Prestige 660H Series

ADSL 2/2+ Gateway

User's Guide

Version 3.40 (QT)
April 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:

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

Notice 1

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

Certifications

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

FC Tested To Comply
With FCC Standards
FOR HOME OR OFFICE USE

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	SUPPORT E-MAIL	TELEPHONE[1]	WEB SITE	REGULAR MAIL
LOCATION	SALES E-MAIL	FAX[1]	FTP SITE	
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

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

Table of Contents

List of Figures

List of Tables

List of Charts

Preface

Congratulations on your purchase of the Prestige 660H Series ADSL 2/2+ Gateway.

☞ **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.

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

Related Documentation

- ➢ Supporting Disk

  Refer to the included CD for support documents.

- ➢ Compact Guide

  The Compact 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!

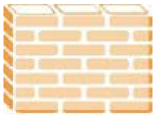
Syntax Conventions

- "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 660H series may be referred to as the Prestige in this user's guide. This refers all models (ADSL over POTS, ADSL over ISDN and T-ISDN (UR-2)) unless specifically identified.

Graphics Icons Key

Prestige	Computer	Notebook computer
Server	DSLAM	 Firewall
Telephone	Switch	Router

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

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.

Part I:

Getting Started

This part is structured as a step-by-step guide to help you access your Prestige. It covers key features and applications, accessing the web configurator and configuring the wizard screens for initial setup.

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.

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

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

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

Three Prestige models are included in this user’s guide at the time of writing. In the product name, “H” denotes an integrated 4-port switch (hub).

Models ending in “1”, for example P660H-61, denote a device that works over the analog telephone system, POTS (Plain Old Telephone Service). Models ending in “3” denote a device that works over ISDN (Integrated Synchronous Digital System). Models ending in “7” denote a device that works over T-ISDN (UR-2).

☞ **Only use firmware for your Prestige’s specific model. Refer to the label on the bottom of your Prestige.**

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

1.2 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.

➢ Firewall

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

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

➢ Content Filtering

Content filtering allows you to block access to forbidden Internet web sites, schedule when the Prestige should perform the filtering and give trusted LAN IP addresses unfiltered Internet access.

➢ 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 Transmission Rate 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.

1.3 Applications for the Prestige

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

1.3.1 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.

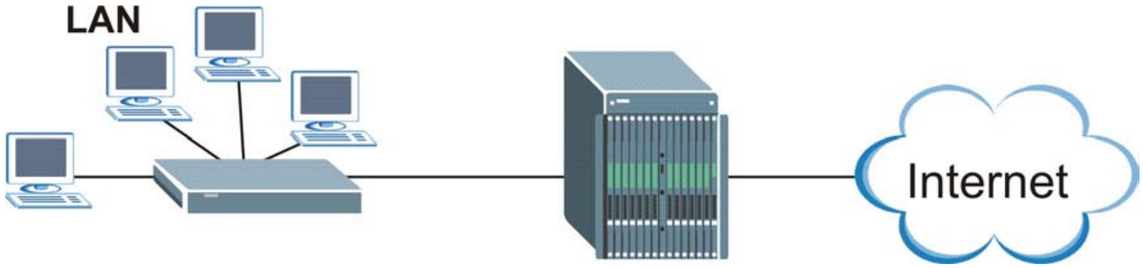


Figure 1-1 Prestige Internet Access Application

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.

1.3.2 Firewall for Secure Broadband Internet Access

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

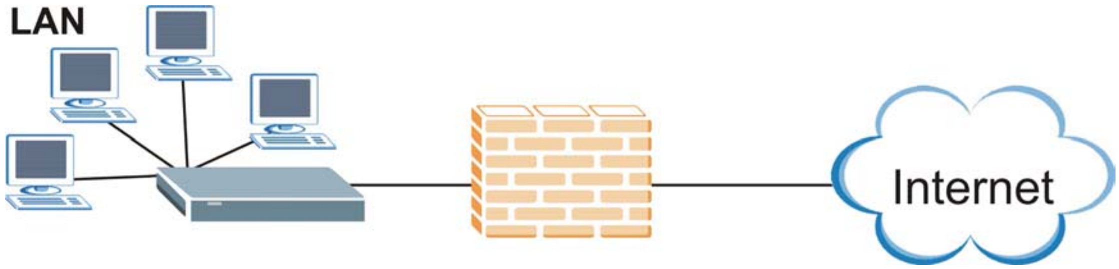


Figure 1-2 Firewall Application

1.3.3 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.

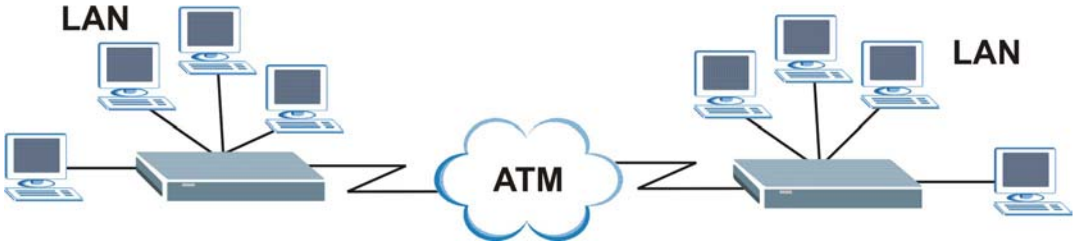


Figure 1-3 Prestige LAN-to-LAN Application

Chapter 2 Introducing the Web Configurator

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

2.1 Web Configurator Overview

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

2.2 Accessing the Prestige Web Configurator

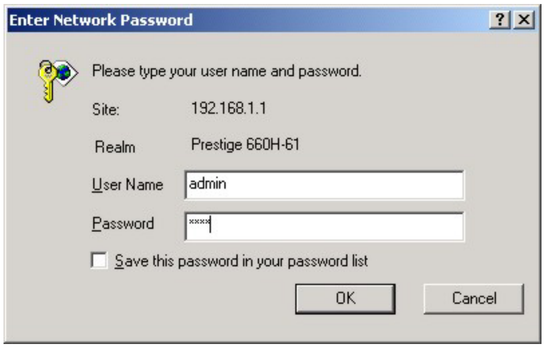
Step 1. Make sure your Prestige hardware is properly connected (refer to the *Compact Guide*).

Step 2. Prepare your computer/computer network to connect to the Prestige (refer to the *Compact Guide*).

Step 3. Launch your web browser.

Step 4. Type "192.168.1.1" as the URL.

Step 5. An **Enter Network Password** window displays. Enter the user name ("admin" is the default), password ("1234" is the default) and click **OK**.



Enter Network Password

Please type your user name and password.

Site: 192.168.1.1

Realm Prestige 660H-61

User Name admin

Password ****

□ Save this password in your password list

Figure 2-1 Password Screen

Step 6. You should now see the **SITE MAP** screen.

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

2.3 Resetting the Prestige

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

2.3.1 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.

2.4 Navigating the Prestige Web Configurator

The following summarizes how to navigate the web configurator from the **SITE MAP** screen. We use the Prestige 660H-61 web screens in this guide as an example. Screens vary slightly for different Prestige models.

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

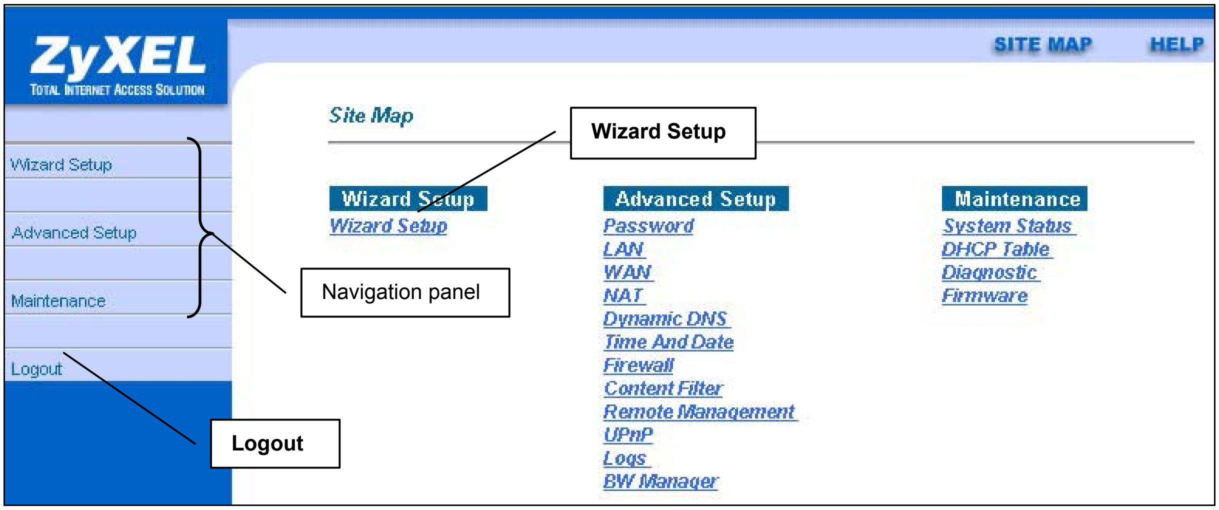


Figure 2-2 Web Configurator SITE MAP Screen

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

Table 2-1 Web Configurator Screens Summary

LINK	SUB-LINK	FUNCTION
Wizard Setup		Use these screens for initial configuration including general setup, ISP parameters for Internet Access and WAN IP/DNS Server/MAC address assignment.
Advanced Setup		

Table 2-1 Web Configurator Screens Summary

LINK	SUB-LINK	FUNCTION
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.
Dynamic DNS		Use this screen to set up dynamic DNS.
Time and Date		Use this screen to change your Prestige’s time and date.
Firewall	Default Policy	Use this screen to activate/deactivate the firewall and the direction of network traffic to which to apply the rule.
	Rule Summary	This screen shows a summary of the firewall rules, and allows you to edit/add a firewall rule.
	Anti Probing	Use this screen to change your anti-probing settings.
	Threshold	Use this screen to configure the threshold for DoS attacks.
Content Filter	Keyword	Use this screen to block sites containing certain keywords in the URL.
	Schedule	Use this screen to set the days and times for the Prestige to perform content filtering.
	Trusted	Use this screen to exclude a range of users on the LAN from content filtering on your Prestige.
Remote Management		Use this screen to configure through which interface(s) and from which IP address(es) users can use Telnet/FTP/Web to manage the Prestige.
UPnP		Use this screen to enable UPnP on the Prestige.
Logs	Log Settings	Use this screen to change your Prestige’s log settings.
	View Log	Use this screen to view the logs for the categories that you selected.
BW Manager	Summary	Use this screen to configure bandwidth manager on the interfaces.
	Class Setup	Use this screen to configure bandwidth classes.
	Monitor	Use this screen to view current bandwidth usage for the classes on the interfaces.
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 in the web configurator.

3.1 Wizard Setup Introduction

Use the Wizard Setup screens to configure your system for Internet access settings and fill in the fields with the information in the *Internet Account Information* table of the *Compact Guide*. Your ISP may have already configured some of the fields in the wizard screens for you.

3.2 Encapsulation

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

3.2.1 ENET ENCAP

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

3.2.2 PPP over Ethernet

PPPoE provides access control and billing functionality in a manner similar to dial-up services using PPP. The Prestige bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your computer to an ATM PVC (Permanent Virtual Circuit) which connects to 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.

3.2.3 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.

3.2.4 RFC 1483

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

3.3 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.

3.3.1 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.

3.3.2 LLC-based Multiplexing

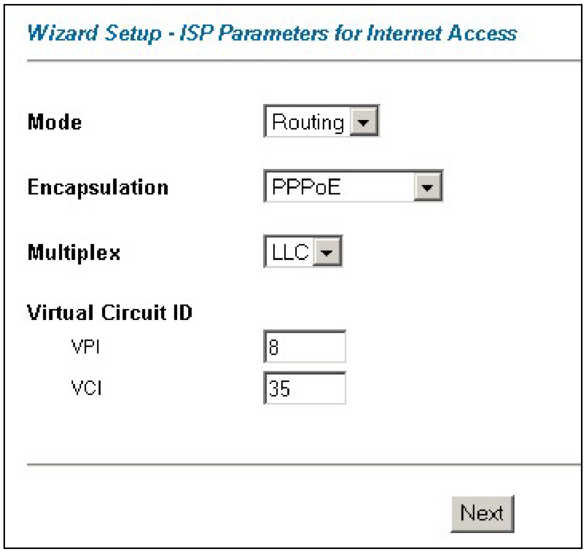
In this case one VC carries multiple protocols with protocol identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method may be advantageous if it is not practical to have a separate VC for each carried protocol, for example, if charging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

3.4 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.

3.5 Wizard Setup Configuration: First Screen

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



Wizard Setup - ISP Parameters for Internet Access

Mode: Routing

Encapsulation: PPPoE

Multiplex: LLC

Virtual Circuit ID

VPI: 8

VCI: 35

Figure 3-1 Wizard Screen 1

The following table describes the fields in this screen.

Table 3-1 Wizard Screen 1

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.

3.6 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.

3.7 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.

3.7.1 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.

3.7.2 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.

3.7.3 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.

3.7.4 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.

☞ **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.***

3.8 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.

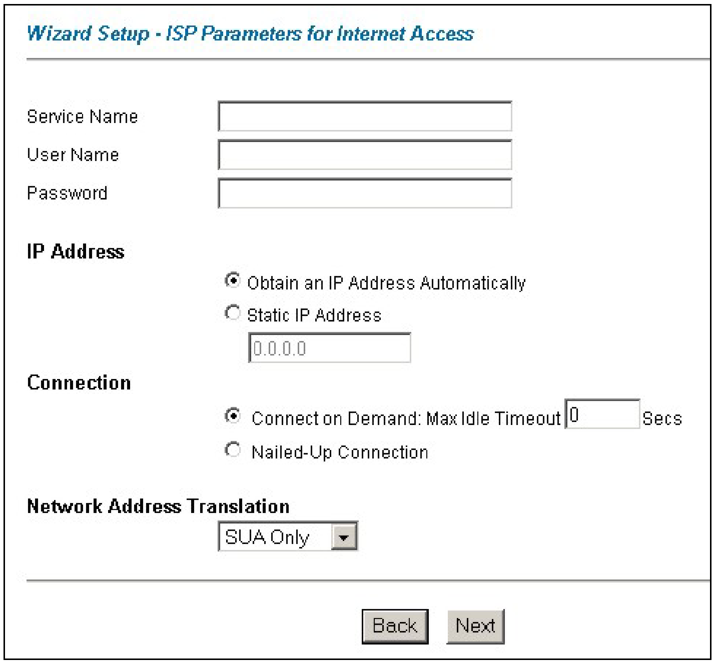
Do not specify a nailed-up connection unless your telephone company offers flat-rate service or you need a constant connection and the cost is of no concern

3.9 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.

3.10 Wizard Setup Configuration: 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.



Wizard Setup - ISP Parameters for Internet Access

Service Name

User Name

Password

IP Address

● Obtain an IP Address Automatically

○ Static IP Address 0.0.0.0

Connection

● Connect on Demand: Max Idle Timeout 0 Secs

○ Nailed-Up Connection

Network Address Translation

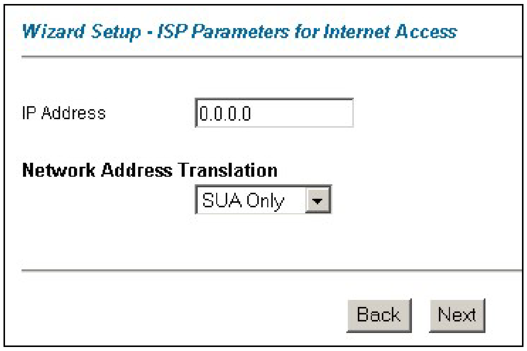
SUA Only

Figure 3-2 Internet Connection with PPPoE

The following table describes the fields in this screen.

Table 3-2 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. The Single User Account feature can be used with either a dynamic or static IP address. 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.
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.



Wizard Setup - ISP Parameters for Internet Access

IP Address: 0.0.0.0

Network Address Translation: SUA Only

Figure 3-3 Internet Connection with RFC 1483

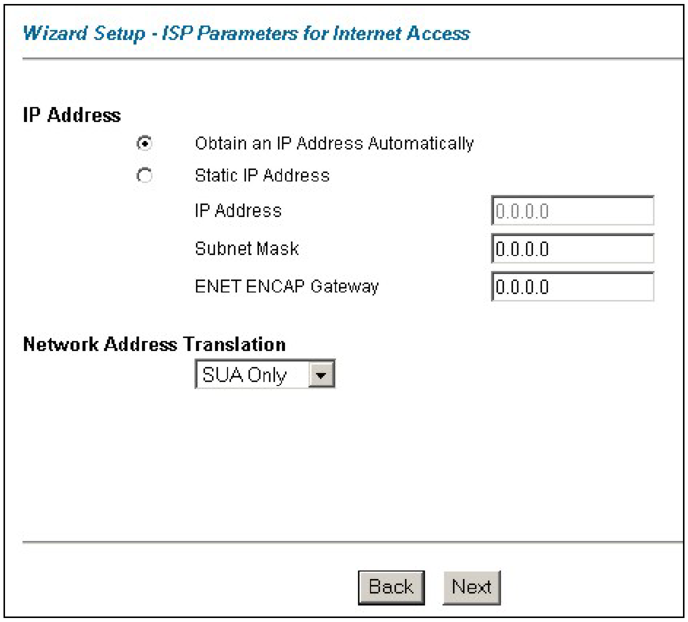
The following table describes the fields in this screen.

Table 3-3 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.

Table 3-3 Internet Connection with RFC 1483

LABEL	DESCRIPTION
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.



Wizard Setup - ISP Parameters for Internet Access

IP Address

● Obtain an IP Address Automatically

○ Static IP Address

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

ENET ENCAP Gateway: 0.0.0.0

Network Address Translation

SUA Only ▾

Figure 3-4 Internet Connection with ENET ENCAP

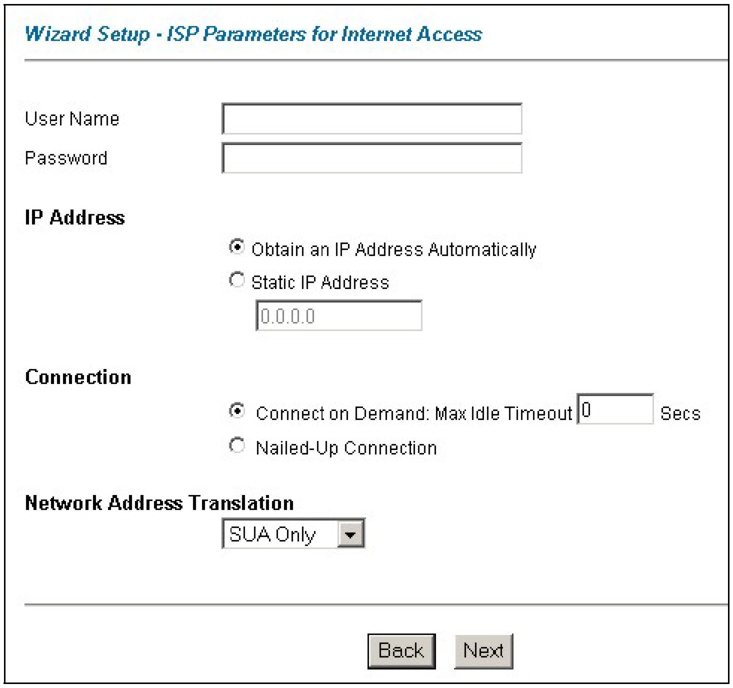
The following table describes the fields in this screen.

Table 3-4 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. The Single User Account feature can be used with either a dynamic or static IP address. 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 the *IP Subnetting* appendix 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.

Table 3-4 Internet Connection with ENET ENCAP

LABEL	DESCRIPTION
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.



Wizard Setup - ISP Parameters for Internet Access

User Name

Password

IP Address

● Obtain an IP Address Automatically

○ Static IP Address

0.0.0.0

Connection

● Connect on Demand: Max Idle Timeout 0 Secs

○ Nailed-Up Connection

Network Address Translation

SUA Only

Figure 3-5 Internet Connection with PPPoA

The following table describes the fields in this screen.

Table 3-5 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. The Single User Account feature can be used with either a dynamic or static IP address. 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.

Table 3-5 Internet Connection with PPPoA

LABEL	DESCRIPTION
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 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.

3.11 DHCP Setup

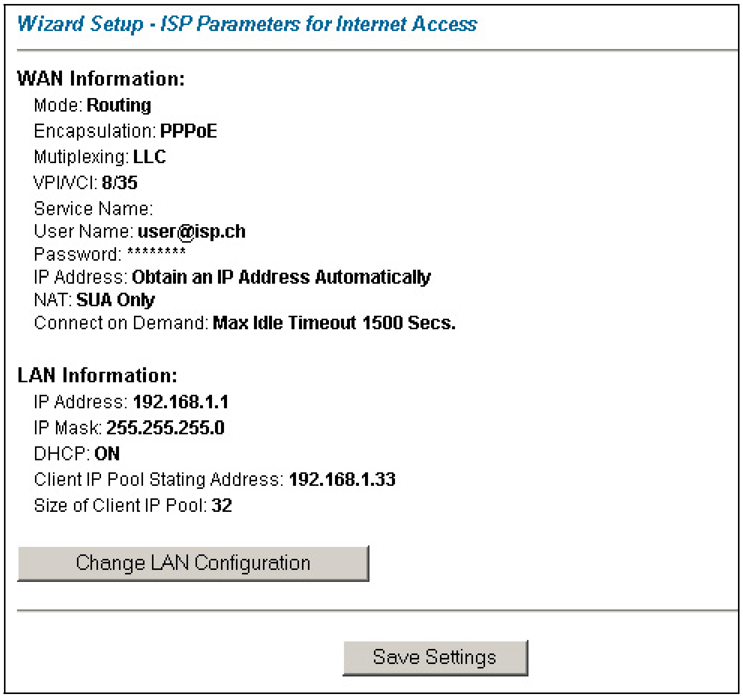
DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the Prestige as a DHCP server or disable it. When configured as a server, the Prestige provides the TCP/IP configuration for the clients.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

3.11.1 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.

3.12 Wizard Setup Configuration: Third Screen

Step 1. 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.



Wizard Setup - ISP Parameters for Internet Access

WAN Information:

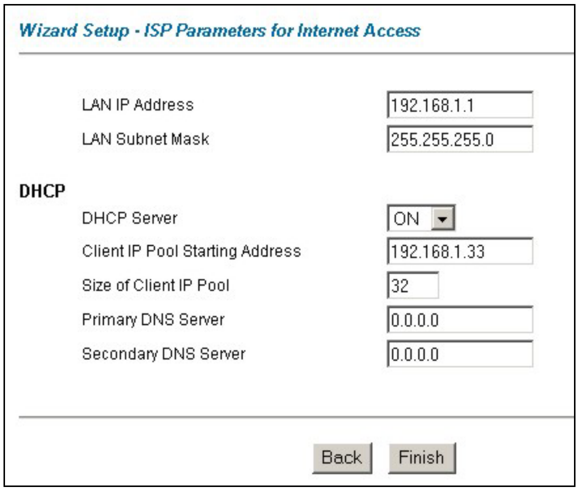
Mode: **Routing**
Encapsulation: **PPPoE**
Mutiplexing: **LLC**
VPI/VCI: **8/35**
Service Name:
User Name: **user@isp.ch**
Password: ********
IP Address: **Obtain an IP Address Automatically**
NAT: **SUA Only**
Connect on Demand: **Max Idle Timeout 1500 Secs.**

LAN Information:

IP Address: **192.168.1.1**
IP Mask: **255.255.255.0**
DHCP: **ON**
Client IP Pool Stating Address: **192.168.1.33**
Size of Client IP Pool: **32**

Figure 3-6 Wizard Screen 3

Step 1. If you want to change your Prestige LAN settings, click **Change LAN Configuration** to display the screen as shown next.



Wizard Setup - ISP Parameters for Internet Access

LAN IP Address: 192.168.1.1
LAN Subnet Mask: 255.255.255.0

DHCP

DHCP Server: ON
Client IP Pool Starting Address: 192.168.1.33
Size of Client IP Pool: 32
Primary DNS Server: 0.0.0.0
Secondary DNS Server: 0.0.0.0

Figure 3-7 Wizard: LAN Configuration

The following table describes the fields in this screen.

Table 3-6 Wizard: LAN Configuration

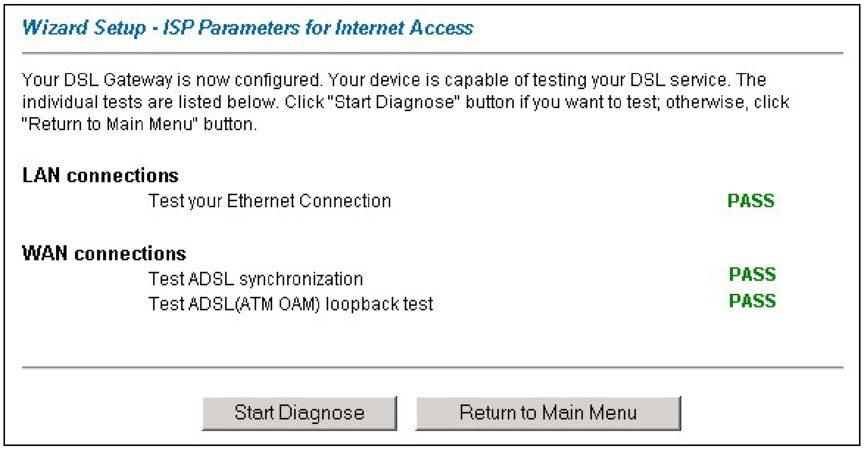
LABEL	DESCRIPTION

Table 3-6 Wizard: LAN Configuration

LABEL	DESCRIPTION
LAN IP Address	Enter the IP address of your Prestige in dotted decimal notation, for example, 192.168.1.1 (factory default). ☞ **If you changed the Prestige's LAN IP address, you must use the new IP address if you want to access the web configurator again.**
LAN Subnet Mask	Enter a subnet mask in dotted decimal notation.
DHCP	
DHCP Server	From the **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.

