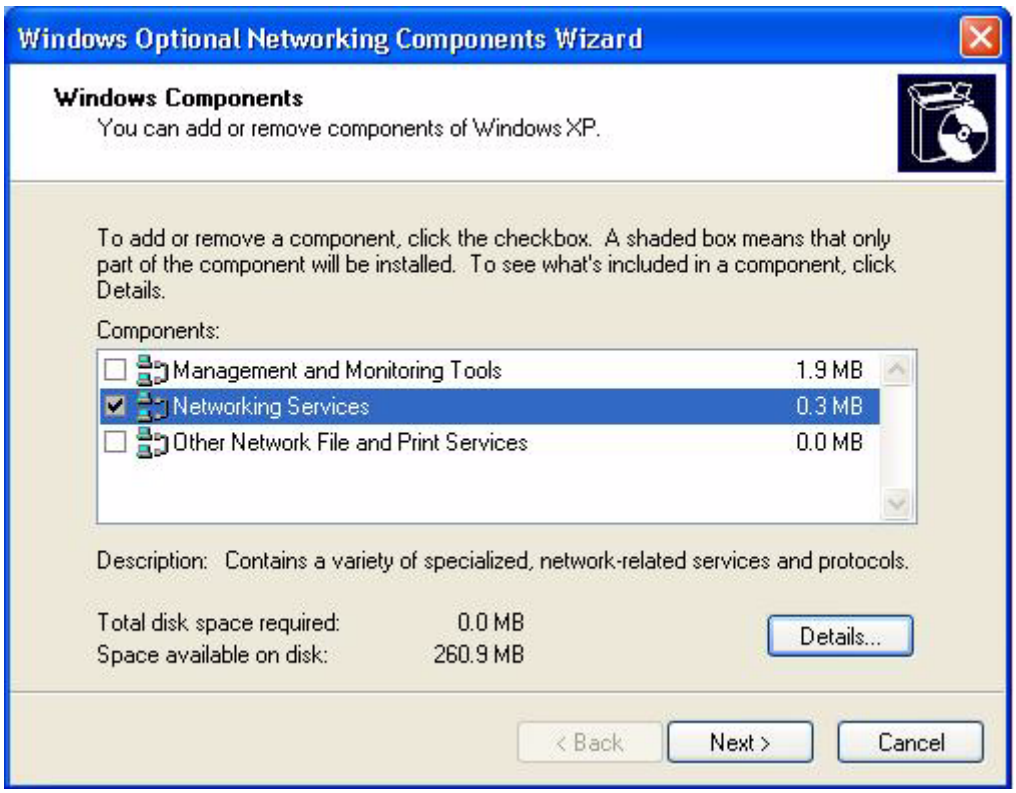
2 Double-click **Network Connections**.

3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components …**.

Figure 36 Network Connections

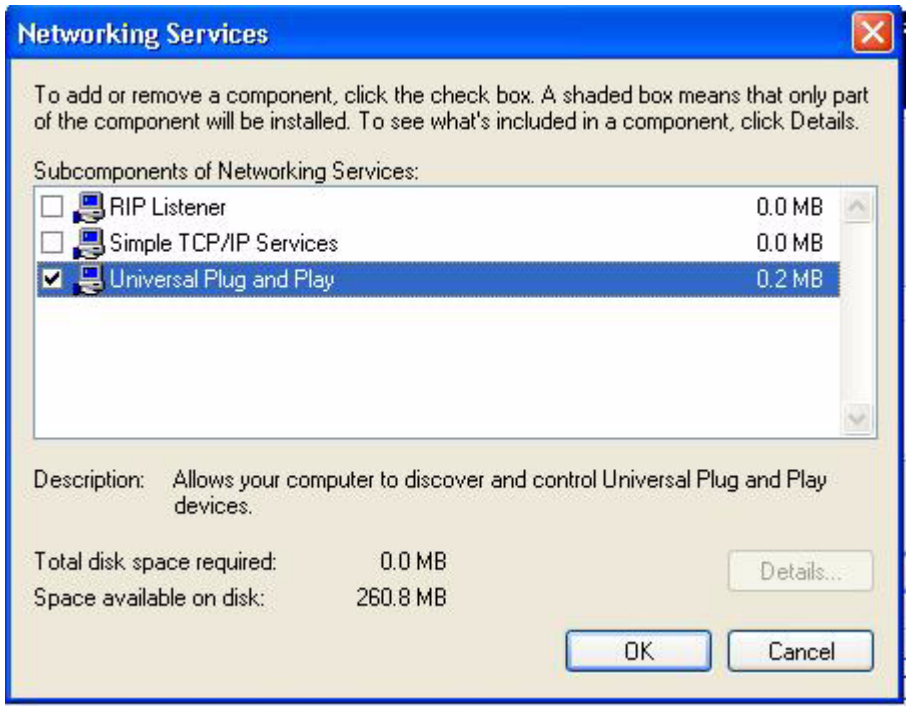
4 The **Windows Optional Networking Components Wizard** window displays. Select **Networking Service** in the **Components** selection box and click **Details**.

Figure 37 Windows Optional Networking Components Wizard



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

Figure 38 Networking Services



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

11.4 Using UPnP in Windows XP Example

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

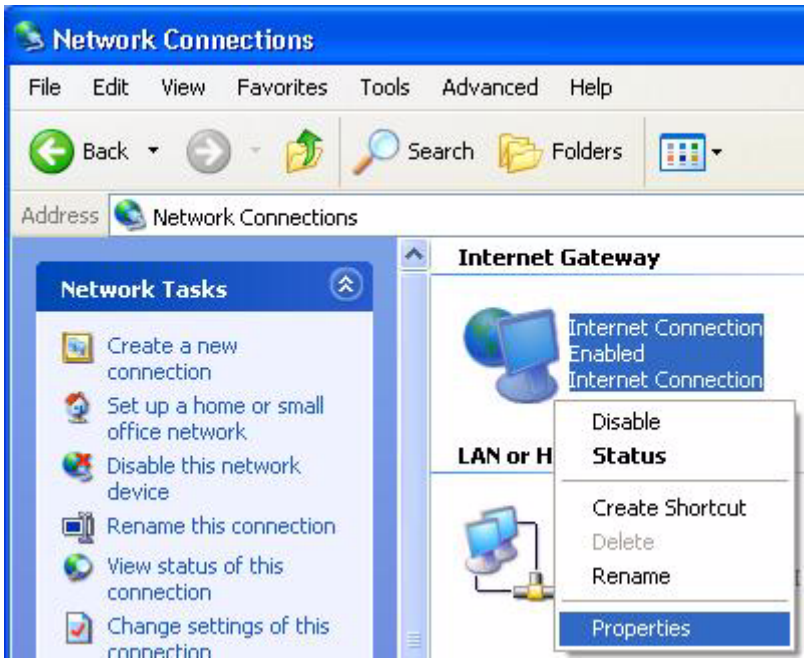
Make sure the computer is connected to a LAN port of the Prestige. Turn on your computer and the Prestige.

Auto-discover Your UPnP-enabled Network Device

1 Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.

2 Right-click the icon and select **Properties**.

Figure 39 Network Connections



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

Figure 40 Internet Connection Properties

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

Figure 41 Internet Connection Properties: Advanced Settings

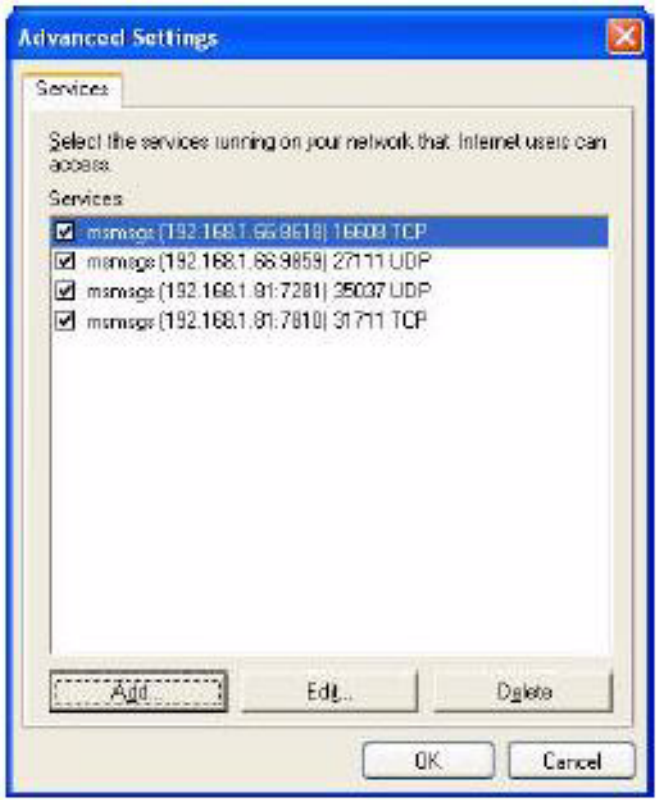
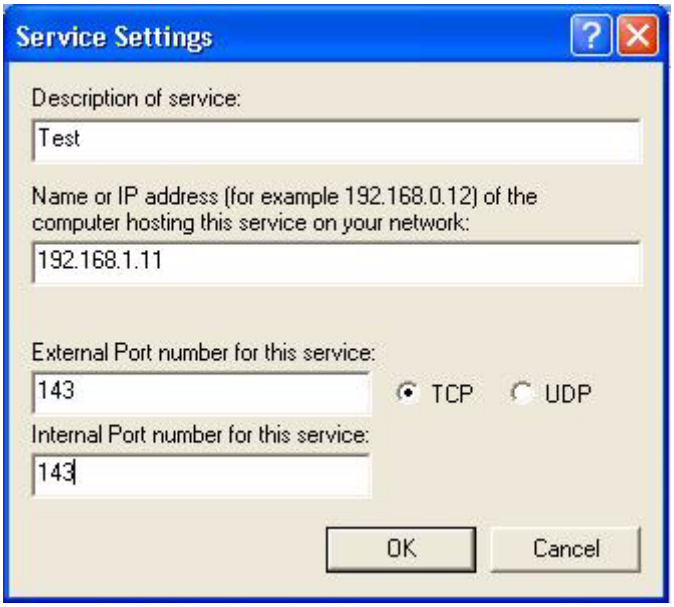


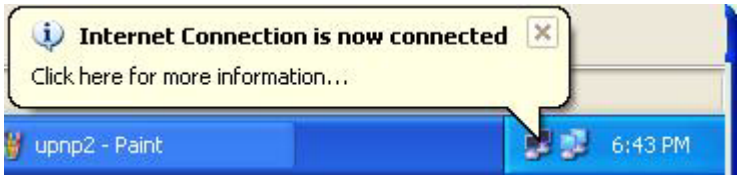
Figure 42 Internet Connection Properties: Advanced Settings: Add



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

6 Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray.

Figure 43 System Tray Icon



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

Figure 44 Internet Connection Status

Web Configurator Easy Access

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

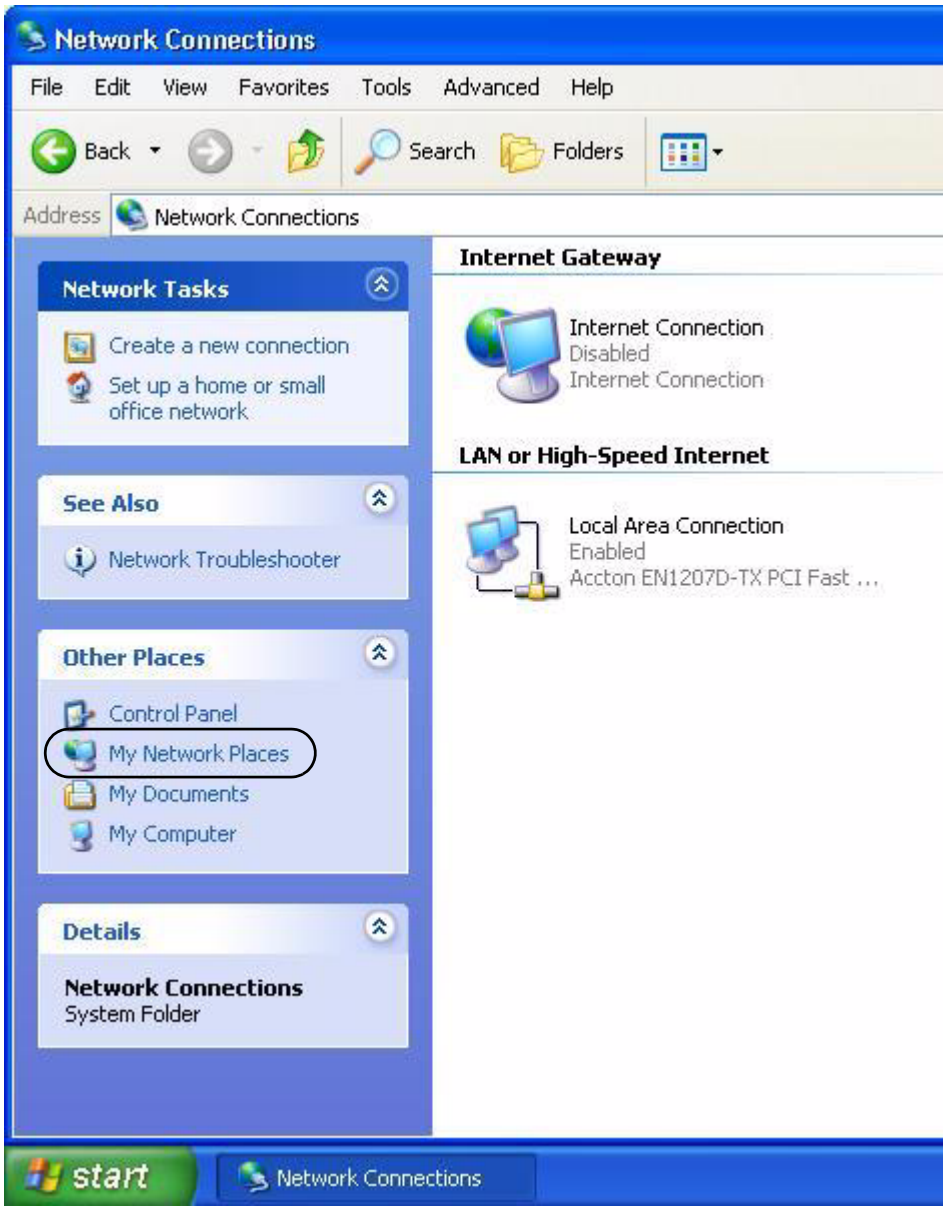
Follow the steps below to access the web configurator.

1 Click **Start** and then **Control Panel**.

2 Double-click **Network Connections**.

3 Select **My Network Places** under **Other Places**.

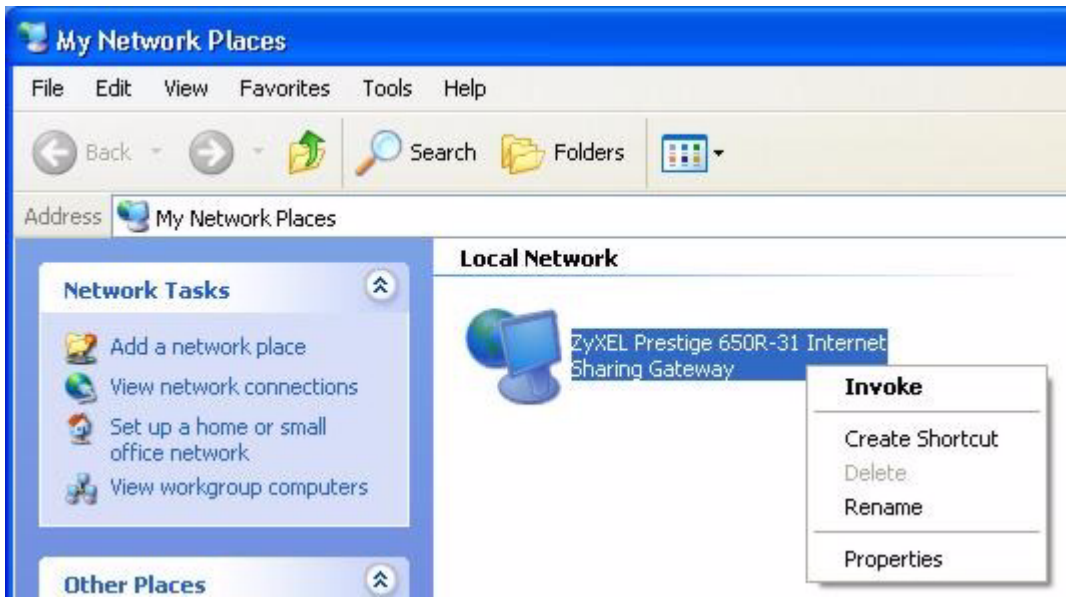
Figure 45 Network Connections



4 An icon with the description for each UPnP-enabled device displays under **Local Network**.

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

Figure 46 Network Connections: My Network Places



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

Figure 47 Network Connections: My Network Places: Properties: Example

CHAPTER 12
Maintenance

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

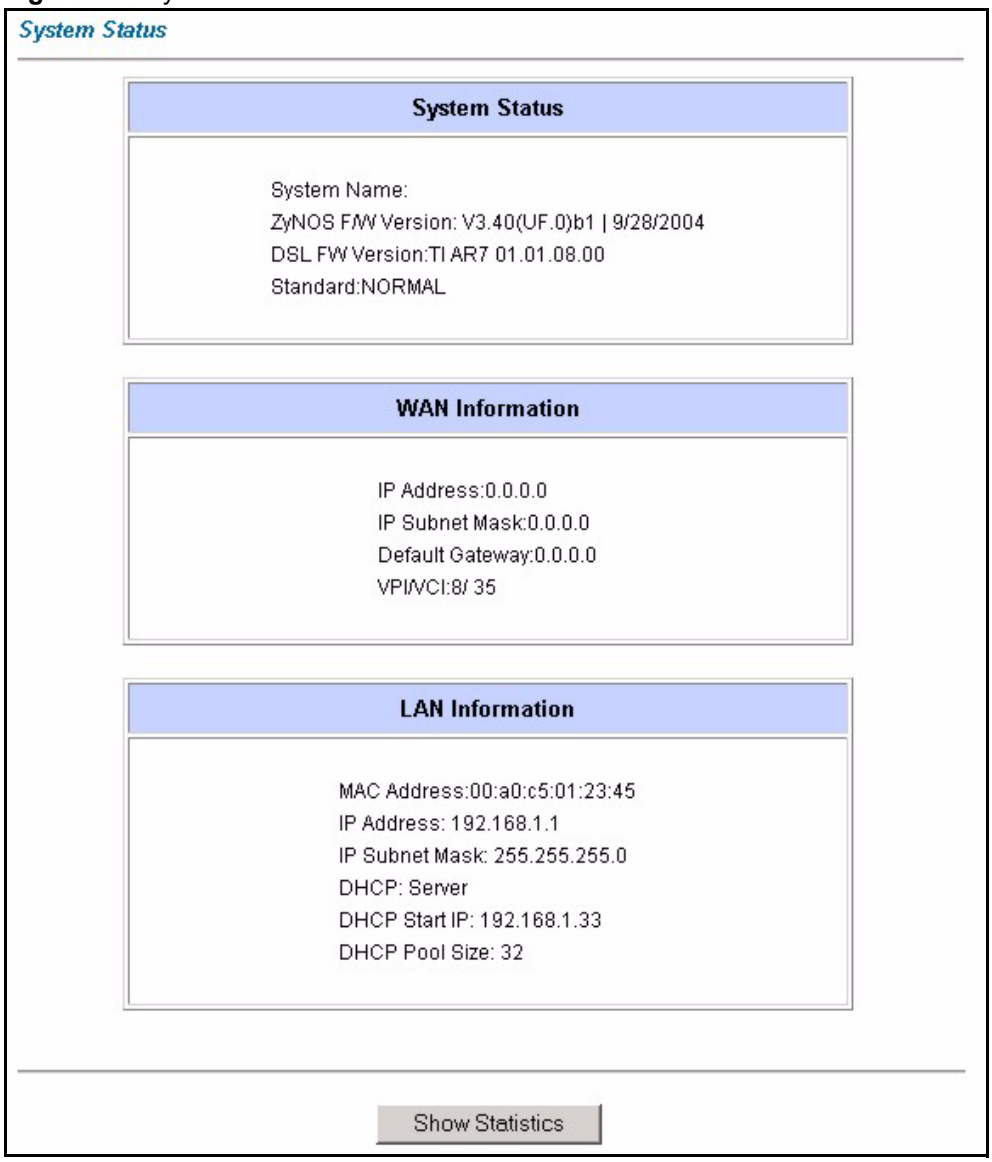
12.1 Maintenance Overview

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

12.2 System Status Screen

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

Figure 48 System Status



The following table describes the fields in this screen.

Table 24 System Status

LABEL	DESCRIPTION
System Status	
System Name	This is the name of your Prestige. It is for identification purposes.
ZyNOS Firmware Version	This is the ZyNOS firmware version and the date the firmware was created. ZyNOS is ZyXEL's proprietary Network Operating System design.
DSL FW Version	This is the DSL firmware version associated with your Prestige.
Standard	This is the standard that your Prestige is using.
WAN Information	
IP Address	This is the WAN port IP address.

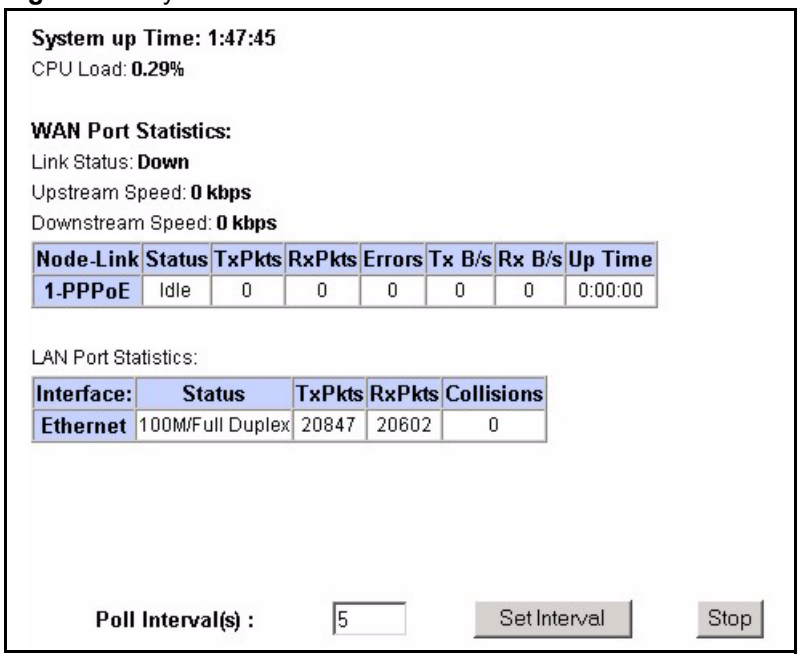
Table 24 System Status (continued)

LABEL	DESCRIPTION
IP Subnet Mask	This is the WAN port IP subnet mask.
Default Gateway	This is the IP address of the default gateway, if applicable.
VPI/VCI	This is the Virtual Path Identifier and Virtual Channel Identifier that you entered in the first Wizard screen.
LAN Information	
MAC Address	This is the MAC (Media Access Control) or Ethernet address unique to your Prestige.
IP Address	This is the LAN port IP address.
IP Subnet Mask	This is the LAN port IP subnet mask.
DHCP	This is the WAN port DHCP role - **Server**, **Relay** (not all Prestige models) or **None**.
DHCP Start IP	This is the first of the contiguous addresses in the IP address pool.
DHCP Pool Size	This is the number of IP addresses in the IP address pool.
Show Statistics	Click **Show Statistics** to see the performance statistics such as number of packets sent and number of packets received for each port.

12.2.1 System Statistics

Click **Show Statistics** in the **System Status** screen to open the following screen. Read-only information here includes port status and packet specific statistics. Also provided are "system up time" and "poll interval(s)". The **Poll Interval(s)** field is configurable.

Figure 49 System Status: Show Statistics



The following table describes the labels in this screen.

Table 25 System Status: Show Statistics

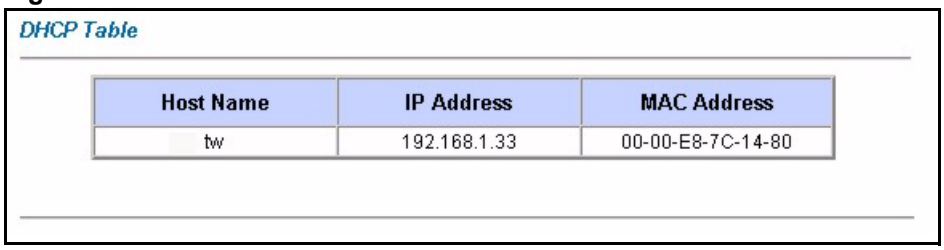
LABEL	DESCRIPTION
System up Time	This is the elapsed time the system has been up.
CPU Load	This field specifies the percentage of CPU utilization.
LAN or WAN Port Statistics	This is the WAN or LAN port.
Link Status	This is the status of your WAN link.
Upstream Speed	This is the upstream speed of your Prestige.
Downstream Speed	This is the downstream speed of your Prestige.
Node-Link	This field displays the remote node index number and link type. Link types are PPPoA, ENET, RFC 1483 and PPPoE.
Interface	This field displays the type of port.
Status	For the WAN port, this displays the port speed and duplex setting if you're using Ethernet encapsulation and **Down** (line is down), **Idle** (line (ppp) idle), **Dial** (starting to trigger a call) and **Drop** (dropping a call) if you're using PPPoE encapsulation. For a LAN port, this shows the port speed and duplex setting.
TxPkts	This field displays the number of packets transmitted on this port.
RxPkts	This field displays the number of packets received on this port.
Errors	This field displays the number of error packets on this port.
Tx B/s	This field displays the number of bytes transmitted in the last second.
Rx B/s	This field displays the number of bytes received in the last second.
Up Time	This field displays the elapsed time this port has been up.
Collisions	This is the number of collisions on this port.
Poll Interval(s)	Type the time interval for the browser to refresh system statistics.
Set Interval	Click this button to apply the new poll interval you entered in the **Poll Interval** field above.
Stop	Click this button to halt the refreshing of the system statistics.

12.3 DHCP Table Screen

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the Prestige as a DHCP server or disable it. When configured as a server, the Prestige provides the TCP/IP configuration for the clients. If set to **None**, DHCP service will be disabled and you must have another DHCP server on your LAN, or else the computer must be manually configured.

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

Figure 50 DHCP Table



The following table describes the fields in this screen.