3.13 Wizard Setup Configuration: Connection Tests

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.



Wizard Setup - ISP Parameters for Internet Access

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

LAN connections

Test your Ethernet Connection	PASS

WAN connections

Test ADSL synchronization	PASS
Test ADSL(ATM OAM) loopback test	PASS

Figure 3-8 Wizard Screen 4

3.14 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.

Part II:

Password, LAN and WAN

This part covers the password, LAN (Local Area Network) and WAN setup.

Chapter 4
Password Setup

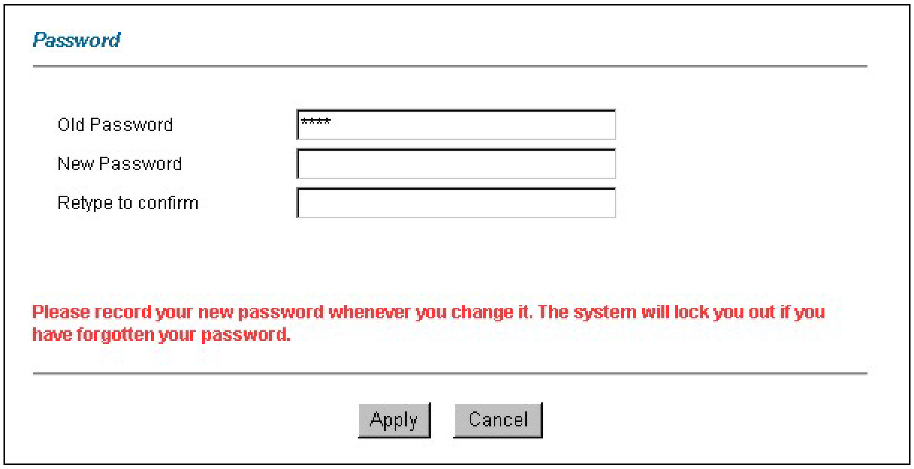
*This chapter provides information on the **Password** screen.*

4.1 Password Overview

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

4.2 Configuring Password

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



Password

Old Password: ****
New Password:
Retype to confirm:

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

Figure 4-1 Password

The following table describes the fields in this screen.

Table 4-1 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:

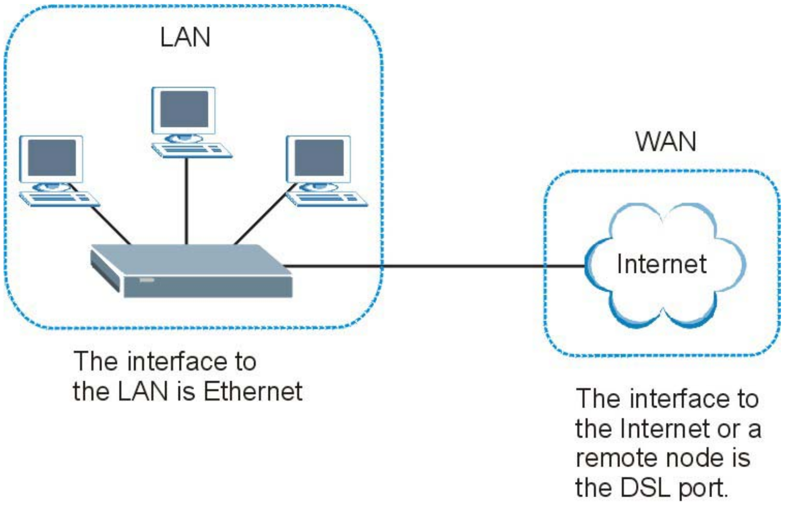

LAN
WAN
Internet
The interface to the LAN is Ethernet
The interface to the Internet or a remote node is the DSL port.

Figure 5-1 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 **Primary** and **Secondary DNS Server** fields in **LAN Setup**, otherwise, leave them blank.

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

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

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

5.3 DNS Server Address Assignment

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

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

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

5.4 LAN TCP/IP

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

5.4.1 Factory LAN Defaults

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

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

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

5.4.2 IP Address and Subnet Mask

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

5.4.3 RIP Setup

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

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

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

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

5.4.4 Multicast

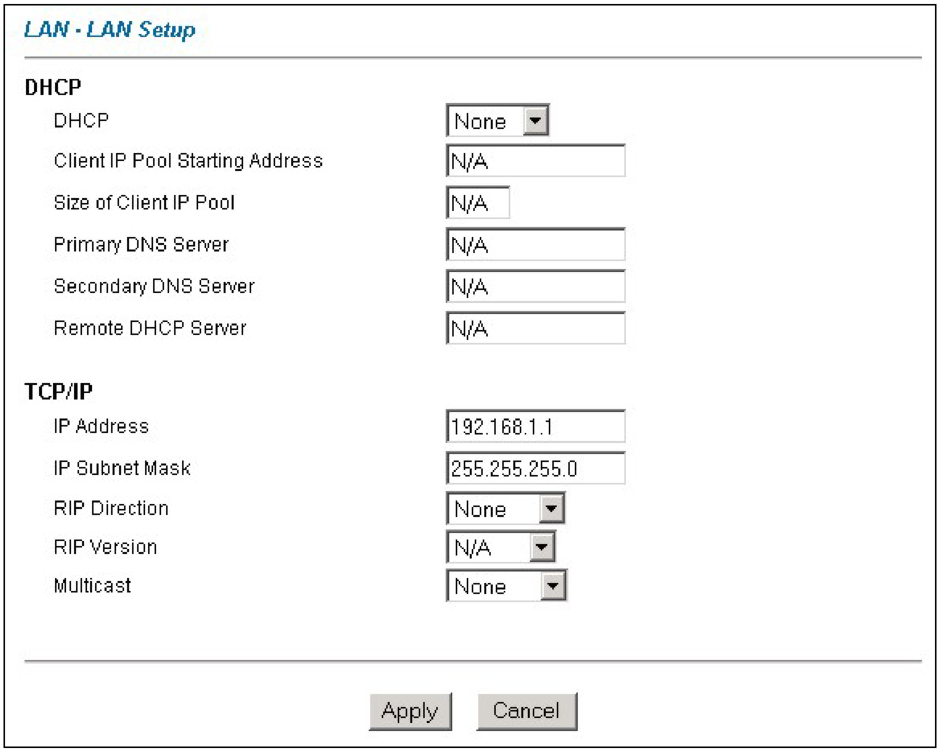
Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender - 1 recipient) or Broadcast (1 sender - everybody on the network). Multicast delivers IP packets to a group of hosts on the network - not everybody and not just 1.

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

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

5.5 Configuring LAN

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



LAN - LAN Setup

DHCP

DHCP: None

Client IP Pool Starting Address: N/A

Size of Client IP Pool: N/A

Primary DNS Server: N/A

Secondary DNS Server: N/A

Remote DHCP Server: N/A

TCP/IP

IP Address: 192.168.1.1

IP Subnet Mask: 255.255.255.0

RIP Direction: None

RIP Version: N/A

Multicast: None

Figure 5-2 LAN Setup

The following table describes the fields in this screen.

Table 5-1 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.

Table 5-1 LAN Setup

LABEL	DESCRIPTION
TCP/IP	
IP Address	Enter the IP address of your Prestige in dotted decimal notation, for example, 192.168.1.1 (factory default).
IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
RIP Direction	Select the RIP direction from **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 the *Wizard Setup* chapter for 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 *section 6.5*)
- Traffic-redirect route (see *section 6.6*)
- WAN-backup route, also called dial-backup (see *section 6.6*)

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

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

IP Policy Routing overrides the default routing behavior and takes priority over all of the routes mentioned above (see the *IP Policy Routing* chapter).

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.

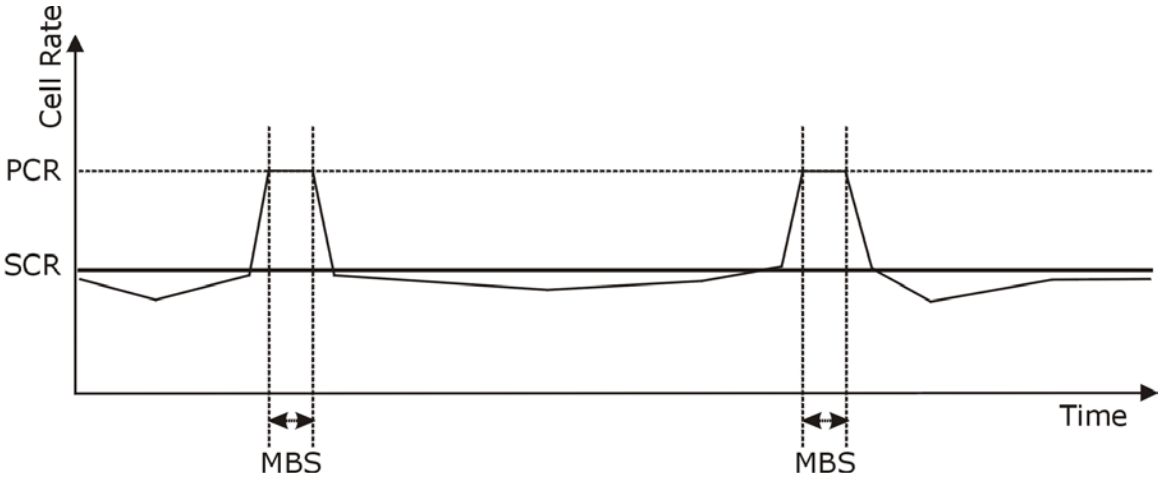
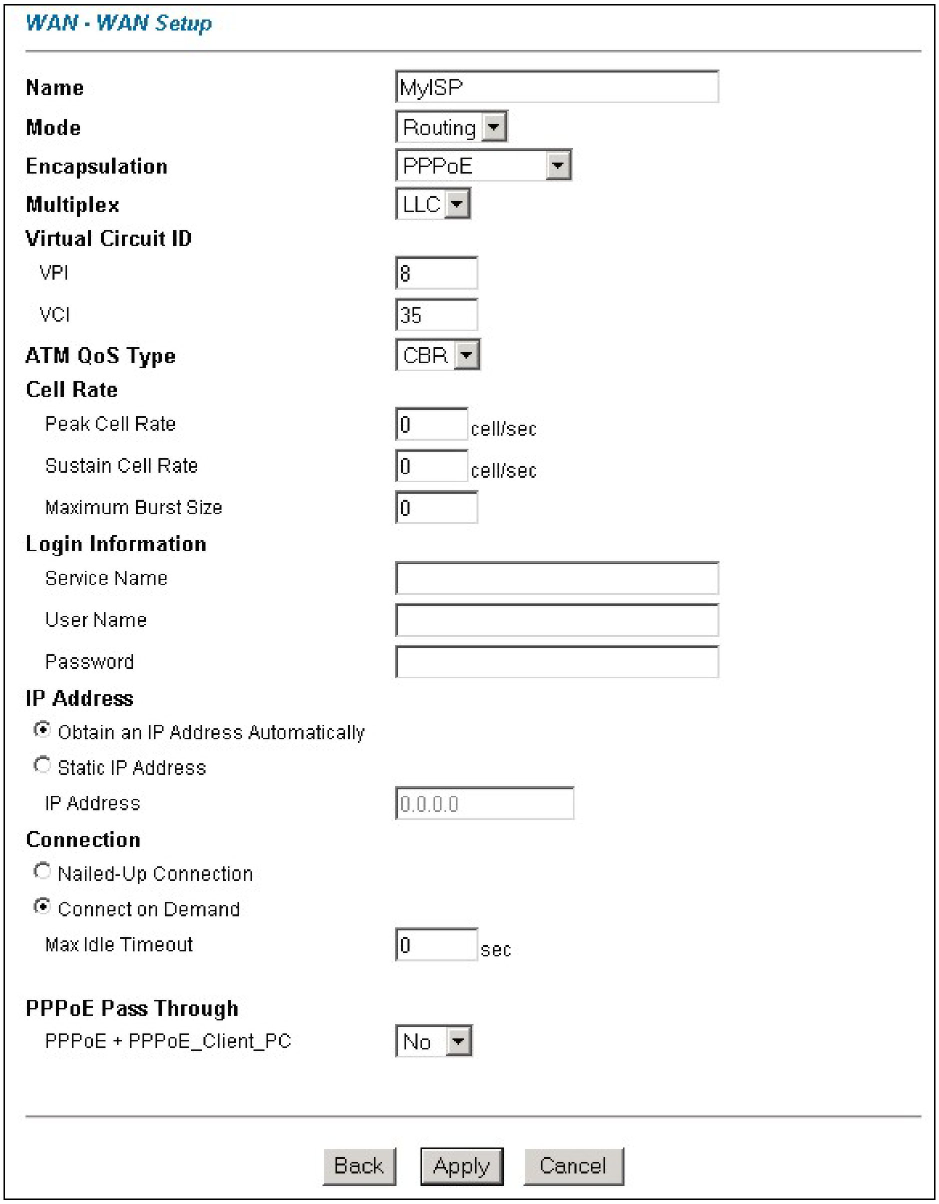


Figure 6-1 Example of Traffic Shaping

6.5 Configuring WAN Setup

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



WAN - WAN Setup

Name	MyISP
Mode	Routing
Encapsulation	PPPoE
Multiplex	LLC
Virtual Circuit ID	
VPI	8
VCI	35
ATM QoS Type	CBR
Cell Rate	
Peak Cell Rate	0 cell/sec
Sustain Cell Rate	0 cell/sec
Maximum Burst Size	0
Login Information	
Service Name	
User Name	
Password	
IP Address	
● Obtain an IP Address Automatically	
○ Static IP Address	
IP Address	0.0.0.0
Connection	
○ Nailed-Up Connection	
● Connect on Demand	
Max Idle Timeout	0 sec
PPPoE Pass Through	
PPPoE + PPPoE_Client_PC	No

Figure 6-2 WAN Setup (PPPoE)

The following table describes the fields in this screen.

Table 6-1 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 6-1 WAN Setup

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. The Single User Account feature can be used with either a dynamic or static IP address. 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.

Table 6-1 WAN Setup

LABEL	DESCRIPTION
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.
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 Pass Through	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 the *Subnetting* appendix on how 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.

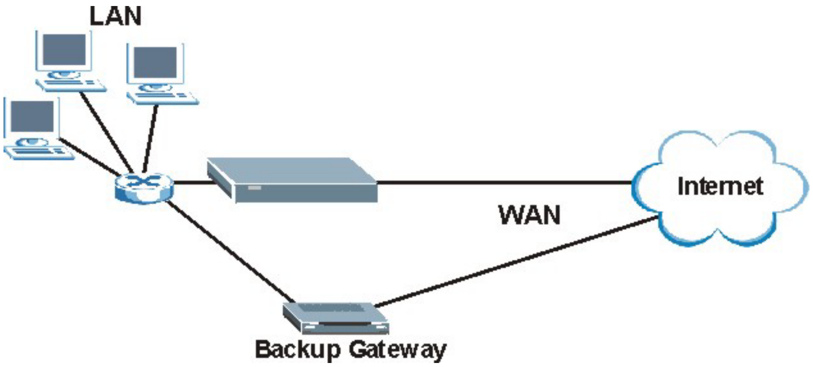


Figure 6-3 Traffic Redirect Example

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).

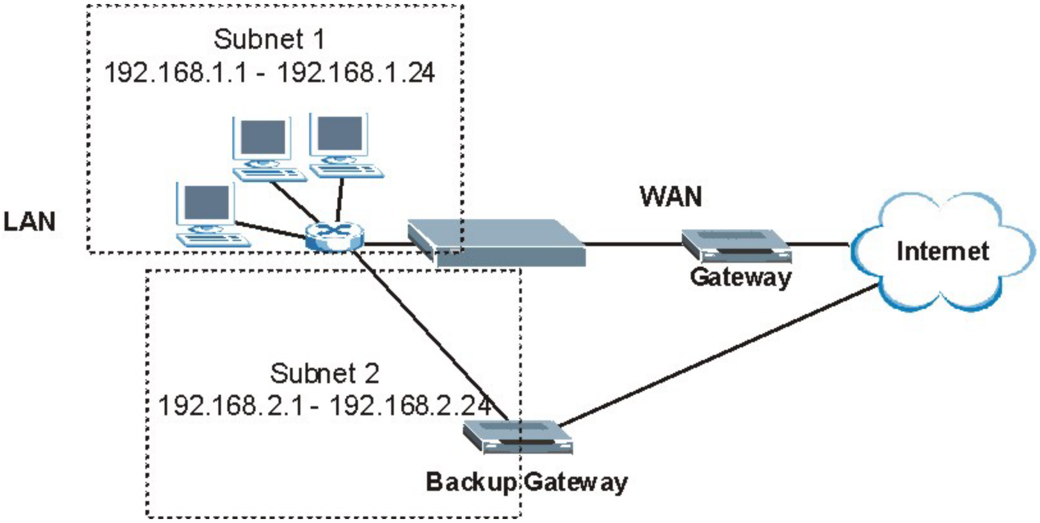
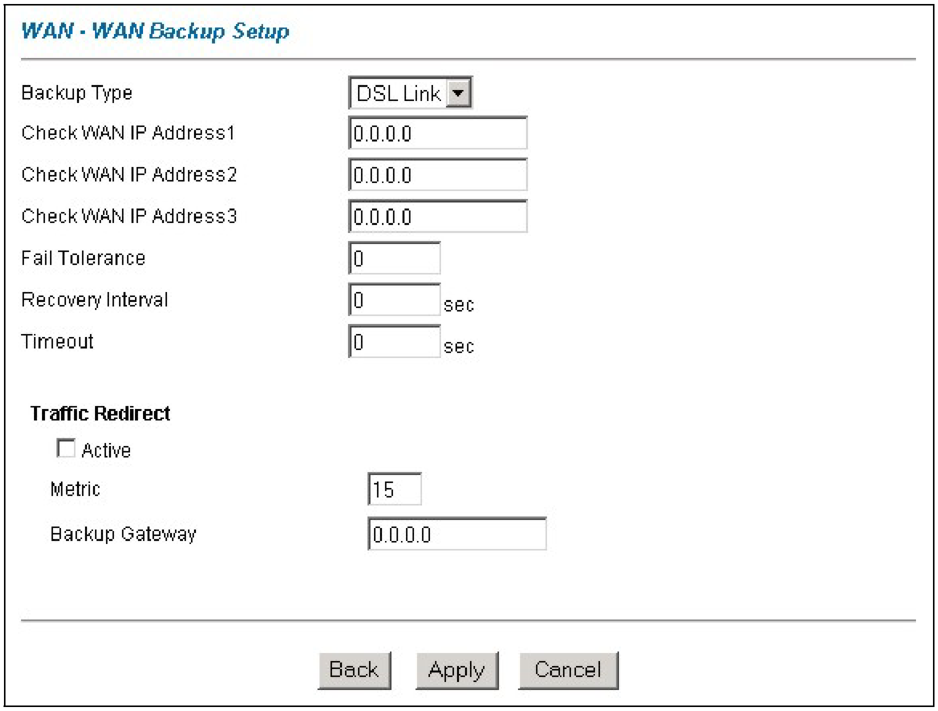


Figure 6-4 Traffic Redirect LAN Setup

6.7 Configuring WAN Backup

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



WAN - WAN Backup Setup

Backup Type	DSL Link
Check WAN IP Address1	0.0.0.0
Check WAN IP Address2	0.0.0.0
Check WAN IP Address3	0.0.0.0
Fail Tolerance	0
Recovery Interval	0 sec
Timeout	0 sec

Traffic Redirect

□ Active

Metric	15
Backup Gateway	0.0.0.0

Figure 6-5 WAN Backup

The following table describes the fields in this screen.

Table 6-2 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 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.
Fail Tolerance	Type the number of times (2 recommended) that your Prestige may ping the IP addresses configured in the **Check WAN IP Address** fields 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** fields 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.
Traffic Redirect	

Table 6-2 WAN Backup

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

Part III:

NAT, Dynamic DNS and Time and Date

This part covers NAT (Network Address Translation), dynamic DNS (Domain Name Sever) and Time and Date setup.

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 7-1 NAT Definitions

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

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

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 7-2*), NAT offers the additional benefit of firewall protection. With no servers defined, your Prestige filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631*, *The IP Network Address Translator (NAT)*.

7.1.3 How NAT Works

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

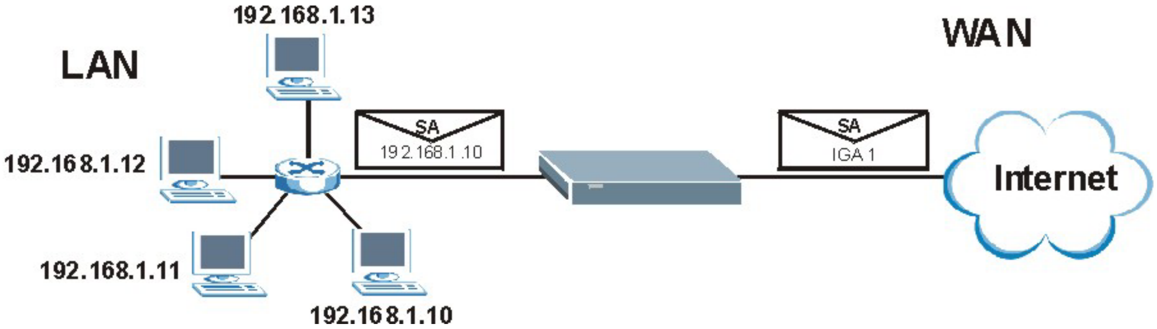


Figure 7-1 How NAT Works

7.1.4 NAT Application

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

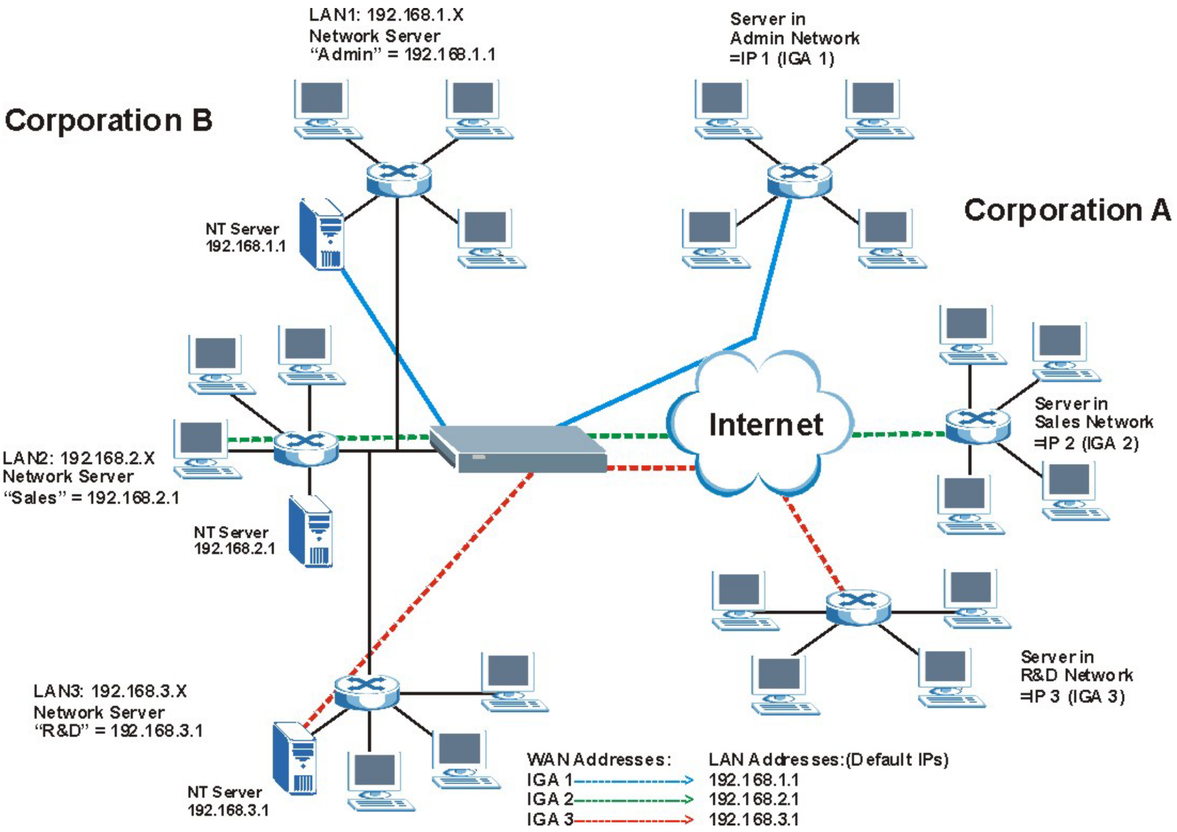


Figure 7-2 NAT Application With IP Alias

7.1.5 NAT Mapping Types

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

One to One: In One-to-One mode, the Prestige maps one local IP address to one global IP address.

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

Many to Many Overload: In Many-to-Many Overload mode, the Prestige maps the multiple local IP addresses to shared global IP addresses.

Many-to-Many No Overload: In Many-to-Many No Overload mode, the Prestige maps each local IP address to a unique global IP address.

Server: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.

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

The following table summarizes these types.

Table 7-2 NAT Mapping Types

TYPE	IP MAPPING	SMT ABBREVIATION
One-to-One	ILA1←→ IGA1	1:1
Many-to-One (SUA/PAT)	ILA1←→ IGA1	M:1

Table 7-2 NAT Mapping Types

TYPE	IP MAPPING	SMT ABBREVIATION
	ILA2←→ IGA1 …	

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 7-2*.

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

7.3 SUA Server

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

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

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

Default Server IP Address

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

If you do not assign 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.

7.3.1 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 7-3 Services and Port Numbers

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

7.3.2 Configuring Servers Behind SUA (Example)

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

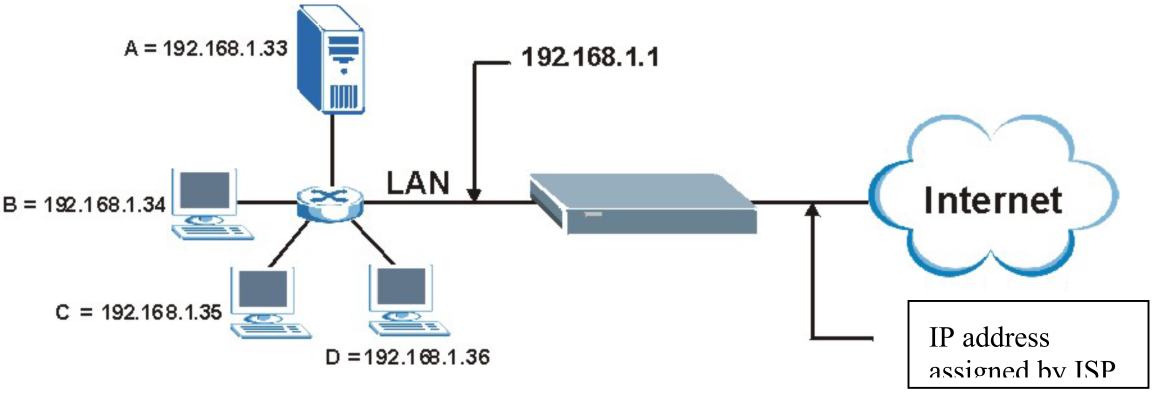
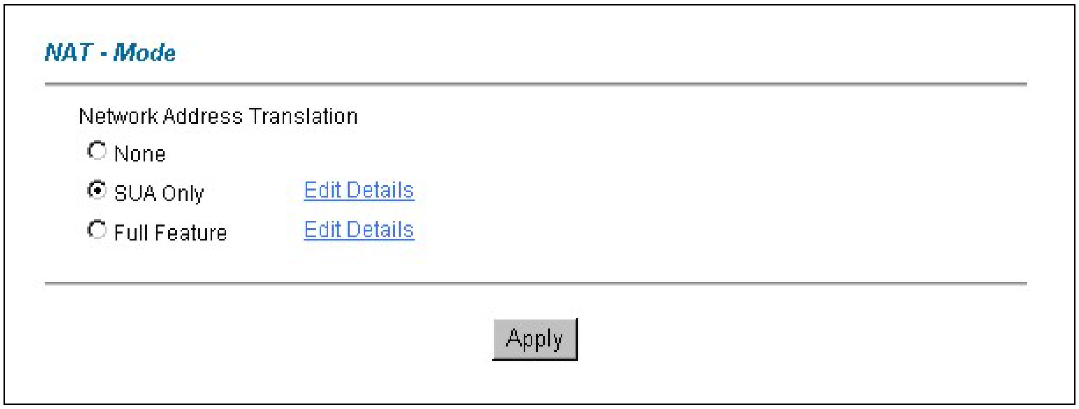


Figure 7-3 Multiple Servers Behind NAT Example

7.4 Selecting the NAT Mode

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

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



NAT - Mode

Network Address Translation

○ None

● SUA Only

○ Full Feature

Figure 7-4 NAT Mode

The following table describes the labels in this screen.

Table 7-4 NAT Mode

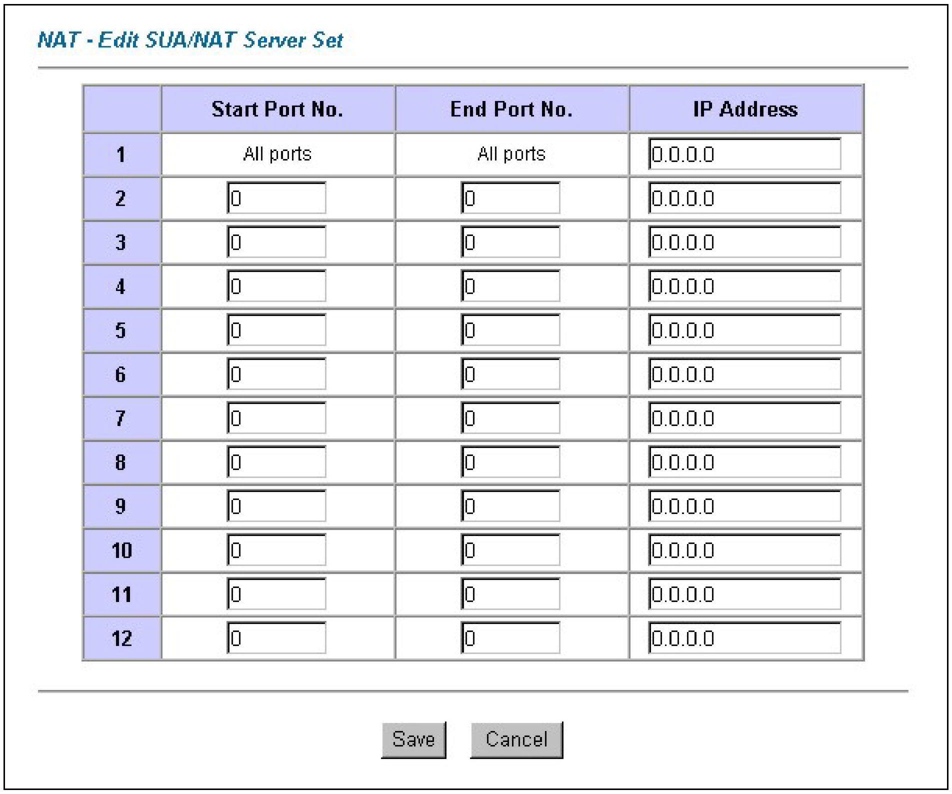
LABEL	DESCRIPTION
None	Select this radio button to disable NAT.
SUA Only	Select this radio button if you have just one public WAN IP address for your Prestige. The Prestige uses Address Mapping Set 1 in the **NAT - Edit SUA/NAT Server Set** screen.
Edit Details	Click this link to go to the **NAT - Edit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

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



NAT - Edit SUA/NAT Server Set

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

Figure 7-5 Edit SUA/NAT Server Set

The following table describes the fields in this screen.

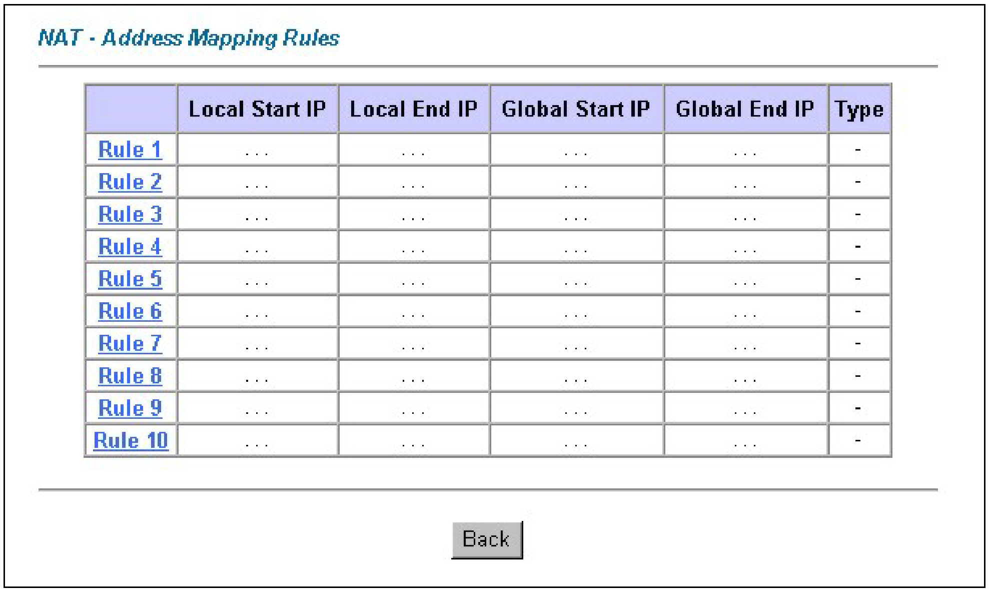
Table 7-5 Edit SUA/NAT Server Set

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.
Server 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.



NAT - Address Mapping Rules

	Local Start IP	Local End IP	Global Start IP	Global End IP	Type
Rule 1	...	...	...	...	-
Rule 2	...	...	...	...	-
Rule 3	...	...	...	...	-
Rule 4	...	...	...	...	-
Rule 5	...	...	...	...	-
Rule 6	...	...	...	...	-
Rule 7	...	...	...	...	-
Rule 8	...	...	...	...	-
Rule 9	...	...	...	...	-
Rule 10	...	...	...	...	-

Figure 7-6 Address Mapping Rules

The following table describes the fields in this screen.

Table 7-6 Address Mapping Rules

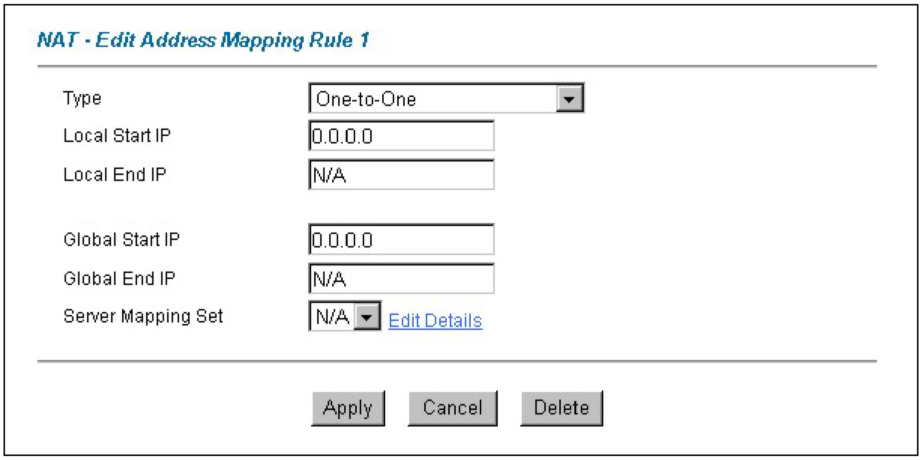
LABEL	DESCRIPTION
Local Start IP	This is the starting Inside Local IP Address (ILA). Local IP addresses are **N/A** for **Server** port mapping.
Local End IP	This is the end Inside Local IP Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 as the **Local Start 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 7-6 Address Mapping Rules

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.



NAT - Edit Address Mapping Rule 1

Type	One-to-One
Local Start IP	0.0.0.0
Local End IP	N/A
Global Start IP	0.0.0.0
Global End IP	N/A
Server Mapping Set	N/A

Figure 7-7 Address Mapping Rule Edit

The following table describes the fields in this screen.

Table 7-7 Address Mapping Rule Edit

LABEL	DESCRIPTION
Type	Choose the port mapping type from one of the following. 1. **One-to-One**: One-to-One mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-one NAT mapping type. 2. **Many-to-One**: Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature that previous ZyXEL routers supported only. 3. **Many-to-Many Overload**: Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. 4. **Many-to-Many No Overload**: Many-to-Many No Overload mode maps each local IP address to unique global IP addresses. 5. **Server**: This type allows you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Local Start IP	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.

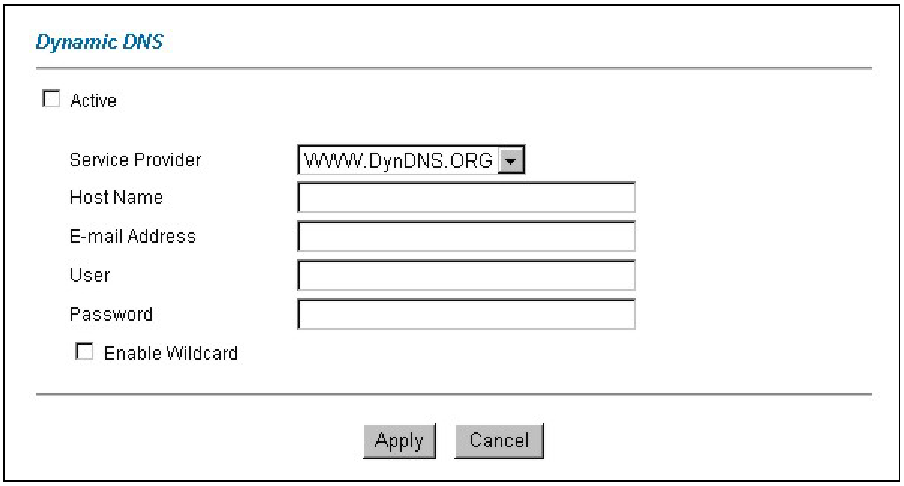
8.1.1 DYNDNS Wildcard

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.

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.



Dynamic DNS

☐ Active

Service Provider	WWW.DynDNS.ORG
Host Name	
E-mail Address	
User	
Password	

☐ Enable Wildcard

Figure 8-1 Dynamic DNS

The following table describes the fields in this screen.

Table 8-1 Dynamic DNS

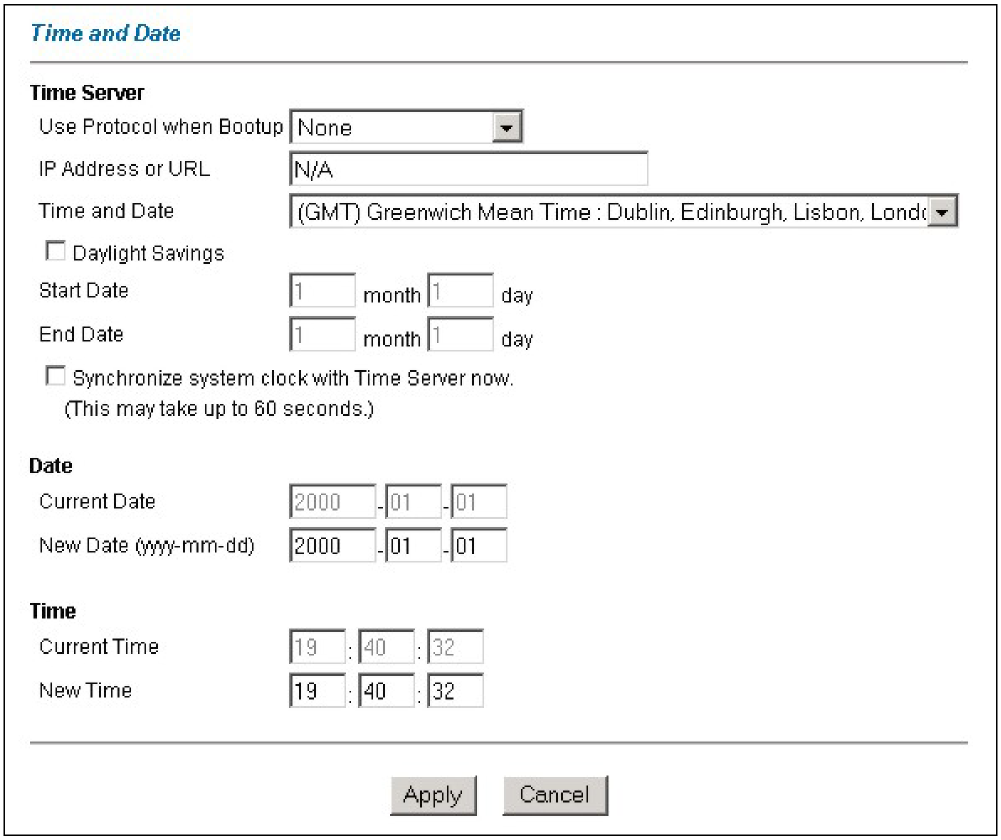
LABEL	DESCRIPTION
Active	Select this check box to use dynamic DNS.
Service Provider	This is the name of your Dynamic DNS service provider.
Host Names	Type the domain name assigned to your Prestige by your Dynamic DNS provider.
E-mail Address	Type your e-mail address.
User	Type your user name.
Password	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.



Time and Date

Time Server

Use Protocol when Bootup	None
IP Address or URL	N/A
Time and Date	(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, Londo

□ Daylight Savings

Start Date	1 month 1 day
End Date	1 month 1 day

□ Synchronize system clock with Time Server now.
(This may take up to 60 seconds.)

Date

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

Time

Current Time	19 : 40 : 32
New Time	19 : 40 : 32

Figure 9-1 Time and Date

The following table describes the fields in this screen.

Table 9-1 Time and Date

LABEL	DESCRIPTION
Time Server	

Table 9-1 Time and Date

LABEL	DESCRIPTION
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 (the default is tick.stdtime.gov.tw).
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.

Part IV:

Firewall and Content Filter

This part introduces firewalls in general and the Prestige firewall. It also explains customized services and logs and gives example firewall rules and an overview of content filtering.

Chapter 10 Firewalls

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

10.1 Firewall Overview

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

10.2 Types of Firewalls

There are three main types of firewalls:

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

10.2.1 Packet Filtering Firewalls

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

10.2.2 Application-level Firewalls

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

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

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

10.2.3 Stateful Inspection Firewalls

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also "inspect" the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency, however, they may lack the granular application level access control or caching that some proxies support. See *section 10.5* for more information on Stateful Inspection.

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

10.3 Introduction to ZyXEL's Firewall

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

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

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

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

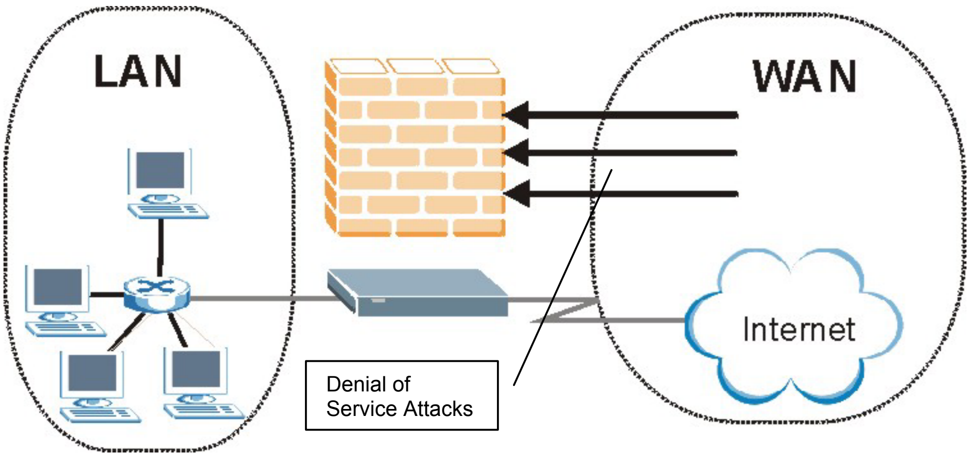


Figure 10-1 Prestige Firewall Application

10.4 Denial of Service

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

10.4.1 Basics

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

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

Some of the most common IP ports are:

Table 10-1 Common IP Ports

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

10.4.2 Types of DoS Attacks

There are four types of DoS attacks:

1. Those that exploit bugs in a TCP/IP implementation.
2. Those that exploit weaknesses in the TCP/IP specification.
3. Brute-force attacks that flood a network with useless data.
4. IP Spoofing.

1. "**Ping of Death**" and "**Teardrop**" attacks exploit bugs in the TCP/IP implementations of various computer and host systems.

   ♦ Ping of Death uses a "ping" utility to create an IP packet that exceeds the maximum 65,536 bytes of data allowed by the IP specification. The oversize packet is then sent to an unsuspecting system. Systems may crash, hang or reboot.

   ♦ Teardrop attack exploits weaknesses in the re-assembly of IP packet fragments. As data is transmitted through a network, IP packets are often broken up into smaller chunks. Each fragment looks like the original IP packet except that it contains an offset field that says, for instance, "This fragment is carrying bytes 200 through 400 of the original (non fragmented) IP packet." The Teardrop program creates a series of IP fragments with overlapping offset fields. When these fragments are reassembled at the destination, some systems will crash, hang, or reboot.

2. Weaknesses in the TCP/IP specification leave it open to "**SYN Flood**" and "**LAND**" attacks. These attacks are executed during the handshake that initiates a communication session between two applications.

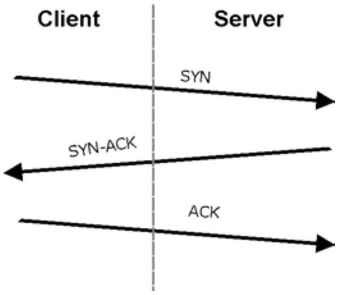


Figure 10-2 Three-Way Handshake

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

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

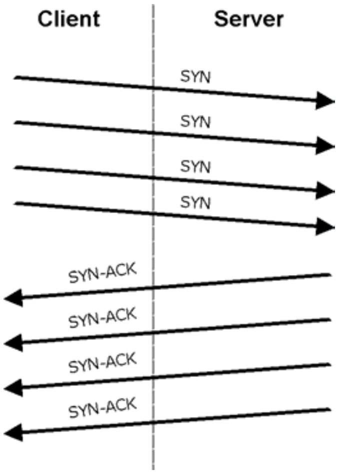


Figure 10-3 SYN Flood

- In a **LAND Attack**, hackers flood SYN packets into the network with a spoofed source IP address of the targeted system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

3. A **brute-force** attack, such as a "Smurf" attack, targets a feature in the IP specification known as directed or subnet broadcasting, to quickly flood the target network with useless data. A Smurf hacker floods a router with Internet Control Message Protocol (ICMP) echo request packets (pings). Since the destination IP address of each packet is the broadcast address of the network, the router will broadcast the ICMP echo request packet to all hosts on the network. If there are

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

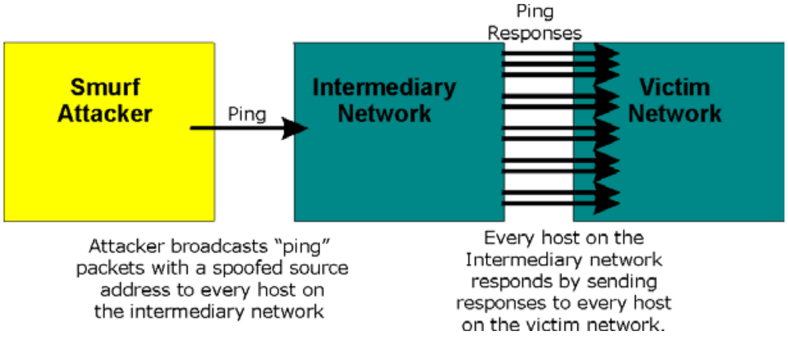

Ping
Responses
Smurf
Attacker
Ping
Intermediary
Network
Victim
Network
Attacker broadcasts "ping" packets with a spoofed source address to every host on the intermediary network
Every host on the Intermediary network responds by sending responses to every host on the victim network.