Table 26 DHCP Table

LABEL	DESCRIPTION
Host Name	This is the name of the host computer.
IP Address	This field displays the IP address relative to the **Host Name** field.
MAC Address	This field displays the MAC (Media Access Control) address of the computer with the displayed host name. Every Ethernet device has a unique MAC address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

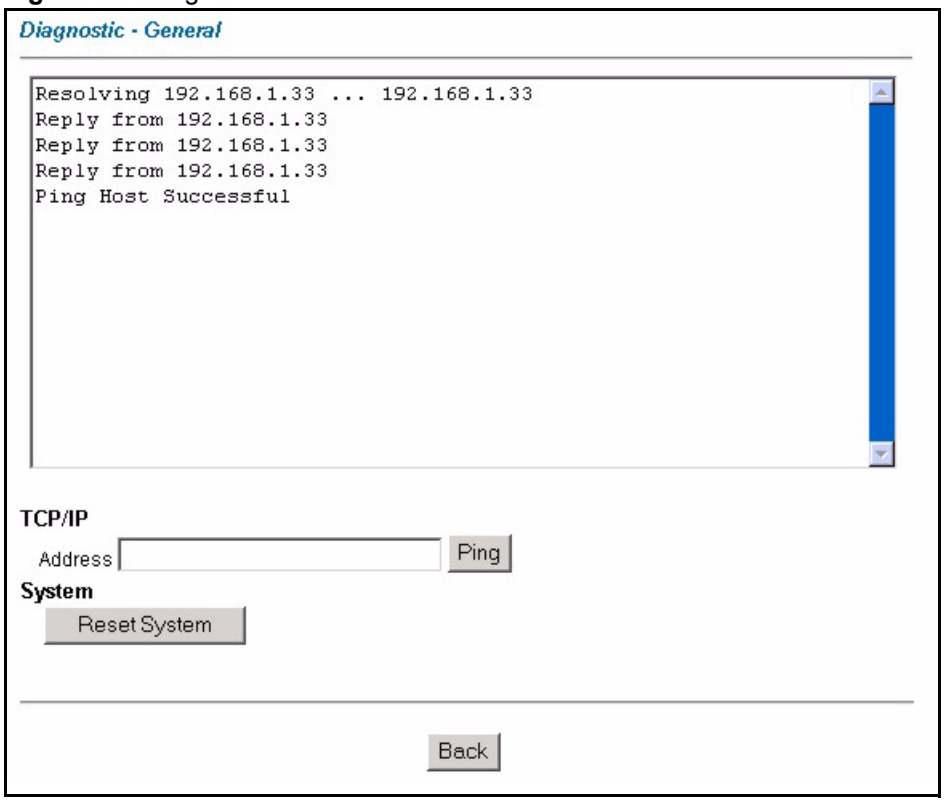
12.4 Diagnostic Screens

These read-only screens display information to help you identify problems with the Prestige.

12.4.1 Diagnostic General Screen

Click **Diagnostic** and then **General** to open the screen shown next.

Figure 51 Diagnostic: General



The following table describes the labels in this screen.

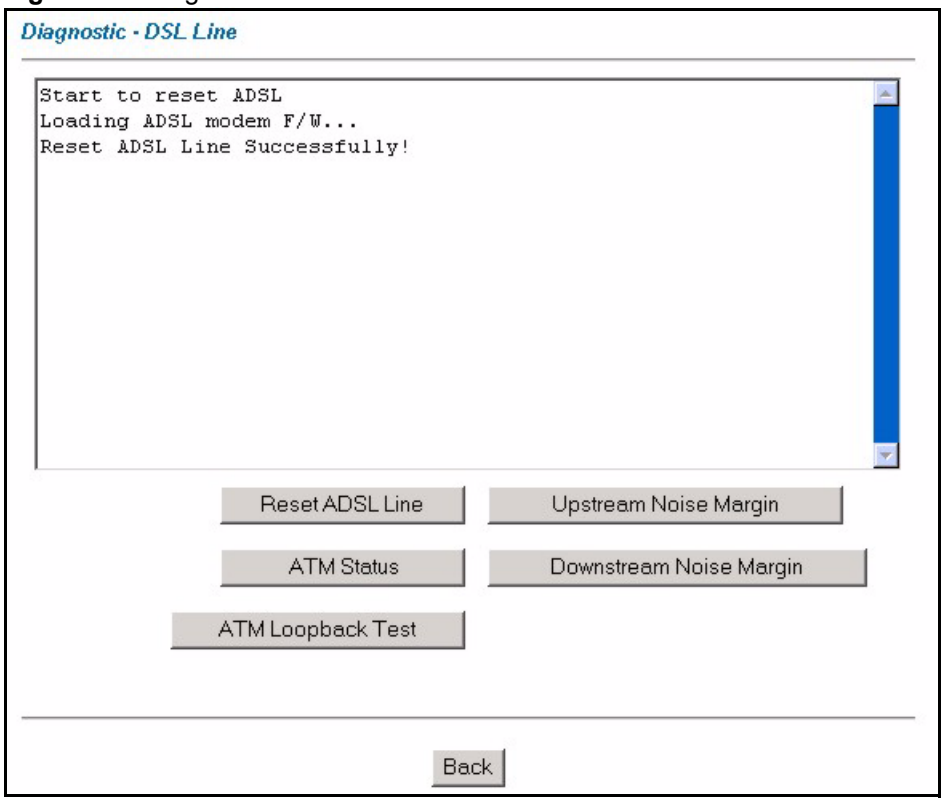
Table 27 Diagnostic: General

LABEL	DESCRIPTION
TCP/IP Address	Type the IP address of a computer that you want to ping in order to test a connection.
Ping	Click this button to ping the IP address that you entered.
Reset System	Click this button to reboot the Prestige. A warning dialog box is then displayed asking you if you're sure you want to reboot the system. Click **OK** to proceed.
Back	Click this button to go back to the main **Diagnostic** screen.

12.4.2 Diagnostic DSL Line Screen

Click **Diagnostic** and then **DSL Line** to open the screen shown next.

Figure 52 Diagnostic: DSL Line



The following table describes the labels in this screen.

Table 28 Diagnostic: DSL Line

LABEL	DESCRIPTION
Reset ADSL Line	Click this button to reinitialize the ADSL line. The large text box above then displays the progress and results of this operation, for example: "Start to reset ADSL Loading ADSL modem F/W... Reset ADSL Line Successfully!"
ATM Status	Click this button to view ATM status.
ATM Loopback Test	Click this button to start the ATM loopback test. Make sure you have configured at least one PVC with proper VPIs/VCIs before you begin this test. The Prestige sends an OAM F5 packet to the DSLAM/ATM switch and then returns it (loops it back) to the Prestige. The ATM loopback test is useful for troubleshooting problems with the DSLAM and ATM network.
Upstream Noise Margin	Click this button to display the upstream noise margin.
Downstream Noise Margin	Click this button to display the downstream noise margin.
Back	Click this button to go back to the main **Diagnostic** screen.

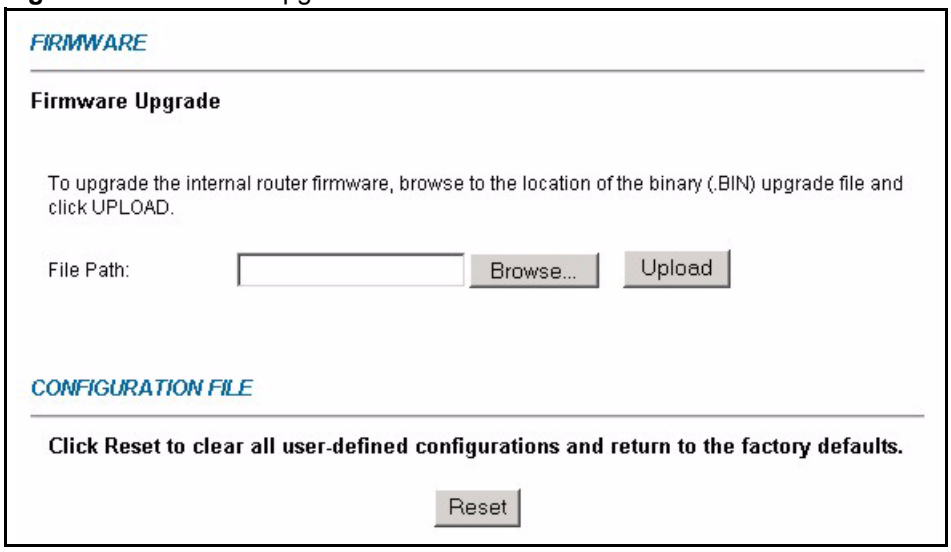
12.5 Firmware Screen

Find firmware at www.zyxel.com in a file that (usually) uses the system model name with a .bin extension, for example, "Prestige.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot. See Chapter 25 Firmware and Configuration File Maintenance in the parts that document the SMT for upgrading firmware using FTP/TFTP commands.

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

Click **Firmware** to open the following screen. Follow the instructions in this screen to upload firmware to your Prestige.

Figure 53 Firmware Upgrade



The following table describes the labels in this screen.

Table 29 Firmware Upgrade

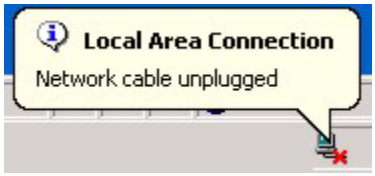
LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.
Reset	Click this button to clear all user-entered configuration information and return the Prestige to its factory defaults. Refer to the *Resetting the Prestige* section.

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

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

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

Figure 54 Network Temporarily Disconnected



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

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

Figure 55 Error Message

CHAPTER 13
Introducing the SMT

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

13.1 SMT Introduction

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

13.1.1 Procedure for SMT Configuration via Telnet

The following procedure details how to telnet into your Prestige.

1. In Windows, click **Start** (usually in the bottom left corner), **Run** and then type "`telnet 192.168.1.1`" (the default IP address) and click **OK**.
2. Enter "`1234`" in the **Password** field.
3. After entering the password you will see the main menu.

Please note that if there is no activity for longer than five minutes (default timeout period) after you log in, your Prestige will automatically log you out. You will then have to telnet into the Prestige again.

13.1.2 Entering Password

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

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

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

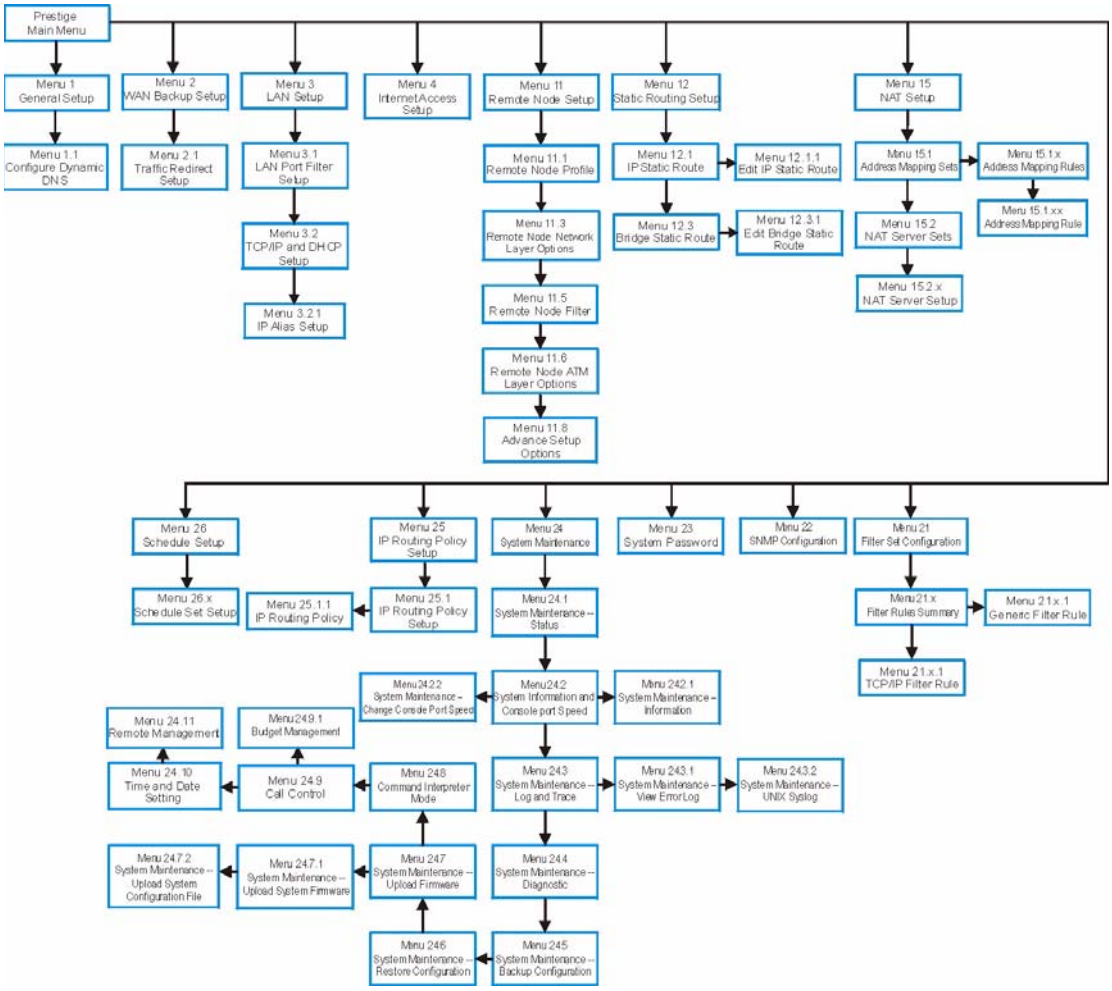
Figure 56 Login Screen

```
Enter Password : ****
```

13.1.3 Prestige SMT Menu Overview

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

Figure 57 Prestige SMT Menu Overview



13.2 Navigating the SMT Interface

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

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

Table 30 Navigating the SMT Interface

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

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

Table 31 SMT Main Menu

```
          Copyright (c) 1994 - 2004 ZyXEL Communications Corp.

                        Prestige 660R-63/67C Main Menu

 Getting Started                       Advanced Management
   1. General Setup                      21. Filter Set Configuration
   2. WAN Backup Setup                   22. SNMP Configuration
   3. LAN Setup                          23. System Password
   4. Internet Access Setup              24. System Maintenance
                                         25. IP Routing Policy Setup
 Advanced Applications                   26. Schedule Setup
   11. Remote Node Setup
   12. Static Routing Setup
   15. NAT Setup                         99. Exit


                     Enter Menu Selection Number:
```

13.2.1 System Management Terminal Interface Summary

Table 32 Main Menu Summary

#	MENU TITLE	DESCRIPTION
1	General Setup	Use this menu to set up your general information.
2	WAN Backup Setup	Use this menu to setup traffic redirect.
3	LAN Setup	Use this menu to set up your LAN connection.
4	Internet Access Setup	A quick and easy way to set up an Internet connection.
11	Remote Node Setup	Use this menu to set up the Remote Node for LAN-to-LAN connection, including Internet connection.
12	Static Routing Setup	Use this menu to set up static routes.
15	NAT Setup	Use this menu to specify inside servers when NAT is enabled.
21	Filter Set Configuration	Use this menu to configure filters.
22	SNMP Configuration	Use this menu to set up SNMP related parameters.
23	System Password	Use this menu to change your password.
24	System Maintenance	This menu provides system status, diagnostics, software upload, etc.
25	IP Routing Policy Setup	Use this menu to configure your IP routing policy.
26	Schedule Setup	Use this menu to schedule outgoing calls.
99	Exit	Use this to exit from SMT and return to a blank screen.

13.3 Changing the System Password

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

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

Figure 58 Menu 23 Change Password

```
Menu 23 - System Password

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

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

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

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

CHAPTER 14
Menu 1 General Setup

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

14.1 General Setup

Menu 1 — General Setup contains administrative and system-related information (shown next). The **System Name** field is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

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

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

14.2 Procedure To Configure Menu 1

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

Figure 59 Menu 1 General Setup

```
                Menu 1 General Setup

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

                      Route IP= Yes
                      Bridge= No

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

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

Table 33 Menu 1 General Setup

FIELD	DESCRIPTION
System Name	Choose a descriptive name for identification purposes. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.
Location (optional)	Enter the geographic location (up to 31 characters) of your Prestige.
Contact Person's Name (optional)	Enter the name (up to 30 characters) of the person in charge of this Prestige.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP may assign a domain name via DHCP. You can go to menu 24.8 and type "sys domainname" to see the current domain name used by your gateway. If you want to clear this field just press the [SPACE BAR]. The domain name entered by you is given priority over the ISP assigned domain name.
Edit Dynamic DNS	Press the [SPACE BAR] to select **Yes** or **No** (default). Select **Yes** to configure **Menu 1.1 — Configure Dynamic DNS** (discussed next).
Route IP	Set this field to **Yes** to enable or **No** to disable IP routing. You must enable IP routing for Internet access.
Bridge	Turn on/off bridging for protocols not supported (for example, SNA) or not turned on in the previous **Route IP** field. Select **Yes** to turn bridging on; select **No** to turn bridging off.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

14.2.1 Procedure to Configure Dynamic DNS

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

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

Figure 60 Menu 1.1 Configure Dynamic DNS

```
                Menu 1.1 - Configure Dynamic DNS

           Service Provider= WWW.DynDNS.ORG
           Active= Yes
           Host= me.dyndns.org
           EMAIL= mail@mailserver
           USER= username
           Password= ********
           Enable Wildcard= No

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

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

Table 34 Menu 1.1 Configure Dynamic DNS

FIELD	DESCRIPTION
Service Provider	This is the name of your dynamic DNS service provider.
Active	Press [SPACE BAR] to select **Yes** and then press [ENTER] to make dynamic DNS active.
Host	Enter the domain name assigned to your Prestige by your dynamic DNS provider.
EMAIL	Enter your e-mail address.
User	Enter your user name.
Password	Enter the password assigned to you.
Enable Wildcard	Your Prestige supports DYNDNS Wildcard. Press [SPACE BAR] and then [ENTER] to select **Yes** or **No** This field is **N/A** when you choose DDNS client as your service provider.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

CHAPTER 15
Menu 2 WAN Backup Setup

This chapter describes how to configure traffic redirect using menu 2 and 2.1.

15.1 Introduction to WAN Backup Setup

This chapter explains how to configure the Prestige for traffic redirect and dial backup connections.

15.2 Configuring Dial Backup in Menu 2

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

Figure 61 Menu 2 WAN Backup Setup

```
                          Menu 2 - Wan Backup Setup

                      Check Mechanism = DSL Link
                      Check WAN IP Address1 = 0.0.0.0
                      Check WAN IP Address2 = 0.0.0.0
                      Check WAN IP Address3 = 0.0.0.0
                        KeepAlive Fail Tolerance = 0
                        Recovery Interval(sec) = 0
                        ICMP Timeout(sec) = 0
                      Traffic Redirect = No

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

The following table describes the fields in this menu.

Table 35 Menu 2 WAN Backup Setup

FIELD	DESCRIPTION
Check Mechanism	Press [SPACE BAR] and then press [ENTER] to select the method that the Prestige uses to check the DSL connection. Select **DSL Link** to have the Prestige check the DSL connection's physical layer. Select **ICMP** to have the Prestige periodically ping the IP addresses configured in the **Check WAN IP Address** fields.
Check WAN IP Address1-3	Configure this field to test your Prestige's WAN accessibility. Type the IP address of a reliable nearby computer (for example, your ISP's DNS server address). When using a WAN backup connection, the Prestige periodically pings the addresses configured here and uses the other WAN backup connection (if configured) if there is no response.
KeepAlive Fail Tolerance	Type the number of times (2 recommended) that your Prestige may ping the IP addresses configured in the **Check WAN IP Address** field without getting a response before switching to a WAN backup connection (or a different WAN backup connection).
Recovery Interval(sec)	When the Prestige is using a lower priority connection (usually a WAN backup connection), it periodically checks to whether or not it can use a higher priority connection. Type the number of seconds (30 recommended) for the Prestige to wait between checks. Allow more time if your destination IP address handles lots of traffic.
ICMP Timeout	Type the number of seconds for an ICMP session to wait for the ICMP response.
Traffic Redirect	Press [SPACE BAR] to select **Yes** or **No**. Select **Yes** and press [ENTER] to configure **Menu 2.1 Traffic Redirect Setup**. Select **No** (default) if you do not want to configure this feature.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

15.2.1 Traffic Redirect Setup

Configure parameters that determine when the Prestige will forward WAN traffic to the backup gateway using **Menu 2.1 — Traffic Redirect Setup**.

Figure 62 Menu 2.1Traffic Redirect Setup

```
                Menu 2.1 - Traffic Redirect Setup

            Active= No
            Configuration:
              Backup Gateway IP Address= 0.0.0.0
              Metric= 15

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

The following table describes the fields in this menu.

Table 36 Menu 2.1Traffic Redirect Setup

FIELD	DESCRIPTION
Active.	Press [SPACE BAR] and select **Yes** (to enable) or **No** (to disable) traffic redirect setup. The default is **No**
Configuration	
Backup Gateway IP Address	Enter the IP address of your backup gateway in dotted decimal notation. The Prestige automatically forwards traffic to this IP address if the Prestige's Internet connection terminates.
Metric	This field sets this route's priority among the routes the Prestige uses. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost"
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

CHAPTER 16
Menu 3 LAN Setup

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

16.1 LAN Setup

This section describes how to configure the Ethernet using **Menu 3 — LAN Setup**. From the main menu, enter 3 to display menu 3.

Figure 63 Menu 3 LAN Setup

```
Menu 3 - LAN Setup

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

Enter Menu Selection Number:
```

16.1.1 General Ethernet Setup

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

Figure 64 Menu 3.1 LAN Port Filter Setup

```
Menu 3.1 - LAN Port Filter Setup

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

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

If you need to define filters, please read Chapter 22 Filter Configuration first, then return to this menu to define the filter sets.

16.2 Protocol Dependent Ethernet Setup

Depending on the protocols for your applications, you need to configure the respective Ethernet Setup, as outlined below.

- For TCP/IP Ethernet setup refer to the Internet Access Configuration section.
- For bridging Ethernet setup refer to Chapter 20 Bridging Setup.

16.3 CP/IP Ethernet Setup and DHCP

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

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

Figure 65 Menu 3.2 TCP/IP and DHCP Ethernet Setup

```
                Menu 3.2 - TCP/IP and DHCP Setup

DHCP Setup
  DHCP= Server
  Client IP Pool Starting Address= 192.168.1.33
  Size of Client IP Pool= 32
  Primary DNS Server= 0.0.0.0
  Secondary DNS Server= 0.0.0.0
  Remote DHCP Server= N/A
TCP/IP Setup:
  IP Address= 192.168.1.1
  IP Subnet Mask= 255.255.255.0
  RIP Direction= Both
    Version= RIP-2B
  Multicast= None
  IP Policies=
  Edit IP Alias= No

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

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

Table 37 DHCP Ethernet Setup

FIELD	DESCRIPTION
DHCP Setup	
DHCP	If set to **Server**, your Prestige can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT and other systems that support the DHCP client. If set to **None**, the DHCP server will be disabled. If set to **Relay**, the Prestige acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the Remote DHCP Server in this case. When DHCP server is used, the following items need to be set:
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Size of Client IP Pool	This field specifies the size or count of the IP address pool.
Primary DNS Server Secondary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Remote DHCP Serve	If **Relay** is selected in the **DHCP** field above then enter the IP address of the actual remote DHCP server here.

Follow the instructions in the following table to configure TCP/IP parameters for the Ethernet port.

Table 38 TCP/IP Ethernet Setup

FIELD	DESCRIPTION
TCP/IP Setup	
IP Address	Enter the (LAN) IP address of your Prestige in dotted decimal notation
IP Subnet Mask	Your Prestige will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Prestige (refer to Appendix C IP Subnetting for more information).
RIP Direction	Press [SPACE BAR] to select the RIP direction. Choices are **Both**, **In Only**, **Out Only** or **None**.
Version	Press [SPACE BAR] to select the RIP version. Choices are **RIP-1**, **RIP-2B** or **RIP-2M**.
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group. The Prestige supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). Press the [SPACE BAR] to enable IP Multicasting or select **None** to disable it.
IP Policies	Create policies using SMT menu 25 (see Chapter 28 IP Policy Routing) and apply them on the Prestige LAN interface here. You can apply up to four IP policy sets (from twelve) by entering their numbers separated by commas.
Edit IP Alias	The Prestige supports three logical LAN interfaces via its single physical Ethernet interface with the Prestige itself as the gateway for each LAN network. Press [SPACE BAR] to change **No** to **Yes** and press [ENTER] to display Menu 3.2.1.

CHAPTER 17
Internet Access

This chapter shows you how to configure the LAN and WAN of your Prestige for Internet access.

17.1 Internet Access Overview

Refer to the chapters on the web configurator's wizard, LAN and WAN screens for more background information on fields in the SMT screens covered in this chapter.

17.2 IP Policies

Traditionally, routing is based on the destination address *only* and the router takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing. Create policies using SMT menu 25 (see Chapter 28 IP Policy Routing) and apply them on the Prestige LAN and/or WAN interfaces using menus 3.2 (LAN) and 11.3 (WAN).

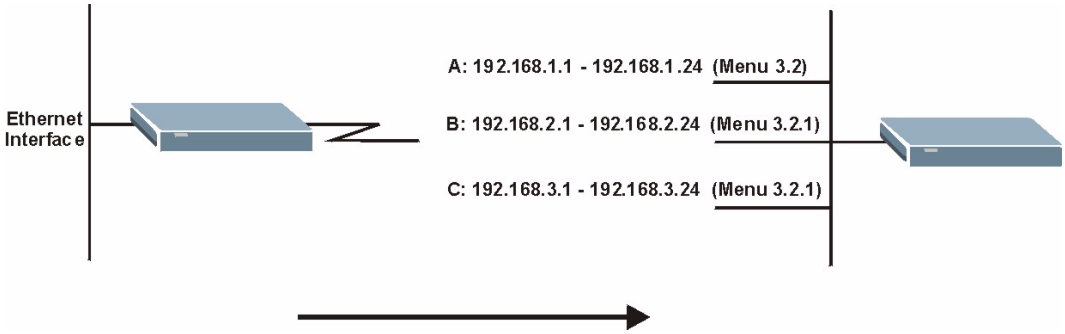
17.3 IP Alias

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

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

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

Figure 66 IP Alias Network Example



Use menu 3.2.1 to configure IP Alias on your Prestige.

17.4 IP Alias Setup

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

Figure 67 Menu 3.2 TCP/IP and DHCP Setup