Figure 10-4 Smurf Attack

ICMP Vulnerability

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

Table 10-2 ICMP Commands That Trigger Alerts

5	REDIRECT
13	TIMESTAMP_REQUEST
14	TIMESTAMP_REPLY
17	ADDRESS_MASK_REQUEST
18	ADDRESS_MASK_REPLY

Illegal Commands (NetBIOS and SMTP)

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

Table 10-3 Legal NetBIOS Commands

MESSAGE:
REQUEST:
POSITIVE:
NEGATIVE:
RETARGET:
KEEPALIVE:

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

Table 10-4 Legal SMTP Commands

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

Traceroute

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

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

10.5 Stateful Inspection

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

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

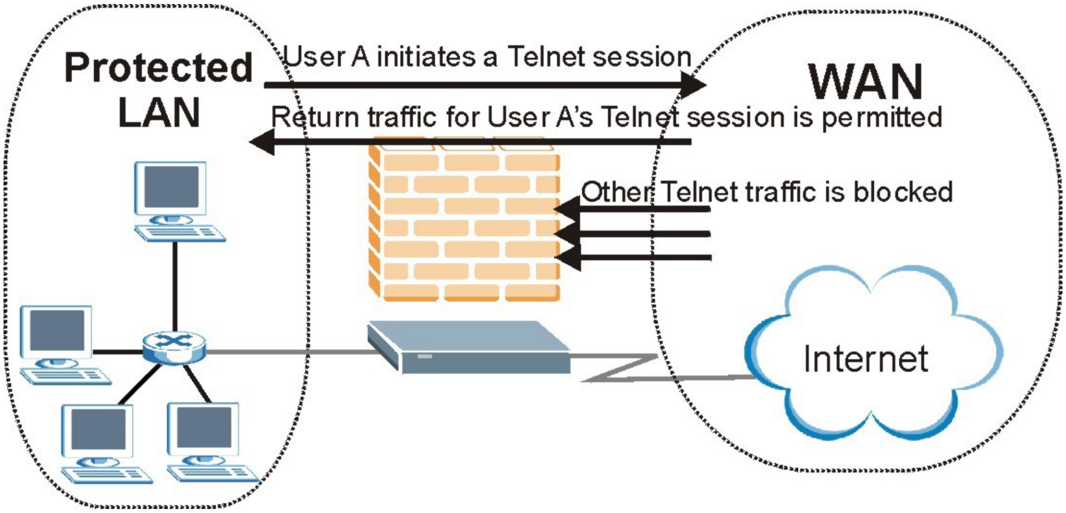

Protected LAN
User A initiates a Telnet session
WAN
Return traffic for User A's Telnet session is permitted
Other Telnet traffic is blocked
Internet

Figure 10-5 Stateful Inspection

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

10.5.1 Stateful Inspection Process

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

1. The packet travels from the firewall's LAN to the WAN.
2. The packet is evaluated against the interface's existing outbound access list, and the packet is permitted (a denied packet would simply be dropped at this point).
3. The packet is inspected by a firewall rule to determine and record information about the state of the packet's connection. This information is recorded in a new state table entry created for the new connection. If there is not a firewall rule for this packet and it is not an attack, then **The default action for packets not matching following rules** field (see *Figure 12-3*) determines the action for this packet.
4. Based on the obtained state information, a firewall rule creates a temporary access list entry that is inserted at the beginning of the WAN interface's inbound extended access list. This temporary access list entry is designed to permit inbound packets of the same connection as the outbound packet just inspected.
5. The outbound packet is forwarded out through the interface.
6. Later, an inbound packet reaches the interface. This packet is part of the connection previously established with the outbound packet. The inbound packet is evaluated against the inbound access list, and is permitted because of the temporary access list entry previously created.
7. The packet is inspected by a firewall rule, and the connection's state table entry is updated as necessary. Based on the updated state information, the inbound extended access list temporary entries might be modified, in order to permit only packets that are valid for the current state of the connection.
8. Any additional inbound or outbound packets that belong to the connection are inspected to update the state table entry and to modify the temporary inbound access list entries as required, and are forwarded through the interface.
9. When the connection terminates or times out, the connection's state table entry is deleted and the connection's temporary inbound access list entries are deleted.

10.5.2 Stateful Inspection and the Prestige

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

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

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

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

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

10.5.3 TCP Security

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

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

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

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

10.5.4 UDP/ICMP Security

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

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

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

10.5.5 Upper Layer Protocols

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

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

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

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

10.6 Guidelines for Enhancing Security with Your Firewall

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

10.6.1 Security In General

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

- Encourage your company or organization to develop a comprehensive security plan. Good network administration takes into account what hackers can do and prepares against attacks. The best defense against hackers and crackers is information. Educate all employees about the importance of security and how to minimize risk. Produce lists like this one!
- DSL or cable modem connections are "always-on" connections and are particularly vulnerable because they provide more opportunities for hackers to crack your system. Turn your computer off when not in use.
- Never give out a password or any sensitive information to an unsolicited telephone call or e-mail.
- Never e-mail sensitive information such as passwords, credit card information, etc., without encrypting the information first.
- Never submit sensitive information via a web page unless the web site uses secure connections. You can identify a secure connection by looking for a small "key" icon on the bottom of your browser (Internet Explorer 3.02 or better or Netscape 3.0 or better). If a web

site uses a secure connection, it is safe to submit information. Secure web transactions are quite difficult to crack.

- Never reveal your IP address or other system networking information to people outside your company. Be careful of files e-mailed to you from strangers. One common way of getting BackOrifice on a system is to include it as a Trojan horse with other files.
- Change your passwords regularly. Also, use passwords that are not easy to figure out. The most difficult passwords to crack are those with upper and lower case letters, numbers and a symbol such as % or #.
- Upgrade your software regularly. Many older versions of software, especially web browsers, have well known security deficiencies. When you upgrade to the latest versions, you get the latest patches and fixes.
- If you use "chat rooms" or IRC sessions, be careful with any information you reveal to strangers.
- If your system starts exhibiting odd behavior, contact your ISP. Some hackers will set off hacks that cause your system to slowly become unstable or unusable.
- Always shred confidential information, particularly about your computer, before throwing it away. Some hackers dig through the trash of companies or individuals for information that might help them in an attack.

10.7 Packet Filtering Vs Firewall

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

10.7.1 Packet Filtering:

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

When To Use Filtering

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

10.7.2 Firewall

- The firewall inspects packet contents as well as their source and destination addresses. Firewalls of this type employ an inspection module, applicable to all protocols, that understands data in the packet is intended for other layers, from the network layer (IP headers) up to the application layer.

- The firewall performs stateful inspection. It takes into account the state of connections it handles so that, for example, a legitimate incoming packet can be matched with the outbound request for that packet and allowed in. Conversely, an incoming packet masquerading as a response to a nonexistent outbound request can be blocked.
- The firewall uses session filtering, i.e., smart rules, that enhance the filtering process and control the network session rather than control individual packets in a session.
- The firewall provides e-mail service to notify you of routine reports and when alerts occur.

When To Use The Firewall

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

Chapter 11
Firewall Configuration

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

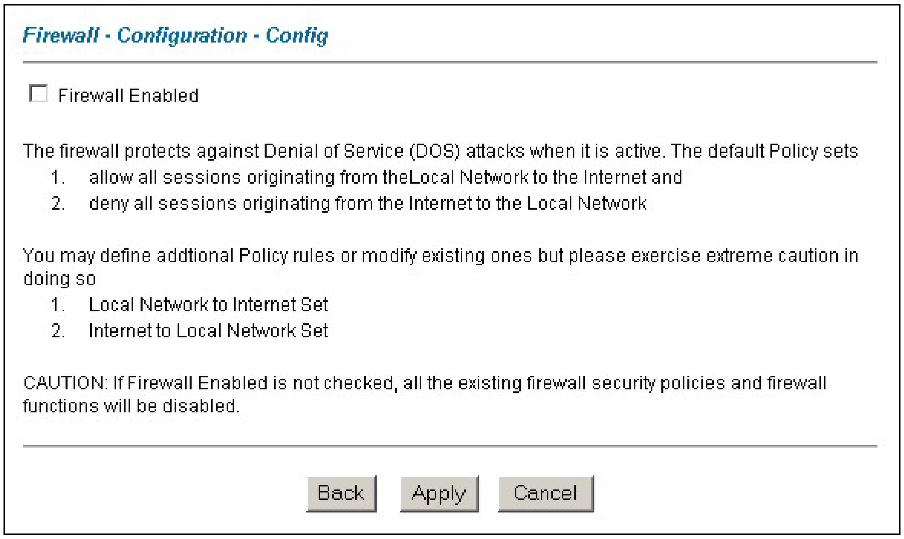
11.1 Remote Management and the Firewall

When remote management is configured to allow management (see the *Remote Management* chapter) and the firewall is enabled:

- The firewall blocks remote management from the WAN unless you configure a firewall rule to allow it.
- The firewall allows remote management from the LAN.

11.2 Enabling the Firewall

Click **Firewall** and then **Config** to display the following screen. Select the **Firewall Enabled** check box and click **Apply** to enable (or activate) the firewall.



Firewall - Configuration - Config

□ Firewall Enabled

The firewall protects against Denial of Service (DOS) attacks when it is active. The default Policy sets
1. allow all sessions originating from theLocal Network to the Internet and
2. deny all sessions originating from the Internet to the Local Network

You may define addtional Policy rules or modify existing ones but please exercise extreme caution in doing so
1. Local Network to Internet Set
2. Internet to Local Network Set

CAUTION: If Firewall Enabled is not checked, all the existing firewall security policies and firewall functions will be disabled.

Figure 11-1 Enabling the Firewall

11.3 Attack Alert

Attack alerts are real-time reports of DoS attacks. In the **Alert** screen, shown later, you may choose to generate an alert whenever an attack is detected. For DoS attacks, the Prestige uses thresholds to determine when to drop sessions that do not become fully established. These thresholds apply globally to all sessions.

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

11.3.1 Alerts

Alerts are reports on events, such as attacks, that you may want to know about right away. You can choose to generate an alert when an attack is detected in the **Alert** screen *(Figure 11-2* - select the **Generate alert when attack detected** checkbox) or when a rule is matched in the **Edit Rule** screen (see *Figure 12-4).* When an event generates an alert, a message can be immediately sent to an e-mail account that you specify in the **Log Settings** screen (see the chapter on logs).

11.3.2 Threshold Values

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

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

If your network is slower than average for any of these factors (especially if you have servers that are slow or handle many tasks and are often busy), then the default values should be reduced.
You should make any changes to the threshold values before you continue configuring firewall rules.

11.3.3 Half-Open Sessions

An unusually high number of half-open sessions (either an absolute number or measured as the arrival rate) could indicate that a Denial of Service attack is occurring. For TCP, "half-open" means that the session has not reached the established state-the TCP three-way handshake has not yet been completed (see *Figure 10-2*). For UDP, "half-open" means that the firewall has detected no return traffic.

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

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

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

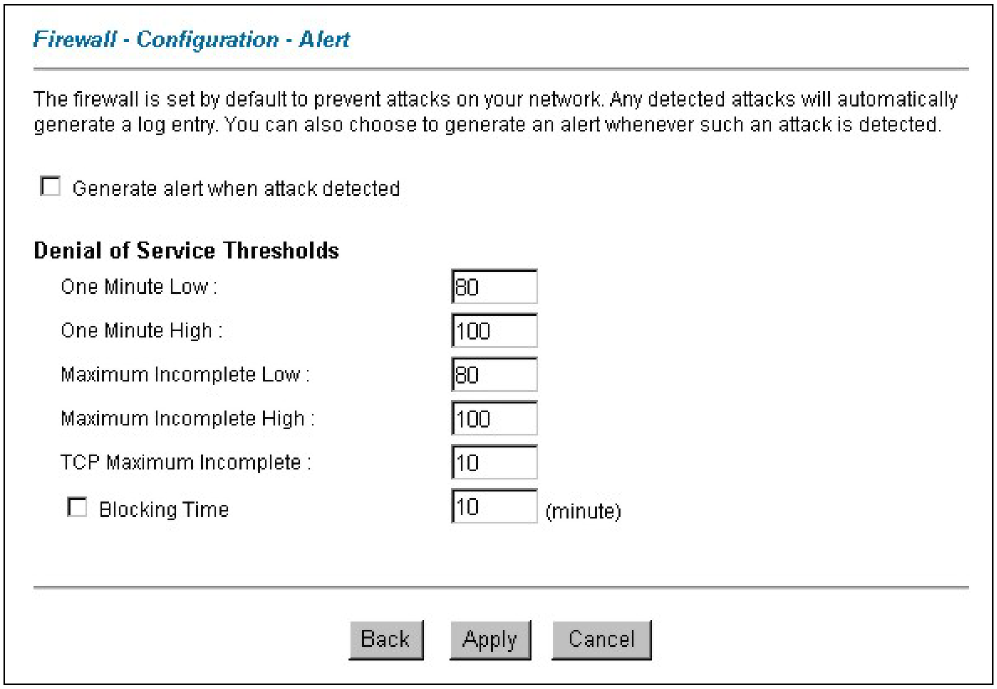
TCP Maximum Incomplete and Blocking Time

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

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

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

The Prestige also sends alerts whenever **TCP Maximum Incomplete** is exceeded. The global values specified for the threshold and timeout apply to all TCP connections. Click **Firewall**, and **Alert** to bring up the next screen.



Firewall - Configuration - Alert

The firewall is set by default to prevent attacks on your network. Any detected attacks will automatically generate a log entry. You can also choose to generate an alert whenever such an attack is detected.

□ Generate alert when attack detected

Denial of Service Thresholds

One Minute Low :	80
One Minute High :	100
Maximum Incomplete Low :	80
Maximum Incomplete High :	100
TCP Maximum Incomplete :	10
□ Blocking Time	10 (minute)

Figure 11-2 Alert

The following table describes the labels in this screen.

Table 11-1 Alert

LABEL	DESCRIPTION
Generate alert when attack detected	Select this check box to generate an alert whenever an attack is detected.
Denial of Services Thresholds	
One Minute Low	This is the rate of new half-open sessions that causes the firewall to stop deleting half-open sessions. The Prestige continues to delete half-open sessions as necessary, until the rate of new connection attempts drops below this number. "80" is the default.
One Minute High	This is the rate of new half-open sessions that causes the firewall to start deleting half-open sessions. The default is "100". When the rate of new connection attempts rises above this number, the Prestige deletes half-open sessions as required to accommodate new connection attempts. The Prestige stops deleting half-open sessions when the number is less than the **One Minute Low.**

Table 11-1 Alert

LABEL	DESCRIPTION
Maximum Incomplete Low	This is the number of existing half-open sessions (default "80") that causes the firewall to stop deleting half-open sessions. The Prestige continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below this number.
Maximum Incomplete High	This is the number of existing half-open sessions (default "100") that causes the firewall to start deleting half-open sessions. When the number of existing half-open sessions rises above this number, the Prestige deletes half-open sessions as required to accommodate new connection requests. The Prestige stops deleting half-open sessions when the number is less than the **Max Incomplete Low**. Do not set **Maximum Incomplete High** to lower than the current **Max Incomplete Low** number.
TCP Maximum Incomplete	This is the number of existing half-open TCP sessions (default "10") with the same destination host IP address that causes the firewall to start dropping half-open sessions to that same destination host IP address. Enter a number between **1** and **256**. As a general rule, you should choose a smaller number for a smaller network, a slower system or limited bandwidth.
Blocking Time	When **TCP Maximum Incomplete** is reached you can choose if the next session should be allowed or blocked. If you select **Blocking Time**, any new sessions will be blocked for the length of time you specify in the next field **(minute)** and all old incomplete sessions will be cleared during this period. If you want strong security, it is better to block the traffic for a short time, as it will give the server some time to digest the loading.
(minute)	Type the length of **Blocking Time** in minutes (1-256). The default is "0".
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to return to the previously saved settings.

Chapter 12
Creating Custom Rules

This chapter contains instructions for defining both Local Network and Internet rules.

12.1 Rules Overview

Firewall rules are subdivided into "Local Network" and "Internet". By default, the Prestige's stateful packet inspection allows all communications to the Internet that originate from the local network, and blocks all traffic to the LAN that originates from the Internet. You may define additional rules and sets or modify existing ones but please exercise extreme caution in doing so.

You might inadvertently introduce security risks to the firewall and to the protected network, if you try to configure rules without a good understanding of how rules work. Make sure you test your rules after you configure them.

For example, you may create rules to:

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

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

12.2 Rule Logic Overview

Study these points carefully before configuring rules.

12.2.1 Rule Checklist

1. State the intent of the rule. For example, "This restricts all IRC access from the LAN to the Internet." Or, "This allows a remote Lotus Notes server to synchronize over the Internet to an inside Notes server."
2. Is the intent of the rule to forward or block traffic?
3. What is the direction connection: from the LAN to the Internet, or from the Internet to the LAN?
4. What IP services will be affected?
5. What computers on the LAN are to be affected (if any)?
6. What computers on the Internet will be affected? The more specific, the better. For example, if traffic is being allowed from the Internet to the LAN, it is better to allow only certain machines on the Internet to access the LAN.

12.2.2 Security Ramifications

1. Once the logic of the rule has been defined, it is critical to consider the security ramifications created by the rule:
2. Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?
3. Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, will a rule that blocks just certain users be more effective?
4. Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users may be able to connect to computers with running FTP servers.
5. Does this rule conflict with any existing rules?
6. Once these questions have been answered, adding rules is simply a matter of plugging the information into the correct fields in the **Rules** screen in the web configurator.

12.2.3 Key Fields For Configuring Rules

Action

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

"Block" means the firewall silently discards the packet.

Service

Select the service from the **Service** scrolling list box. If the service is not listed, it is necessary to first define it. See *section 12.5* for more information on predefined services.

Source Address

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

Destination Address

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

12.3 Connection Direction

This section talks about configuring firewall rules for connections going from LAN to WAN and WAN to LAN in your firewall.

12.3.1 LAN to WAN Rules

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

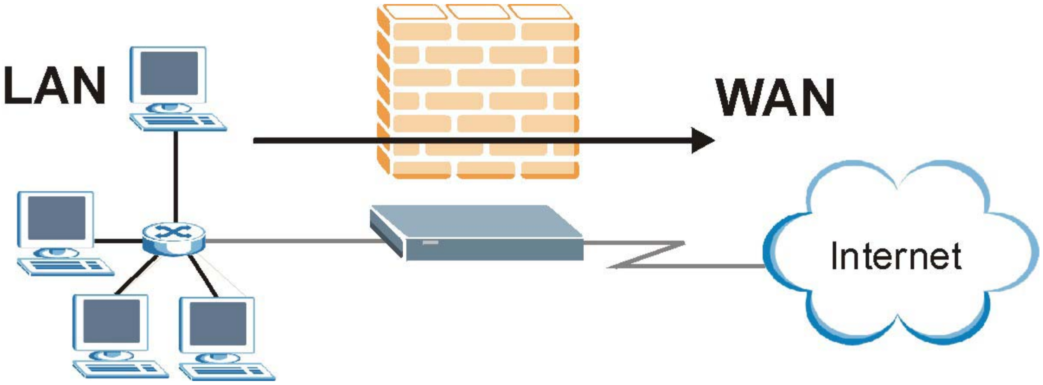


Figure 12-1 LAN to WAN Traffic

12.3.2 WAN to LAN Rules

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

See the following figure.

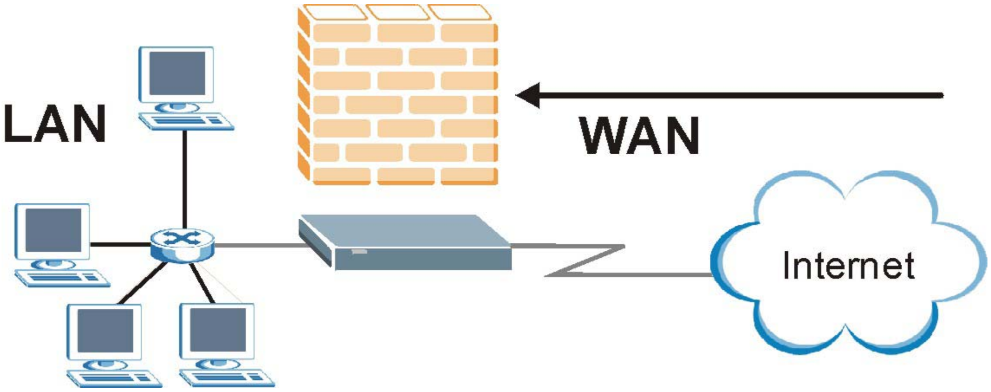


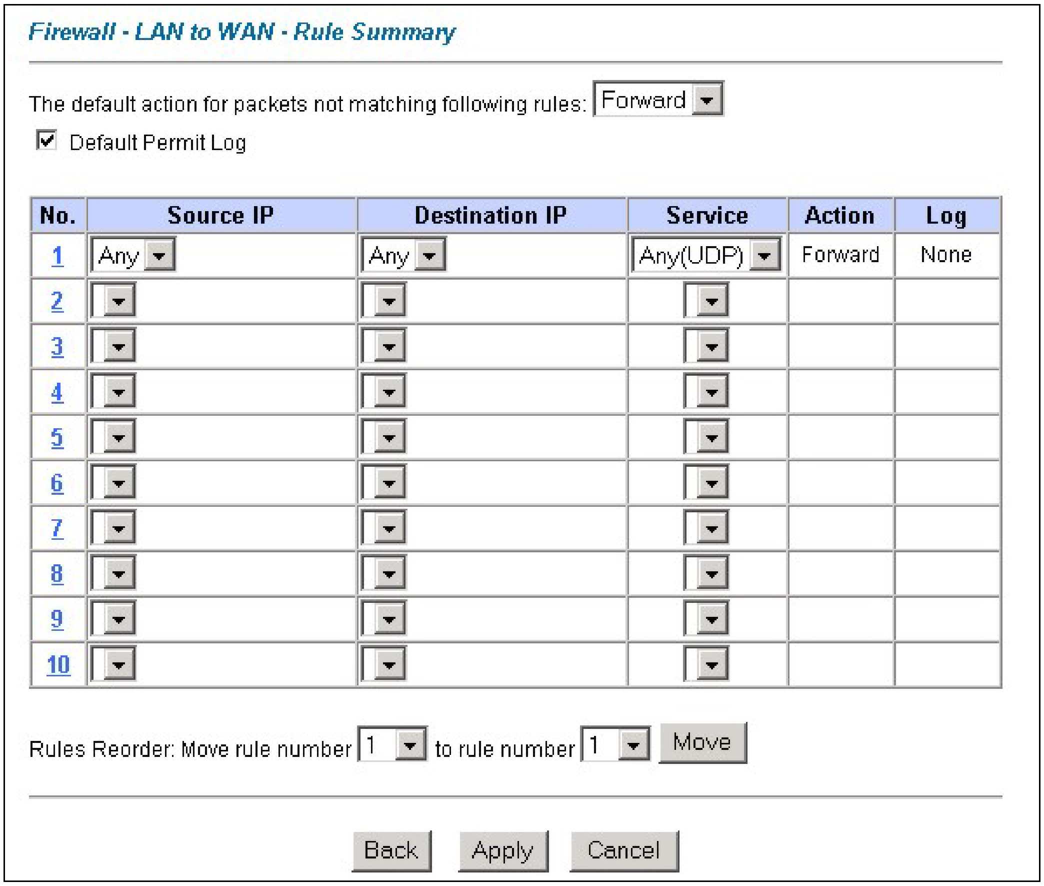
Figure 12-2 WAN to LAN Traffic

12.4 Rule Summary

The fields in the **Rule Summary** screens are the same for **Local Network to Internet Set** and **Internet to Local Network Set**, so the discussion below refers to both.

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

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



Firewall - LAN to WAN - Rule Summary

The default action for packets not matching following rules: Forward

☑ Default Permit Log

No.	Source IP	Destination IP	Service	Action	Log
1	Any	Any	Any(UDP)	Forward	None
2					
3					
4					
5					
6					
7					
8					
9					
10					

Rules Reorder: Move rule number 1 to rule number 1

Figure 12-3 Firewall Rules Summary: First Screen

The following table describes the labels in this screen.

Table 12-1 Firewall Rules Summary: First Screen

LABEL	DESCRIPTION
The default action for packets not matching following rules	Use the drop-down list box to select whether to **Block** (silently discard) or **Forward** (allow the passage of) packets that do not match the following rules.
Default Permit Log	Select this check box to log all matched rules in the default set.
The following fields summarize the rules you have created. Note that these fields are read only. Click the tab at the top of the box to order the rules according to that tab.	
No.	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn. The **Move** field below allows you to reorder your rules. Click a rule's number to edit the rule.
Source IP	This is the source address of the packet. Please note that a blank source or destination address is equivalent to **Any**.
Destination IP	This is the destination address of the packet. Please note that a blank source or destination address is equivalent to **Any**.
Service	This is the service to which the rule applies. See *Table 12-2* for more information.
Action	This is the specified action for that rule, whether to **Block** (discard) or **Forward** (allow the passage of) packets.

Table 12-1 Firewall Rules Summary: First Screen

LABEL	DESCRIPTION
Log	This field shows you if a log is created for packets that match the rule (**Match**), don't match the rule (**Not Match**), both (**Both**) or no log is created (**None**).
Rules Reorder	You may reorder your rules using this function. Use the drop-down list box to select the number of the rule you want to move. The ordering of your rules is important as rules are applied in turn.
To Rule Number	Use the drop-down list box to select to where you want to move the rule.
Move	Click **Move** to move the rule.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to return to the previously saved settings.

12.5 Predefined Services

The **Available Services** list box in the **Edit Rule** screen (see *Figure 12-4*) displays all predefined services that the Prestige already supports. Next to the name of the service, two fields appear in brackets. The first field indicates the IP protocol type (TCP, UDP, or ICMP). The second field indicates the IP port number that defines the service. (Note that there may be more than one IP protocol type. For example, look at the default configuration labeled "(**DNS**)". **(UDP/TCP:53)** means UDP port 53 and TCP port 53. Up to 128 entries are supported. Custom services may also be configured using the **Custom Ports** function discussed later.

Table 12-2 Predefined Services

SERVICE	DESCRIPTION
AIM/NEW_ICQ(TCP:5190)	AOL's Internet Messenger service, used as a listening port by ICQ.
AUTH(TCP:113)	Authentication protocol used by some servers.
BGP(TCP:179)	Border Gateway Protocol.
BOOTP_CLIENT(UDP:68)	DHCP Client.
BOOTP_SERVER(UDP:67)	DHCP Server.
CU-SEEME(TCP/UDP:7648, 24032)	A popular videoconferencing solution from White Pines Software.
DNS(UDP/TCP:53)	Domain Name Server, a service that matches web names (e.g. www.zyxel.com) to IP numbers.
FINGER(TCP:79)	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP(TCP:20.21)	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323(TCP:1720)	Net Meeting uses this protocol.
HTTP(TCP:80)	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	HTTPS is a secured http session often used in e-commerce.
ICQ(UDP:4000)	This is a popular Internet chat program.
IPSEC_TRANSPORT/TUNN	The IPSEC AH (Authentication Header) tunneling protocol uses this

Table 12-2 Predefined Services

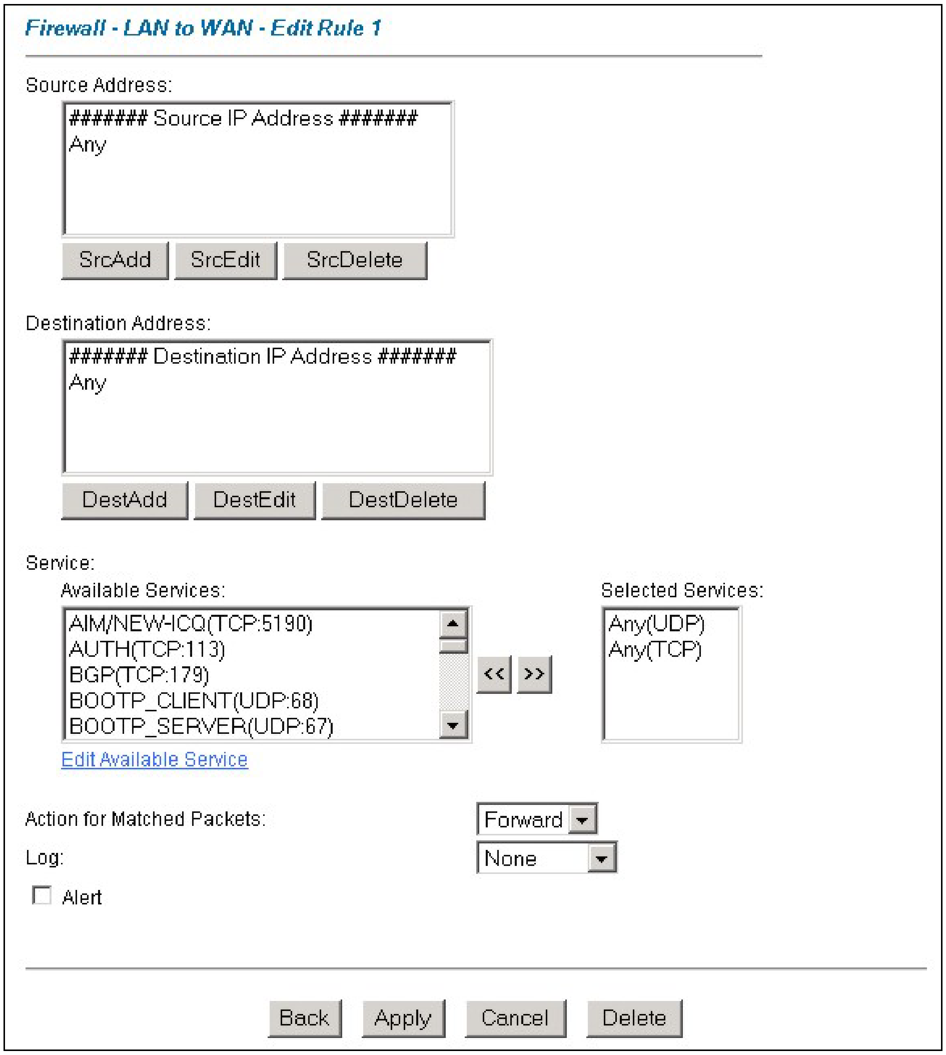
SERVICE	DESCRIPTION
EL(AH:0)	service.
IPSEC_TUNNEL(ESP:0)	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
IRC(TCP/UDP:6667)	This is another popular Internet chat program.
MSN Messenger(TCP:1863)	Microsoft Networks' messenger service uses this protocol.
MULTICAST(IGMP:0)	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
NEWS(TCP:144)	A protocol for news groups.
NFS(UDP:2049)	Network File System - NFS is a client/server distributed file service that provides transparent file-sharing for network environments.
NNTP(TCP:119)	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING(ICMP:0)	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3(TCP:110)	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP(TCP:1723)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL(GRE:0)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the data channel.
RCMD(TCP:512)	Remote Command Service.
REAL_AUDIO(TCP:7070)	A streaming audio service that enables real time sound over the web.
REXEC(TCP:514)	Remote Execution Daemon.
RLOGIN(TCP:513)	Remote Login.
RTELNET(TCP:107)	Remote Telnet.
RTSP(TCP/UDP:554)	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP(TCP:115)	Simple File Transfer Protocol.
SMTP(TCP:25)	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP(TCP/UDP:161)	Simple Network Management Program.
SNMP-TRAPS (TCP/UDP:162)	Traps for use with the SNMP (RFC:1215).
SQL-NET(TCP:1521)	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSDP(UDP:1900)	Simple Service Discovery Protocol (SSDP) is a discovery service searching for Universal Plug and Play devices on your home network or upstream Internet gateways using UDP port 1900.
SSH(TCP/UDP:22)	Secure Shell Remote Login Program.

Table 12-2 Predefined Services

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

12.6 Creating/Editing Firewall Rules

To create a new rule, click a number (**No.**) in the last screen shown to display the following screen.



Firewall - LAN to WAN - Edit Rule 1

Source Address:

####### Source IP Address #######
Any

Destination Address:

####### Destination IP Address #######
Any

Service:

Available Services:

AIM/NEW-ICQ(TCP:5190)
AUTH(TCP:113)
BGP(TCP:179)
BOOTP_CLIENT(UDP:68)
BOOTP_SERVER(UDP:67)

Selected Services:

Any(UDP)
Any(TCP)

Action for Matched Packets: Forward

Log: None

☐ Alert

Figure 12-4 Creating/Editing A Firewall Rule

The following table describes the labels in this screen.

Table 12-3 Creating/Editing A Firewall Rule

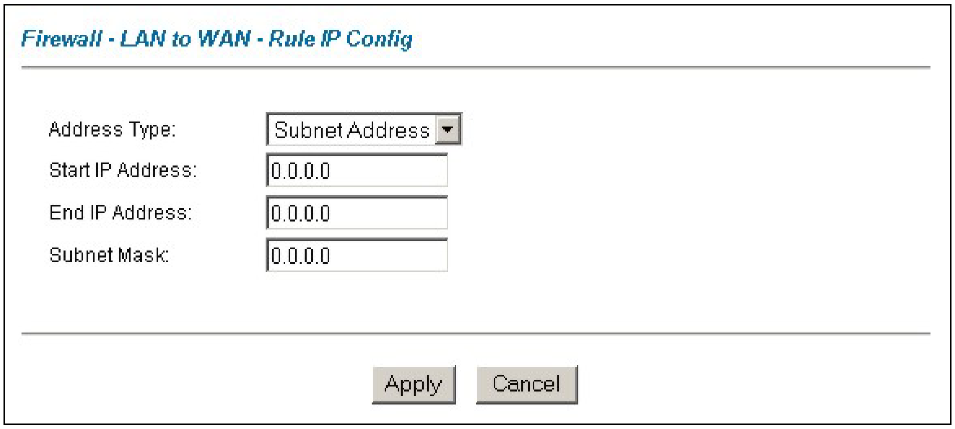
LABEL	DESCRIPTION
Source Address	Click **SrcAdd** to add a new address, **SrcEdit** to edit an existing one or **SrcDelete** to delete one.
Destination Address	Click **DestAdd** to add a new address, **DestEdit** to edit an existing one or **DestDelete** to delete one.
Services	Select a service in the **Available Services** box on the left, then click **>>** to select. The selected service shows up on the **Selected Services** box on the right. To remove a service, click on it in the **Selected Services** box on the right, then click **<<**.
Edit Available Service	Click this button to go to the **Customized Services** screen. Refer to *Chapter 13* for more information.
Action for Matched Packets	Use the drop down list box to select whether to **Block** (silently discard) or **Forward** (allow the passage of) packets that match this rule.

Table 12-3 Creating/Editing A Firewall Rule

LABEL	DESCRIPTION
Log	This field determines if a log is created for packets that match the rule (**Match**), don't match the rule (**Not Match**), match either rule (**Both**) or no log is created (**None**).
Alert	Select the **Alert** check box to determine that this rule generates an alert when the rule is matched.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to exit this screen without saving.
Delete	Click **Delete** to remove the current rule.

12.6.1 Source and Destination Addresses

To add a new source or destination address, click **SrcAdd** or **DestAdd** from the previous screen. To edit an existing source or destination address, select it from the box and click **SrcEdit** or **DestEdit** from the previous screen. Either action displays the following screen.



Firewall - LAN to WAN - Rule IP Config

Address Type: Subnet Address

Start IP Address: 0.0.0.0

End IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Figure 12-5 Adding/Editing Source and Destination Addresses

The following table describes the labels in this screen.

Table 12-4 Adding/Editing Source and Destination Addresses

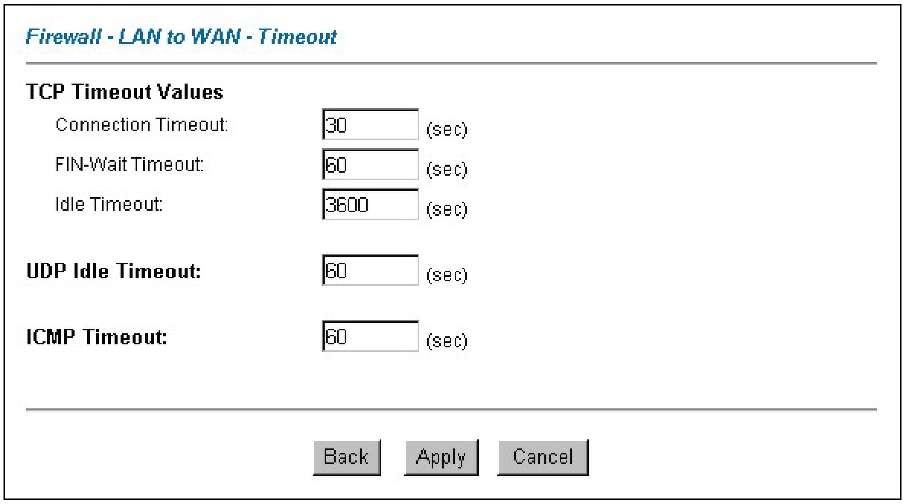
LABEL	DESCRIPTION
Address Type	Do you want your rule to apply to packets with a particular (single) IP address, a range of IP addresses (e.g., 192.168.1.10 to 192.169.1.50), a subnet or any IP address? Select an option from the drop-down list box that includes: **Single Address**, **Range Address**, **Subnet Address** and **Any Address.**
Start IP Address	Type the single IP address or the starting IP address in a range here.
End IP Address	Type the ending IP address in a range here.
Subnet Mask	Type the subnet mask here, if applicable.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to return to the previously saved settings.

12.7 Timeout

The fields in the **Timeout** screens are the same for **Local** and **Internet networks**, so the discussion below refers to both.

12.7.1 Factors Influencing Choices for Timeout Values

The factors influencing choices for timeout values are the same as the factors influencing choices for threshold values – see *section 11.3.2*. Click **Timeout** for either **Local Network to Internet Set** or **Internet to Local Network Set**.



Firewall - LAN to WAN - Timeout

TCP Timeout Values

Connection Timeout: 30 (sec)

FIN-Wait Timeout: 60 (sec)

Idle Timeout: 3600 (sec)

UDP Idle Timeout: 60 (sec)

ICMP Timeout: 60 (sec)

Figure 12-6 Timeout

The following table describes the labels in this screen.

Table 12-5 Timeout

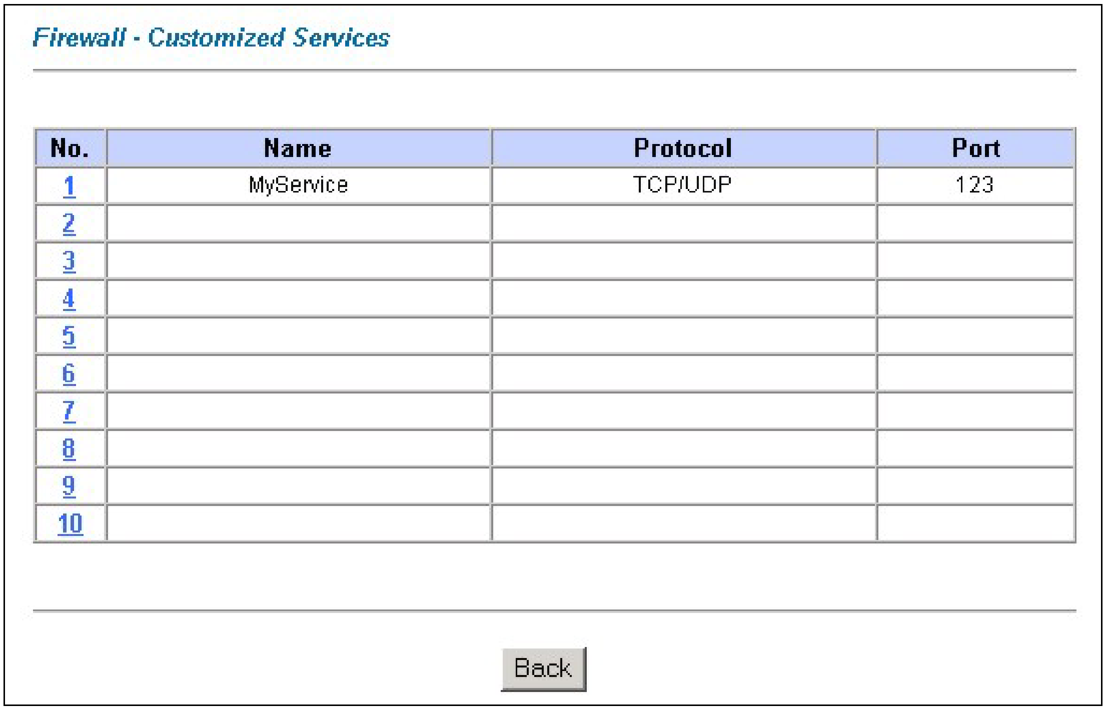
LABEL	DESCRIPTION
TCP Timeout Values	
Connection Timeout	Type the number of seconds (default 30) for the Prestige to wait for a TCP session to reach the established state before dropping the session.
FIN-Wait Timeout	Type the number of seconds (default 60) for a TCP session to remain open after the firewall detects a FIN-exchange (indicating the end of the TCP session).
Idle Timeout	Type the number of seconds (default 3600) for an inactive TCP connection to remain open before the Prestige considers the connection closed.
UDP Idle Timeout	Type the number of seconds (default 60) for an inactive UDP connection to remain open before the Prestige considers the connection closed.
ICMP Timeout	Type the number of seconds (default 60) for an ICMP session to wait for the ICMP response.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to return to the previous configuration.

Chapter 13 Customized Services

This chapter covers creating, viewing and editing custom services.

13.1 Introduction to Customized Services

Configure customized services and port numbers not predefined by the Prestige (see *Figure 12-4)*. For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) website. For further information on these services, please read *section 12.5*. To configure a custom service, click **Edit Available Service** in an edit rule screen to bring up the following screen.



Firewall - Customized Services

No.	Name	Protocol	Port
1	MyService	TCP/UDP	123
2			
3			
4			
5			
6			
7			
8			
9			
10			

Figure 13-1 Customized Services

The next table describes the labels in this screen.

Table 13-1 Customized Services

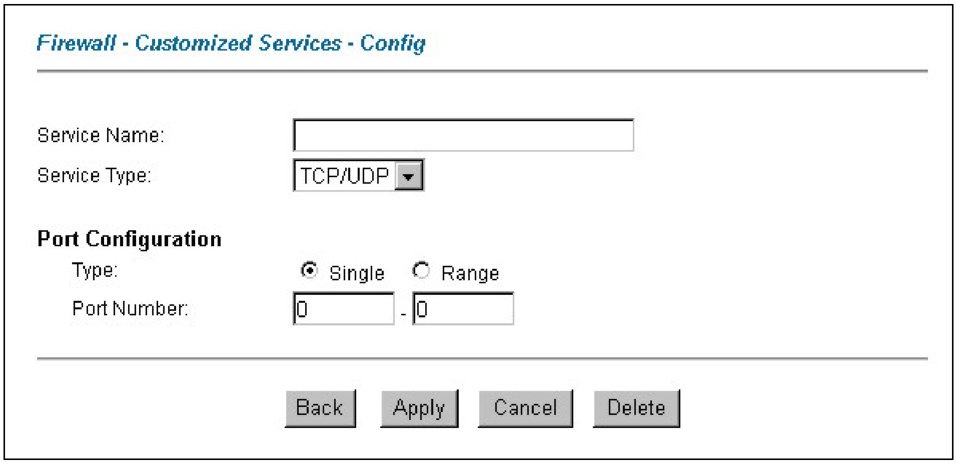
LABEL	DESCRIPTION
Customized Services	
No.	This is the number of your customized port. Click a rule's number of a service to go to the **Firewall Customized Services Config** screen to configure or edit a customized service.
Name	This is the name of your customized service.
Protocol	This shows the IP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

Table 13-1 Customized Services

LABEL	DESCRIPTION
Back	Click **Back** to return the **Firewall Edit Rule** screen.

13.2 Creating/Editing A Customized Service

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



Firewall - Customized Services - Config

Service Name:

Service Type: TCP/UDP

Port Configuration

Type: ● Single ○ Range

Port Number: 0 - 0

Figure 13-2 Creating/Editing A Customized Service

The next table describes the labels in this screen.

Table 13-2 Creating/Editing A Customized Service

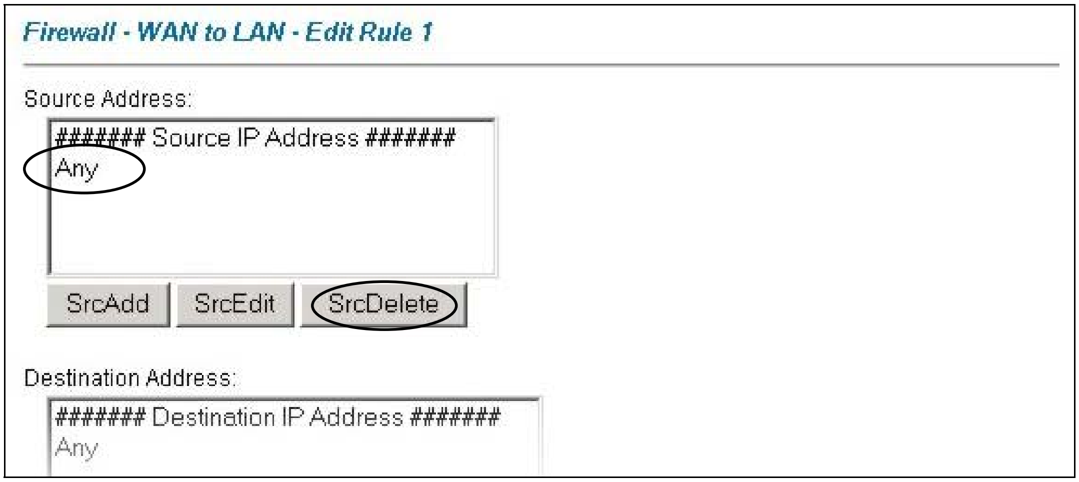
LABEL	DESCRIPTION
Service Name	Type a unique name for your custom port.
Service Type	Choose the IP port (**TCP**, **UDP** or **TCP/UDP**) that defines your customized port from the drop down list box.
Port Configuration	
Type	Click **Single** to specify one port only or **Range** to specify a span of ports that define your customized service.
Port Number	Type a single port number or the range of port numbers that define your customized service.
Back	Click **Back** to return to the **Firewall Customized Services** screen.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to return to the previously saved settings.
Delete	Click **Delete** to delete the current rule.

13.3 Example Custom Service Firewall Rule

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

1. Click **Rule Summary** under **Internet to Local Network Set**.

2. Click a rule number to open the edit rule screen.
3. Click **Any** in the **Source Address** box and then click **ScrDelete**.



Firewall - WAN to LAN - Edit Rule 1

Source Address:

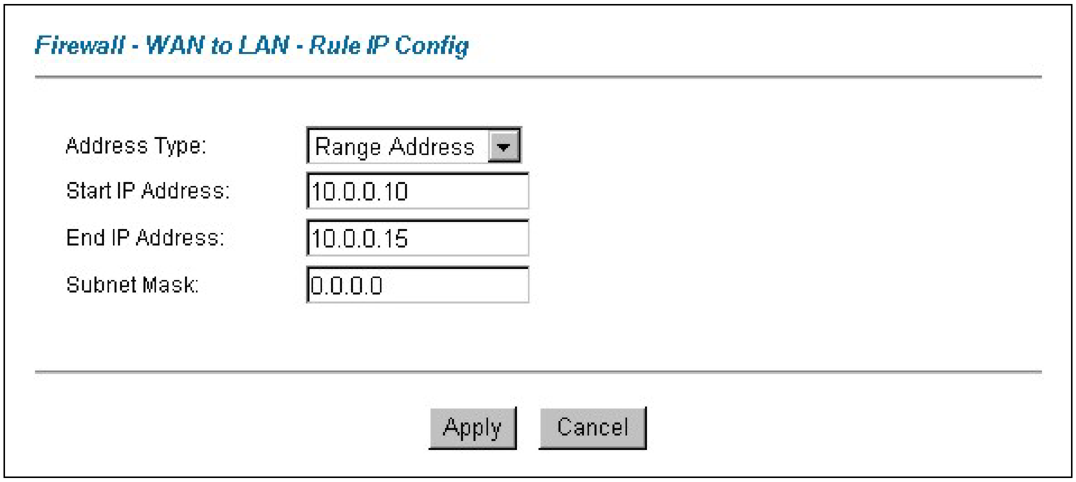
####### Source IP Address #######
Any

Destination Address:

####### Destination IP Address #######
Any

Figure 13-3 Edit Rule Example

4. Click **ScrAdd** to open the **Rule IP Config** screen. Configure it as follows and click **Apply**.

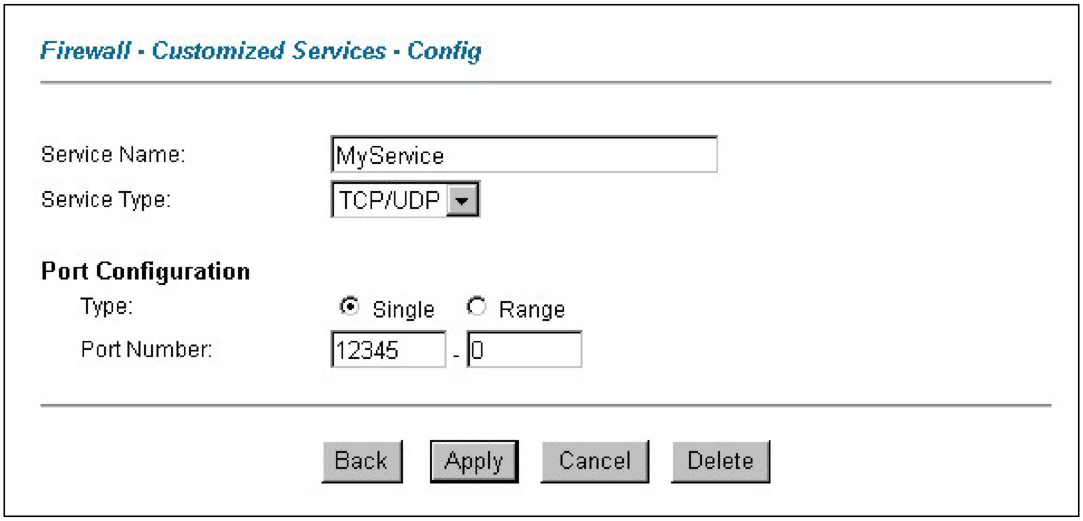


Firewall - WAN to LAN - Rule IP Config

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

Figure 13-4 Configure Source IP Example

5. Click **Edit Available Service** in the **Edit rule** screen and then click a rule number to bring up the **Firewall Customized Services Config** screen. Configure as follows.