```
                Menu 3.2 - TCP/IP and DHCP Setup

            DHCP Setup
              DHCP= Server
              Client IP Pool Starting Address= 192.168.1.33
              Size of Client IP Pool= 32
              Primary DNS Server= 0.0.0.0
              Secondary DNS Server= 0.0.0.0
              Remote DHCP Server= N/A
            TCP/IP Setup:
              IP Address= 192.168.1.1
              IP Subnet Mask= 255.255.255.0
              RIP Direction= None
                Version= RIP-2B
              Multicast= None
              IP Policies=
              Edit IP Alias= Yes

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

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

Figure 68 Menu 3.2.1 IP Alias Setup

```
              Menu 3.2.1 - IP Alias Setup

                IP Alias 1= Yes
                  IP Address= 192.168.2.1
                  IP Subnet Mask= 255.255.255.0
                  RIP Direction= None
                  Version= RIP-1
                  Incoming protocol filters=
                  Outgoing protocol filters=
                IP Alias 2= No
                  IP Address= N/A
                  IP Subnet Mask= N/A
                  RIP Direction= N/A
                  Version= N/A
                  Incoming protocol filters= N/A
                  Outgoing protocol filters= N/A

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

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

Table 39 Menu 3.2.1 IP Alias Setup

FIELD	DESCRIPTION
IP Alias	Choose **Yes** to configure the LAN network for the Prestige.
IP Address	Enter the IP address of your Prestige in dotted decimal notation
IP Subnet Mask	Your Prestige will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Prestige
RIP Direction	Press [SPACE BAR] to select the RIP direction. Choices are **None**, **Both**, **In Only** or **Out Only**.
Version	Press [SPACE BAR] to select the RIP version. Choices are **RIP-1**, **RIP-2B** or **RIP-2M**.
Incoming Protocol Filters	Enter the filter set(s) you wish to apply to the incoming traffic between this node and the Prestige.
Outgoing Protocol Filters	Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the Prestige.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

17.5 Route IP Setup

The first step is to enable the IP routing in **Menu 1 - General Setup**.

To edit menu 1, type 1 in the main menu and press [ENTER]. Set the **Route IP** field to **Yes** by pressing [SPACE BAR].

Figure 69 Menu 1 General Setup

```
Menu 1 - General Setup

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

            Route IP= Yes
            Bridge= No

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

17.6 Internet Access Configuration

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

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

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

Figure 70 Menu 4 Internet Access Setup

```
              Menu 4 - Internet Access Setup

                ISP's Name= MyISP
                Encapsulation= RFC 1483
                Multiplexing= LLC-based
                VPI #= 8
                VCI #= 35
                ATM QoS Type= CBR
                  Peak Cell Rate (PCR)= 0
                  Sustain Cell Rate (SCR)= 0
                  Maximum Burst Size (MBS)= 0
                My Login= N/A
                My Password= N/A
                ENET ENCAP Gateway= N/A
                IP Address Assignment= Static
                  IP Address= 0.0.0.0
                Network Address Translation= SUA Only
                  Address Mapping Set= N/A

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

The following table contains instructions on how to configure your Prestige for Internet access.

Table 40 Menu 4 Internet Access Setup

FIELD	DESCRIPTION
ISP's Name	Enter the name of your Internet Service Provider (ISP). This information is for identification purposes only.
Encapsulation	Press [SPACE BAR] to select the method of encapsulation used by your ISP. Choices are **PPPoE**, **PPPoA**, **RFC 1483** or **ENET ENCAP**.
Multiplexing	Press [SPACE BAR] to select the method of multiplexing used by your ISP. Choices are **VC-based** or **LLC-based**.
VPI #	Enter the Virtual Path Identifier (VPI) assigned to you.
VCI #	Enter the Virtual Channel Identifier (VCI) assigned to you.
ATM QoS Type	Press [SPACE BAR] and select **CBR** (Continuous Bit Rate) to specify fixed (always-on) bandwidth. Select **UBR** (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select **VBR** (Variable Bit Rate) for bursty traffic and bandwidth sharing with other applications.
Peak Cell Rate (PCR)	This is the maximum rate at which the sender can send cells. Type the PCR.
Sustain Cell Rate (SCR)	Sustained Cell Rate is the mean cell rate of a bursty, on-off traffic source that can be sent at the peak rate, and a parameter for burst-traffic. Type the SCR; it must be less than the PCR.
Maximum Burst Size (MBS)	Refers to the maximum number of cells that can be sent at the peak rate. Type the MBS. The MBS must be less than 65535.
My Login	Configure the **My Login** and **My Password** fields for PPPoA and PPPoE encapsulation only. Enter the login name that your ISP gives you. If you are using PPPoE encapsulation**,** then this field must be of the form user@domain where domain identifies your PPPoE service name.

Table 40 Menu 4 Internet Access Setup (continued)

FIELD	DESCRIPTION
My Password	Enter the password associated with the login name above.
ENET ENCAP Gateway	Enter the gateway IP address supplied by your ISP when you are using **ENET ENCAP** encapsulation.
Idle Timeout	This value specifies the number of idle seconds that elapse before the Prestige automatically disconnects the PPPoE session.
IP Address Assignment	Press [SPACE BAR] to select **Static** or **Dynamic** address assignment.
IP Address	Enter the IP address supplied by your ISP if applicable.
Network Address Translation	Press [SPACE BAR] to select **None**, **SUA Only** or **Full Feature**. Please see Chapter 21 Network Address Translation (NAT) for more details on the SUA (Single User Account) feature.
Address Mapping Set	Type the numbers of mapping sets (1-8) to use with NAT. See Chapter 21 Network Address Translation (NAT) for details.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

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

CHAPTER 18
Remote Node Configuration

This chapter covers remote node configuration.

18.1 Remote Node Setup Overview

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

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

18.2 Remote Node Setup

This section describes the protocol-independent parameters for a remote node.

18.2.1 Remote Node Profile

To configure a remote node, follow these steps:

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

Figure 71 Menu 11 Remote Node Setup

```
                    Menu 11 - Remote Node Setup

                1. MyISP (ISP, SUA)
                2. _________
                3. _________
                4. _________
                5. _________
                6. _________
                7. _________
                8. _________

                        Enter Node # to Edit:
```

18.2.2 Encapsulation and Multiplexing Scenarios

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

18.2.2.1 Scenario 1: One VC, Multiple Protocols

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

18.2.2.2 Scenario 2: One VC, One Protocol (IP)

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

18.2.2.3 Scenario 3: Multiple VCs

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

Figure 72 Menu 11.1 Remote Node Profile

```
Menu 11.1 - Remote Node Profile

Rem Node Name= MyISP                    Route= IP
Active= Yes                             Bridge= No

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

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

In **Menu 11.1 – Remote Node Profile**, fill in the fields as described in the following table.

Table 41 Menu 11.1 Remote Node Profile

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

Table 41 Menu 11.1 Remote Node Profile (continued)

FIELD	DESCRIPTION
Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are: **CHAP**/**PAP** – Your Prestige will accept either **CHAP** or **PAP** when requested by this remote node. **CHAP** – accept **CHAP** (Challenge Handshake Authentication Protocol) only. **PAP** – accept PAP (Password Authentication Protocol) only.
Route	This field determines the protocol used in routing. Options are **IP** and **None.**
Bridge	When bridging is enabled, your Prestige will forward any packet that it does not route to this remote node; otherwise, the packets are discarded. Select **Yes** to enable and **No** to disable.
Edit IP/Bridge	Press [SPACE BAR] to select **Yes** and press [ENTER] to display **Menu 11.3 – Remote Node Network Layer Options**.
Edit ATM Options	Press [SPACE BAR] to select **Yes** and press [ENTER] to display **Menu 11.6 – Remote Node ATM Layer Options**.
Edit Advance Options	This field is only available when you select **PPPoE** in the **Encapsulation** field. Press [SPACE BAR] to select **Yes** and press [ENTER] to display **Menu 11.8 – Advance Setup Options**.
Telco Option	
Allocated Budget (min)	This sets a ceiling for outgoing call time for this remote node. The default for this field is 0 meaning no budget control.
Period (hr)	This field is the time period that the budget should be reset. For example, if we are allowed to call this remote node for a maximum of 10 minutes every hour, then the **Allocated Budget** is (10 minutes) and the **Period (hr)** is 1 (hour).
Schedule Sets	This field is only applicable for **PPPoE** and **PPPoA** encapsulation. You can apply up to four schedule sets here. For more details please refer to Chapter 29 Call Scheduling.
Nailed up Connection	This field is only applicable for **PPPoE** and **PPPoA** encapsulation. This field specifies if you want to make the connection to this remote node a nailed-up connection. More details are given earlier in this section.
Session Options	
Edit Filter Sets	Use [SPACE BAR] to choose **Yes** and press [ENTER] to open menu 11.5 to edit the filter sets. See the Remote Node Filter section for more details.
Idle Timeout (sec)	Type the number of seconds (0-9999) that can elapse when the Prestige is idle (there is no traffic going to the remote node), before the Prestige automatically disconnects the remote node. 0 means that the session will not timeout.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

18.2.3 Outgoing Authentication Protocol

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

18.3 Remote Node Network Layer Options

For the TCP/IP parameters, perform the following steps to edit **Menu 11.3 – Remote Node Network Layer Options** as shown next.

1. In menu 11.1, make sure **IP** is among the protocols in the **Route** field.
2. Move the cursor to the **Edit IP/Bridge** field, press [SPACE BAR] to select **Yes,** then press [ENTER] to display **Menu 11.3 – Remote Node Network Layer Options.**

Figure 73 Menu 11.3 Remote Node Network Layer Options

```
            Menu 11.3 - Remote Node Network Layer Options

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

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

The next table explains fields in **Menu 11.3 – Remote Node Network Layer Options**.

Table 42 Menu 11.3 Remote Node Network Layer Options

FIELD	DESCRIPTION
IP Address Assignment	Press [SPACE BAR] and then [ENTER] to select **Dynamic** if the remote node is using a dynamically assigned IP address or **Static** if it is using a static (fixed) IP address. You will only be able to configure this in the ISP node (also the one you configure in menu 4), all other nodes are set to **Static**.
Rem IP Addr	This is the IP address you entered in the previous menu.
Rem Subnet Mask	Type the subnet mask assigned to the remote node.
My WAN Addr	Some implementations, especially UNIX derivatives, require separate IP network numbers for the WAN and LAN links and each end to have a unique address within the WAN network number. In that case, type the IP address assigned to the WAN port of your Prestige. NOTE: Refers to local Prestige address, not the remote router address.
NAT	Press [SPACE BAR] and then [ENTER] to select **Full Feature** if you have multiple public WAN IP addresses for your Prestige. Select **SUA Only** if you have just one public WAN IP address for your Prestige. The SMT uses Address Mapping Set 255 (menu 15.1 - see Figure 95). Select **None** to disable NAT.

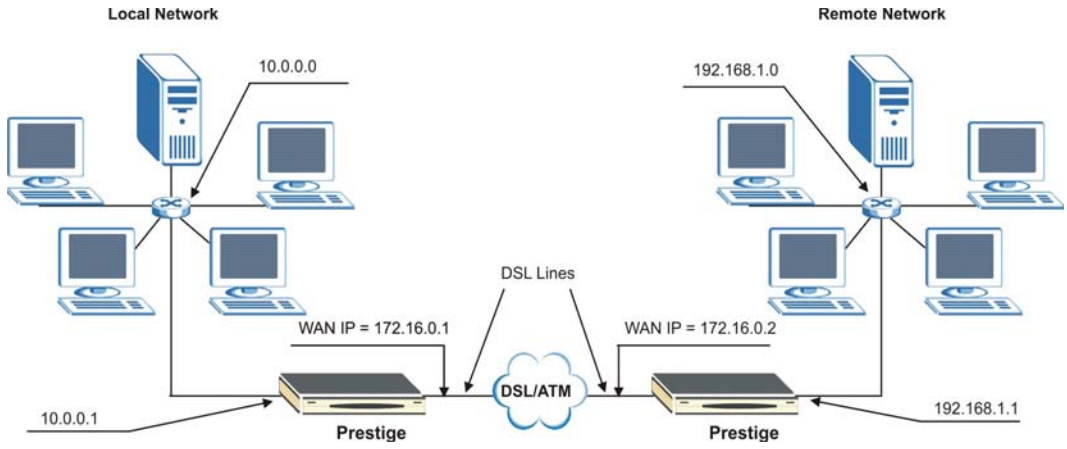
Table 42 Menu 11.3 Remote Node Network Layer Options (continued)

FIELD	DESCRIPTION
Address Mapping Set	When **Full Feature** is selected in the **NAT** field, configure address mapping sets in menu 15.1. Select one of the NAT server sets (2-10) in menu 15.2 (see Chapter 21 Network Address Translation (NAT) for details) and type that number here. When **SUA Only** is selected in the NAT field, the SMT uses NAT server set 1 in menu 15.2 (see Chapter 21 Network Address Translation (NAT) for details).
Metric	The metric represents the cost of transmission for routing purposes. IP routing uses hop count as the cost measurement, with a minimum of 1 for directly connected networks. Type a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Private	This determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and not included in RIP broadcast. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP Direction. Options are **Both**, **In Only**, **Out Only** or **None**.
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are **RIP-1**, **RIP-2B** or **RIP-2M**.
Multicast	**IGMP-v1** sets IGMP to version 1, **IGMP-v2** sets IGMP to version 2 and **None** disables IGMP.
IP Policies	You can apply up to four IP Policy sets (from 12) by typing in their numbers separated by commas. Configure the filter sets in menu 25 first (see Chapter 28 IP Policy Routing) and then apply them here.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

18.3.1 My WAN Addr Sample IP Addresses

The following figure uses sample IP addresses to help you understand the field of **My WAN Addr** in menu 11.3. Refer to the previous Figure 15 in Chapter 5 LAN Setup for a brief review of what a WAN IP is. **My WAN Addr** indicates the local Prestige WAN IP (172.16.0.1 in the following figure) while **Rem IP Addr** indicates the peer WAN IP (172.16.0.2 in the following figure).

Figure 74 Sample IP Addresses for a TCP/IP LAN-to-LAN Connection



18.4 Remote Node Filter

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

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

Note that spaces are accepted in this field. The Prestige has a prepackaged filter set, NetBIOS_WAN, that blocks NetBIOS packets. Include this in the call filter sets if you want to prevent NetBIOS packets from triggering calls to a remote node.

Figure 75 Menu 11.5 Remote Node Filter (RFC 1483 or ENET Encapsulation)

```
            Menu 11.5 - Remote Node Filter
                     Input Filter Sets:
                       protocol filters= 1, 5, 9, 12
                         device filters=
                     Output Filter Sets:
                       protocol filters=
                         device filters=

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

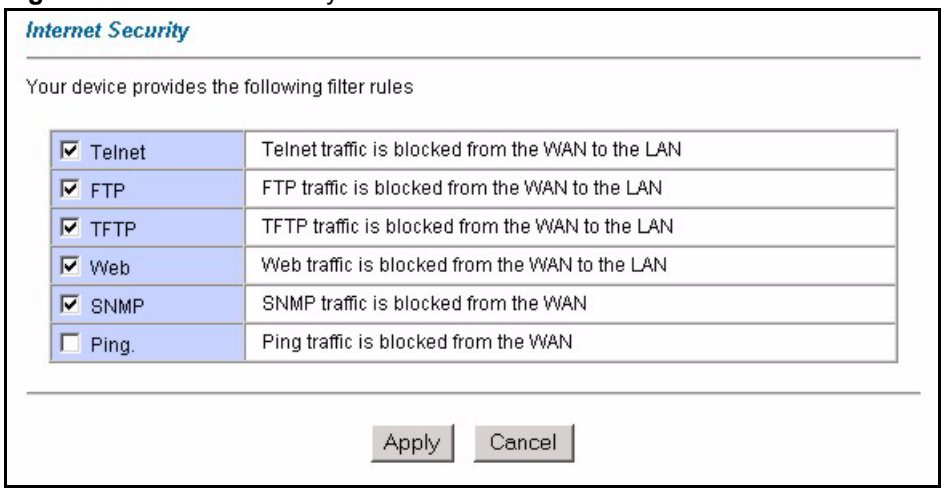
Figure 76 Menu 11.5 Remote Node Filter (PPPoA or PPPoE Encapsulation)

```
                Menu 11.5 - Remote Node Filter
Input Filter Sets:
  protocol filters= 1, 5, 9, 12
    device filters=
Output Filter Sets:
  protocol filters=
    device filters=
Call Filter Sets:
  protocol filters=
    device filters=

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

18.4.1 Web Configurator Internet Security Filter Rules

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

Figure 77 Internet Security



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

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

18.4.2 Web Configurator Filter Sets

When you apply filter rules using the web configurator, filter sets 11 and 12 are automatically generated in SMT menu 21. This feature is not available on all models.

Figure 78 Menu 21 Filer Set Configuration

```
                    Menu 21 - Filter Set Configuration

Filter                                  Filter
Set #        Comments                   Set #        Comments
------  -----------------               ------  -----------------
  1      ________________                  7      ________________
  2      NetBIOS_WAN                       8      ________________
  3      NetBIOS_LAN                       9      ________________
  4      ________________                 10      ________________
  5      ________________                 11      WebSet1
  6      ________________                 12      WebSet2



                Enter Filter Set Number to Configure= 0
```

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

Figure 79 Menu 21.11 WebSet 11

```
                        Menu 21.11 - Filter Rules Summary
# A Type                          Filter Rules                          M m n
- - ---- ------------------------------------------------------------ - - -
1 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=161                        N D N
2 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=162                        N D F
3 N
4 N
5 N
6 N
                  Enter Filter Rule Number (1-6) to Configure:
```

Figure 80 Menu 21.12 WebSet 12

```
                        Menu 21.12 - Filter Rules Summary

# A Type                          Filter Rules                          M m n
- - ---- ------------------------------------------------------------ - - -
1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23                          N D N
2 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=21                          N D N
3 Y IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=69                         N D N
4 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=80                          N D N
5 N
6 N
                  Enter Filter Rule Number (1-6) to Configure
```

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

18.5 Editing ATM Layer Options

Follow the steps shown next to edit **Menu 11.6 – Remote Node ATM Layer Options**.

In menu 11.1, move the cursor to the **Edit ATM Options** field and then press [SPACE BAR] to select **Yes**. Press [ENTER] to display **Menu 11.6 – Remote Node ATM Layer Options**.

There are two versions of menu 11.6 for the Prestige, depending on whether you chose **VC-based**/**LLC-based** multiplexing and **PPP** encapsulation in menu 11.1.

18.5.1 VC-based Multiplexing (non-PPP Encapsulation)

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

Figure 81 Menu 11.6 for VC-based Multiplexing

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

 VC Options for IP:                VC Options for Bridge:
   VPI #= 8                          VPI #= 1
   VCI #= 35                         VCI #= 36
   ATM QoS Type= UBR                 ATM QoS Type= N/A
   Peak Cell Rate (PCR)= 0           Peak Cell Rate (PCR)= N/A
   Sustain Cell Rate (SCR)= 0        Sustain Cell Rate (SCR)= N/A
   Maximum Burst Size (MBS)= 0       Maximum Burst Size (MBR)= N/A

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

18.5.2 LLC-based Multiplexing or PPP Encapsulation

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

Figure 82 Menu 11.6 for LLC-based Multiplexing or PPP Encapsulation

```
            Menu 11.6 - Remote Node ATM Layer Options
            VPI/VCI (LLC-Multiplexing or PPP-Encapsulation)

                       VPI #= 8
                       VCI #= 35
                       ATM QoS Type= UBR
                       Peak Cell Rate (PCR)= 0
                       Sustain Cell Rate (SCR)= 0
                       Maximum Burst Size (MBS)= 0

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

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

18.5.3 Advance Setup Options

In menu 11.1, select **PPPoE** in the **Encapsulation** field.

Figure 83 Menu 11.1 Remote Node Profile

```
          Menu 11.1 - Remote Node Profile

      Rem Node Name= MyISP                  Route= IP
      Active= Yes                           Bridge= No

      Encapsulation= PPPoE                  Edit IP/Bridge= No
      Multiplexing= LLC-based               Edit ATM Options= No
      Service Name=                         Edit Advance Options= Yes
      Incoming:                             Telco Option:
        Rem Login=                            Allocated Budget(min)= 0
        Rem Password= ********                Period(hr)= 0
      Outgoing:                               Schedule Sets=
        My Login= ?                           Nailed-Up Connection= No
        My Password= ?                      Session Options:
        Authen= CHAP/PAP                      Edit Filter Sets= No
                                              Idle Timeout(sec)= 0

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

Move the cursor to the **Edit Advance Options** field, press [SPACE BAR] to select **Yes,** then press [ENTER] to display **Menu 11.8 – Advance Setup Options**.

Figure 84 Menu 11.8 Advance Setup Options

```
                    Menu 11.8 - Advance Setup Options

               PPPoE pass-through= No


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

The following table describes the fields in this menu.

Table 43 Menu 11.8 Advance Setup Options

FIELD	DESCRIPTION
PPPoE pass-through	Press [SPACE BAR] to select **Yes** and press [ENTER] to enable PPPoE pass through. In addition to the Prestige's built-in PPPoE client, you can enable PPPoE pass through to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP via the Prestige. Each host can have a separate account and a public WAN IP address. PPPoE pass through is an alternative to NAT for applications where NAT is not appropriate. Press [SPACE BAR] to select **No** and press [ENTER] to disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

CHAPTER 19
Static Route Setup

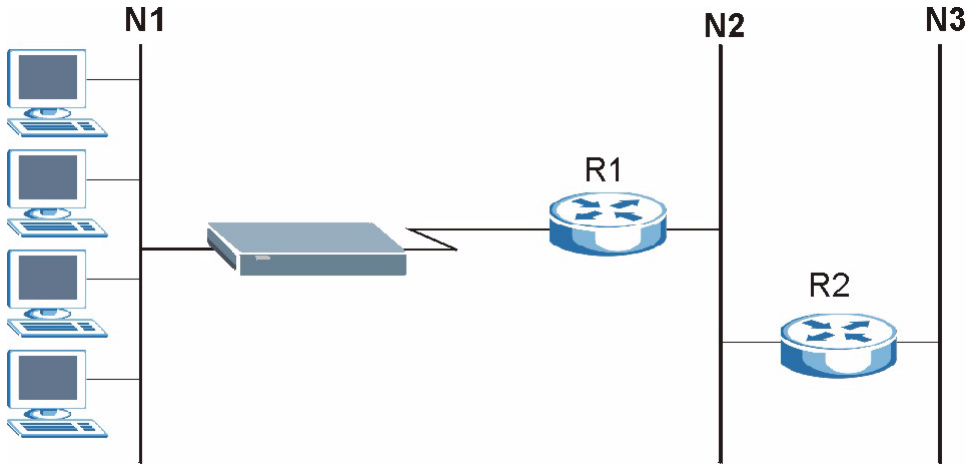
This chapter shows how to setup IP static routes.

19.1 IP Static Route Overview

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

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

Figure 85 Sample Static Routing Topology



19.2 Configuration

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

Figure 86 Menu 12 Static Route Setup

```
                    Menu 12 - Static Route Setup

               1. IP Static Route
               3. Bridge Static Route


                       Please enter selection:
```

2 From menu 12, select 1 to open **Menu 12.1 — IP Static Route Setup** (shown next).

Figure 87 Menu 12.1 IP Static Route Setup

```
                    Menu 12.1 - IP Static Route Setup
                  1. _________
                  2. _________
                  3. _________
                  4. _________
                  5. _________
                  6. _________
                  7. _________
                  8. _________
                  9. _________
                  10. _________
                  11. _________
                  12. _________
                  13. _________
                  14. _________
                  15. _________
                  16. _________

             Enter selection number:
```

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

Figure 88 Menu12.1.1 Edit IP Static Route

```
          Menu 12.1.1 - Edit IP Static Route

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

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

The following table describes the fields for **Menu 12.1.1 – Edit IP Static Route Setup**.

Table 44 Menu12.1.1 Edit IP Static Route

FIELD	DESCRIPTION
Route #	This is the index number of the static route that you chose in menu 12.1.
Route Name	Type a descriptive name for this route. This is for identification purpose only.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Type the subnet mask for this destination. Seethe IP Address and Subnet Mask sectionin this manual.
Gateway IP Address	Type the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Metric	Metric represents the cost of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Type a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Private	This parameter determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and is not included in RIP broadcasts. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

CHAPTER 20
Bridging Setup

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

20.1 Bridging in General

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

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

20.2 Bridge Ethernet Setup

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

20.2.1 Remote Node Bridging Setup

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

1. To setup **Menu 11.3 – Remote Node Network Layer Options** shown in the next figure, follow these steps:
2. In menu 11.1, make sure the **Bridge** field is set to **Yes**.

Figure 89 Menu 11.1 Remote Node Profile

```
                Menu 11.1 - Remote Node Profile

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

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

3 Move the cursor to the **Edit IP/Bridge** field, then press [SPACE BAR] to set the value to **Yes** and press [ENTER] to edit **Menu 11.3 – Remote Node Network Layer Options**.

Figure 90 Menu 11.3 Remote Node Network Layer Options

```
            Menu 11.3 - Remote Node Network Layer Options
IP Options:                          Bridge Options:
  IP Address Assignment= Static        Ethernet Addr Timeout (min)= 0
  Rem IP Addr: 0.0.0.0
  Rem Subnet Mask= 0.0.0.0
  My WAN Addr= 0.0.0.0
  NAT= Full Feature
    Address Mapping Set=2
  Metric= 2
  Private= No
  RIP Direction= Both
    Version= RIP-2B
  Multicast= IGMP-v2
  IP Policies=

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

Table 45 Remote Node Network Layer Options: Bridge Fields

FIELD	DESCRIPTION
Bridge (menu 11.1)	Make sure this field is set to **Yes**.

Table 45 Remote Node Network Layer Options: Bridge Fields (continued)

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

20.2.2 Bridge Static Route Setup

Similar to network layer static routes, a bridging static route tells the Prestige the route to a node before a connection is established. You configure bridge static routes in menu 12.3.1 (go to menu 12, choose option 3, then choose a static route to edit) as shown next.

Figure 91 Menu 12.3.1 Edit Bridge Static Route

```
            Menu 12.3.1 - Edit Bridge Static Route

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

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

The following table describes the **Edit Bridge Static Route** menu.

Table 46 Menu 12.3.1 Edit Bridge Static Route

FIELD	DESCRIPTION
Route #	This is the route index number you typed in **Menu 12.3 – Bridge Static Route Setup**.
Route Name	Type a name for the bridge static route for identification purposes.
Active	Indicates whether the static route is active (**Yes**) or not (**No**).
Ether Address	Type the MAC address of the destination computer that you want to bridge the packets to.
IP Address	If available, type the IP address of the destination computer that you want to bridge the packets to.
Gateway Node	Press [SPACE BAR] and then [ENTER] to select the number of the remote node (one to eight) that is the gateway of this static route.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

CHAPTER 21
Network Address Translation (NAT)

This chapter discusses how to configure NAT on the Prestige.

21.1 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. See the NAT Setup section or a detailed description of the NAT set for SUA. The Prestige also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types.

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

21.2 Applying NAT

You apply NAT via menus 4 or 11.3 as displayed next. The next figure shows you how to apply NAT for Internet access in menu 4. Enter 4 from the main menu to go to **Menu 4 - Internet Access Setup**.

Figure 92 Menu 4 Applying NAT for Internet Access

```
            Menu 4 - Internet Access Setup

                        ISP's Name= MyISP
                        Encapsulation= RFC 1483
                        Multiplexing= LLC-based
                        VPI #= 8
                        VCI #= 35
                        ATM QoS Type= UBR
                          Peak Cell Rate (PCR)= 0
                          Sustain Cell Rate (SCR)= 0
                          Maximum Burst Size (MBS)= 0
                        My Login= N/A
                        My Password= N/A
                        ENET ENCAP Gateway= N/A
                        IP Address Assignment= Static
                          IP Address= 0.0.0.0
                        Network Address Translation= SUA Only
                          Address Mapping Set= N/A

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

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

1. Enter 11 from the main menu.
2. When menu 11 appears, as shown in the following figure, type the number of the remote node that you want to configure.
3. Move the cursor to the **Edit IP/Bridge** field, press [SPACE BAR] to select **Yes** and then press [ENTER] to bring up **Menu 11.3 - Remote Node Network Layer Options.**

Figure 93 Applying NAT in Menus 4 & 11.3

```
            Menu 11.3 - Remote Node Network Layer Options

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

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

The following table describes the options for Network Address Translation.

Table 47 Applying NAT in Menus 4 & 11.3

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

21.3 NAT Setup

Use the address mapping sets menus and submenus to create the mapping table used to assign global addresses to computers on the LAN. **Set 255** is used for SUA. When you select **Full Feature** in menu 4 or 11.3, the SMT will use **Set 1**. When you select **SUA Only**, the SMT will use the pre-configured **Set 255** (read only).

The server set is a list of LAN servers mapped to external ports. To use this set, a server rule must be set up inside the NAT address mapping set. Please see the section on port forwarding in the chapter on NAT web configurator screens for further information on these menus. To configure NAT, enter 15 from the main menu to bring up the following screen.

Figure 94 Menu 15 NAT Setup

```
            Menu 15 - NAT Setup

                  1. Address Mapping Sets
                  2. NAT Server Sets


            Enter Menu Selection Number:
```

21.3.1 Address Mapping Sets

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

Figure 95 Menu 15.1 Address Mapping Sets

```
              Menu 15.1 - Address Mapping Sets

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

              Enter Menu Selection Number:
```

21.3.1.1 SUA Address Mapping Set

Enter 255 to display the next screen (see also the SUA (Single User Account) Versus NAT section). The fields in this menu cannot be changed.

Figure 96 Menu 15.1.255 SUA Address Mapping Rules

```
              Menu 15.1.255 - Address Mapping Rules
 Set Name= SUA
Idx  Local Start IP   Local End IP     Global Start IP  Global End IP  Type
---  ---------------  ---------------  ---------------  -------------  ----
 1.  0.0.0.0          255.255.255.255  0.0.0.0                          M-1
 2.                                    0.0.0.0                       Server+
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.
               Press ENTER to Confirm or ESC to Cancel:
```

The following table explains the fields in this menu.

Note: Menu 15.1.255 is read-only.

Table 48 SUA Address Mapping Rules

FIELD	DESCRIPTION
Set Name	This is the name of the set you selected in menu 15.1 or enter the name of a new set you want to create.
Idx	This is the index or rule number.
Local Start IP	**Local Start IP** is the starting local IP address (ILA).

Table 48 SUA Address Mapping Rules (continued)

FIELD	DESCRIPTION
Local End IP	**Local End IP** is the ending local IP address (ILA). If the rule is for all local IPs, then the Start IP is 0.0.0.0 and the End IP is 255.255.255.255.
Global Start IP	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global Start IP**.
Global End IP	This is the ending global IP address (IGA).
Type	These are the mapping types. **Server allows us to specify multiple servers of different types behind NAT to this machine. See later for some examples.**
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

21.3.1.2 User-Defined Address Mapping Sets

Now let's look at option 1 in menu 15.1. Enter 1 to bring up this menu. We'll just look at the differences from the previous menu. Note the extra **Action** and **Select Rule** fields mean you can configure rules in this screen. Note also that the [?] in the **Set Name** field means that this is a required field and you must enter a name for the set.

Figure 97 Menu 15.1.1 First Set

```
             Menu 15.1.1 - Address Mapping Rules

 Set Name= ACL Default Set
Idx  Local Start IP   Local End IP     Global Start IP  Global End IP  Type
---  ---------------  ---------------  ---------------  -------------  ----
 1.
 2
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.

                Action= Edit          Select Rule=
             Press ENTER to Confirm or ESC to Cancel:
```

Note: If the **Set Name** field is left blank, the entire set will be deleted.

Note: The Type, Local and Global Start/End IPs are configured in menu 15.1.1.1 (described later) and the values are displayed here.

21.3.1.3 Ordering Your Rules

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

Now if you delete rule 4, rules 5 to 7 will be pushed up by 1 rule, so as old rule 5 becomes rule 4, old rule 6 becomes rule 5 and old rule 7 becomes rule 6.

Table 49 Menu 15.1.1 First Set

FIELD	DESCRIPTION
Set Name	Enter a name for this set of rules. This is a required field. If this field is left blank, the entire set will be deleted.
Action	The default is **Edit**. **Edit** means you want to edit a selected rule (see following field). **Insert Before** means to insert a rule before the rule selected. The rules after the selected rule will then be moved down by one rule. **Delete** means to delete the selected rule and then all the rules after the selected one will be advanced one rule. **None** disables the **Select Rule** item.
Select Rule	When you choose **Edit**, **Insert Before** or **Delete** in the previous field the cursor jumps to this field to allow you to select the rule to apply the action in question.

Note: You must press [ENTER] at the bottom of the screen to save the whole set. You must do this again if you make any changes to the set – including deleting a rule. No changes to the set take place until this action is taken.

Selecting **Edit** in the **Action** field and then selecting a rule brings up the following menu, **Menu 15.1.1.1 - Address Mapping Rule** in which you can edit an individual rule and configure the **Type**, **Local** and **Global Start/End IPs**.

Note: An End IP address must be numerically greater than its corresponding IP Start address.

Figure 98 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set

```
              Menu 15.1.1.1 Address Mapping Rule

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

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

The following table explains the fields in this menu.

Table 50 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set

FIELD	DESCRIPTION
Type	Press [SPACE BAR] and then [ENTER] to select from a total of five types. These are the mapping types discussed in the chapter on NAT web configurator screens. **Server** allows you to specify multiple servers of different types behind NAT to this computer. See the Example 3: Multiple Public IP Addresses With Inside Servers section for an example.
Local IP	Only local IP fields are **N/A** for server; Global IP fields MUST be set for **Server**.
Start	This is the starting local IP address (ILA).
End	This is the ending local IP address (ILA). If the rule is for all local IPs, then put the Start IP as 0.0.0.0 and the End IP as 255.255.255.255. This field is **N/A** for One-to-One and Server types.
Global IP	
Start	This is the starting inside global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global IP Start**. **Note:** Note that **Global IP Start** can be set to 0.0.0.0 only if the types are **Many-to-One** or **Server.**
End	This is the ending inside global IP address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server types**.
Server Mapping Set	Only available when **Type** is set to **Server**. Type a number from 1 to 10 to choose a server set from menu 15.2.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

21.4 Configuring a Server behind NAT

Follow these steps to configure a server behind NAT:

1. Enter 15 in the main menu to go to **Menu 15 - NAT Setup**.
2. Enter 2 to display **Menu 15.2 - NAT Server Sets** as shown next.

Figure 99 Menu 15.2 NAT Server Setup

```
            Menu 15.2 - NAT Server Sets

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

                     Enter Set Number to Edit:
```

3 Enter 1 to go to **Menu 15.2.1 NAT Server Setup** as follows.

Figure 100 Menu 15.2.1 NAT Server Setup

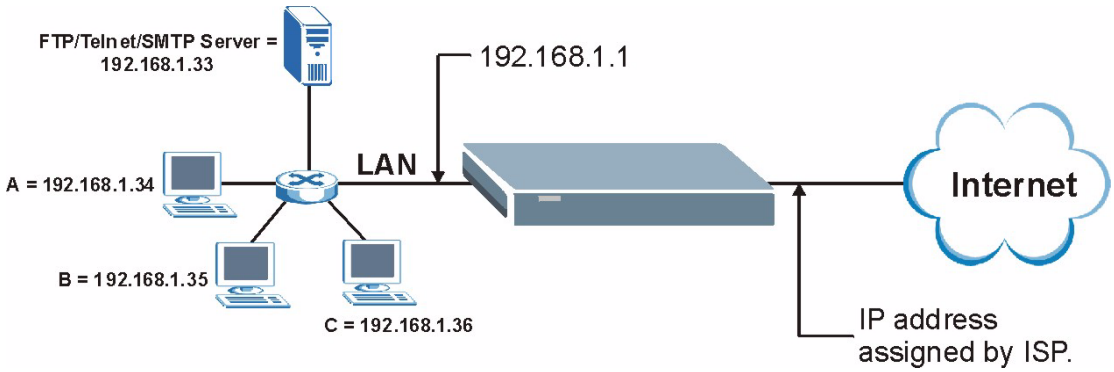
```
                Menu 15.2 - NAT Server Setup
     Rule   Start Port No.   End Port No.   IP Address
    ------------------------------------------------
       1.    Default          Default        0.0.0.0
       2.      21               21           192.168.1.33
       3.      0                0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

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

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

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

6 Press [ENTER] at the "`Press ENTER to confirm ...`" prompt to save your configuration after you define all the servers or press [ESC] at any time to cancel.

Figure 101 Multiple Servers Behind NAT Example



21.5 General NAT Examples

The following are some examples of NAT configuration.

21.5.1 Example 1: Internet Access Only

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

Figure 102 NAT Example 1

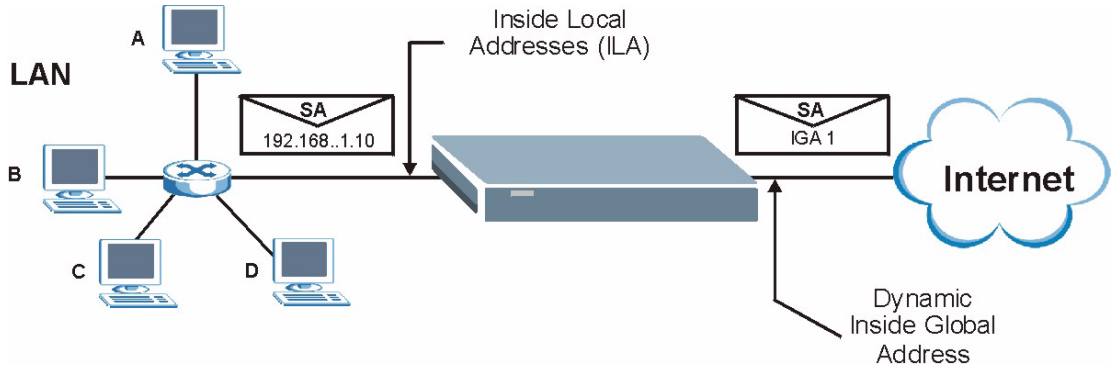


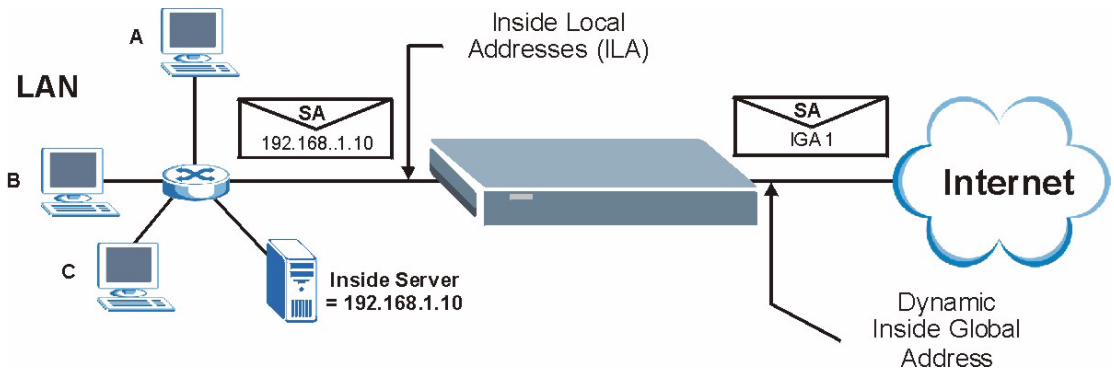
Figure 103 Menu 4 Internet Access & NAT Example

```
                Menu 4 - Internet Access Setup
ISP's Name= MyISP
Encapsulation= RFC 1483
Multiplexing= LLC-based
VPI #= 8
VCI #= 35
ATM QoS Type= UBR
  Peak Cell Rate (PCR)= 0
  Sustain Cell Rate (SCR)= 0
  Maximum Burst Size (MBS)= 0
My Login= N/A
My Password= N/A
ENET ENCAP Gateway= N/A
IP Address Assignment= Static
  IP Address= 0.0.0.0
Network Address Translation= SUA Only
  Address Mapping Set= N/A

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

From menu 4, choose the **SUA Only** option from the **Network Address Translation** field. This is the **Many-to-One** mapping discussed in the General NAT Examples section. The **SUA Only** read-only option from the **Network Address Translation** field in menus 4 and 11.3 is specifically pre-configured to handle this case.

21.5.2 Example 2: Internet Access with an Inside Server

Figure 104 NAT Example 2



In this case, you do exactly as above (use the convenient pre-configured **SUA Only** set) and also go to menu 15.2 to specify the inside server behind the NAT as shown in the next figure.

Figure 105 Menu 15.2.1 Specifying an Inside Server

```
            Menu 15.2.1 - NAT Server Setup (Used for SUA Only)

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

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

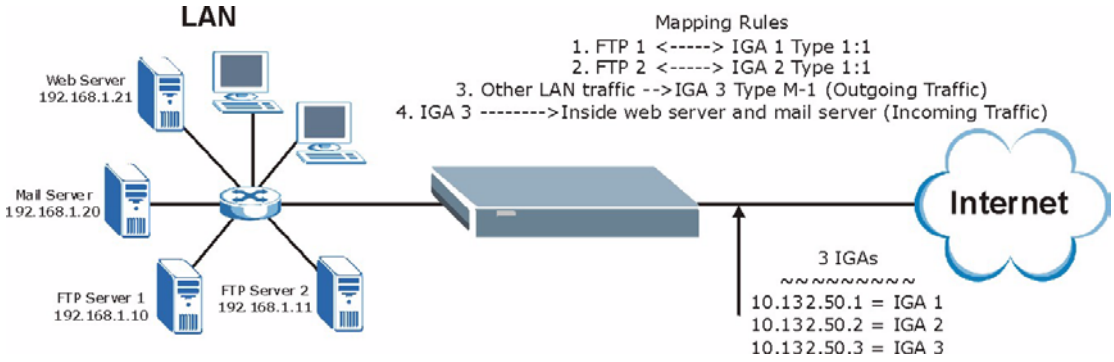
21.5.3 Example 3: Multiple Public IP Addresses With Inside Servers

In this example, there are 3 IGAs from our ISP. There are many departments but two have their own FTP server. All departments share the same router. The example will reserve one IGA for each department with an FTP server and all departments use the other IGA. Map the FTP servers to the first two IGAs and the other LAN traffic to the remaining IGA. Map the third IGA to an inside web server and mail server. Four rules need to be configured, two bi-directional and two unidirectional as follows.

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

The example situation looks somewhat like this:

Figure 106 NAT Example 3



In this case you need to configure **Address Mapping Set 1** from **Menu 15.1 - Address Mapping Sets**. Therefore you must choose the **Full Feature** option from the **Network Address Translation** field (in menu 4 or menu 11.3) in Figure 107.

1. Enter 15 from the main menu.
2. Enter 1 to configure the **Address Mapping Sets**.
3. Enter 1 to begin configuring this new set. Enter a Set Name, choose the **Edit Action** and then enter 1 for the **Select Rule** field. Press [ENTER] to confirm.
4. Select **Type** as **One-to-One** (direct mapping for packets going both ways), and enter the local **Start IP** as 192.168.1.10 (the IP address of FTP Server 1), the global **Start IP** as 10.132.50.1 (our first IGA). (See Figure 108).
5. Repeat the previous step for rules 2 to 4 as outlined above.

When finished, menu 15.1.1 should look like as shown in Figure 109.

Figure 107 Example 3: Menu 11.3

```
            Menu 11.3 - Remote Node Network Layer Options
IP Options:                          Bridge Options:
  IP Address Assignment= Static        Ethernet Addr Timeout (min)= 0
  Rem IP Addr: 0.0.0.0
  Rem Subnet Mask= 0.0.0.0
  My WAN Addr= 0.0.0.0
  NAT= Full Feature
    Address Mapping Set= 2
  Metric= 2
  Private= No
  RIP Direction= Both
    Version= RIP-2B
  Multicast= IGMP-v2
  IP Policies=

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

The following figures show how to configure the first rule

Figure 108 Example 3: Menu 15.1.1.1

```
            Menu 15.1.1.1 Address Mapping Rule

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

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

Figure 109 Example 3: Final Menu 15.1.1

```
                Menu 15.1.1 - Address Mapping Rules

 Set Name= Example3
 Idx  Local Start IP  Local End IP    Global Start IP  Global End IP   Type
 ---  --------------  --------------  ---------------  --------------  -----
  1. 192.168.1.10                     10.132.50.1                      1-1
  2  192.168.1.11                     10.132.50.2                      1-1
  3. 0.0.0.0          255.255.255.255  10.132.50.3                     M-1
  4.                                  10.132.50.3                    Server
  5.
  6.
  7.
  8.
  9.
 10.

Action= Edit          Select Rule=
Press ENTER to Confirm or ESC to Cancel:
```

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

1. Enter 15 from the main menu.
2. Enter 2 in **Menu 15 - NAT Setup**.
3. Enter 1 in **Menu 15.2 - NAT Server Sets** to see the following menu. Configure it as shown.

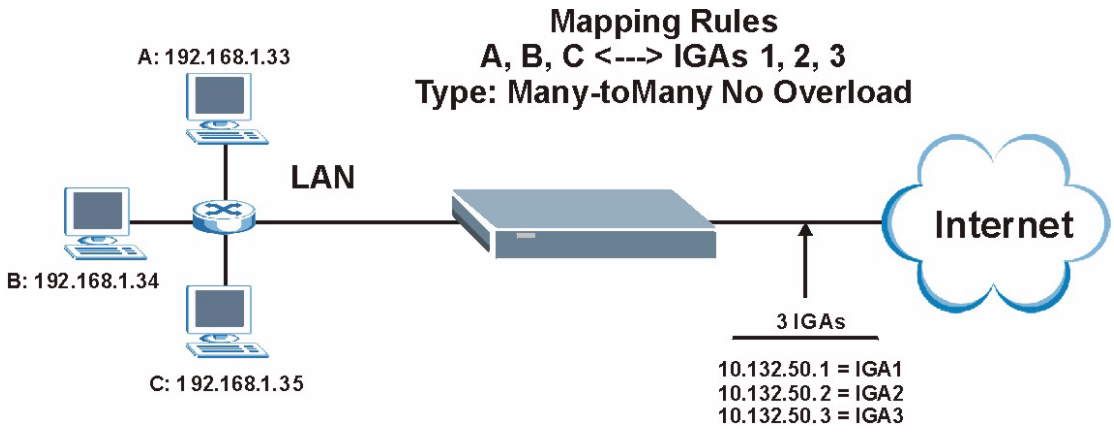
Figure 110 Example 3: Menu 15.2.1

```
          Menu 15.2.1 - NAT Server Setup
Rule   Start Port No.   End Port No.   IP Address
-------------------------------------------------
  1.     Default          Default        0.0.0.0
  2.       80               80           192.168.1.21
  3.       25               25           192.168.1.20
  4.       0                0            0.0.0.0
  5.       0                0            0.0.0.0
  6.       0                0            0.0.0.0
  7.       0                0            0.0.0.0
  8.       0                0            0.0.0.0
  9.       0                0            0.0.0.0
 10.       0                0            0.0.0.0
 11.       0                0            0.0.0.0
 12.       0                0            0.0.0.0

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

21.5.4 Example 4: NAT Unfriendly Application Programs

Some applications do not support NAT Mapping using TCP or UDP port address translation. In this case it is better to use **Many-to-Many No Overload** mapping as port numbers do *not* change for **Many-to-Many No Overload** (and **One-to-One**) NAT mapping types. The following figure illustrates this.

Figure 111 NAT Example 4



Other applications such as some gaming programs are NAT unfriendly because they embed addressing information in the data stream. These applications won't work through NAT even when using **One-to-One** and **Many-to-Many No Overload** mapping types.

Follow the steps outlined in example 3 to configure these two menus as follows.

Figure 112 Example 4: Menu 15.1.1.1 Address Mapping Rule

```
            Menu 15.1.1.1 Address Mapping Rule

                 Type= Many-to-Many No Overload
                 Local IP:
                   Start= 192.168.1.10
                   End  = 192.168.1.12
                 Global IP:
                   Start= 10.132.50.1
                   End  = 10.132.50.3
                 Server Mapping Set= N/A

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

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

Figure 113 Example 4: Menu 15.1.1 Address Mapping Rules

```
                  Menu 15.1.1 - Address Mapping Rules

 Set Name= Example4
Idx  Local Start IP   Local End IP    Global Start IP  Global End IP  Type
---  ---------------  --------------  ---------------  -------------  ---
 1.  192.168.1.10     192.168.1.12    10.132.50.1      10.132.50.3 M:M NO OV
 2.
 3.
 4.
 5.
 6.
 7.
 8.
 9.
10.

                  Action= Edit          Select Rule=
Press ENTER to Confirm or ESC to Cancel:
```

CHAPTER 22
Filter Configuration

This chapter shows you how to create and apply filters.

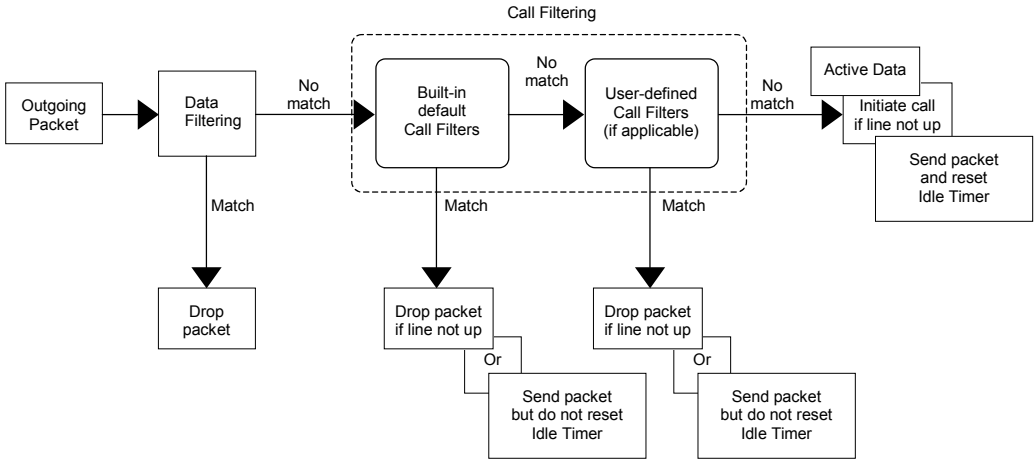
22.1 About Filtering

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

Data filtering screens data to determine if the packet should be allowed to pass. Data filters are divided into incoming and outgoing filters, depending on the direction of the packet relative to a port. Data filtering can be applied on either the WAN side or the Ethernet side. Call filtering is used to determine if a packet should be allowed to trigger a call.

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

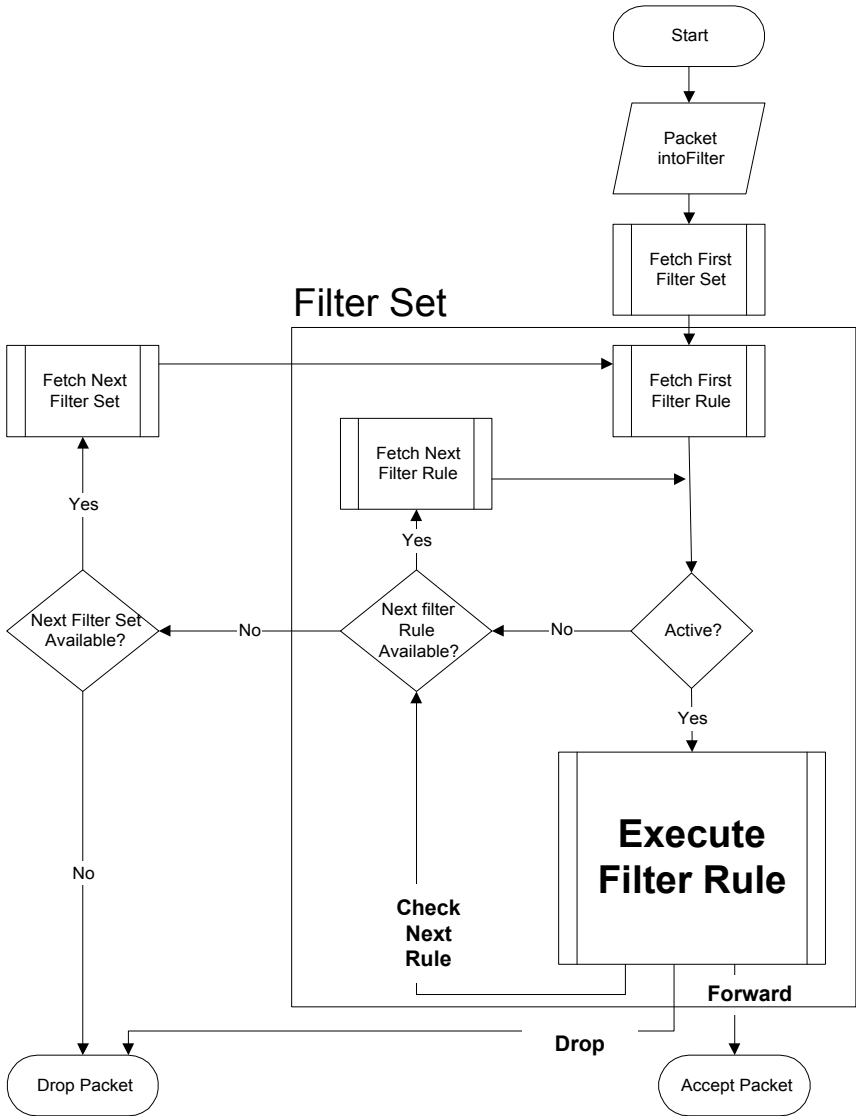
Figure 114 Outgoing Packet Filtering Process



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

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

Figure 115 Filter Rule Process



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

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

22.1.1 The Filter Structure of the Prestige

A filter set consists of one or more filter rules. Usually, you would group related rules, for example, all the rules for NetBIOS, into a single set and give it a descriptive name. You can configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system.