Firewall - Customized Services - Config

Service Name:	MyService
Service Type:	TCP/UDP

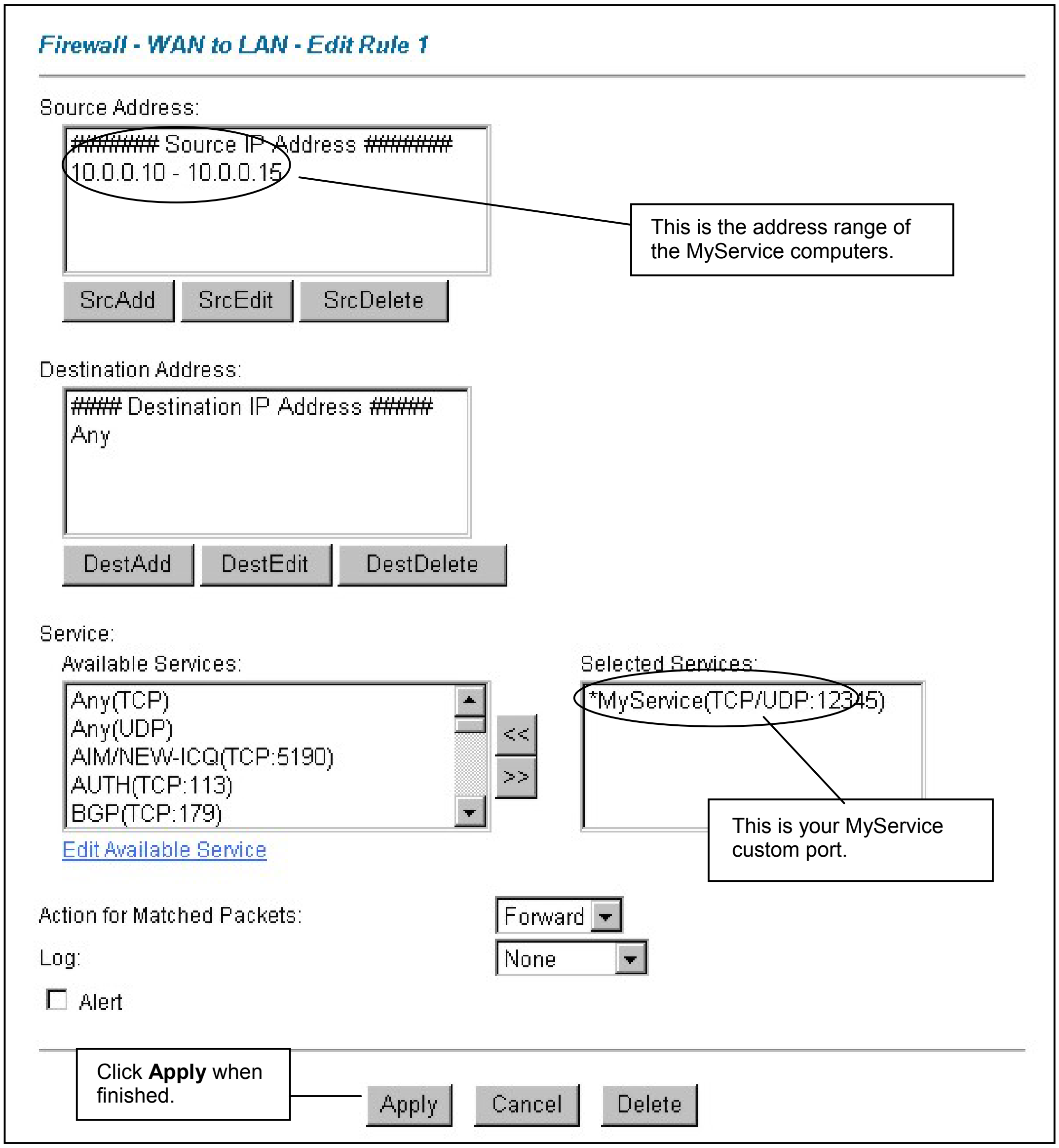
Port Configuration

Type:	● Single ○ Range
Port Number:	12345 - 0

Figure 13-5 Customized Service for MyService Example

6. Customized services show up with an "*" before their names in the **Services** list box and the Rule Summary list box. Click **Apply** after you've created your customized service.

Follow the procedures outlined earlier in this chapter to configure all your rules. Configure the rule configuration screen like the one below and apply it.



Firewall - WAN to LAN - Edit Rule 1

Source Address:

```
####### Source IP Address #######
10.0.0.10 - 10.0.0.15
```

This is the address range of the MyService computers.

Destination Address:

```
#### Destination IP Address #####
Any
```

Service:

Available Services:

```
Any(TCP)
Any(UDP)
AIM/NEW-ICQ(TCP:5190)
AUTH(TCP:113)
BGP(TCP:179)
```

Selected Services:

```
*MyService(TCP/UDP:12345)
```

This is your MyService custom port.

Action for Matched Packets: Forward

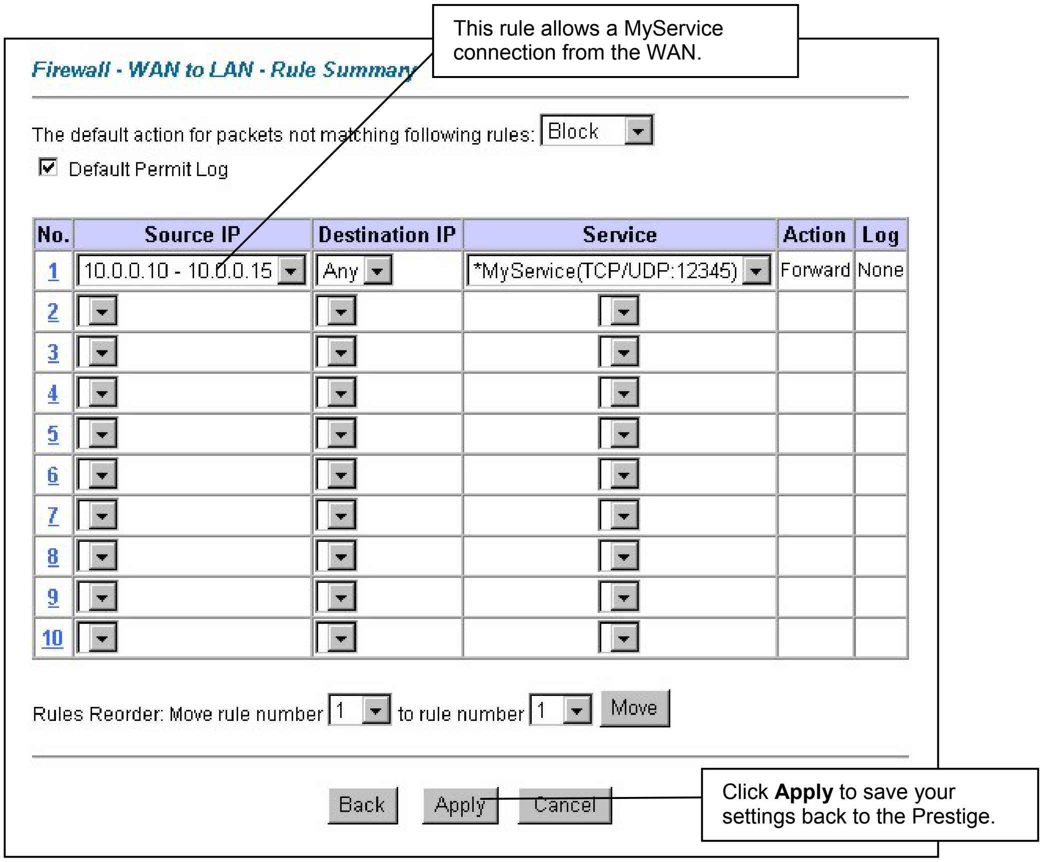
Log: None

□ Alert

Click **Apply** when finished.

Figure 13-6 Syslog Rule Configuration Example

On completing the configuration procedure for these Internet firewall rules, the **Rule Summary** screen should look like the following. Don't forget to click **Apply** when you have finished configuring your rule(s) to save your settings back to the Prestige.



Firewall - WAN to LAN - Rule Summary

The default action for packets not matching following rules: Block

☑ Default Permit Log

No.	Source IP	Destination IP	Service	Action	Log
1	10.0.0.10 - 10.0.0.15	Any	*MyService(TCP/UDP:12345)	Forward	None
2					
3					
4					
5					
6					
7					
8					
9					
10					

Rules Reorder: Move rule number 1 to rule number 1

This rule allows a MyService connection from the WAN.

Click **Apply** to save your settings back to the Prestige.

Figure 13-7 Rule Summary Example

Chapter 14
Content Filtering

This chapter covers how to configure content filtering.

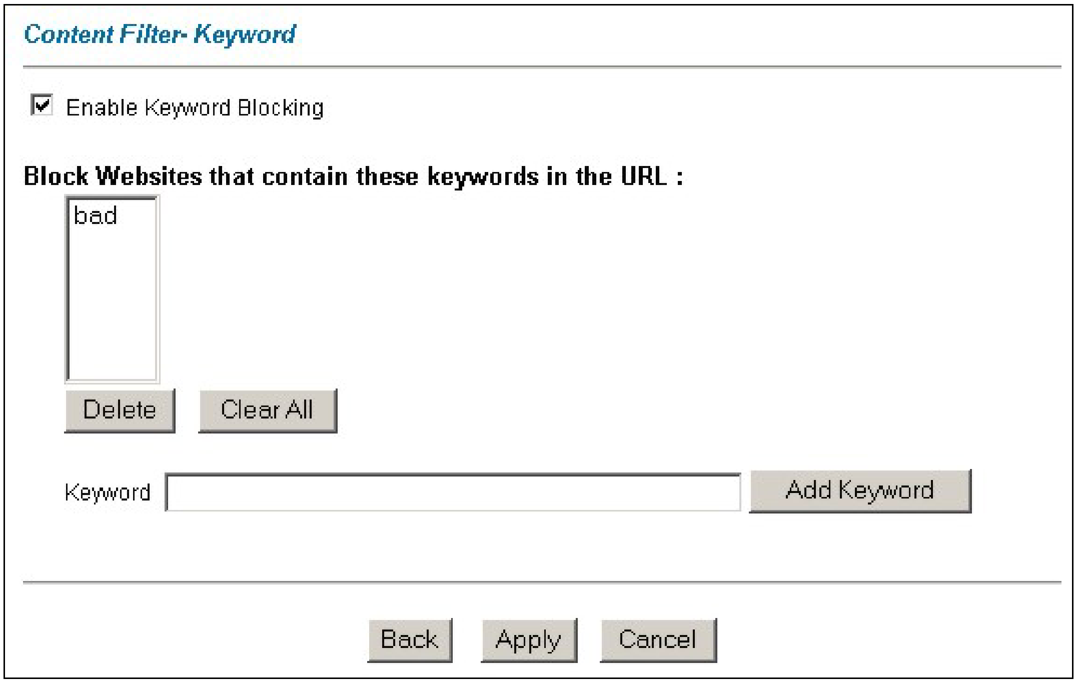
14.1 Content Filtering Overview

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

14.2 Configuring Keyword Blocking

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

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



Content Filter- Keyword

☑ Enable Keyword Blocking

Block Websites that contain these keywords in the URL :

bad

Figure 14-1 Content Filter: Keyword

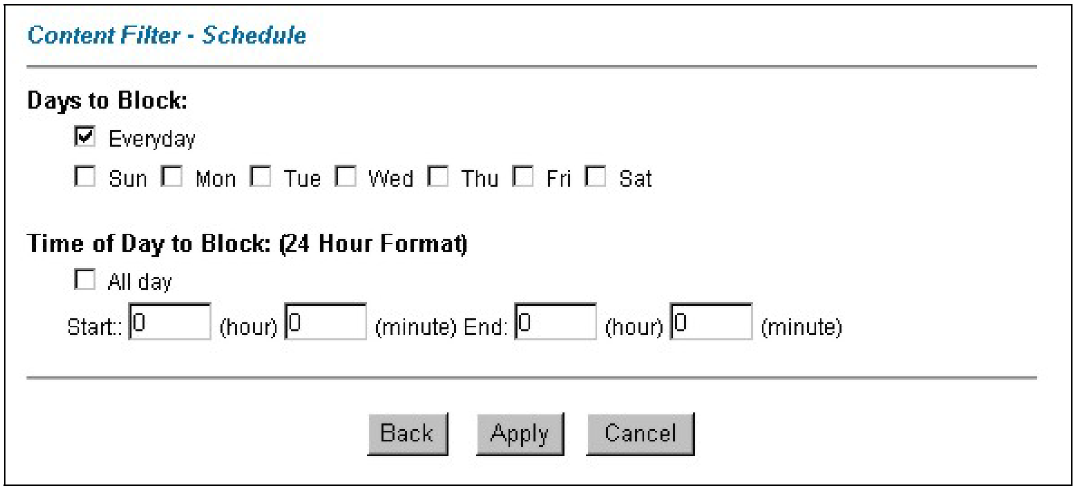
The following table describes the labels in this screen.

Table 14-1 Content Filter: Keyword

LABEL	DESCRIPTION
Enable Keyword Blocking	Select this check box to enable this feature.
Block Websites that contain these keywords in the URL:	This box contains the list of all the keywords that you have configured the Prestige to block.
Delete	Highlight a keyword in the box and click **Delete** to remove it.
Clear All	Click **Clear All** to remove all of the keywords from the list.
Keyword	Type a keyword in this field. You may use any character (up to 127 characters). Wildcards are not allowed.
Add Keyword	Click **Add Keyword** after you have typed a keyword. Repeat this procedure to add other keywords. Up to 64 keywords are allowed. When you try to access a web page containing a keyword, you will get a message telling you that the content filter is blocking this request.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to return to the previously saved settings.

14.3 Configuring the Schedule

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



Content Filter - Schedule

Days to Block:

☑ Everyday

□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

Time of Day to Block: (24 Hour Format)

□ All day

Start:: 0 (hour) 0 (minute) End: 0 (hour) 0 (minute)

Figure 14-2 Content Filter: Schedule

The following table describes the labels in this screen.

Table 14-2 Content Filter: Schedule

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

14.4 Configuring Trusted Computers

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

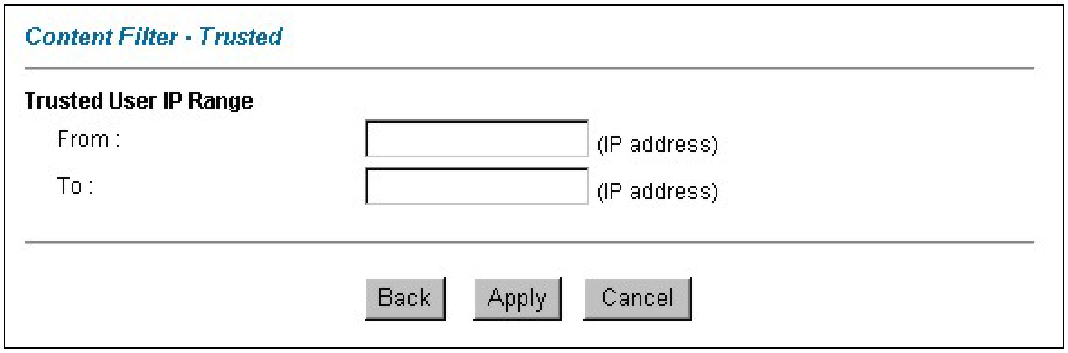


Figure 14-3 Content Filter: Trusted

The following table describes the labels in this screen.

Table 14-3 Content Filter: Trusted

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

Part V:

Remote Management, UPnP and Logs

This part contains information on how to configure the Prestige for remote management, setting up Universal Plug and Play (UPnP) and setting up and displaying logs.

Chapter 15
Remote Management Configuration

This chapter provides information on configuring remote management.

15.1 Remote Management Overview

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

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

You may manage your Prestige from a remote location via:

Internet (WAN only)

LAN only,

ALL (LAN and WAN)

Neither (Disable).

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

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

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

1. Telnet
2. HTTP

15.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

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

15.1.2 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.

15.1.3 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.

15.2 Telnet

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

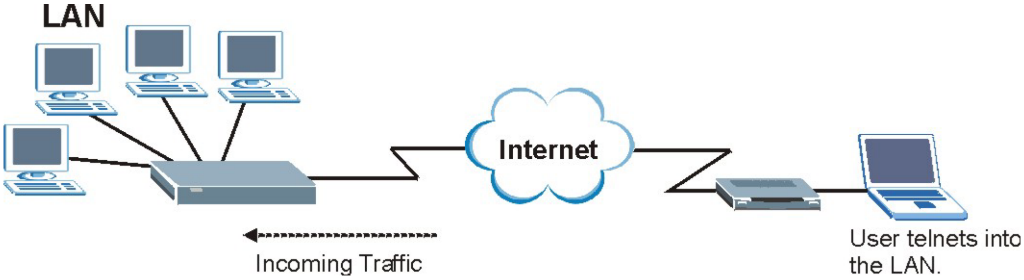


Figure 15-1 Telnet Configuration on a TCP/IP Network

15.3 FTP

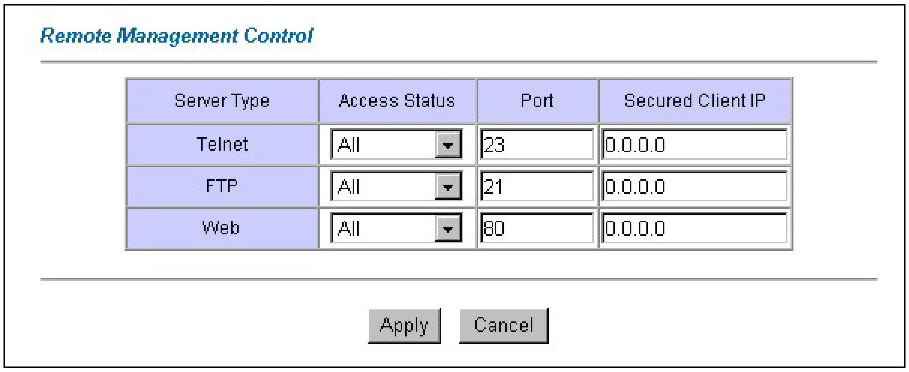
You can upload and download Prestige firmware and configuration files using FTP. To use this feature, your computer must have an FTP client.

15.4 Web

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

15.5 Configuring Remote Management

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



Remote Management Control

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

Figure 15-2 Remote Management Control

The following table describes the fields in this screen.

Table 15-1 Remote Management Control

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 16 Universal Plug-and-Play (UPnP)

This chapter introduces the UPnP feature in the web configurator.

16.1 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.

16.1.1 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.

16.1.2 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)* chapter for further information about NAT.

16.1.3 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.

16.2 UPnP and ZyXEL

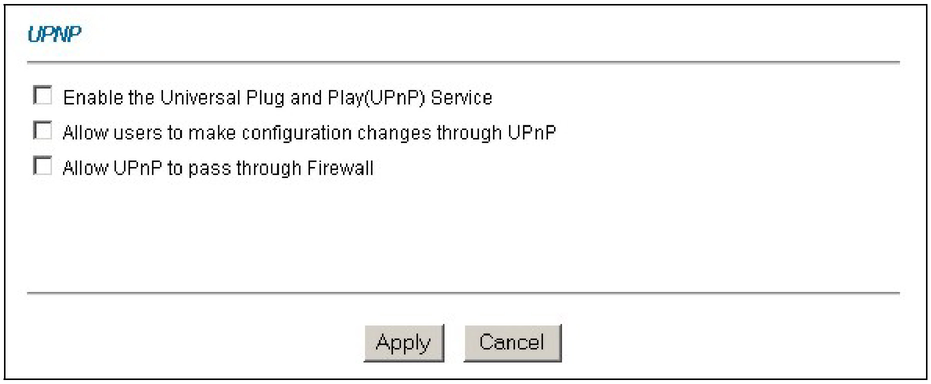
ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum Creates UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports IGD 1.0 (Internet Gateway Device). At the time of writing ZyXEL's UPnP implementation supports Windows Messenger 4.6 and 4.7 while Windows Messenger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

16.2.1 Configuring UPnP

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



UPNP

□ Enable the Universal Plug and Play(UPnP) Service

□ Allow users to make configuration changes through UPnP

□ Allow UPnP to pass through Firewall

Figure 16-1 Configuring UPnP

The following table describes the fields in this screen.

Table 16-1 Configuring UPnP

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

16.3 Installing UPnP in Windows Example

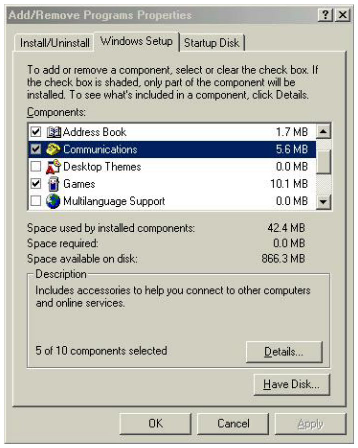
This section shows how to install UPnP in Windows Me and Windows XP.

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**.



To add or remove a component, select or clear the check box. If the check box is shaded, only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑	Address Book	1.7 MB
☑	Communications	5.6 MB
☐	Desktop Themes	0.0 MB
☑	Games	10.1 MB
☐	Multilanguage Support	0.0 MB

Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 866.3 MB

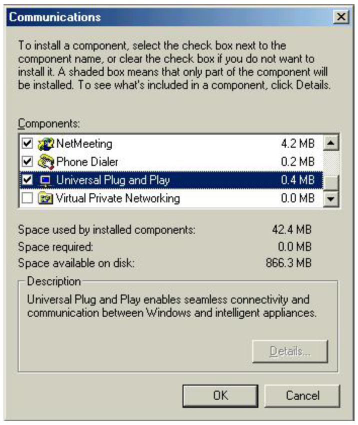
Description
Includes accessories to help you connect to other computers and online services.

5 of 10 components selected

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

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

5. Restart the computer when prompted.



To install a component, select the check box next to the component name, or clear the check box if you do not want to install it. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑	NetMeeting	4.2 MB
☑	Phone Dialer	0.2 MB
☑	Universal Plug and Play	0.4 MB
☐	Virtual Private Networking	0.0 MB

Space used by installed components: 42.4 MB
Space required: 0.0 MB
Space available on disk: 866.3 MB

Description
Universal Plug and Play enables seamless connectivity and communication between Windows and intelligent appliances.

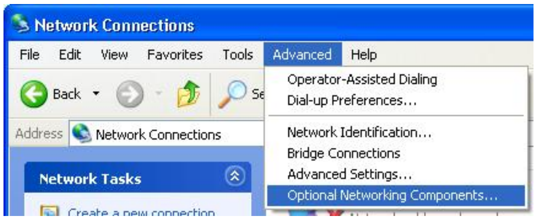
Installing UPnP in Windows XP

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

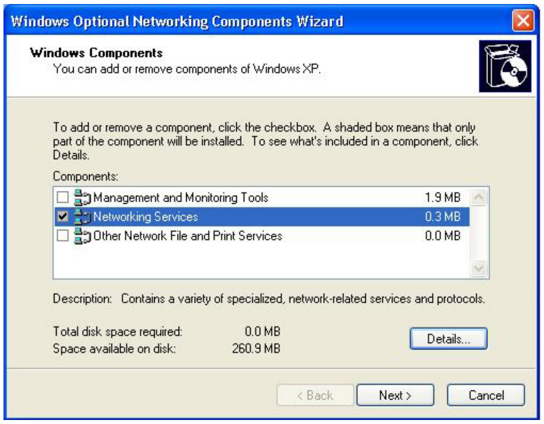
1. Click Start and Control Panel.

2. Double-click **Network Connections**.

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



4. Select **Networking Service** in the **Components** selection box and click **Details**.



You can add or remove components of Windows XP.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

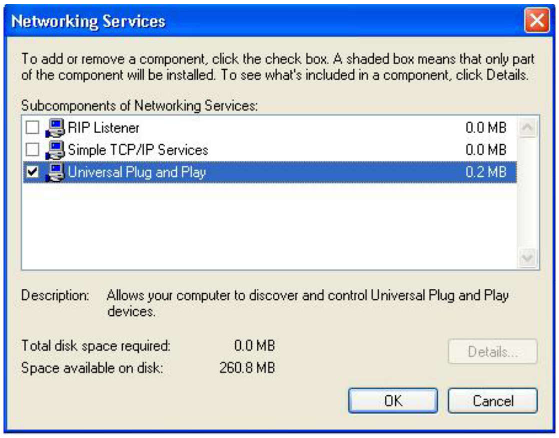
Components:

☐	Management and Monitoring Tools	1.9 MB
☑	Networking Services	0.3 MB
☐	Other Network File and Print Services	0.0 MB

Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 0.0 MB
Space available on disk: 260.9 MB

5. In the **Networking Services** window, select the **Universal Plug and Play** check box.
6. Click **OK** to go back to the **Windows Optional Networking Component Wizard** window and click **Next**.



Networking Services

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Networking Services:

☐	RIP Listener	0.0 MB
☐	Simple TCP/IP Services	0.0 MB
☑	Universal Plug and Play	0.2 MB

Description: Allows your computer to discover and control Universal Plug and Play devices.

Total disk space required: 0.0 MB

Space available on disk: 260.8 MB

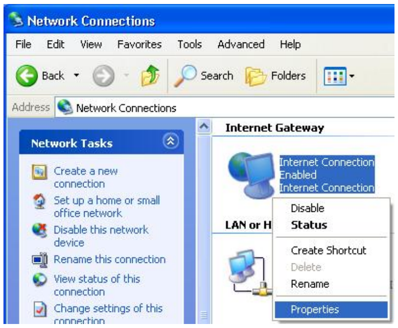
16.4 Using UPnP in Windows XP Example

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.

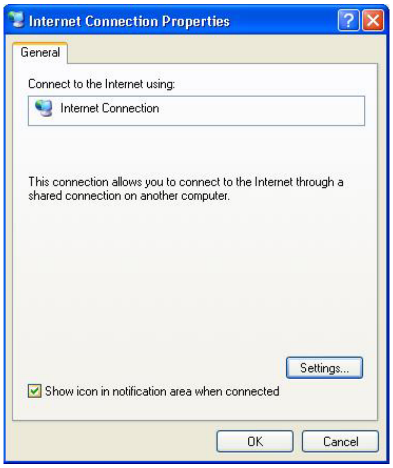
Make sure the computer is connected to a LAN port of the Prestige. Turn on your computer and the Prestige.

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**.



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


Internet Connection Properties

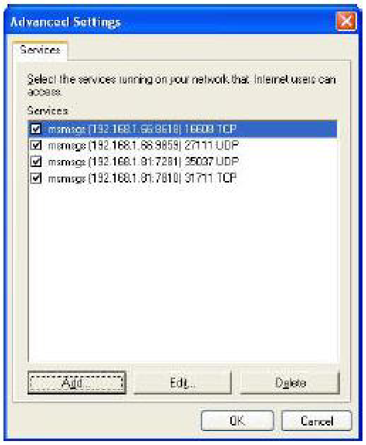
Connect to the Internet using:

Internet Connection

This connection allows you to connect to the Internet through a shared connection on another computer.

☑ Show icon in notification area when connected

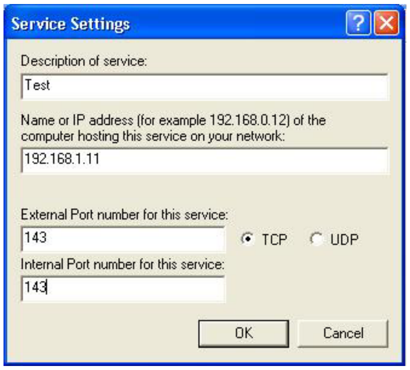
4. You may edit or delete the port mappings or click **Add** to manually add port mappings.


Advanced Settings

Select the services running on your network that Internet users can access.

Services

☑ msmsgs (192.168.1.66:8618) 16608 TCP
☑ msmsgs (192.168.1.66:9859) 27111 UDP
☑ msmsgs (192.168.1.81:7281) 35037 UDP
☑ msmsgs (192.168.1.81:7810) 31711 TCP


Service Settings

Description of service:
Test

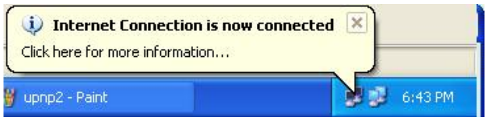
Name or IP address (for example 192.168.0.12) of the computer hosting this service on your network:
192.168.1.11

External Port number for this service:
143 ● TCP ○ UDP

Internal Port number for this service:
143

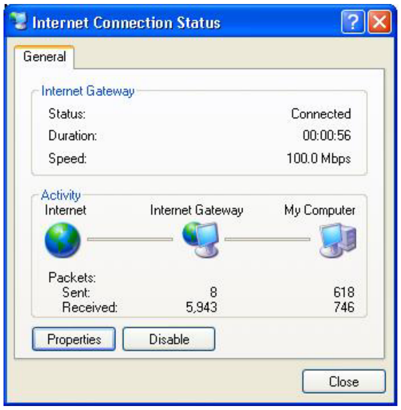
5. When the UPnP-enabled device is disconnected from your computer, all port mappings will be deleted automatically.

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


Internet Connection is now connected

Click here for more information...

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


Internet Connection Status

Internet Gateway

Status:	Connected
Duration:	00:00:56
Speed:	100.0 Mbps

Activity

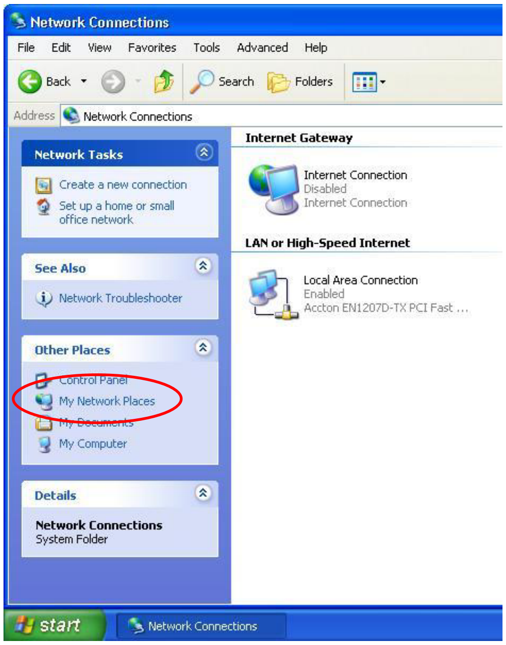
	Internet	Internet Gateway	My Computer
Packets:			
Sent:		8	618
Received:		5,943	746

Web Configurator Easy Access

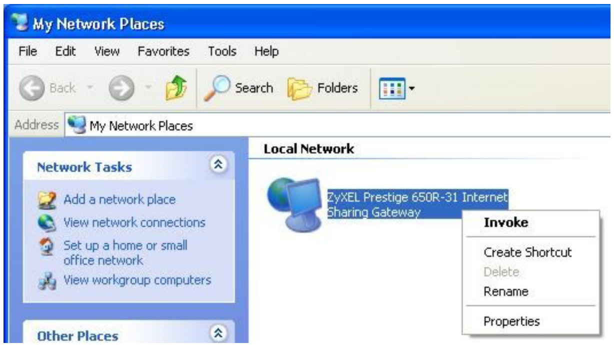
With UPnP, you can access the web-based configurator on the Prestige without finding out the IP address of the Prestige first. This comes helpful if you do not know the IP address of the Prestige.

Follow the steps below to access the web configurator.

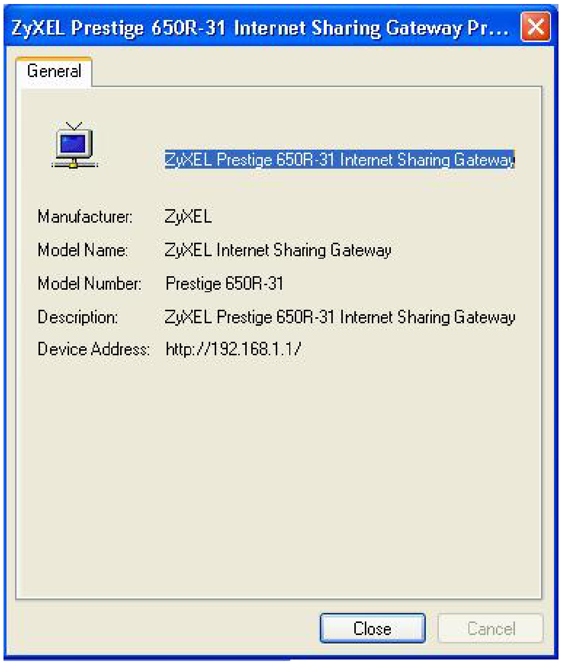
1. Click **Start** and then **Control Panel**.
2. Double-click **Network Connections**.
3. Select **My Network Places** under **Other Places**.



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.



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


ZyXEL Prestige 650R-31 Internet Sharing Gateway Pr...

ZyXEL Prestige 650R-31 Internet Sharing Gateway

Manufacturer: ZyXEL
Model Name: ZyXEL Internet Sharing Gateway
Model Number: Prestige 650R-31
Description: ZyXEL Prestige 650R-31 Internet Sharing Gateway
Device Address: http://192.168.1.1/

Chapter 17 Logs Screens

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

17.1 Logs Overview

The web configurator allows you to choose which categories of events and/or alerts to have the Prestige log and then display the logs or have the Prestige send them to an administrator (as e-mail) or to a syslog server.

17.1.1 Alerts and Logs

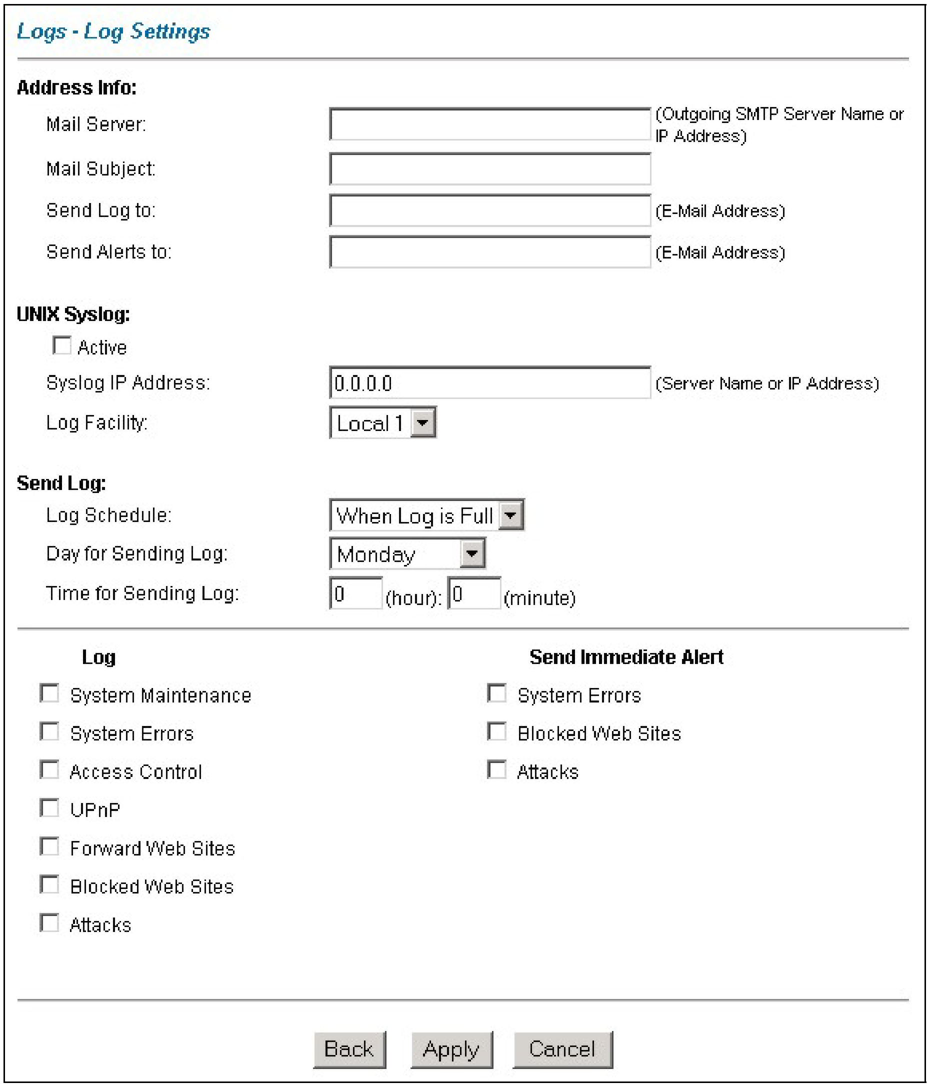
An alert is a type of log that warrants more serious attention. They include system errors, attacks (access control) and attempted access to blocked web sites. Some categories such as **System Errors** consist of both logs and alerts. You may differentiate them by their color in the **View Log** screen. Alerts display in red and logs display in black.

17.2 Configuring Log Settings

Use the **Log Settings** screen to configure to where the Prestige is to send logs; the schedule for when the Prestige is to send the logs and which logs and/or immediate alerts the Prestige is to record.

To change your Prestige's log settings, click **Logs**, then the **Log Settings**. The screen appears as shown.

Alerts are e-mailed as soon as they happen. Logs may be e-mailed as soon as the log is full (see **Log Schedule**). Selecting many alert and/or log categories (especially **Access Control**) may result in many e-mails being sent.



Logs - Log Settings

Address Info:

Mail Server: (Outgoing SMTP Server Name or IP Address)

Mail Subject:

Send Log to: (E-Mail Address)

Send Alerts to: (E-Mail Address)

UNIX Syslog:

□ Active

Syslog IP Address: 0.0.0.0 (Server Name or IP Address)

Log Facility: Local 1

Send Log:

Log Schedule: When Log is Full

Day for Sending Log: Monday

Time for Sending Log: 0 (hour): 0 (minute)

Log	Send Immediate Alert
□ System Maintenance	□ System Errors
□ System Errors	□ Blocked Web Sites
□ Access Control	□ Attacks
□ UPnP	
□ Forward Web Sites	
□ Blocked Web Sites	
□ Attacks	

Figure 17-1 Log Settings

The following table describes the fields in this screen.

Table 17-1 Log Settings

LABEL	DESCRIPTION
Address Info	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via e-mail.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the Prestige sends.
Send log to	Logs are sent to the e-mail address specified in this field. If this field is left blank, logs will not be sent via e-mail.
Send alerts to	Alerts are sent to the e-mail address specified in this field. If this field is left blank, alerts will not be sent via e-mail.

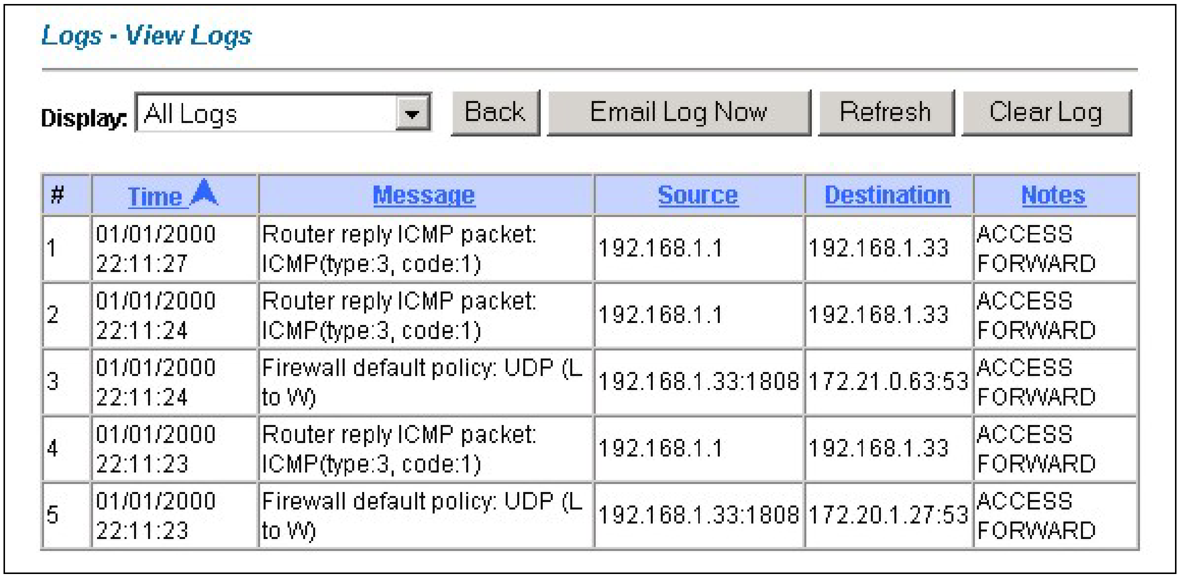
Table 17-1 Log Settings

LABEL	DESCRIPTION
UNIX Syslog	Syslog logging sends a log to an external syslog server used to store logs.
Active	Click **Active** to enable syslog logging.
Syslog IP Address	Enter the server name or IP address of the syslog server that will log the selected categories of logs.
Log Facility	Select a location from the drop down list box. The log facility allows you to log the messages to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Send Log	
Log Schedule	This drop-down menu is used to configure the frequency of log messages being sent as E-mail: **Daily** **Weekly** **Hourly** **When Log is Full** **None.** If you select **Weekly** or **Daily**, specify a time of day when the E-mail should be sent. If you select **Weekly**, then also specify which day of the week the E-mail should be sent. If you select **When Log is Full**, an alert is sent when the log fills up. If you select **None**, no log messages are sent
Day for Sending Log	Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Log	Select the categories of logs that you want to record. Logs include alerts.
Send Immediate Alert	Select the categories of alerts for which you want the Prestige to instantly e-mail alerts to the e-mail address specified in the **Send Alerts To** field.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your customized settings and exit this screen.
Cancel	Click **Cancel** to return to the previously saved settings.

17.3 Displaying the Logs

Click **Logs** and then **View Log** to open the **View Logs** screen. Use the **View Logs** screen to see the logs for the categories that you selected in the **Log Settings** screen (see *section 17.2*).

Log entries in red indicate alerts. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.



Display: All Logs

#	Time	Message	Source	Destination	Notes
1	01/01/2000 22:11:27	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.33	ACCESS FORWARD
2	01/01/2000 22:11:24	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.33	ACCESS FORWARD
3	01/01/2000 22:11:24	Firewall default policy: UDP (L to W)	192.168.1.33:1808	172.21.0.63:53	ACCESS FORWARD
4	01/01/2000 22:11:23	Router reply ICMP packet: ICMP(type:3, code:1)	192.168.1.1	192.168.1.33	ACCESS FORWARD
5	01/01/2000 22:11:23	Firewall default policy: UDP (L to W)	192.168.1.33:1808	172.20.1.27:53	ACCESS FORWARD

Figure 17-2 View Logs

The following table describes the fields in this screen.

Table 17-2 View Logs

LABEL	DESCRIPTION
Display	The categories that you select in the **Log Settings** screen (see *section 17.2*) display in the drop-down list box. Select a category of logs to view; select **All Logs** to view logs from all of the log categories that you selected in the **Log Settings** page.
Time	This field displays the time the log was recorded. See the chapter on system maintenance and information to configure the Prestige's time and date.
Message	This field states the reason for the log.
Source	This field lists the source IP address and the port number of the incoming packet.
Destination	This field lists the destination IP address and the port number of the incoming packet.
Notes	This field displays additional information about the log entry.
Back	Click **Back** to return to the previous screen
Email Log Now	Click **Email Log Now** to send the log screen to the e-mail address specified in the **Log Settings** page (make sure that you have first filled in the **Address Info** fields in **Log Settings**, see *section 17.2*).
Refresh	Click **Refresh** to renew the log screen.
Clear Log	Click **Clear Log** to delete all the logs.

17.4 SMTP Error Messages

If there are difficulties in sending e-mail the following error messages appear. Please see the *Support Notes* on the included disk for information on other types of error messages.

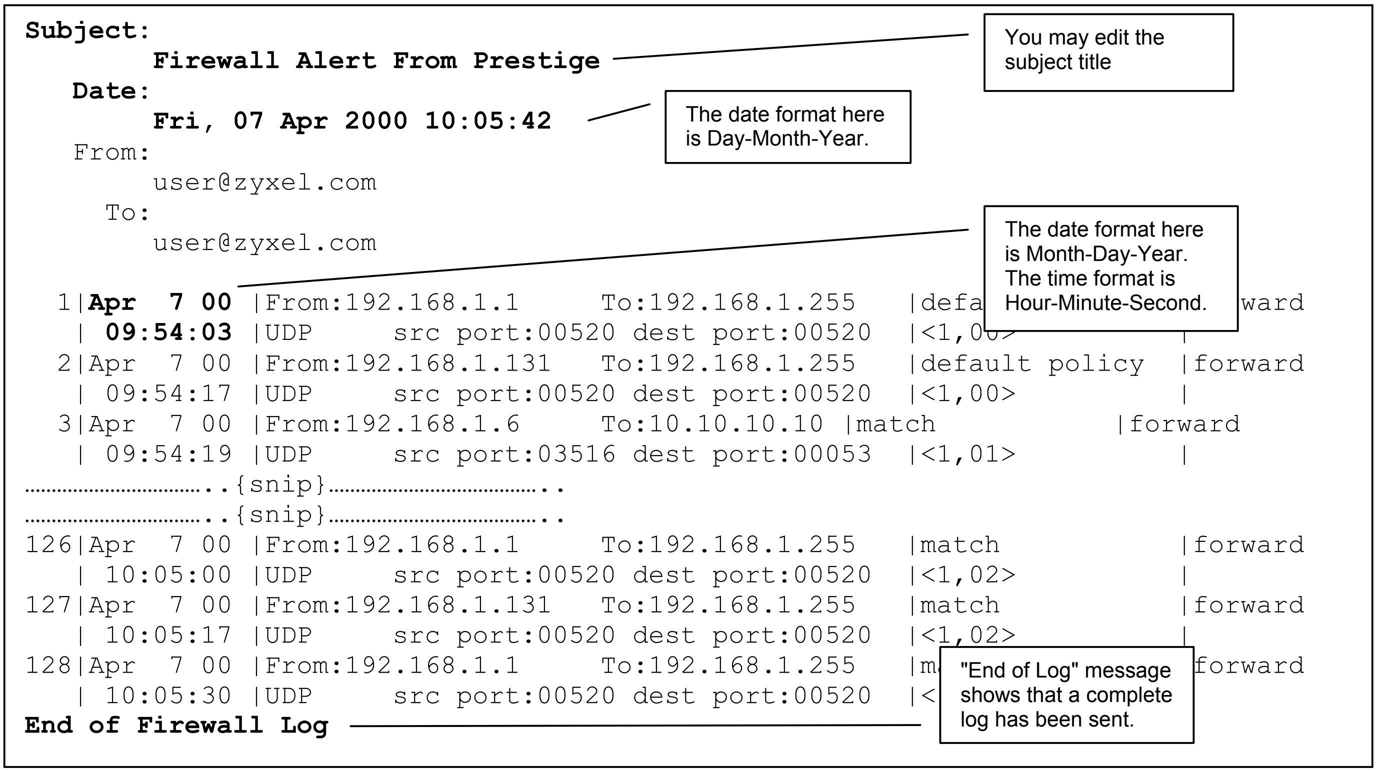
E-mail error messages appear in SMT menu 24.3.1 as "SMTP action request failed. ret= ??". The "??"are described in the following table.

Table 17-3 SMTP Error Messages

-1 means Prestige out of socket
-2 means tcp SYN fail
-3 means smtp server OK fail
-4 means HELO fail
-5 means MAIL FROM fail
-6 means RCPT TO fail
-7 means DATA fail
-8 means mail data send fail

17.4.1 Example E-mail Log

An "End of Log" message displays for each mail in which a complete log has been sent. The following is an example of a log sent by e-mail.



```
Subject:
        Firewall Alert From Prestige
   Date:
        Fri, 07 Apr 2000 10:05:42
   From:
        user@zyxel.com
     To:
        user@zyxel.com

  1|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |defa                  ward
   | 09:54:03 |UDP     src port:00520 dest port:00520  |<1,00>               |
  2|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |default policy  |forward
   | 09:54:17 |UDP     src port:00520 dest port:00520  |<1,00>          |
  3|Apr  7 00 |From:192.168.1.6     To:10.10.10.10 |match          |forward
   | 09:54:19 |UDP     src port:03516 dest port:00053  |<1,01>          |
.................{snip}...................
.................{snip}...................
126|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |match           |forward
   | 10:05:00 |UDP     src port:00520 dest port:00520  |<1,02>          |
127|Apr  7 00 |From:192.168.1.131   To:192.168.1.255   |match           |forward
   | 10:05:17 |UDP     src port:00520 dest port:00520  |<1,02>          |
128|Apr  7 00 |From:192.168.1.1     To:192.168.1.255   |m                forward
   | 10:05:30 |UDP     src port:00520 dest port:00520  |<
End of Firewall Log
```

You may edit the subject title

The date format here is Day-Month-Year.

The date format here is Month-Day-Year. The time format is Hour-Minute-Second.

"End of Log" message shows that a complete log has been sent.

Figure 17-3 E-mail Log Example

Part VI:

Bandwidth Management

This part provides information on the functions and configuration of Bandwidth Management.

Chapter 18
Bandwidth Management

This chapter describes the functions and configuration of bandwidth management.

18.1 Bandwidth Management Overview

Bandwidth management allows you to allocate an interface's outgoing capacity to specific types of traffic. It can also help you make sure that the Prestige forwards certain types of traffic (especially real-time applications) with minimum delay. With the use of real-time applications such as Voice-over-IP (VoIP) increasing, the requirement for bandwidth allocation is also increasing.

Bandwidth management addresses questions such as:

- Who gets how much access to specific applications?
- What priority level should you give to each type of traffic?
- Which traffic must have guaranteed delivery?
- How much bandwidth should be allotted to guarantee delivery?

Bandwidth management also allows you to configure the allowed output for an interface to match what the network can handle. This helps reduce delays and dropped packets at the next routing device. For example, you can set the WAN interface speed to 1000kbps if the ADSL connection has an upstream speed of 1000kbps. All configuration screens display measurements in kbps (kilobits per second), but this *User's Guide* also uses Mbps (megabits per second) for brevity's sake.

18.2 Bandwidth Classes and Filters

Use bandwidth classes and child-classes to allocate specific amounts of bandwidth capacity (bandwidth budgets). Configure a bandwidth filter to define a bandwidth class (or child-class) based on a specific application and/or subnet. Use the **Class Configuration** tab (see *section 18.9.1*) to set up a bandwidth class's name, bandwidth allotment, and bandwidth filter. You can configure up to one bandwidth filter per bandwidth class. You can also configure bandwidth classes without bandwidth filters. However, it is recommended that you configure child-classes with filters for any classes that you configure without filters. The Prestige leaves the bandwidth budget allocated and unused for a class that does not have a filter itself or child-classes with filters. View your configured bandwidth classes and child-classes in the **Class Setup** tab (see *section 18.9* for details).

The total of the configured bandwidth budgets for child-classes cannot exceed the configured bandwidth budget speed of the parent class.

18.3 Proportional Bandwidth Allocation

Bandwidth management allows you to define how much bandwidth each class gets; however, the actual bandwidth allotted to each class decreases or increases in proportion to actual available bandwidth.

18.4 Bandwidth Management Usage Examples

These examples show bandwidth management allotments on a WAN interface that is configured for 640Kbps.

18.4.1 Application-based Bandwidth Management Example

The bandwidth classes in the following example are based solely on application. Each bandwidth class (VoIP, Web, FTP, E-mail and Video) is allotted 128kbps.

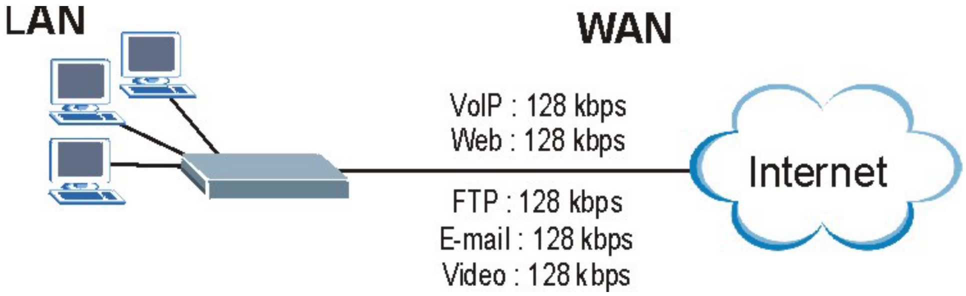


Table 18-1 Application-based Bandwidth Management Example

18.4.2 Subnet-based Bandwidth Management Example

The following example uses bandwidth classes based solely on LAN subnets. Each bandwidth class (Subnet A and Subnet B) is allotted 320kbps.