22.2 Configuring a Filter Set for the Prestige

To configure a filter set, follow the steps shown next.

1 Enter 21 in the main menu to display **Menu 21 – Filter Set Configuration** as shown next.

Figure 116 Menu 21 Filter Set Configuration

```
                  Menu 21 - Filter Set Configuration

Filter                                Filter
Set #        Comments                 Set #        Comments

------  -----------------            ------  -----------------
  1      _________________             7      _________________
  2      NetBIOS_WAN                   8      _________________
  3      NetBIOS_LAN                   9      _________________
  4      _________________            10      _________________
  5      _________________            11      WebSet1
  6      _________________            12      WebSet2



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

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

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

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

Figure 117 NetBIOS_WAN Filter Rules Summary

```
            Menu 21.2 - Filter Rules Summary

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

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

Figure 118 NetBIOS_LAN Filter Rules Summary

```
             Menu 21.1.3 - Filter Rules Summary

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

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

22.3 Filter Rules Summary Menus

The following tables briefly describe the abbreviations used in menus 21.1.1 and 21.1.2.

Table 51 Abbreviations Used in the Filter Rules Summary Menu

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

The protocol dependent filter rules abbreviation are listed as follows:

Table 52 Rule Abbreviations Used

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

22.4 Configuring a Filter Rule

To configure a filter rule, type its number in **Menu 21.x – Filter Rules Summary** and press [ENTER] to open menu 21.x.1 for the rule.

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

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

22.4.1 TCP/IP Filter Rule

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

To configure TCP/IP rules, select TCP/IP Filter Rule from the **Filter Type** field and press [ENTER] to open **Menu 21.x.1 – TCP/IP Filter Rule**, as shown next.

Figure 119 Menu 21.x.1 TCP/IP Filter Rule

```
                    Menu 21.1.1 - TCP/IP Filter Rule

                Filter #: 1,1
                Filter Type= TCP/IP Filter Rule
                Active= No
                IP Protocol= 0     IP Source Route= No
                Destination: IP Addr=
                             IP Mask=
                             Port #=
                             Port # Comp= None
                     Source: IP Addr=
                             IP Mask=
                             Port #=
                             Port # Comp= None
                TCP Estab= N/A
                More= No           Log= None
                Action Matched= Check Next Rule
                Action Not Matched= Check Next Rule

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

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

Table 53 Menu 21.x.1 TCP/IP Filter Rule

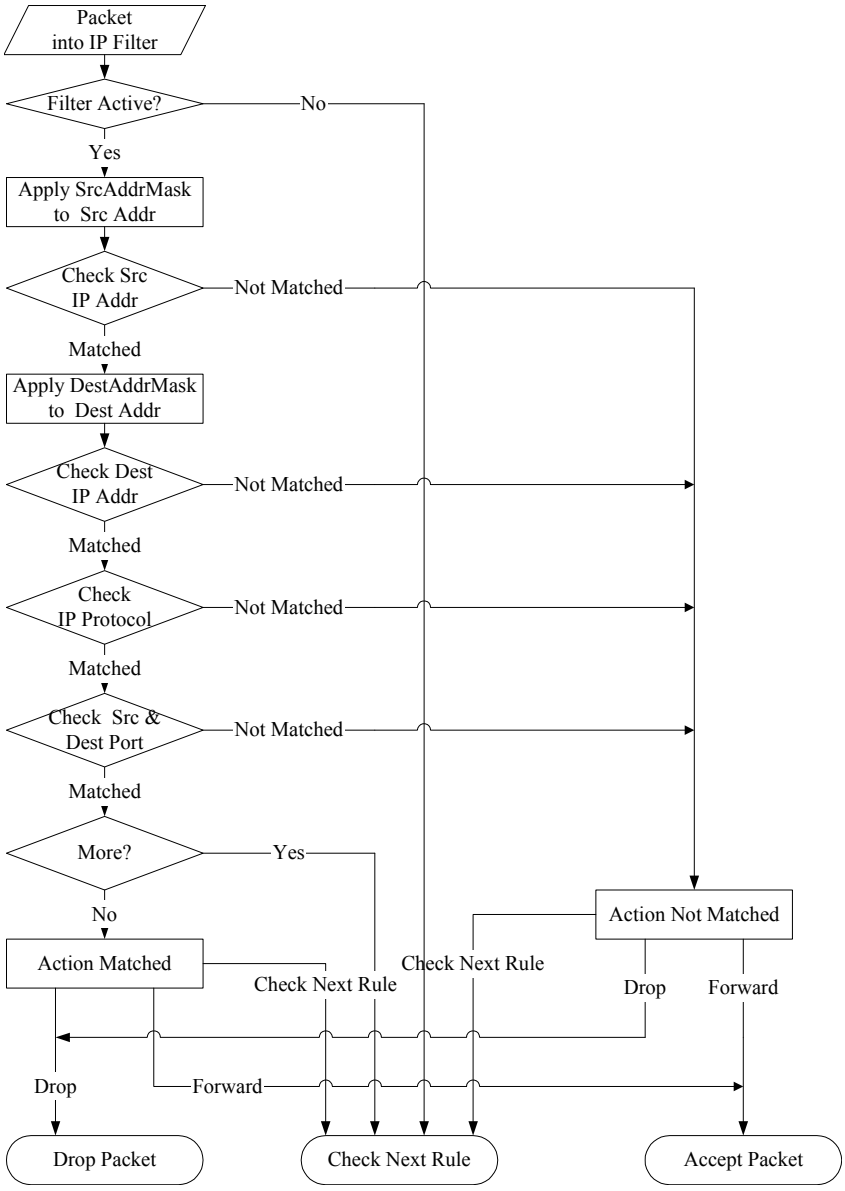
FIELD	DESCRIPTION
Filter #	This is the filter set, filter rule coordinates, for instance, 2, 3 refers to the second filter set and the third filter rule of that set.
Filter Type	Use [SPACE BAR] and then [ENTER] to choose a rule. Parameters displayed for each type will be different. Choices are **TCP/IP Filter Rule** or **Generic Filter Rule**.
Active	Select **Yes** to activate or **No** to deactivate the filter rule.
IP Protocol	This is the upper layer protocol, for example, TCP is 6, UDP is 17 and ICMP is 1. The value must be between 0 and 255. A value of 0 matches ANY protocol.
IP Source Route	IP Source Route is an optional header that dictates the route an IP packet takes from its source to its destination. If **Yes**, the rule applies to any packet with an IP source route. The majority of IP packets do not have source route.
Destination:	
IP Addr	Type the destination IP address of the packet you want to filter. This field is ignored if it is 0.0.0.0.
IP Mask	Type the IP mask to apply to the **Destination: IP Addr** field.
Port #	Type the destination port of the packets you want to filter. The field range is 0 to 65535. A 0 field is ignored.
Port # Comp	Select the comparison to apply to the destination port in the packet against the value given in **Destination: Port #.** Choices are **None**, **Less**, **Greater**, **Equal** or **Not Equal**.
Source:	
IP Addr	Type the source IP Address of the packet you want to filter. A 0.0.0.0 field is ignored.
IP Mask	Type the IP mask to apply to the **Source: IP Addr** field.

Table 53 Menu 21.x.1 TCP/IP Filter Rule (continued)

FIELD	DESCRIPTION
Port #	Type the source port of the packets you want to filter. The range of this field is 0 to 65535. A 0 field is ignored.
Port # Comp	Select the comparison to apply to the source port in the packet against the value given in **Source: Port #** field. Choices are **None**, **Less**, **Greater**, **Equal** or **Not Equal**.
TCP Estab	This applies only when the IP Protocol field is 6, TCP. If **Yes**, the rule matches packets that want to establish TCP connection(s) (SYN=1 and ACK=0); else it is ignored.
More	If **Yes**, a matching packet is passed to the next filter rule before an action is taken or else the packet is disposed of according to the action fields. If **More** is **Yes**, then **Action Matched** and **Action Not Matched** will be N/A.
Log	Select the logging option from the following: **None** – No packets will be logged. **Action Matched** – Only packets that match the rule parameters will be logged. **Action Not Matched** – Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.
Action Matched	Select the action for a matching packet. Choices are **Check Next Rule**, **Forward** or **Drop**.
Action Not Matched	Select the action for a packet not matching the rule. Choices are **Check Next Rule**, **Forward** or **Drop**.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

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

Figure 120 Executing an IP Filter



22.4.2 Generic Filter Rule

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

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

To configure a generic rule select an empty filter set in menu 21, for example 5. Select **Generic Filter Rule** in the **Filter Type** field and press [ENTER] to open **Menu 21.5.1 – Generic Filter Rule**, as shown in the following figure.

Figure 121 Menu 21.5.1 Generic Filter Rule

```
Menu 21.5.1 - Generic Filter Rule

Filter #: 5,1
Filter Type= Generic Filter Rule
Active= No
Offset= 0
Length= 0
Mask= N/A
Value= N/A
More= No            Log= None
Action Matched= Check Next Rule
Action Not Matched= Check Next Rule

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

The next table describes the fields in the **Generic Filter Rule** menu.

Table 54 Menu 21.1.5.1 Generic Filter Rule

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

Table 54 Menu 21.1.5.1 Generic Filter Rule (continued)

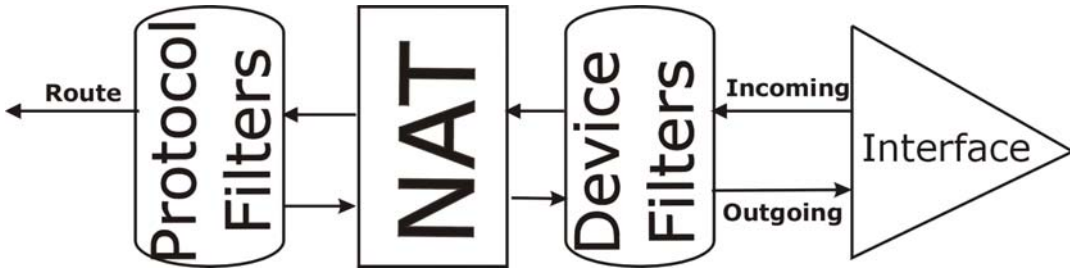
FIELD	DESCRIPTION
Action Not Matched	Select the action for a packet not matching the rule. Choices are **Check Next Rule**, **Forward** or **Drop**.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

22.5 Filter Types and NAT

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

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

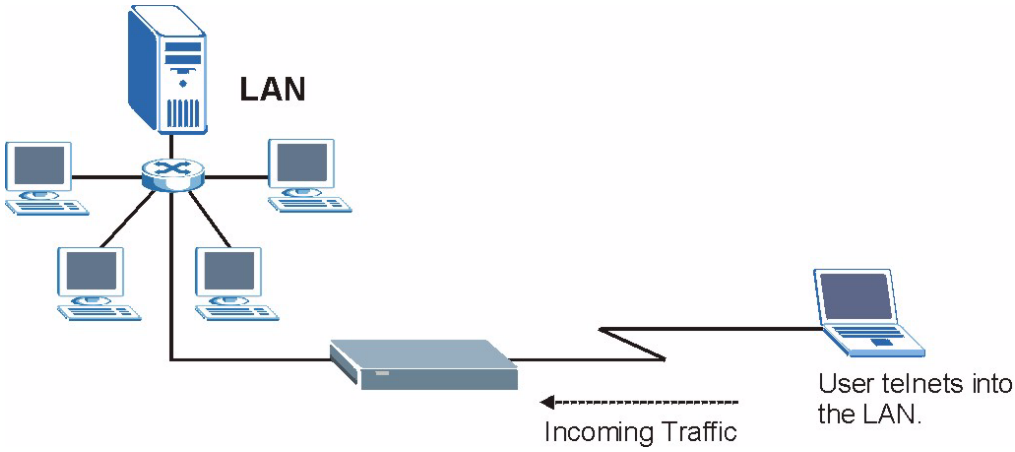
Figure 122 Protocol and Device Filter Sets



22.6 Example Filter

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

Figure 123 Sample Telnet Filter



1. Enter 21 in the main menu to display **Menu 21 — Filter Set Configuration**.
2. Enter the index number of the filter set you want to configure (in this case 6).
3. Type a descriptive name or comment in the **Edit Comments** field (for example, TELNET_WAN) and press [ENTER].
4. Press [ENTER] at the message "`Press [ENTER] to confirm or [ESC] to cancel ...`" to open **Menu 21.6 — Filter Rules Summary**.
5. Type 1 to configure the first filter rule. Make the entries in this menu as shown next.

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

Figure 124 Menu 21.6.1 Sample Filter

```
            Menu 21.6.1 - TCP/IP Filter Rule

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

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

Figure 125 Menu 21.6.1 Sample Filter Rules Summary

```
            Menu 21.1.6 - Filter Rules Summary

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



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

This shows you that you have configured and activated (**A = Y**) a TCP/IP filter rule (**Type = IP**, **Pr = 6**) for destination telnet ports (**DP = 23**).

M = N means an action can be taken immediately. The action is to drop the packet (**m = D**) if the action is matched and to forward the packet immediately (**n = F**) if the action is not matched no matter whether there are more rules to be checked (there aren't in this example).

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

1. Enter 11 in the main menu to display menu 11 and type the remote node number to edit.
2. Go to the **Edit Filter Sets** field, press [SPACE BAR] to choose **Yes** and press [ENTER].
3. This brings you to menu 11.5. Apply the example filter set (for example, filter set 3) in this menu as shown in the next section.

22.7 Applying Filters and Factory Defaults

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

Table 55 Filter Sets Table

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

22.7.1 Ethernet Traffic

You seldom need to filter Ethernet traffic; however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 3.1 (shown next) and type the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by typing their numbers separated by commas, for example, 3, 4, 6, 11. The factory default filter set, `NetBIOS_LAN`, is inserted in the **protocol filters** field under **Input Filter Sets** in menu 3.1 in order to prevent local NetBIOS messages from triggering calls to the DNS server.

Figure 126 Filtering Ethernet Traffic

```
Menu 3.1 - LAN Port Filter Setup


Input Filter Sets:
protocol filters= 3
device filters=
Output Filter Sets:
protocol filters=
device filters=


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

Apply filter 3 to block NETBIOS traffic from the LAN.

22.7.2 Remote Node Filters

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

Figure 127 Filtering Remote Node Traffic

```
            Menu 11.5 - Remote Node Filter

                      Input Filter Sets:
                        protocol filters= 6
                        device filters=
                      Output Filter Sets:
                        protocol filters= 2
                        device filters=
                      Call Filter Sets:
                        Protocol filters=
                        Device filters=


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

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

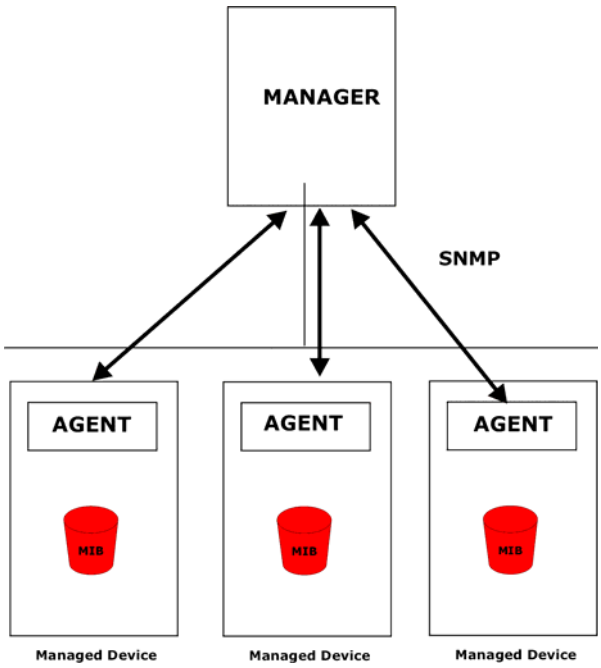
CHAPTER 23
SNMP Configuration

This chapter explains SNMP Configuration menu 22.

23.1 About SNMP

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

Figure 128 SNMP Management Model



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

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

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

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

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

23.2 Supported MIBs

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

23.3 SNMP Configuration

To configure SNMP, select option 22 from the main menu to open **Menu 22 — SNMP Configuration** as shown next. The "community" for Get, Set and Trap fields is SNMP terminology for password.

Figure 129 Menu 22 SNMP Configuration

```
Menu 22 - SNMP Configuration

SNMP:
  Get Community= public
  Set Community= public
  Trusted Host= 0.0.0.0
  Trap:
    Community= public
    Destination= 0.0.0.0

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

The following table describes the SNMP configuration parameters.

Table 56 Menu 22 SNMP Configuration

FIELD	DESCRIPTION
SNMP:	
Get Community	Type the **Get Community**, which is the password for the incoming Get- and GetNext requests from the management station.
Set Community	Type the **Set** community, which is the password for incoming Set requests from the management station.
Trusted Host	If you enter a trusted host, your Prestige will only respond to SNMP messages from this address. A blank (default) field means your Prestige will respond to all SNMP messages it receives, regardless of source.
Trap:	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager.
Destination	Type the IP address of the station to send your SNMP traps to.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

23.4 SNMP Traps

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

Table 57 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
1	coldStart (*defined in RFC-1215*)	A trap is sent after booting (power on).
2	warmStart (*defined in RFC-1215*)	A trap is sent after booting (software reboot).
3	linkDown (*defined in RFC-1215*)	A trap is sent with the port number when any of the links are down. See the following table.
4	linkUp (*defined in RFC-1215*)	A trap is sent with the port number.
5	authenticationFailure (*defined in RFC-1215*)	A trap is sent to the manager when receiving any SNMP gets or sets requirements with wrong community (password).
6	whyReboot (defined in ZYXEL-MIB)	A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start).
6a	For intentional reboot :	A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (for example, download new files, CI command "sys reboot", etc.).

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

Table 58 Ports and Permanent Virtual Circuits

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

CHAPTER 24
System Information and Diagnosis

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

24.1 Overview

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

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

Figure 130 Menu 24 System Maintenance

```
Menu 24 - System Maintenance

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

Enter Menu Selection Number:
```

24.2 System Status

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

To get to System Status, type 24 to go to **Menu 24 — System Maintenance.** From this menu, type 1**. System Status**. There are two commands in **Menu 24.1 — System Maintenance — Status**. Entering 1 resets the counters; [ESC] takes you back to the previous screen.

The following table describes the fields present in **Menu 24.1 — System Maintenance — Status** which are read-only and meant for diagnostic purposes.

Figure 131 Menu 24.1 System Maintenance : Status

```
                  Menu 24.1 - System Maintenance - Status          03:05:59
                                                          Sat. Jan. 01, 2000

Node-Lnk Status      TxPkts      RxPkts      Errors  Tx B/s  Rx B/s    Up Time
 1-PPPoE Idle             0           0           0       0       0     0:00:00
 2       N/A              0           0           0       0       0     0:00:00
 3       N/A              0           0           0       0       0     0:00:00
 4       N/A              0           0           0       0       0     0:00:00
 5       N/A              0           0           0       0       0     0:00:00
 6       N/A              0           0           0       0       0     0:00:00
 7       N/A              0           0           0       0       0     0:00:00
 8       N/A              0           0           0       0       0     0:00:00

My WAN IP (from ISP): 0.0.0.0

    Ethernet:                                       WAN:
      Status: 100M/Full Duplex Tx Pkts: 23216       Line Status: Down
      Collisions: 0           Rx Pkts: 23740      Upstream Speed:     0 kbps
    CPU Load =    1.65%                         Downstream Speed:     0 kbps
                                  Press Command:
                       COMMANDS: 1-Reset Counters  ESC-Exit
```

The following table describes the fields present in **Menu 24.1 — System Maintenance — Status**.

Table 59 Menu 24.1 System Maintenance : Status

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

Table 59 Menu 24.1 System Maintenance : Status (continued)

FIELD	DESCRIPTION
WAN	This shows statistics for the WAN.
Line Status	This shows the current status of the xDSL line, which can be **Up** or **Down**.
Upstream Speed	This shows the upstream transfer rate in kbps.
Downstream Speed	This shows the downstream transfer rate in kbps.
CPU Load	This specifies the percentage of CPU utilization.

24.3 System Information

To get to the System Information:

1. Enter 24 to display **Menu 24 — System Maintenance**.
2. Enter 2 to display **Menu 24.2 — System Information and Console Port Speed**.

From this menu you have two choices as shown in the next figure:

Figure 132 Menu 24.2 System Information and Console Port Speed

```
Menu 24.2 - System Information and Console Port Speed

1. System Information
2. Console Port Speed

Please enter selection:
```

Note: The Prestige has an internal console port for support personnel only. Do not open the Prestige as it will void your warranty.

24.3.1 System Information

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

Figure 133 Menu 24.2.1 System Maintenance: Information

```
                Menu 24.2.1 - System Maintenance - Information

          Name:
          Routing: IP
          ZyNOS F/W Version: V3.40(UF.0)b1 | 9/28/2004
          ADSL Chipset Vendor: TI AR7 01.01.08.00
          Standard: ADSL_G.dmt

          LAN
            Ethernet Address: 00:a0:c5:01:23:45
            IP Address: 192.168.1.1
            IP Mask: 255.255.255.0
            DHCP: Server

                Press ESC or RETURN to Exit:
```

The following table describes the fields in this menu.

Table 60 Menu 24.2.1 System Maintenance: Information

FIELD	DESCRIPTION
Name	Displays the system name of your Prestige. This information can be changed in **Menu 1 – General Setup**.
Routing	Refers to the routing protocol used.
ZyNOS F/W Version	Refers to the ZyNOS (ZyXEL Network Operating System) system firmware version. ZyNOS is a registered trademark of ZyXEL Communications Corporation.
ADSL Chipset Vendor	Displays the vendor of the ADSL chipset and DSL version.
Standard	This refers to the operational protocol the Prestige and the DSLAM (Digital Subscriber Line Access Multiplexer) are using.
LAN	
Ethernet Address	Refers to the Ethernet MAC (Media Access Control) of your Prestige.
IP Address	This is the IP address of the Prestige in dotted decimal notation.
IP Mask	This shows the subnet mask of the Prestige.
DHCP	This field shows the DHCP setting (None, Relay or Server) of the Prestige.

24.3.2 Console Port Speed

You can set up different port speeds for the console port through **Menu 24.2.2 – System Maintenance – Console Port Speed**. Your Prestige supports 9600 (default), 19200, 38400, 57600 and 115200 bps. Press [SPACE BAR] and then [ENTER] to select the desired speed in menu 24.2.2, as shown in the following figure.

Figure 134 Menu 24.2.2 System Maintenance : Change Console Port Speed

```
            Menu 24.2.2 - System Maintenance - Change Console Port Speed

                      Console Port Speed: 9600

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

24.4 Log and Trace

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

24.4.1 Viewing Error Log

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

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

Figure 135 Menu 24.3 System Maintenance: Log and Trace

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

                   1. View Error Log
                   2. UNIX Syslog


            Please enter selection
```

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

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

Figure 136 Sample Error and Information Messages

```
  57 Sat Jan 01 02:41:48 2000 PP0a  WARN  Last errorlog repeat 1 Times
  58 Sat Jan 01 02:41:48 2000 PP0a -WARN  SNMP TRAP 3: link up
  59 Sat Jan 01 02:41:49 2000 PP10  WARN  netMakeChannDial: err=-3001
rn_p=94451 bc0
  60 Sat Jan 01 02:43:33 2000 PP12  WARN  Last errorlog repeat 14 Times
  61 Sat Jan 01 02:43:33 2000 PP12  INFO  SMT Password pass
  62 Sat Jan 01 02:43:33 2000 PP01  INFO  SMT Session Begin
  63 Sat Jan 01 02:44:29 2000 PP10  WARN  netMakeChannDial: err=-3001
rn_p=94451 bc0
Clear Error Log (y/n):
```

24.4.2 Syslog and Accounting

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

Figure 137 Menu 24.3.2 System Maintenance: Syslog and Accounting

```
              Menu 24.3.2 - System Maintenance - UNIX Syslog

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

                     Types:
                       CDR= No
                       Packet Triggered= No
                       Filter Log= No
                       PPP Log= No

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

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

Table 61 Menu 24.3.2 System Maintenance : Syslog and Accounting

PARAMETER	DESCRIPTION
UNIX Syslog:	
Active	Use [SPACE BAR] and then [ENTER] to turn syslog on or off.
Syslog IP Address	Type the IP address of your syslog server.
Log Facility	Use [SPACE BAR] and then [ENTER] to select one of seven different local options. The log facility lets you log the message in different server files. Refer to your UNIX manual.
Types:	
CDR	Call Detail Record (CDR) logs all data phone line activity if set to **Yes**.

Table 61 Menu 24.3.2 System Maintenance : Syslog and Accounting

PARAMETER	DESCRIPTION
Packet Triggered	The first 48 bytes or octets and protocol type of the triggering packet is sent to the UNIX syslog server when this field is set to **Yes**.
Filter Log	No filters are logged when this field is set to **No**. Filters with the individual filter **Log** field set to **Yes** are logged when this field is set to **Yes**.
PPP Log	PPP events are logged when this field is set to **Yes**.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

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

Figure 138 Syslog Example

```
1 - CDR

SdcmdSyslogSend ( SYSLOG_CDR, SYSLOG_INFO, String);

String = board xx line xx channel xx, call xx, str

board = the hardware board ID

line = the WAN ID in a board

Channel = channel ID within the WAN

call = the call reference number which starts from 1 and increments by 1 for each new
call

str = C01 Outgoing Call dev xx ch xx (dev:device No. ch:channel No.)

C01 Incoming Call xxxxBps xxxxx (L2TP, xxxxx = Remote Call ID)

C01 Incoming Call xxxx (= connected speed) xxxxx (= Remote Call ID)

L02 Tunnel Connected (L2TP)

C02 OutCall Connected xxxx (= connected speed) xxxxx (= Remote Call ID)

C02 CLID call refused

L02 Call Terminated

C02 Call Terminated

Jul 19 11:19:27 192.168.102.2 ZYXEL: board 0 line 0 channel 0, call 1, C01 Outgoing
Call dev=2 ch=0 40002
Jul 19 11:19:32 192.168.102.2 ZYXEL: board 0 line 0 channel 0, call 1, C02 OutCall
Connected 64000 40002
Jul 19 11:20:06 192.168.102.2 ZYXEL: board 0 line 0 channel 0, call 1, C02 Call
Terminated

2 - Packet Triggered

SdcmdSyslogSend (SYSLOG_PKTTRI, SYSLOG_NOTICE, String);

String = Packet trigger: Protocol=xx Data=xxxxxxxxxx…..x

Protocol: (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG)

Data: We will send forty-eight Hex characters to the server
```

Figure 138 Syslog Example (continued)

```
Jul 19 11:28:39 192.168.102.2 ZYXEL: Packet Trigger: Protocol=1,
Data=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a6b6c
6d6e6f7071727374
Jul 19 11:28:56 192.168.102.2 ZYXEL: Packet Trigger: Protocol=1,
Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600220008cd40000
020405b4
Jul 19 11:29:06 192.168.102.2 ZYXEL: Packet Trigger: Protocol=1,
Data=45000028240140001f06ac12c0a86614ca849a7b0427001700195b451d1430135004000077600000

3 - Filter Log

SdcmdSyslogSend (SYSLOG_FILLOG, SYSLOG_NOTICE, String);

String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx] S04>R01mD

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

Src: Source Address

Dst: Destination Address

prot: Protocol ("TCP", "UDP", "ICMP")

spo: Source port

dpo: Destination port

Jul 19 14:43:55 192.168.102.2 ZYXEL: IP [Src=202.132.154.123 Dst=255.255.255.255 UDP
spo=0208 dpo=0208]} S03>R01mF
Jul 19 14:44:00 192.168.102.2 ZYXEL: IP [Src=192.168.102.20 Dst=202.132.154.1 UDP
spo=05d4 dpo=0035]} S03>R01mF
Jul 19 14:44:04 192.168.102.2 ZYXEL: IP [Src=192.168.102.20 Dst=202.132.154.1 UDP
spo=05d4 dpo=0035]} S03>R01mF

4 - PPP Log

SdcmdSyslogSend (SYSLOG_PPPLOG, SYSLOG_NOTICE, String);

String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto
Shutdown

Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP / IPXCP

Jul 19 11:42:44 192.168.102.2 ZYXEL: ppp:LCP Closing
Jul 19 11:42:49 192.168.102.2 ZYXEL: ppp:IPCP Closing
Jul 19 11:42:54 192.168.102.2 ZYXEL: ppp:CCP Closing
```

24.5 Diagnostic

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

Follow the procedure next to get to **Diagnostic**:

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

Figure 139 Menu 24.4 System Maintenance : Diagnostic

```
            Menu 24.4 - System Maintenance - Diagnostic

xDSL                                    System
  1.  Reset xDSL                          21. Reboot System
                                          22. Command Mode


TCP/IP
  12. Ping Host


             Enter Menu Selection Number:

             Host IP Address= N/A
```

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

Table 62 Menu 24.4 System Maintenance Menu: Diagnostic

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

CHAPTER 25
Firmware and Configuration File Maintenance

This chapter tells you how to backup and restore your configuration file as well as upload new firmware and configuration files.

25.1 Filename Conventions

The configuration file (often called the romfile or rom-0) contains the factory default settings in the menus such as password, DHCP Setup, TCP/IP Setup, etc. It arrives from ZyXEL with a "rom" filename extension. Once you have customized the Prestige's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System sometimes referred to as the "ras" file) is the system firmware and has a "bin" filename extension. With many FTP and TFTP clients, the filenames are similar to those seen next.

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

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file " firmware.bin" to the Prestige.

```
ftp> get rom-0 config.cfg
```

This is a sample FTP session saving the current configuration to the computer file "`config.cfg`".

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the Prestige only recognizes "rom-0" and "ras". Be sure you keep unaltered copies of both files for later use.

The following table is a summary. Please note that the internal filename refers to the filename on the Prestige and the external filename refers to the filename not on the Prestige, that is, on your computer, local network or FTP site and so the name (but not the extension) may vary. After uploading new firmware, see the **ZyNOS F/W Version** field in **Menu 24.2.1 – System Maintenance – Information** to confirm that you have uploaded the correct firmware version. The AT command is the command you enter after you press "y" when prompted in the SMT menu to go into debug mode.

Table 63 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	Rom-0	This is the configuration filename on the Prestige. Uploading the rom-0 file replaces the entire ROM file system, including your Prestige configurations, system-related data (including the default password), the error log and the trace log.	*.rom
Firmware	Ras	This is the generic name for the ZyNOS firmware on the Prestige.	*.bin

25.2 Backup Configuration

Option 5 from **Menu 24 – System Maintenance** allows you to backup the current Prestige configuration to your computer. Backup is highly recommended once your Prestige is functioning properly. FTP is the preferred methods for backing up your current configuration to your computer since they are faster. Any serial communications program should work fine; however, you must use Xmodem protocol to perform the download/upload and you don't have to rename the files.

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

25.2.1 Backup Configuration

Follow the instructions as shown in the next screen.

Figure 140 Telnet in Menu 24.5

```
              Menu 24.5 - System Maintenance - Backup Configuration

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

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your Prestige. Then type "root" and SMT
password as requested.
3. Locate the 'rom-0' file.
4. Type 'get rom-0' to back up the current Prestige configuration to
   your workstation.
For details on FTP commands, please consult the documentation of your FTP
client program. For details on backup using TFTP (note that you must remain
in this menu to back up using TFTP), please see your Prestige manual.


              Press ENTER to Exit:
```

25.2.2 Using the FTP Command from the Command Line

1. Launch the FTP client on your computer.
2. Enter "`open`", followed by a space and the IP address of your Prestige.
3. Press [ENTER] when prompted for a username.
4. Enter your password as requested (the default is "1234").
5. Enter "`bin`" to set transfer mode to binary.
6. Use "`get`" to transfer files from the Prestige to the computer, for example, "`get rom-0 config.rom`" transfers the configuration file on the Prestige to your computer and renames it "`config.rom`". See earlier in this chapter for more information on filename conventions.
7. Enter "`quit`" to exit the ftp prompt.

25.2.3 Example of FTP Commands from the Command Line

Figure 141 FTP Session Example

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> get rom-0 zyxel.rom
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 16384 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

25.2.4 GUI-based FTP Clients

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

Table 64 General Commands for GUI-based FTP Clients

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

25.2.5 TFTP and FTP over WAN Management Limitations

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

- You have disabled Telnet service in menu 24.11.
- You have applied a filter in menu 3.1 (LAN) or in menu 11.5 (WAN) to block Telnet service.
- The IP address in the **Secured Client IP** field in menu 24.11 does not match the client IP. If it does not match, the Prestige will disconnect the Telnet session immediately.
- You have an SMT console session running.

25.2.6 Backup Configuration Using TFTP

The Prestige supports the up/downloading of the firmware and the configuration file using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To backup the configuration file, follow the procedure shown next.

1. Use telnet from your computer to connect to the Prestige and log in. Because TFTP does not have any security checks, the Prestige records the IP address of the telnet client and accepts TFTP requests only from this address.
2. Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
3. Enter command "`sys stdio 0`" to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command "`sys stdio 5`" to restore the five-minute SMT timeout (default) when the file transfer is complete.
4. Launch the TFTP client on your computer and connect to the Prestige. Set the transfer mode to binary before starting data transfer.
5. Use the TFTP client (see the example below) to transfer files between the Prestige and the computer. The file name for the configuration file is "`rom-0`" (rom-zero, not capital o).

Note that the telnet connection must be active and the SMT in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use "`get`" to transfer from the Prestige to the computer and "binary" to set binary transfer mode.

25.2.7 TFTP Command Example

The following is an example TFTP command:

```
tftp [-i] host get rom-0 config.rom
```

where "`i`" specifies binary image transfer mode (use this mode when transferring binary files), "`host`" is the Prestige IP address, "`get`" transfers the file source on the Prestige (`rom-0`, name of the configuration file on the Prestige) to the file destination on the computer and renames it config.rom.

25.2.8 GUI-based TFTP Clients

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

Table 65 General Commands for GUI-based TFTP Clients

COMMAND	DESCRIPTION
Host	Enter the IP address of the Prestige. 192.168.1.1 is the Prestige's default IP address when shipped.
Send/Fetch	Use "Send" to upload the file to the Prestige and "Fetch" to back up the file on your computer.
Local File	Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer.
Remote File	This is the filename on the Prestige. The filename for the firmware is "ras" and for the configuration file, is "rom-0".
Binary	Transfer the file in binary mode.
Abort	Stop transfer of the file.

Refer to the TFTP and FTP over WAN Management Limitations section to read about configurations that disallow TFTP and FTP over WAN.

25.3 Restore Configuration

This section shows you how to restore a previously saved configuration. Note that this function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

FTP is the preferred method for restoring your current computer configuration to your Prestige since FTP is faster. Please note that you must wait for the system to automatically restart after the file transfer is complete.

Note: Do not interrupt the file transfer process as this may permanently damage your Prestige.

25.3.1 Restore Using FTP

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

Figure 142 Telnet into Menu 24.6

```
              Menu 24.6 -- System Maintenance - Restore Configuration
To transfer the firmware and configuration file to your workstation, follow
the procedure below:

1. Launch the FTP client on your workstation.
2. Type "open" and the IP address of your Prestige. Then type "root" and SMT
password as requested.
3. Type "put backupfilename rom-0" where backupfilename is the name of
   your backup configuration file on your workstation and rom-0 is the
   remote file name on the Prestige. This restores the configuration   to
your Prestige.
4. The system reboots automatically after a successful file transfer

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


              Press ENTER to Exit:
```

1. Launch the FTP client on your computer.
2. Enter "`open`", followed by a space and the IP address of your Prestige.
3. Press [ENTER] when prompted for a username.
4. Enter your password as requested (the default is "1234").
5. Enter "`bin`" to set transfer mode to binary.
6. Find the "`rom`" file (on your computer) that you want to restore to your Prestige.
7. Use "`put`" to transfer files from the Prestige to the computer, for example, "`put config.rom rom-0`" transfers the configuration file "`config.rom`" on your computer to the Prestige. See earlier in this chapter for more information on filename conventions.
8. Enter "`quit`" to exit the ftp prompt. The Prestige will automatically restart after a successful restore process.

25.3.2 Restore Using FTP Session Example

Figure 143 Restore Using FTP Session Example

```
ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16384 bytes sent in 0.06Seconds 273.07Kbytes/sec.
ftp>quit
```

Refer to the TFTP and FTP over WAN Management Limitations section to read about configurations that disallow TFTP and FTP over WAN.

25.4 Uploading Firmware and Configuration Files

This section shows you how to upload firmware and configuration files. You can upload configuration files by following the procedure in the Backup Configuration section or by following the instructions in **Menu 24.7.2 – System Maintenance – Upload System Configuration File**.

> **Note:** Do not interrupt the file transfer process as this may permanently damage your Prestige.

25.4.1 Firmware File Upload

FTP is the preferred method for uploading the firmware and configuration. To use this feature, your computer must have an FTP client.

When you telnet into the Prestige, you will see the following screens for uploading firmware and the configuration file using FTP.

Figure 144 Telnet Into Menu 24.7.1 Upload System Firmware

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

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

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

              Press ENTER to Exit:
```

25.4.2 Configuration File Upload

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

Figure 145 Telnet Into Menu 24.7.2 System Maintenance

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

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

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

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


              Press ENTER to Exit:
```

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

25.4.3 FTP File Upload Command from the DOS Prompt Example

1. Launch the FTP client on your computer.
2. Enter "`open`", followed by a space and the IP address of your Prestige.
3. Press [ENTER] when prompted for a username.
4. Enter your password as requested (the default is "1234").
5. Enter "`bin`" to set transfer mode to binary.
6. Use "`put`" to transfer files from the computer to the Prestige, for example, "`put firmware.bin ras`" transfers the firmware on your computer (firmware.bin) to the Prestige and renames it "`ras`". Similarly, "`put config.rom rom-0`" transfers the configuration file on your computer (config.rom) to the Prestige and renames it "`rom-0`". Likewise "`get rom-0 config.rom`" transfers the configuration file on the Prestige to your computer and renames it "`config.rom`." See earlier in this chapter for more information on filename conventions.
7. Enter "`quit`" to exit the ftp prompt.

Note: The Prestige automatically restarts after a successful file upload.

25.4.4 FTP Session Example of Firmware File Upload

Figure 146 FTP Session Example of Firmware File Upload

```
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put firmware.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 1103936 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

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

Refer to the TFTP and FTP over WAN Management Limitations section to read about configurations that disallow TFTP and FTP over WAN.

25.4.5 TFTP File Upload

The Prestige also supports the uploading of firmware files using TFTP (Trivial File Transfer Protocol) over LAN. Although TFTP should work over WAN as well, it is not recommended.

To use TFTP, your computer must have both telnet and TFTP clients. To transfer the firmware and the configuration file, follow the procedure shown next.

1. Use telnet from your computer to connect to the Prestige and log in. Because TFTP does not have any security checks, the Prestige records the IP address of the telnet client and accepts TFTP requests only from this address.
2. Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.
3. Enter the command "`sys stdio 0`" to disable the console timeout, so the TFTP transfer will not be interrupted. Enter "`sys stdio 5`" to restore the five-minute console timeout (default) when the file transfer is complete.
4. Launch the TFTP client on your computer and connect to the Prestige. Set the transfer mode to binary before starting data transfer.
5. Use the TFTP client (see the example below) to transfer files between the Prestige and the computer. The file name for the firmware is "`ras`".

Note that the telnet connection must be active and the Prestige in CI mode before and during the TFTP transfer. For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use "`get`" to transfer from the Prestige to the computer, "`put`" the other way around, and "`binary`" to set binary transfer mode.

25.4.6 TFTP Upload Command Example

The following is an example TFTP command:

```
tftp [-i] host put firmware.bin ras
```

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

Commands that you may see in GUI-based TFTP clients are listed earlier in this chapter.

CHAPTER 26
System Maintenance

This chapter leads you through SMT menus 24.8 to 24.10.

26.1 Command Interpreter Mode

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

Figure 147 Command Mode in Menu 24

```
                Menu 24 - System Maintenance

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

             Enter Menu Selection Number:
```

Figure 148 Valid Commands

```
Copyright (c) 1994 - 2004 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys             exit            device          ether
wan             poe             ip              ppp
bridge          hdap            lan
ras>
```

26.2 Call Control Support

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

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

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

Figure 149 Menu 24.9 System Maintenance: Call Control

```
Menu 24.9 - System Maintenance - Call Control

1. Budget Management

Enter Menu Selection Number:
```

26.2.1 Budget Management

Menu 24.9.1 shows the budget management statistics for outgoing calls. Enter 1 from **Menu 24.9 — System Maintenance — Call Control** to bring up the following menu.

Figure 150 Menu 24.9.1 System Maintenance: Budget Management

```
          Menu 24.9.1 - System Maintenance - Budget Management

  Remote Node   Connection Time/Total Budget      Elapsed Time/Total Period
1.MyIsp                 No Budget                        No Budget
2.--------                ---                              ---
3.--------                ---                              ---
4.--------                ---                              ---
5.--------                ---                              ---
6.--------                ---                              ---
7.--------                ---                              ---
8.--------                ---                              ---

                    Reset Node (0 to update screen):
```

The total budget is the time limit on the accumulated time for outgoing calls to a remote node. When this limit is reached, the call will be dropped and further outgoing calls to that remote node will be blocked. After each period, the total budget is reset. The default for the total budget is 0 minutes and the period is 0 hours, meaning no budget control. You can reset the accumulated connection time in this menu by entering the index of a remote node. Enter 0 to update the screen. The budget and the reset period can be configured in menu 11.1 for the remote node when PPPoE encapsulation is selected.

Table 66 Menu 24.9.1 System Maintenance : Budget Management

FIELD	DESCRIPTION
Remote Node	Enter the index number of the remote node you want to reset (just one in this case)
Connection Time/Total Budget	This is the total connection time that has gone by (within the allocated budget that you set in menu 11.1.
Elapsed Time/Total Period	The period is the time cycle in hours that the allocation budget is reset (see menu 11.1.) The elapsed time is the time used up within this period.
Enter "0" to update the screen or press [ESC] to return to the previous screen.	

26.3 Time and Date Setting

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

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

Figure 151 Menu 24 System Maintenance

```
Menu 24 - System Maintenance

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

Enter Menu Selection Number:
```

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

Figure 152 Menu 24.10 System Maintenance: Time and Date Setting

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


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

      Current Time:                          03 : 10 : 50
      New Time (hh:mm:ss):                   03 : 10 : 43

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

      Time Zone= GMT

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

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

Table 67 Menu 24.10 System Maintenance: Time and Date Setting

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

26.3.1 Resetting the Time

The Prestige resets the time in three instances:

- On leaving menu 24.10 after making changes.
- When the Prestige starts up, if there is a timeserver configured in menu 24.10.
- 24-hour intervals after starting.

CHAPTER 27
Remote Management

This chapter covers remote management (SMT menu 24.11).

27.1 Remote Management Overview

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

27.2 Remote Management

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

Enter 11 from menu 24 to display **Menu 24.11 — Remote Management Control**.

27.2.1 Remote Management Setup

You may manage your Prestige from a remote location via:

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

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

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

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

Figure 153 Menu 24.11 Remote Management Control

```
            Menu 24.11 - Remote Management Control

TELNET Server:
  Server Port = 23                  Server Access = LAN only
  Secured Client IP = 0.0.0.0

FTP Server:
  Server Port = 21                  Server Access = LAN only
  Secured Client IP = 0.0.0.0

Web Server:
  Server Port = 80                  Server Access = LAN only
  Secured Client IP = 0.0.0.0

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

The following table describes the fields in this menu.

Table 68 Menu 24.11 Remote Management Control

FIELD	DESCRIPTION
Telnet Server FTP Server Web Server	Each of these read-only labels denotes a service or protocol.
Port	This field shows the port number for the service or protocol. You may change the port number if needed, but you must use the same port number to access the Prestige.
Access	Select the access interface (if any) by pressing the [SPACE BAR]. Choices are: **LAN only**, **WAN only**, **All** or **Disable**. The default is **LAN only**.
Secured Client IP	The default 0.0.0.0 allows any client to use this service or protocol to access the Prestige. Enter an IP address to restrict access to a client with a matching IP address.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

27.2.2 Remote Management Limitations

Remote management over LAN or WAN will not work when:

- A filter in menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
- You have disabled that service in menu 24.11.
- The IP address in the **Secured Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the Prestige will disconnect the session immediately.
- There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.

27.3 Remote Management and NAT

When NAT is enabled:

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

27.4 System Timeout

There is a default system management idle timeout of five minutes (three hundred seconds). The Prestige automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when it is continuously updating the status in menu 24.1 or when `sys stdio` has been changed on the command line.

CHAPTER 28
IP Policy Routing

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

28.1 IP Policy Routing Overview

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

28.2 Benefits of IP Policy Routing

Source-Based Routing – Network administrators can use policy-based routing to direct traffic from different users through different connections.

Quality of Service (QoS) – Organizations can differentiate traffic by setting the precedence or TOS (Type of Service) values in the IP header at the periphery of the network to enable the backbone to prioritize traffic.

Cost Savings – IPPR allows organizations to distribute interactive traffic on high-bandwidth, high-cost paths while using low-cost paths for batch traffic.

Load Sharing – Network administrators can use IPPR to distribute traffic among multiple paths.

28.3 Routing Policy

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

The actions that can be taken include:

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

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

28.4 IP Routing Policy Setup

Menu 25 shows all the policies defined.

Figure 154 Menu 25 IP Routing Policy Setup

```
                Menu 25 - IP Routing Policy Setup

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

             Enter Policy Set Number to Configure= 0

             Edit Name= N/A

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

To setup a routing policy, perform the following procedures:

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

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

Figure 155 Menu 25.1 IP Routing Policy Setup

```
                Menu 25.1 - IP Routing Policy Setup

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

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

Table 69 Menu 25.1 IP Routing Policy Setup

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

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

Figure 156 Menu 25.1.1 IP Routing Policy

```
                        Menu 25.1.1 - IP Routing Policy

          Policy Set Name= test
          Active= Yes
          Criteria:
            IP Protocol    = 6
            Type of Service= Normal         Packet length= 40
            Precedence     = 0               Len Comp= Not Equal
            Source:
              addr start= 1.1.1.1            end= 1.1.1.1
              port start= 20                 end= 20
            Destination:
              addr start= 2.2.2.2           end= 2.2.2.2
              port start= 20                 end= 20
          Action= Matched
            Gateway addr   = 192.168.1.1    Log= No
            Type of Service= Max Thruput
            Precedence     = 0

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

The following table describes the fields in this menu.

Table 70 Menu 25.1.1 IP Routing Policy

FIELD	DESCRIPTION
Policy Set Name	This is the policy set name assigned in **Menu 25 – IP Routing Policy Setup**.
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** to activate or No to deactivate the policy. Inactive policies are displayed with a minus sign "-" in SMT menu 25.
Criteria	
IP Protocol	IP layer 4 protocol, for example, **UDP**, **TCP**, **ICMP**, etc.
Type of Service	Prioritize incoming network traffic by choosing from **Don't Care**, **Normal**, **Min Delay**, **Max Thruput, Min Cost** or **Max Reliable**.
Precedence	Precedence value of the incoming packet. Press [SPACE BAR] and then [ENTER] to select a value from **0** to **7** or **Don't Care**.
Packet Length	Type the length of incoming packets (in bytes). The operators in the **Len Comp** (next field) apply to packets of this length.
Len Comp	Press [SPACE BAR] and then [ENTER] to choose from **Equal**, **Not Equal**, **Less**, **Greater**, **Less or Equal** or **Greater or Equal**.
Source:	
addr start / end	Source IP address range from start to end.
port start / end	Source port number range from start to end; applicable only for TCP/UDP.
Destination:	
addr start / end	Destination IP address range from start to end.
port start / end	Destination port number range from start to end; applicable only for TCP/UDP.
Action	Specifies whether action should be taken on criteria **Matched** or **Not Matched**.

Table 70 Menu 25.1.1 IP Routing Policy (continued)

FIELD	DESCRIPTION
Gateway addr	Defines the outgoing gateway address. The gateway must be on the same subnet as the Prestige if it is on the LAN, otherwise, the gateway must be the IP address of a remote node. The default gateway is specified as 0.0.0.0.
Type of Service	Set the new TOS value of the outgoing packet. Prioritize incoming network traffic by choosing **No Change**, **Normal**, **Min Delay**, **Max Thruput**, **Max Reliable** or **Min Cost**.
Precedence	Set the new outgoing packet precedence value. Values are **0** to **7** or **No Change**.
Log	Press [SPACE BAR] and then [ENTER] to select **Yes** to make an entry in the system log when a policy is executed.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

28.5 Applying an IP Policy

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

28.5.1 Ethernet IP Policies

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

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

Figure 157 Menu 3.2 TCP/IP and DHCP Ethernet Setup

```
            Menu 3.2 - TCP/IP and DHCP Setup

                    DHCP Setup
                      DHCP= Server
                      Client IP Pool Starting Address= 192.168.1.33
                      Size of Client IP Pool= 32
                      Primary DNS Server= 0.0.0.0
                      Secondary DNS Server= 0.0.0.0
                      Remote DHCP Server= N/A
                    TCP/IP Setup:
                      IP Address= 192.168.1.1
                      IP Subnet Mask= 255.255.255.0
                      RIP Direction= Both
                        Version= RIP-1
                      Multicast= None
                      IP Policies= 2,4,7,9
                      Edit IP Alias= No

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

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

Figure 158 Menu 11.3 Remote Node Network Layer Options

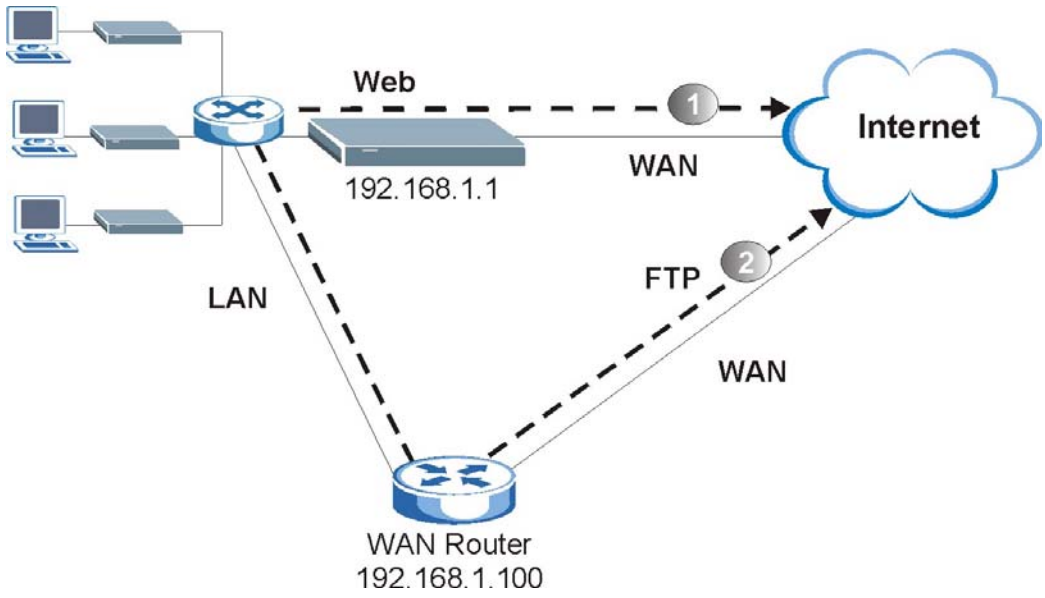
```
            Menu 11.3 - Remote Node Network Layer Options

IP Options:                         Bridge Options:
  IP Address Assignment= Static       Ethernet Addr Timeout (min)= 0
  Rem IP Addr: 0.0.0.0
  Rem Subnet Mask= 0.0.0.0
  My WAN Addr= 0.0.0.0
  NAT= Full Feature
    Address Mapping Set= 2
  Metric= 2
  Private= No
  RIP Direction= Both
    Version= RIP-2B
  Multicast= IGMP-v2
  IP Policies= 2,4,7,9

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

28.6 IP Policy Routing Example

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

Route 1 represents the default IP route and route 2 represents the configured IP route.

Figure 159 Example of IP Policy Routing



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

1 Create a routing policy set in menu 25.

2 Create a rule for this set in **Menu 25.1.1 — IP Routing Policy** as shown next.

Figure 160 IP Routing Policy Example 1

```
                    Menu 25.1.1 - IP Routing Policy

          Policy Set Name= set1
          Active= Yes
          Criteria:
            IP Protocol    = 6
            Type of Service= Don't Care          Packet length= 10
            Precedence     = Don't Care           Len Comp= N/A
            Source:
              addr start= 192.168.1.33           end= 192.168.1.64
              port start= 0                      end= N/A
            Destination:
              addr start= 0.0.0.0                end= N/A
              port start= 80                     end= 80
          Action= Matched
            Gateway addr   = 192.168.1.1         Log= No
            Type of Service= No Change
            Precedence     = No Change

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

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

4 Create another policy set in menu 25.

5 Create a rule in menu 25.1 for this set to route packets from any host (`IP=0.0.0.0` means any host) with protocol TCP and port FTP access through another gateway (192.168.1.100).

Figure 161 IP Routing Policy Example 2

```
                    Menu 25.1.1 - IP Routing Policy

          Policy Set Name= set2
          Active= Yes
          Criteria:
            IP Protocol    = 6
            Type of Service= Don't Care            Packet length= 10
            Precedence     = Don't Care             Len Comp= N/A
            Source:
              addr start= 0.0.0.0end= N/A
              port start= 0                         end= N/A
            Destination:
              addr start= 0.0.0.0                   end= N/A
              port start= 20                        end= 21
          Action= Matched
            Gateway addr  =192.168.1.100            Log= No
            Type of Service= No Change
            Precedence     = No Change

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

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

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

Figure 162 Applying IP Policies Example

```
            Menu 3.2 - TCP/IP and DHCP Ethernet Setup

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


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

CHAPTER 29
Call Scheduling

Call scheduling (applicable for PPPoA or PPPoE encapsulation only) allows you to dictate when a remote node should be called and for how long.

29.1 Introduction

The call scheduling feature allows the Prestige to manage a remote node and dictate when a remote node should be called and for how long. This feature is similar to the scheduler in a videocassette recorder (you can specify a time period for the VCR to record). You can apply up to 4 schedule sets in **Menu 11.1 — Remote Node Profile**. From the main menu, enter 26 to access **Menu 26 — Schedule Setup** as shown next.

Figure 163 Menu 26 Schedule Setup

```
            Menu 26 - Schedule Setup

Schedule                              Schedule
Set #           Name                  Set #           Name
------  -----------------             ------  -----------------
  1       _______________               7       _______________
  2       _______________               8       _______________
  3       _______________               9       _______________
  4       _______________              10       _______________
  5       _______________              11       _______________
  6       _______________              12       _______________

            Enter Schedule Set Number to Configure= 0

            Edit Name= N/A

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

Lower numbered sets take precedence over higher numbered sets thereby avoiding scheduling conflicts. For example, if sets 1, 2 ,3 and 4 in are applied in the remote node then set 1 will take precedence over set 2, 3 and 4 as the Prestige, by default, applies the lowest numbered set first. Set 2 will take precedence over set 3 and 4, and so on.

You can design up to 12 schedule sets but you can only apply up to four schedule sets for a remote node.

Note: To delete a schedule set, enter the set number and press **[SPACE BAR]** and then **[ENTER]** (or delete) in the **Edit Name** field.

To setup a schedule set, select the schedule set you want to setup from menu 26 (1-12) and press [ENTER] to see **Menu 26.1 — Schedule Set Setup** as shown next.

Figure 164 Menu 26.1 Schedule Set Setup

```
            Menu 26.1 Schedule Set Setup

               Active= Yes
               Start Date(yyyy-mm-dd)= 2000 - 01 - 01
               How Often= Once
               Once:
                 Date(yyyy-mm-dd)= 2000 - 01 - 01
               Weekdays:
                 Sunday= N/A
                 Monday= N/A
                 Tuesday= N/A
                 Wednesday= N/A
                 Thursday= N/A
                 Friday= N/A
                 Saturday= N/A
               Start Time(hh:mm)= 00 : 00
               Duration(hh:mm)= 00 : 00
               Action= Forced On

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

If a connection has been already established, your Prestige will not drop it. Once the connection is dropped manually or it times out, then that remote node can't be triggered up until the end of the **Duration**.

Table 71 Menu 26.1 Schedule Set Setup

FIELD	DESCRIPTION
Active	Press [SPACE BAR] to select **Yes** or **No**. Choose **Yes** and press [ENTER] to activate the schedule set.
Start Date	Enter the start date when you wish the set to take effect in year -month-date format. Valid dates are from the present to 2036-12-31.
How Often	Should this schedule set recur weekly or be used just once only? Press the [SPACE BAR] and then [ENTER] to select **Once** or **Weekly**. Both these options are mutually exclusive. If **Once** is selected, then all weekday settings are **N/A**. When **Once** is selected, the schedule rule deletes automatically after the scheduled time elapses.
Once: Date	If you selected **Once** in the **How Often** field above, then enter the date the set should activate here in year-month-date format.
Weekday: Day	If you selected **Weekly** in the **How Often** field above, then select the day(s) when the set should activate (and recur) by going to that day(s) and pressing [SPACE BAR] to select **Yes**, then press [ENTER].
Start Time	Enter the start time when you wish the schedule set to take effect in hour-minute format.
Duration	Enter the maximum length of time this connection is allowed in hour-minute format.

Table 71 Menu 26.1 Schedule Set Setup (continued)

FIELD	DESCRIPTION
Action	**Forced On** means that the connection is maintained whether or not there is a demand call on the line and will persist for the time period specified in the **Duration** field. **Forced Down** means that the connection is blocked whether or not there is a demand call on the line. **Enable Dial-On-Demand** means that this schedule permits a demand call on the line. **Disable Dial-On-Demand** means that this schedule prevents a demand call on the line.
When you have completed this menu, press [ENTER] at the prompt "`Press ENTER to Confirm or ESC to Cancel:`" to save your configuration, or press [ESC] at any time to cancel.	

Once your schedule sets are configured, you must then apply them to the desired remote node(s). Enter 11 from the **Main Menu** and then enter the target remote node index. Using [SPACE BAR], select **PPPoE** or **PPPoA** in the **Encapsulation** field and then press [ENTER] to make the schedule sets field available as shown next.

Figure 165 Applying Schedule Set(s) to a Remote Node (PPPoE)

```
            Menu 11.1 - Remote Node Profile

Rem Node Name= MyISP                    Route= IP
Active= Yes                             Bridge= No
Encapsulation= PPPoA                    Edit IP/Bridge= No
Multiplexing= LLC-based                 Edit ATM Options= No
Service Name= N/A                       Edit Advance Options= N/A
Incoming:                               Telco Option:
  Rem Login=                              Allocated Budget(min)= 0
  Rem Password= ********                  Period(hr)= 0
Outgoing:                                 Schedules Sets= 1,2,3,4
  My Login= ChangeMe                      Nailed-Up Connection= No
  My Password= ********                 Session Options:
  Authen= CHAP/PAP                        Edit Filter Sets= No
                                          Idle Timeout(sec)= 0

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

You can apply up to four schedule sets, separated by commas, for one remote node. Change the schedule set numbers to your preference(s).

CHAPTER 30
Troubleshooting

This chapter covers potential problems and the corresponding remedies.

30.1 Problems Starting Up the Prestige

Table 72 Troubleshooting the Start-Up of Your Prestige

PROBLEM	CORRECTIVE ACTION
None of the LEDs turn on when I turn on the Prestige.	Make sure that the Prestige's power adaptor is connected to the Prestige and plugged in to an appropriate power source. Check that the Prestige and the power source are both turned on. Turn the Prestige off and on. If the error persists, you may have a hardware problem. In this case, you should contact your vendor.

30.2 Problems with the LAN LED

Table 73 Troubleshooting the LAN LED

PROBLEM	CORRECTIVE ACTION
The LAN LEDs do not turn on.	Check your Ethernet cable connections and type (refer to the *Quick Start Guide* for details). Check for faulty Ethernet cables.
	Make sure your computer's Ethernet card is working properly.

30.3 Problems with the DSL LED

Table 74 Troubleshooting the DSL LED

PROBLEM	CORRECTIVE ACTION
The DSL LED is off.	Check the telephone wire and connections between the Prestige DSL port and the wall jack.
	Make sure that the telephone company has checked your phone line and set it up for DSL service.
	Reset your ADSL line to reinitialize your link to the DSLAM. For details, refer to Chapter 12 Maintenance (web configurator) or Chapter 24 System Information and Diagnosis (SMT).

30.4 Problems with the LAN Interface

Table 75 Troubleshooting the LAN Interface

PROBLEM	CORRECTIVE ACTION
I cannot access the Prestige from the LAN.	If the 10M/100M LEDs on the front panel are both off, refer to the Problems with the LAN LED section. Make sure that the IP address and the subnet mask of the Prestige and your computer(s) are on the same subnet.
I cannot ping any computer on the LAN.	If the 10M/100M LEDs on the front panel are both off, refer to the Problems with the LAN LED section. Make sure that the IP address and the subnet mask of the Prestige and the computers are on the same subnet.

30.5 Problems with the WAN Interface

Table 76 Troubleshooting the WAN Interface

PROBLEM	CORRECTIVE ACTION
I cannot get a WAN IP address from the ISP.	The ISP provides the WAN IP address after authenticating you. Authentication may be through the user name and password, the MAC address or the host name. The username and password apply to PPPoE and PPPoA encapsulation only. Make sure that you have entered the correct **Service Type**, **User Name** and **Password** (be sure to use the correct casing). Refer to Chapter 6 WAN Setup (web configurator) or Chapter 17 Internet Access (SMT).

30.6 Problems with Internet Access

Table 77 Troubleshooting Internet Access

PROBLEM	CORRECTIVE ACTION
I cannot access the Internet.	Make sure the Prestige is turned on and connected to the network. If the DSL LED is off, refer to the Problems with the DSL LED section. Verify your WAN settings. Refer to the chapter on WAN setup (web configurator) or the section on Internet Access (SMT). Make sure you entered the correct user name and password. If you use PPPoE pass through, make sure that bridge is turned on. See Chapter 14 Menu 1 General Setup for details.
Internet connection disconnects.	Check the schedule rules. Refer to Chapter 29 Call Scheduling (SMT). If you use PPPoA or PPPoE encapsulation, check the idle time-out setting. Refer to Chapter 6 WAN Setup (web configurator) or Chapter 18 Remote Node Configuration (SMT). Contact your ISP.

30.7 Problems with the Password

Table 78 Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
I cannot access the Prestige.	The username is "admin". The default password is "1234". The **Password** and **Username** fields are case-sensitive. Make sure that you enter the correct password and username using the proper casing. If you have changed the password and have now forgotten it, you will need to upload the default configuration file (Refer to the Resetting the Prestige section in Chapter 2 Introducing the Web Configurator). This restores all of the factory defaults including the password.

30.8 Problems with the Web Configurator

Table 79 Troubleshooting the Web Configurator

PROBLEM	CORRECTIVE ACTION
I cannot access the web configurator.	Refer to the *Quick Start Guide* for hardware connections. Make sure that there is not an SMT console session running. Check that you have enabled web service access. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on remote management for details. For WAN access, you must configure remote management to allow server access from the Wan (or all). Refer to the chapters on remote management for details. Your computer's and the Prestige's IP addresses must be on the same subnet for LAN access. If you changed the Prestige's LAN IP address, then enter the new one as the URL. Remove any filters in SMT menu 3.1 (LAN) or menu 11.5 (WAN) that block web service. See also the Problems with Remote Management section.

30.9 Problems with Remote Management

Table 80 Troubleshooting Remote Management

PROBLEM	CORRECTIVE ACTION
I cannot remotely manage the Prestige from the LAN or WAN.	Refer to the Remote Management Limitations section in Chapter 10 Remote Management Configuration for scenarios when remote management may not be possible.
	Use the Prestige's WAN IP address when configuring from the WAN. Use the Prestige's LAN IP address when configuring from the LAN.
	Refer to for instructions on checking your LAN connection.
	Refer to the Problems with the LAN Interface section for instructions on checking your WAN connection.
	See also the Problems with the Web Configurator section.

Appendix A Splitters and Microfilters

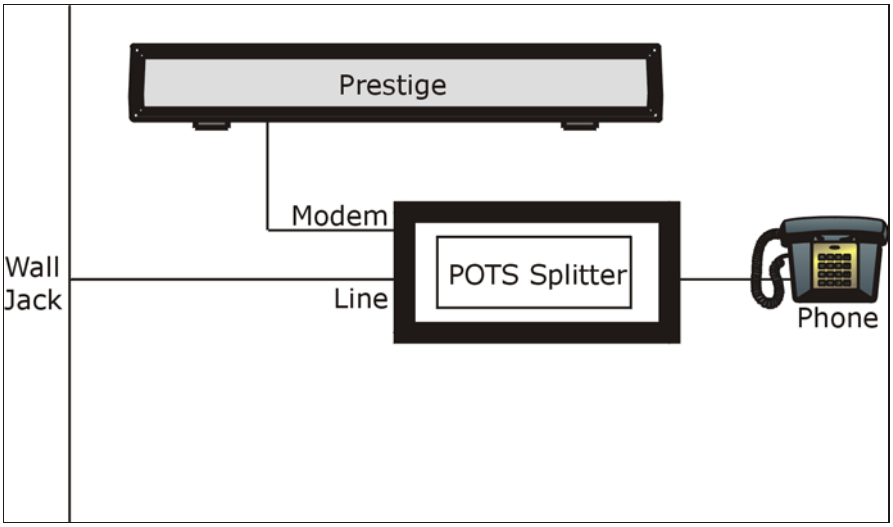
This appendix tells you how to install a POTS splitter or a telephone microfilter.

Connecting a POTS Splitter

When you use the Full Rate (G.dmt) ADSL standard, you can use a POTS (Plain Old Telephone Service) splitter to separate the telephone and ADSL signals. This allows simultaneous Internet access and telephone service on the same line. A splitter also eliminates the destructive interference conditions caused by telephone sets.

Install the POTS splitter at the point where the telephone line enters your residence, as shown in the following figure.

Figure 166 Connecting a POTS Splitter



1. Connect the side labeled "Phone" to your telephone.
2. Connect the side labeled "Modem" to your Prestige.
3. Connect the side labeled "Line" to the telephone wall jack.

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 use of a telephone microfilter is optional.

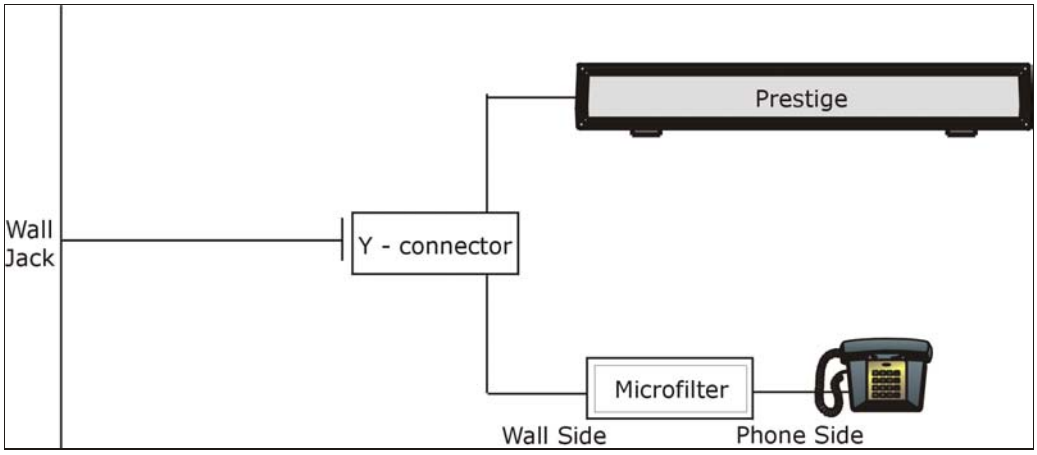
1 Connect a phone cable from the wall jack to the single jack end of the Y- Connector.

2 Connect a cable from the double jack end of the Y-Connector to the "wall side" of the microfilter.

3 Connect another cable from the double jack end of the Y-Connector to the Prestige.

4 Connect the "phone side" of the microfilter to your telephone as shown in the following figure.

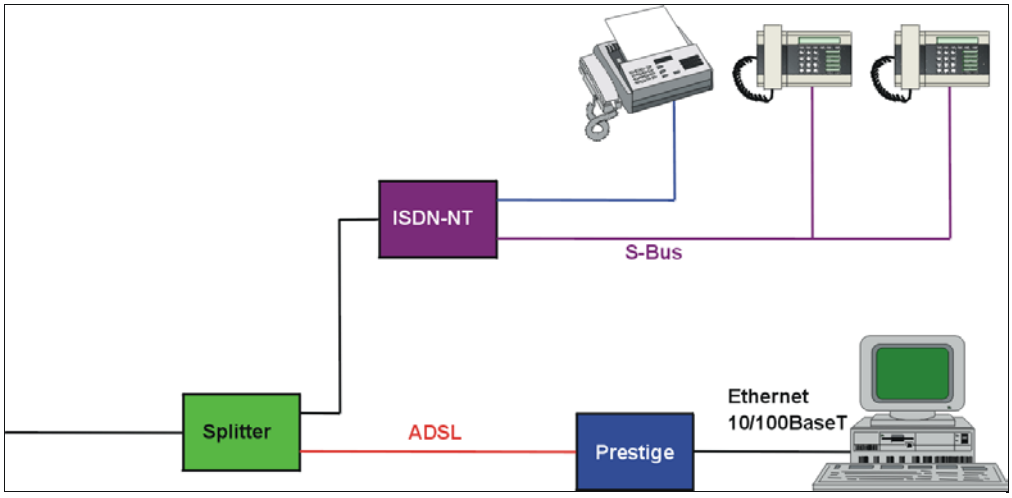
Figure 167 Connecting a Microfilter



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 168 Prestige with ISDN



Appendix B
Setting up Your Computer's IP Address

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

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

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

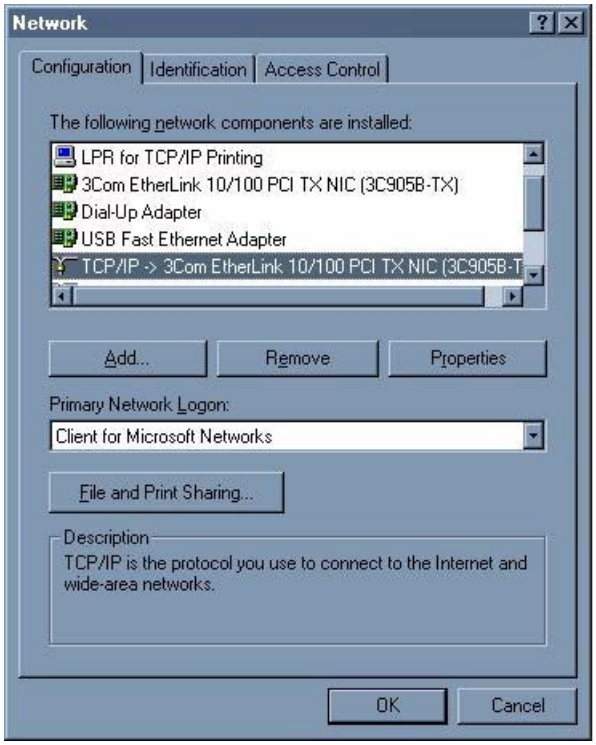
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

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

Windows 95/98/Me

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

Figure 169 WIndows 95/98/Me: Network: Configuration



Installing Components

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

If you need the adapter:

1. In the **Network** window, click **Add**.
2. Select **Adapter** and then click **Add**.
3. Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

1. In the **Network** window, click **Add**.
2. Select **Protocol** and then click **Add**.
3. Select **Microsoft** from the list of **manufacturers**.
4. Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

1. Click **Add**.
2. Select **Client** and then click **Add**.

3 Select **Microsoft** from the list of manufacturers.

4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.

5 Restart your computer so the changes you made take effect.

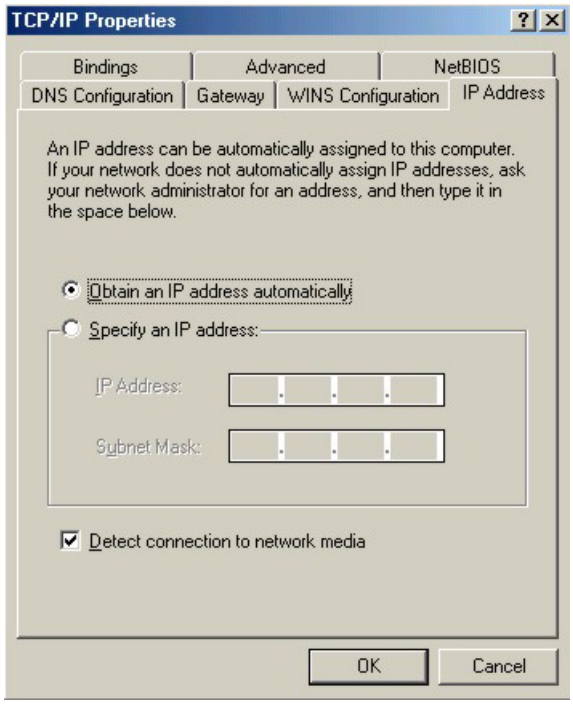
Configuring

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

2 Click the **IP Address** tab.

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

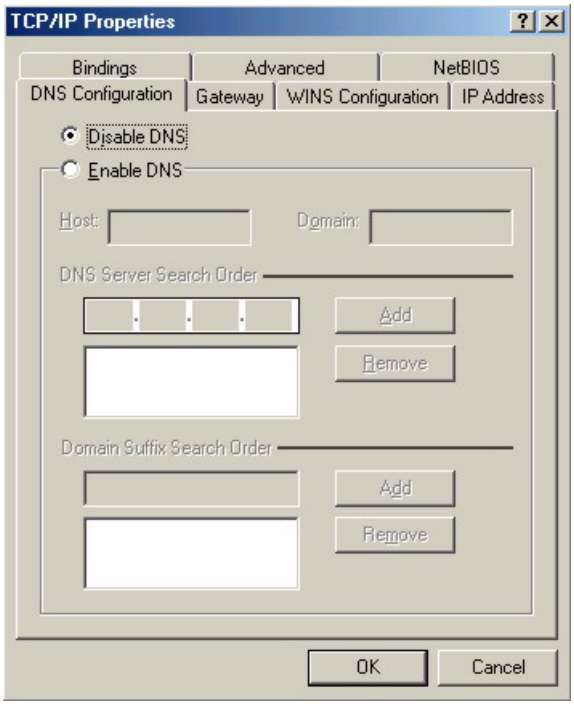
Figure 170 Windows 95/98/Me: TCP/IP Properties: IP Address



3 Click the **DNS** Configuration tab.

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

Figure 171 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



4 Click the **Gateway** tab.

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

5 Click **OK** to save and close the **TCP/IP Properties** window.

6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.

7 Turn on your Prestige and restart your computer when prompted.

Verifying Settings

1 Click **Start** and then **Run**.

2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.

3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

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

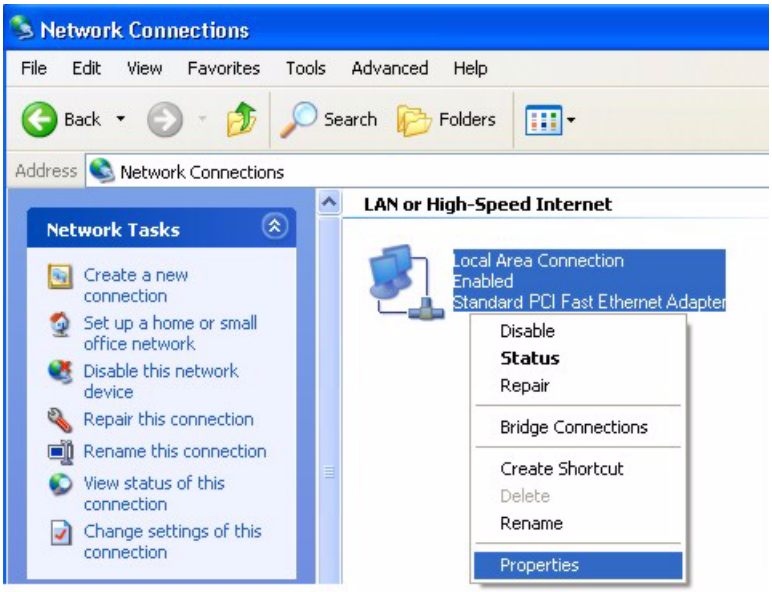
Figure 172 Windows XP: Start Menu

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

Figure 173 Windows XP: Control Panel

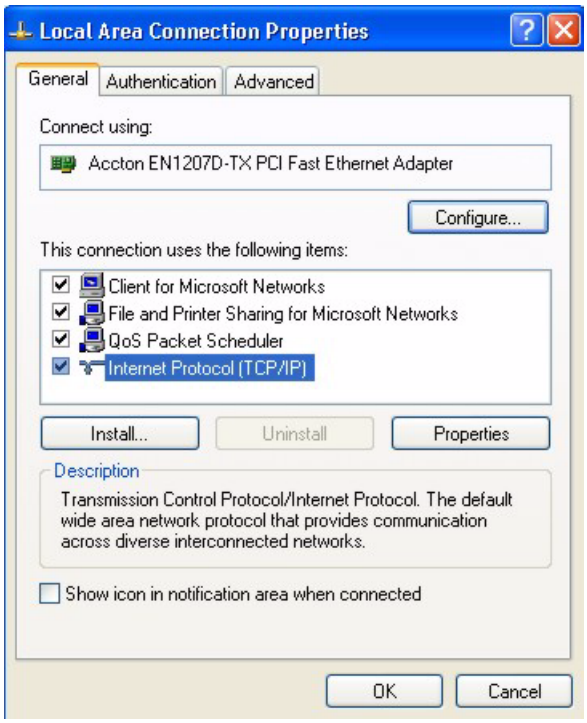
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 174 Windows XP: Control Panel: Network Connections: Properties



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

Figure 175 Windows XP: Local Area Connection Properties

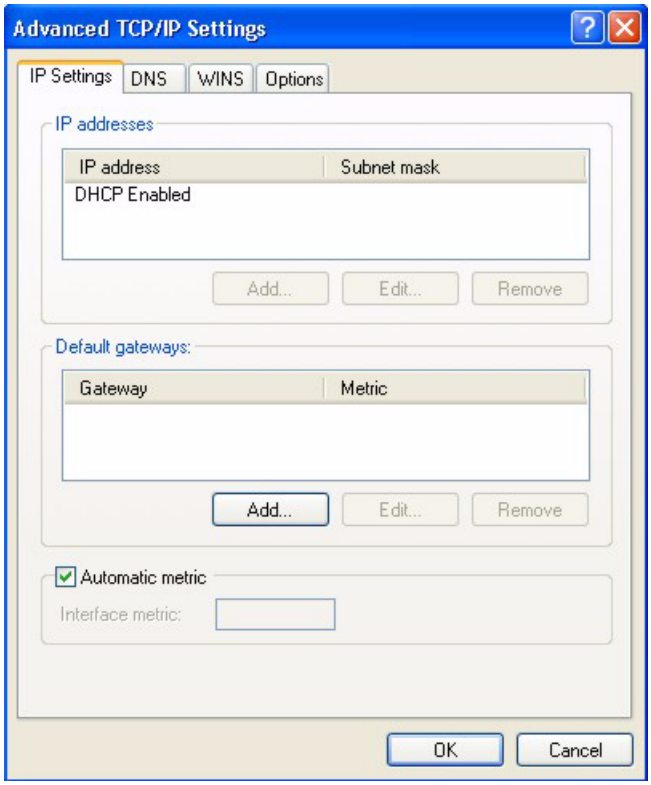


5 The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

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

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

Figure 176 Windows XP: Advanced TCP/IP Settings



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

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

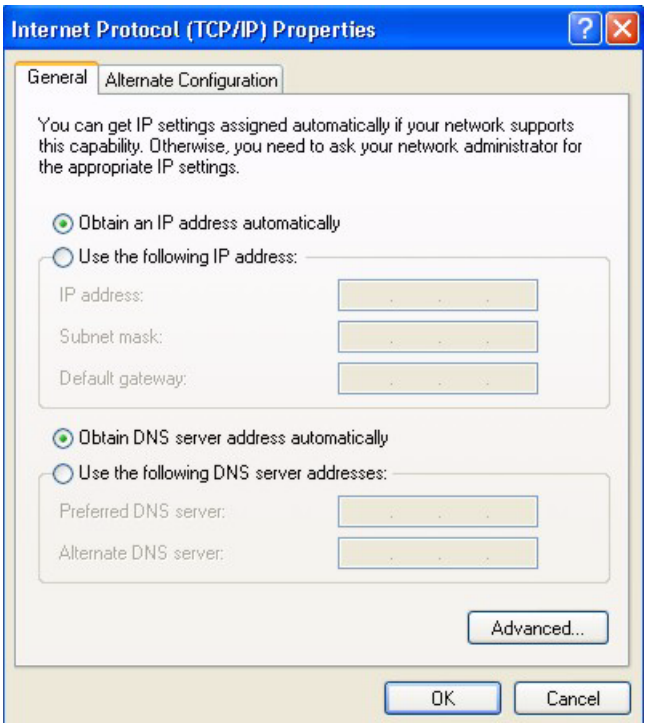
- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

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

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

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

Figure 177 Windows XP: Internet Protocol (TCP/IP) Properties



8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **OK** to close the **Local Area Connection Properties** window.

10 Turn on your Prestige and restart your computer (if prompted).

Verifying Settings

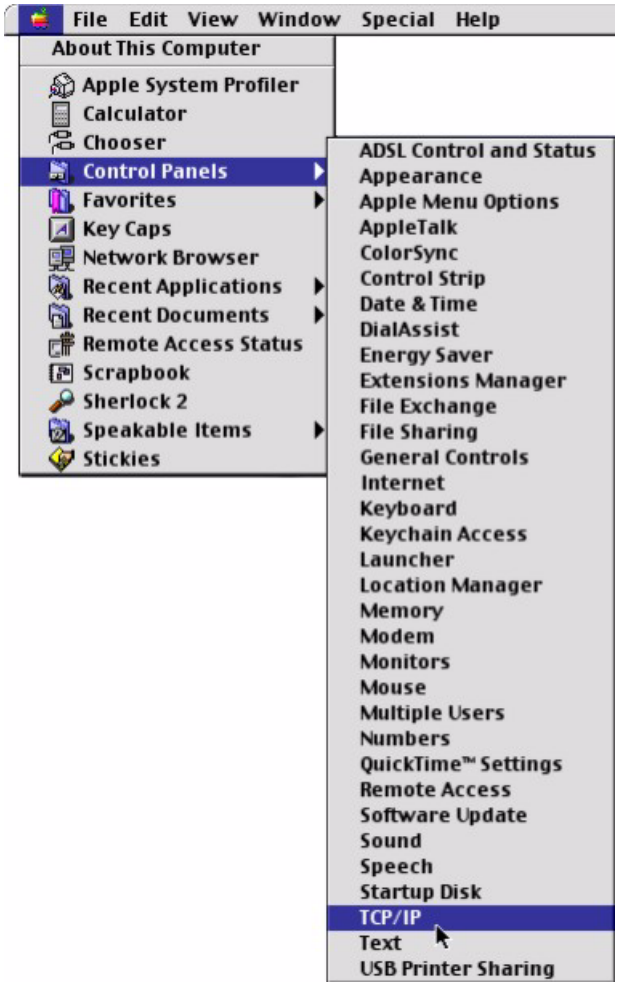
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

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

Macintosh OS 8/9

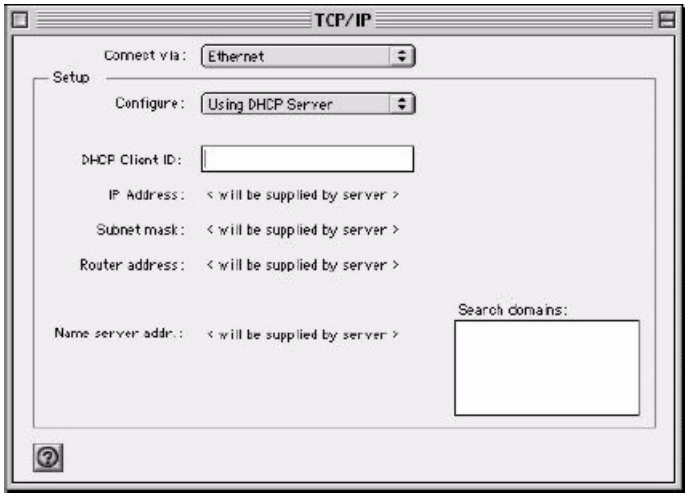
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 178 Macintosh OS 8/9: Apple Menu



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

Figure 179 Macintosh OS 8/9: TCP/IP



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

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your Prestige in the **Router address** box.

5 Close the **TCP/IP Control Panel**.

6 Click **Save** if prompted, to save changes to your configuration.

7 Turn on your Prestige and restart your computer (if prompted).

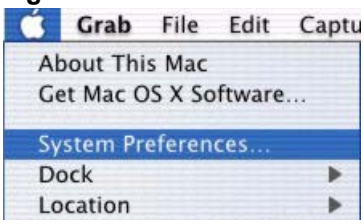
Verifying Settings

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

Macintosh OS X

1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 180 Macintosh OS X: Apple Menu

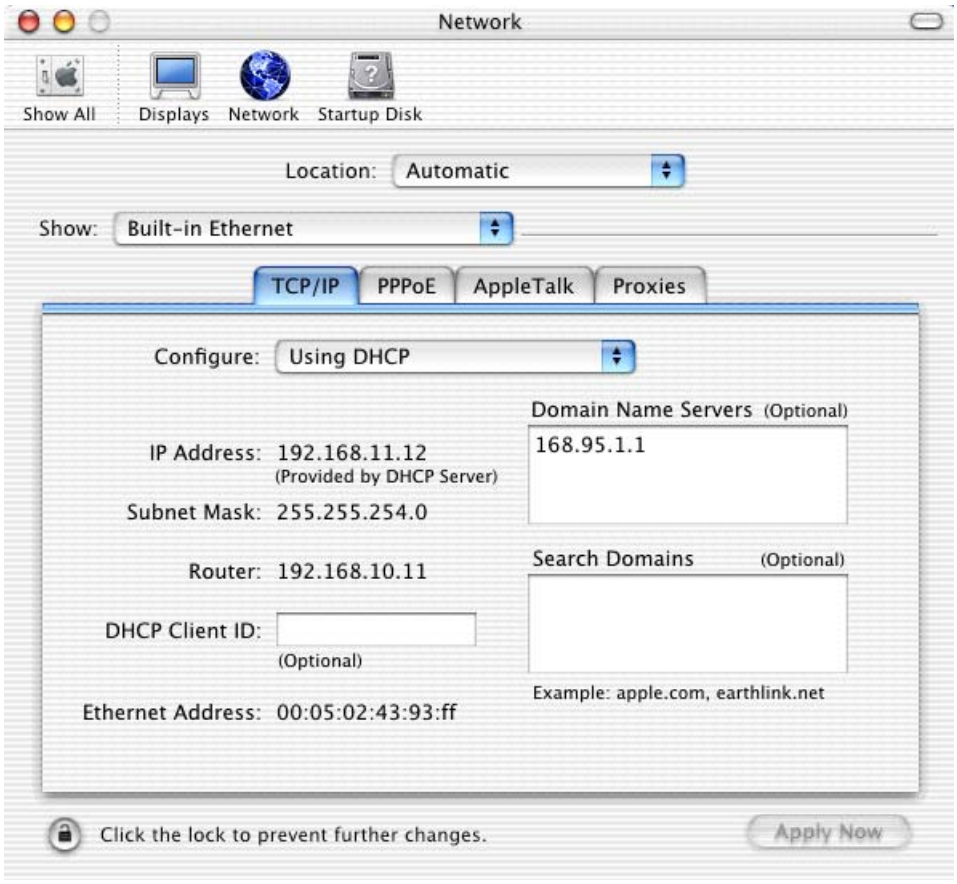


2 Click **Network** in the icon bar.

- Select **Automatic** from the **Location** list.
- Select **Built-in Ethernet** from the **Show** list.
- Click the **TCP/IP** tab.

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

Figure 181 Macintosh OS X: Network



4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your Prestige in the **Router address** box.

5 Click **Apply Now** and close the window.

6 Turn on your Prestige and restart your computer (if prompted).

Verifying Settings

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

Appendix C
IP Subnetting

IP Addressing

Routers "route" based on the network number. The router that delivers the data packet to the correct destination host uses the host ID.

IP Classes

An IP address is made up of four octets (eight bits), written in dotted decimal notation, for example, 192.168.1.1. IP addresses are categorized into different classes. The class of an address depends on the value of its first octet.

- Class "A" addresses have a 0 in the left most bit. In a class "A" address the first octet is the network number and the remaining three octets make up the host ID.
- Class "B" addresses have a 1 in the left most bit and a 0 in the next left most bit. In a class "B" address the first two octets make up the network number and the two remaining octets make up the host ID.
- Class "C" addresses begin (starting from the left) with 1 1 0. In a class "C" address the first three octets make up the network number and the last octet is the host ID.
- Class "D" addresses begin with 1 1 1 0. Class "D" addresses are used for multicasting. (There is also a class "E" address. It is reserved for future use.)

Table 81 Classes of IP Addresses

IP ADDRESS:		OCTET 1	OCTET 2	OCTET 3	OCTET 4
Class A	0	Network number	Host ID	Host ID	Host ID
Class B	10	Network number	Network number	Host ID	Host ID
Class C	110	Network number	Network number	Network number	Host ID

Note: Host IDs of all zeros or all ones are not allowed.

Therefore:

A class "C" network (8 host bits) can have 2^8 –2 or 254 hosts.

A class "B" address (16 host bits) can have 2^{16} –2 or 65534 hosts.

A class "A" address (24 host bits) can have 2^{24} –2 hosts (approximately 16 million hosts).

Since the first octet of a class "A" IP address must contain a "0", the first octet of a class "A" address can have a value of 0 to 127.

Similarly the first octet of a class "B" must begin with "10", therefore the first octet of a class "B" address has a valid range of 128 to 191. The first octet of a class "C" address begins with "110", and therefore has a range of 192 to 223.

Table 82 Allowed IP Address Range By Class

CLASS	ALLOWED RANGE OF FIRST OCTET (BINARY)	ALLOWED RANGE OF FIRST OCTET (DECIMAL)
Class A	**0**0000000 to **0**1111111	0 to 127
Class B	**10**000000 to **10**111111	128 to 191
Class C	**110**00000 to **110**11111	192 to 223
Class D	**1110**0000 to **1110**1111	224 to 239

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). A subnet mask has 32 is a "1" then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is "0" then the corresponding bit in the IP address is part of the host ID.

Subnet masks are expressed in dotted decimal notation just as IP addresses are. The "natural" masks for class A, B and C IP addresses are as follows.

Table 83 "Natural" Masks

CLASS	NATURAL MASK
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Subnetting

With subnetting, the class arrangement of an IP address is ignored. For example, a class C address no longer has to have 24 bits of network number and 8 bits of host ID. With subnetting, some of the host ID bits are converted into network number bits. By convention, subnet masks always consist of a continuous sequence of ones beginning from the left most bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with mask 255.255.255.128.

The following table shows all possible subnet masks for a class "C" address using both notations.

Table 84 Alternative Subnet Mask Notation

SUBNET MASK IP ADDRESS	SUBNET MASK "1" BITS	LAST OCTET BIT VALUE
255.255.255.0	/24	0000 0000
255.255.255.128	/25	1000 0000
255.255.255.192	/26	1100 0000
255.255.255.224	/27	1110 0000
255.255.255.240	/28	1111 0000
255.255.255.248	/29	1111 1000
255.255.255.252	/30	1111 1100

The first mask shown is the class "C" natural mask. Normally if no mask is specified it is understood that the natural mask is being used.

Example: Two Subnets

As an example, you have a class "C" address 192.168.1.0 with subnet mask of 255.255.255.0.

Table 85 Two Subnets Example

	NETWORK NUMBER	HOST ID
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask	255.255.255.	0
Subnet Mask (Binary)	11111111.11111111.11111111.	00000000

The first three octets of the address make up the network number (class "C"). You want to have two separate networks.

Divide the network 192.168.1.0 into two separate subnets by converting one of the host ID bits of the IP address to a network number bit. The "borrowed" host ID bit can be either "0" or "1" thus giving two subnets; 192.168.1.0 with mask 255.255.255.128 and 192.168.1.128 with mask 255.255.255.128.

Note: In the following charts, shaded/bolded last octet bit values indicate host ID bits "borrowed" to form network ID bits. The number of "borrowed" host ID bits determines the number of subnets you can have. The remaining number of host ID bits (after "borrowing") determines the number of hosts you can have on each subnet.

Table 86 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**0**0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	**1**0000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 87 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**1**0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	**1**0000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

The remaining 7 bits determine the number of hosts each subnet can have. Host IDs of all zeros represent the subnet itself and host IDs of all ones are the broadcast address for that subnet, so the actual number of hosts available on each subnet in the example above is $2^7 - 2$ or 126 hosts for each subnet.

192.168.1.0 with mask 255.255.255.128 is the subnet itself, and 192.168.1.127 with mask 255.255.255.128 is the directed broadcast address for the first subnet. Therefore, the lowest IP address that can be assigned to an actual host for the first subnet is 192.168.1.1 and the highest is 192.168.1.126. Similarly the host ID range for the second subnet is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The above example illustrated using a 25-bit subnet mask to divide a class "C" address space into two subnets. Similarly to divide a class "C" address into four subnets, you need to "borrow" two host ID bits to give four possible combinations of 00, 01, 10 and 11. The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192. Each subnet contains 6 host ID bits, giving 2^6-2 or 62 hosts for each subnet (all 0's is the subnet itself, all 1's is the broadcast address on the subnet).

Table 88 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 89 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 90 Subnet 3

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 91 Subnet 4

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example Eight Subnets

Similarly use a 27-bit mask to create 8 subnets (001, 010, 011, 100, 101, 110).

The following table shows class C IP address last octet values for each subnet.

Table 92 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	223	254	255

The following table is a summary for class "C" subnet planning.

Table 93 Class C Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

Subnetting With Class A and Class B Networks.

For class "A" and class "B" addresses the subnet mask also determines which bits are part of the network number and which are part of the host ID.

A class "B" address has two host ID octets available for subnetting and a class "A" address has three host ID octets (see Table 81) available for subnetting.

The following table is a summary for class "B" subnet planning.

Table 94 Class B Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Appendix D PPPoE

PPPoE in Action

An ADSL modem bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your computer to an ATM PVC (Permanent Virtual Circuit) which connects to a DSL Access Concentrator where the PPP session terminates (see Figure 182). One PVC can support any number of PPP sessions from your LAN. PPPoE provides access control and billing functionality in a manner similar to dial-up services using PPP.

Benefits of PPPoE

PPPoE offers the following benefits:

It provides you with a familiar dial-up networking (DUN) user interface.

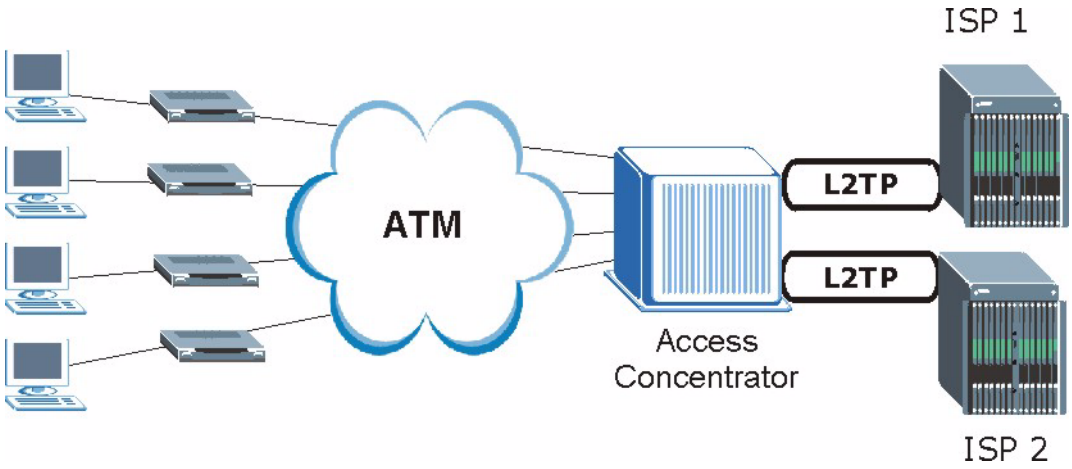
It lessens the burden on the carriers of provisioning virtual circuits all the way to the ISP on multiple switches for thousands of users. For GSTN (PSTN and ISDN), the switching fabric is already in place.

It allows the ISP to use the existing dial-up model to authenticate and (optionally) to provide differentiated services.

Traditional Dial-up Scenario

The following diagram depicts a typical hardware configuration where the computers use traditional dial-up networking.

Figure 182 Single-Computer per Router Hardware Configuration



How PPPoE Works

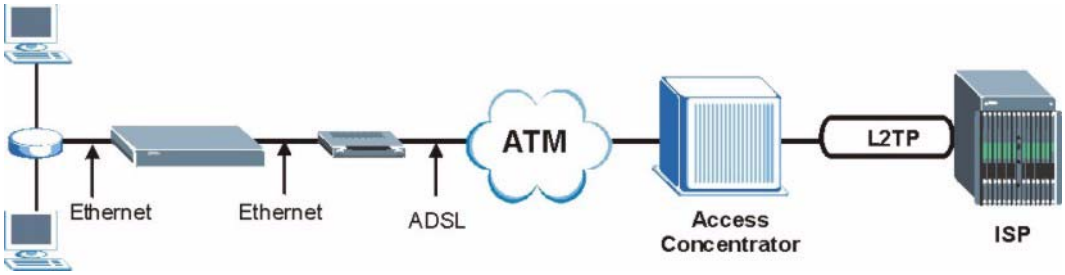
The PPPoE driver makes the Ethernet appear as a serial link to the computer and the computer runs PPP over it, while the modem bridges the Ethernet frames to the Access Concentrator (AC). Between the AC and an ISP, the AC is acting as a L2TP (Layer 2 Tunneling Protocol) LAC (L2TP Access Concentrator) and tunnels the PPP frames to the ISP. The L2TP tunnel is capable of carrying multiple PPP sessions.

With PPPoE, the VC (Virtual Circuit) is equivalent to the dial-up connection and is between the modem and the AC, as opposed to all the way to the ISP. However, the PPP negotiation is between the computer and the ISP.

Prestige as a PPPoE Client

When using the Prestige as a PPPoE client, the computers on the LAN see only Ethernet and are not aware of PPPoE. This alleviates the administrator from having to manage the PPPoE clients on the individual computers.

Figure 183 Prestige as a PPPoE Client

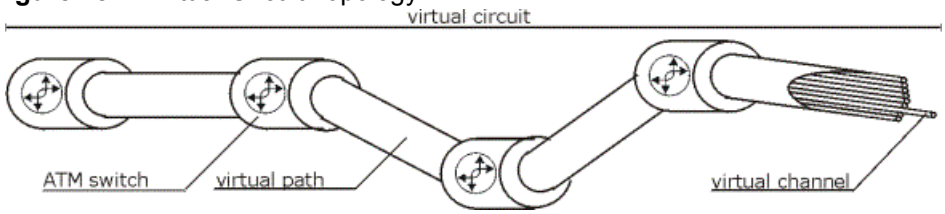


Appendix E
Virtual Circuit Topology

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 CircuitA series of virtual paths between circuit end points

Figure 184 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 ISP (Internet Service Provider) should supply you with VPI/VCI numbers.

Appendix F
Command Interpreter

The following describes how to use the command interpreter. Enter 24 in the main menu to bring up the system maintenance menu. Enter 8 to go to **Menu 24.8 - Command Interpreter Mode**. See the included disk or zyxel.com for more detailed information on these commands.

Note: Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.

Command Syntax

- The command keywords are in `courier new` font.
- Enter the command keywords exactly as shown, do not abbreviate.
- The required fields in a command are enclosed in angle brackets <>.
- The optional fields in a command are enclosed in square brackets `[]`.
- The `|` symbol means or.

  For example,

  sys filter netbios config <type> <on|off>

  means that you must specify the type of netbios filter and whether to turn it on or off.

Command Usage

A list of valid commands can be found by typing `help` or `?` at the command prompt. Always type the full command. Type `exit` to return to the SMT main menu when finished.

Appendix G
Log Descriptions

This appendix provides descriptions of example log messages.

Table 95 System Maintenance Logs

LOG MESSAGE	DESCRIPTION
Time calibration is successful	The router has adjusted its time based on information from the time server.
Time calibration failed	The router failed to get information from the time server.
WAN interface gets IP: %s	A WAN interface got a new IP address from the DHCP, PPPoE, PPTP or dial-up server.
DHCP client IP expired	A DHCP client's IP address has expired.
DHCP server assigns %s	The DHCP server assigned an IP address to a client.
Successful SMT login	Someone has logged on to the router's SMT interface.
SMT login failed	Someone has failed to log on to the router's SMT interface.
Successful WEB login	Someone has logged on to the router's web configurator interface.
WEB login failed	Someone has failed to log on to the router's web configurator interface.
Successful TELNET login	Someone has logged on to the router via telnet.
TELNET login failed	Someone has failed to log on to the router via telnet.
Successful FTP login	Someone has logged on to the router via ftp.
FTP login failed	Someone has failed to log on to the router via ftp.
NAT Session Table is Full!	The maximum number of NAT session table entries has been exceeded and the table is full.
Starting Connectivity Monitor	Starting Connectivity Monitor.
Time initialized by Daytime Server	The router got the time and date from the Daytime server.
Time initialized by Time server	The router got the time and date from the time server.
Time initialized by NTP server	The router got the time and date from the NTP server.
Connect to Daytime server fail	The router was not able to connect to the Daytime server.
Connect to Time server fail	The router was not able to connect to the Time server.
Connect to NTP server fail	The router was not able to connect to the NTP server.
Too large ICMP packet has been dropped	The router dropped an ICMP packet that was too large.
SMT Session Begin	An SMT management session has started.
SMT Session End	An SMT management session has ended.

Table 96 System Error Logs

LOG MESSAGE	DESCRIPTION
`%s exceeds the max. number of session per host!`	This attempt to create a NAT session exceeds the maximum number of NAT session table entries allowed to be created per host.
`setNetBIOSFilter: calloc error`	The router failed to allocate memory for the NetBIOS filter settings.
`readNetBIOSFilter: calloc error`	The router failed to allocate memory for the NetBIOS filter settings.
`WAN connection is down.`	A WAN connection is down. You cannot access the network through this interface.

Table 97 Packet Filter Logs

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

Table 98 ICMP Logs

LOG MESSAGE	DESCRIPTION
`Packet without a NAT table entry blocked: ICMP`	The router blocked a packet that didn't have a corresponding NAT table entry.
`Router reply ICMP packet: ICMP`	The router sent an ICMP reply packet to the sender.

Table 99 CDR Logs

LOG MESSAGE	DESCRIPTION
`board %d line %d channel %d, call %d, %s C01 Outgoing Call dev=%x ch=%x %s`	The router received the setup requirements for a call. "call" is the reference (count) number of the call. "dev" is the device type (3 is for dial-up, 6 is for PPPoE, 10 is for PPTP). "channel" or "ch" is the call channel ID.For example,"board 0 line 0 channel 0, call 3, C01 Outgoing Call dev=6 ch=0 "Means the router has dialed to the PPPoE server 3 times.

Table 99 CDR Logs (continued)

LOG MESSAGE	DESCRIPTION
board %d line %d channel %d, call %d, %s C02 OutCall Connected %d %s	The PPPoE, PPTP or dial-up call is connected.
board %d line %d channel %d, call %d, %s C02 Call Terminated	The PPPoE, PPTP or dial-up call was disconnected.

Table 100 PPP Logs

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

Table 101 ICMP Notes

TYPE	CODE	DESCRIPTION
0		Echo Reply
	0	Echo reply message
3		Destination Unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)
	5	Source route failed
4		Source Quench
	0	A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network

Table 101 ICMP Notes (continued)

TYPE	CODE	DESCRIPTION
	1	Redirect datagrams for the Host
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host
8		Echo
	0	Echo message
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp Reply
	0	Timestamp reply message
15		Information Request
	0	Information request message
16		Information Reply
	0	Information reply message

Table 102 Syslog Logs

LOG MESSAGE	DESCRIPTION
<Facility*8 + Severity>Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>" devID="<mac address last three numbers>" cat="<category>	"This message is sent by the system ("RAS" displays as the system name if you haven't configured one) when the router generates a syslog. The facility is defined in the web MAIN MENU->LOGS->Log Settings page. The severity is the log's syslog class. The definition of messages and notes are defined in the various log charts throughout this appendix. The "devID" is the last three characters of the MAC address of the router's LAN port. The "cat" is the same as the category in the router's logs.

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

Table 103 RFC-2408 ISAKMP Payload Types

LOG DISPLAY	PAYLOAD TYPE
SA	Security Association
PROP	Proposal
TRANS	Transform

Table 103 RFC-2408 ISAKMP Payload Types (continued)

LOG DISPLAY	PAYLOAD TYPE
KE	Key Exchange
ID	Identification
CER	Certificate
CER_REQ	Certificate Request
HASH	Hash
SIG	Signature
NONCE	Nonce
NOTFY	Notification
DEL	Delete
VID	Vendor ID

Index

A

B

C

D

E

F

G

H

I

L

M

N

P

Q

R

S

T

U

V

W

X

Z