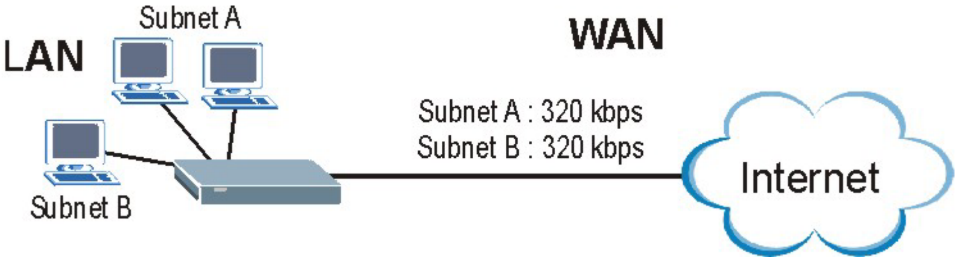


Table 18-2 Subnet-based Bandwidth Management Example

18.4.3 Application and Subnet-based Bandwidth Management Example

The following example uses bandwidth classes based on LAN subnets and applications (specific applications in each subnet are allotted bandwidth).

Table 18-3 Application and Subnet-based Bandwidth Management Example

TRAFFIC TYPE	FROM SUBNET A	FROM SUBNET B
VoIP	64 kbps	64 kbps
Web	64 kbps	64 kbps
FTP	64 kbps	64 kbps
E-mail	64 kbps	64 kbps
Video	64 kbps	64 kbps

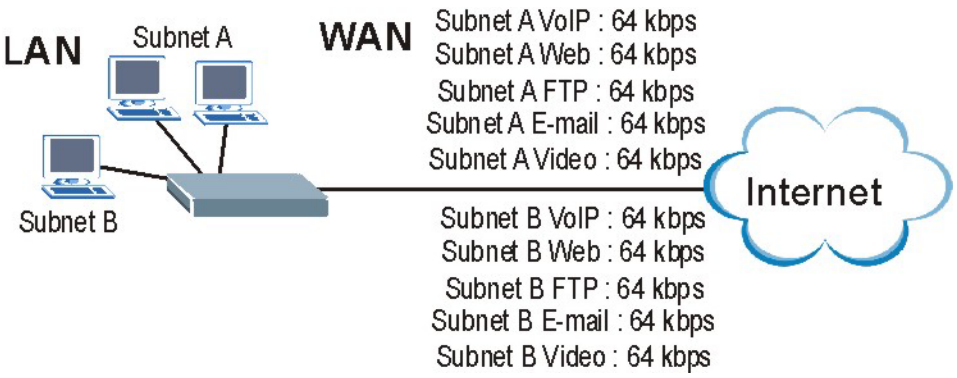


Table 18-4 Application and Subnet-based Bandwidth Management Example

18.5 Scheduler

The scheduler divides up an interface's bandwidth among the bandwidth classes. The Prestige has two types of scheduler: fairness-based and priority-based.

18.5.1 Priority-based Scheduler

With the priority-based scheduler, the Prestige forwards traffic from bandwidth classes according to the priorities that you assign to the bandwidth classes. The larger a bandwidth class's priority number is, the higher the priority. Assign real-time applications (like those using audio or video) a higher priority number to provide smoother operation.

18.5.2 Fairness-based Scheduler

The Prestige divides bandwidth equally among bandwidth classes when using the fairness-based scheduler; thus preventing one bandwidth class from using all of the interface's bandwidth.

18.6 Maximize Bandwidth Usage

The maximize bandwidth usage option (see *Table 18-8*) allows the Prestige to divide up any available bandwidth on the interface (including unallocated bandwidth and any allocated bandwidth that a class is not using) among the bandwidth classes that require more bandwidth.

When you enable maximize bandwidth usage, the Prestige first makes sure that each bandwidth class gets up to its bandwidth allotment. Next, the Prestige divides up an interface's available bandwidth (bandwidth that is unbudgeted or unused by the classes) depending on how many bandwidth classes require more bandwidth and on their priority levels. When only one class requires more bandwidth, the Prestige gives extra bandwidth to that class.

When multiple classes require more bandwidth, the Prestige gives the highest priority classes the available bandwidth first (as much as they require, if there is enough available bandwidth), and then to lower priority classes if there is still bandwidth available. The Prestige distributes the available bandwidth equally among classes with the same priority level.

18.6.1 Reserving Bandwidth for Non-Bandwidth Class Traffic

Do the following three steps to configure the Prestige to allow bandwidth for traffic that is not defined in a bandwidth filter.

1. Leave some of the interface's bandwidth unbudgeted.
2. Do not enable the interface's **Maximize Bandwidth Usage** option.
3. Do not enable bandwidth borrowing on the child-classes that have the root class as their parent (see *section 18.7*).

18.6.2 Maximize Bandwidth Usage Example

Here is an example of a Prestige that has maximized bandwidth usage enabled on an interface. The first figure shows each bandwidth class's bandwidth budget and priority. The classes are set up based on subnets. The interface is set to 10 Mbps. Each subnet is allocated 2 Mbps. The unbudgeted 2 Mbps allows traffic not defined in one of the bandwidth filters to go out when you do not select the maximize bandwidth option.

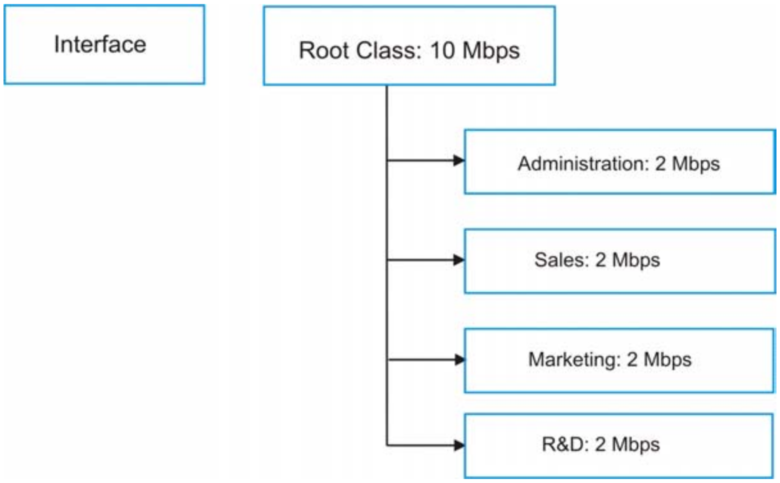


Table 18-5 Bandwidth Allotment Example

The following figure shows the bandwidth usage with the maximize bandwidth usage option enabled. The Prestige divides up the unbudgeted 2 Mbps among the classes that require more bandwidth. If the administration department only uses 1 Mbps of the budgeted 2 Mbps, the Prestige also divides the remaining 1 Mbps among the classes that require more bandwidth. Therefore, the Prestige divides a total of 3 Mbps total of unbudgeted and unused bandwidth among the classes that require more bandwidth.

In this case, suppose that all of the classes except for the administration class need more bandwidth.

- Each class gets up to its budgeted bandwidth. The administration class only uses 1 Mbps of its budgeted 2 Mbps.
- Sales and Marketing are first to get extra bandwidth because they have the highest priority (6). If they each require 1.5 Mbps or more of extra bandwidth, the Prestige divides the total 3 Mbps total of unbudgeted and unused bandwidth equally between the sales and marketing departments (1.5 Mbps extra to each for a total of 3.5 Mbps for each) because they both have the highest priority level.
- R&D requires more bandwidth but only gets its budgeted 2 Mbps because all of the unbudgeted and unused bandwidth goes to the higher priority sales and marketing classes.
- The Prestige does not send any traffic that is not defined in the bandwidth filters because all of the unbudgeted bandwidth goes to the classes that need it.

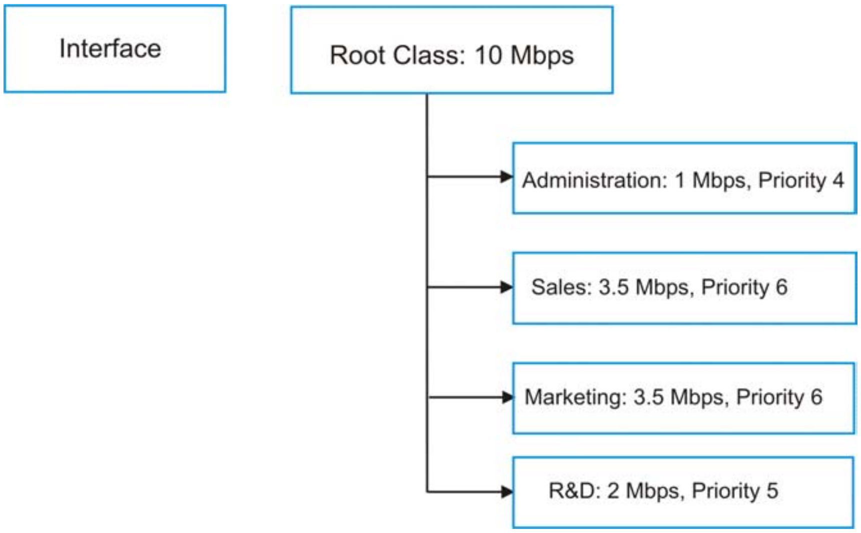

Interface
Root Class: 10 Mbps
Administration: 1 Mbps, Priority 4
Sales: 3.5 Mbps, Priority 6
Marketing: 3.5 Mbps, Priority 6
R&D: 2 Mbps, Priority 5

Table 18-6 Maximize Bandwidth Usage Example

18.7 Bandwidth Borrowing

Bandwidth borrowing allows a child-class to borrow unused bandwidth from its parent class, whereas maximize bandwidth usage allows bandwidth classes to borrow any unused or unbudgeted bandwidth on the whole interface.

Enable bandwidth borrowing on a child-class to allow the child-class to use its parent class's unused bandwidth. A parent class's unused bandwidth is given to the highest priority child-class first. The child-class can also borrow bandwidth from a higher parent class (grandparent class) if the child-class's parent class is also configured to borrow bandwidth from its parent class. This can go on for as many levels as are configured to borrow bandwidth from their parent class (see *section 18.7.1*).

The total of the bandwidth allotments for child-classes cannot exceed the bandwidth allotment of their parent class. The Prestige uses the scheduler to divide a parent class's unused bandwidth among the child-classes.

18.7.1 Bandwidth Borrowing Example

Here is an example of bandwidth management with classes configured for bandwidth borrowing. The classes are set up based on departments and individuals within certain departments.

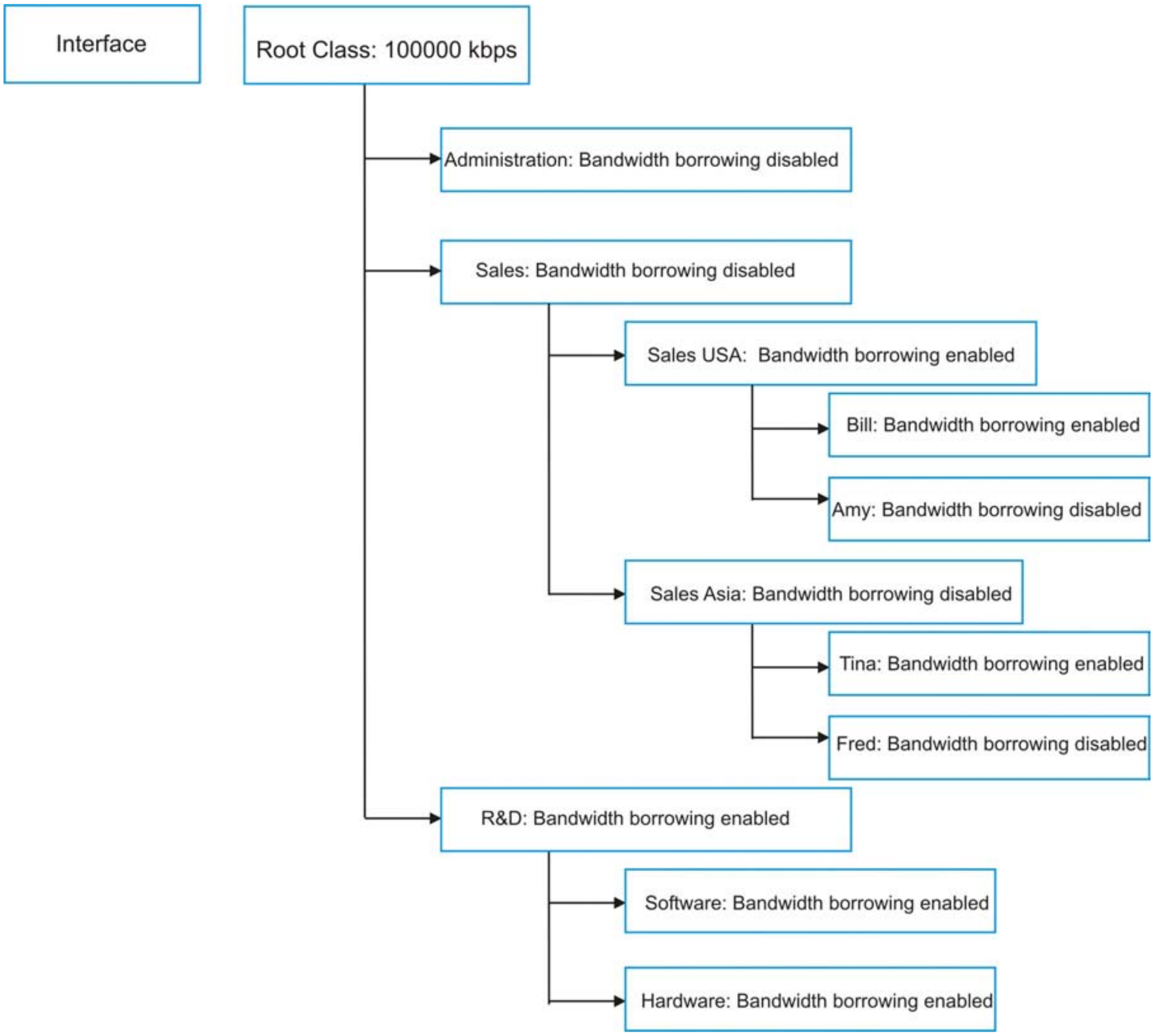

Interface
Root Class: 100000 kbps
Administration: Bandwidth borrowing disabled
Sales: Bandwidth borrowing disabled
Sales USA: Bandwidth borrowing enabled
Bill: Bandwidth borrowing enabled
Amy: Bandwidth borrowing disabled
Sales Asia: Bandwidth borrowing disabled
Tina: Bandwidth borrowing enabled
Fred: Bandwidth borrowing disabled
R&D: Bandwidth borrowing enabled
Software: Bandwidth borrowing enabled
Hardware: Bandwidth borrowing enabled

Table 18-7 Bandwidth Borrowing Example

- The Bill class can borrow unused bandwidth from the Sales USA class because the Bill class has bandwidth borrowing enabled.
- The Bill class can also borrow unused bandwidth from the Sales class because the Sales USA class also has bandwidth borrowing enabled.
- The Bill class cannot borrow unused bandwidth from the Root class because the Sales class has bandwidth borrowing disabled.
- The Amy class cannot borrow unused bandwidth from the Sales USA class because the Amy class has bandwidth borrowing disabled.
- The R&D Software and Hardware classes can both borrow unused bandwidth from the R&D class because the R&D Software and Hardware classes both have bandwidth borrowing enabled.
- The R&D Software and Hardware classes can also borrow unused bandwidth from the Root class because the R&D class also has bandwidth borrowing enabled.

18.7.2 Maximize Bandwidth Usage With Bandwidth Borrowing

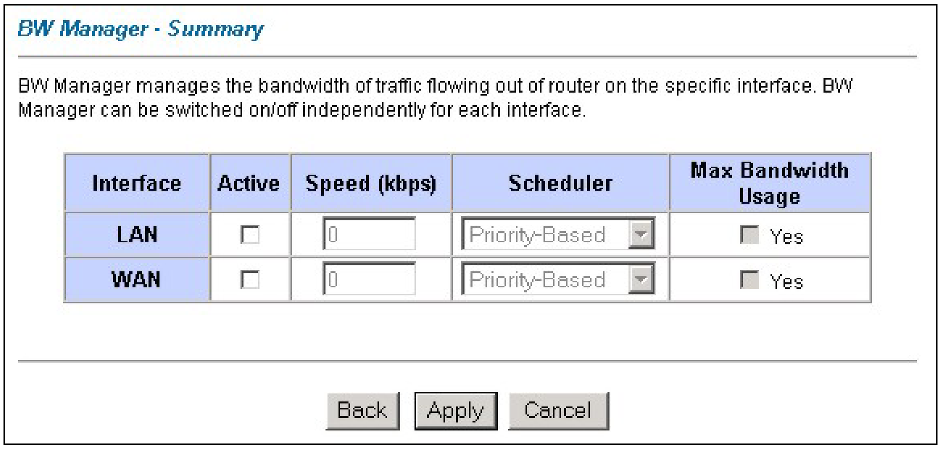
If you configure both maximize bandwidth usage (on the interface) and bandwidth borrowing (on individual child-classes), the Prestige functions as follows.

1. The Prestige sends traffic according to each bandwidth class's bandwidth budget.
2. The Prestige assigns a parent class's unused bandwidth to its child-classes that have more traffic than their budgets and have bandwidth borrowing enabled. The Prestige gives priority to bandwidth child-classes of higher priority and treats bandwidth classes of the same priority equally.
3. The Prestige assigns any remaining unused or unbudgeted bandwidth on the interface to any bandwidth class that requires it. The Prestige gives priority to bandwidth classes of higher priority and treats bandwidth classes of the same level equally.
4. The Prestige assigns any remaining unbudgeted bandwidth to traffic that does not match any of the bandwidth classes.

18.8 Configuring Summary

Click **BW Manager**, **Summary** to open the **Summary** screen.

Enable bandwidth management on an interface and set the maximum allowed bandwidth for that interface.



BW Manager - Summary

BW Manager manages the bandwidth of traffic flowing out of router on the specific interface. BW Manager can be switched on/off independently for each interface.

Interface	Active	Speed (kbps)	Scheduler	Max Bandwidth Usage
LAN	□	0	Priority-Based	□ Yes
WAN	□	0	Priority-Based	□ Yes

Table 18-8 Bandwidth Manager: Summary

The following table describes the labels in this screen.

Table 18-9 Bandwidth Manager: Summary

LABEL	DESCRIPTION
LAN WAN	These read-only labels represent the physical interfaces. Select an interface's check box to enable bandwidth management on that interface. Bandwidth management applies to all traffic flowing out of the router through the interface, regardless of the traffic's source. Traffic redirect or IP alias may cause LAN-to-LAN traffic to pass through the Prestige and be managed by bandwidth management.
Active	Select an interface's check box to enable bandwidth management on that interface.

Table 18-9 Bandwidth Manager: Summary

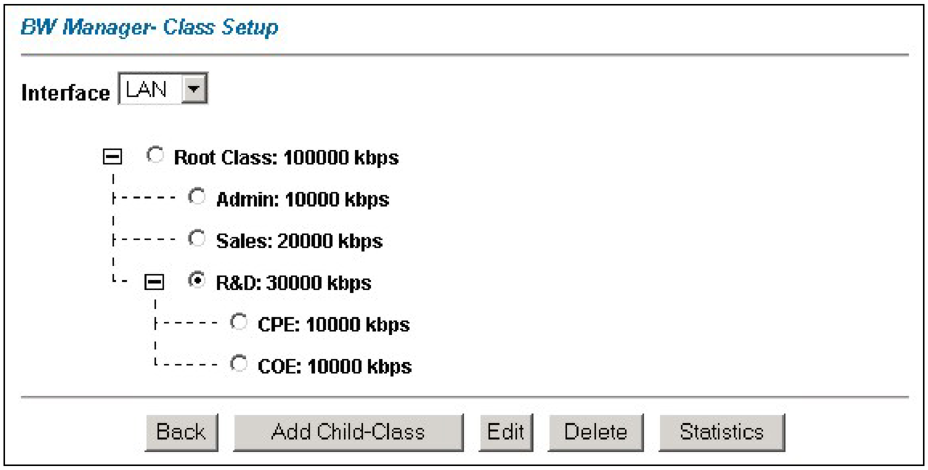
LABEL	DESCRIPTION
Speed (kbps)	Enter the amount of bandwidth for this interface that you want to allocate using bandwidth management. This appears as the bandwidth budget of the interface's root class (see *section 18.9*). The recommendation is to set this speed to match what the interface's connection can handle. For example, set the WAN interface speed to 1000 kbps if the ADSL connection has an upstream speed of 1000 kbps.
Scheduler	Select either **Priority-Based** or **Fairness-Based** from the drop-down menu to control the traffic flow. Select **Priority-Based** to give preference to bandwidth classes with higher priorities. Select **Fairness-Based** to treat all bandwidth classes equally. See *section 18.5*.
Maximize Bandwidth Usage	Select this check box to have the Prestige divide up all of the interface's unallocated and/or unused bandwidth among the bandwidth classes that require bandwidth. Do not select this if you want to reserve bandwidth for traffic that does not match a bandwidth class (see *section 18.6.1*) or you want to limit the speed of this interface (see the **Speed** field description).
Back	Click **Back** to go to the main **BW Manager** screen.
Apply	Click **Apply** to save your settings back to the Prestige.
Cancel	Click **Cancel** to begin configuring this screen afresh.

18.9 Configuring Class Setup

The class setup screen displays the configured bandwidth classes by individual interface. Select an interface and click the buttons to perform the actions described next. Click "+" to expand the class tree or click "-" to collapse the class tree. Each interface has a permanent root class. The bandwidth budget of the root class is equal to the speed you configured on the interface (see *section 18.8* to configure the speed of the interface). Configure child-class layers for the root class.

To add or delete child classes on an interface, click **BW Manager**, then **Class Setup**. The screen appears as shown (with example classes).

The example reserves 10 Mbps of unbudgeted bandwidth for traffic that is not defined in the bandwidth filters (see *section 18.6.1*). The Administration and Sales USA bandwidth classes each have bigger bandwidth budgets than the total of the budgets of their child-classes. The child-classes can borrow the extra bandwidth as long as they have bandwidth borrowing enabled (see *section 18.7*).


BW Manager- Class Setup

Interface: LAN

○ Root Class: 100000 kbps
○ Admin: 10000 kbps
○ Sales: 20000 kbps
● R&D: 30000 kbps
○ CPE: 10000 kbps
○ COE: 10000 kbps

Table 18-10 Bandwidth Manager: Class Setup

The following table describes the labels in this screen.

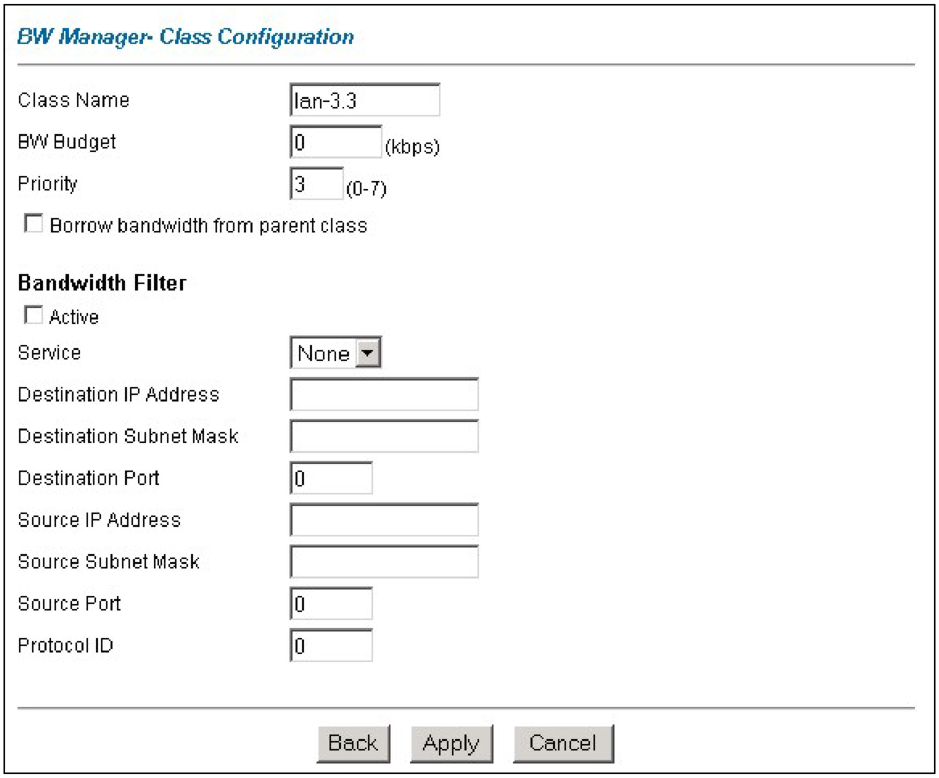
Table 18-11 Bandwidth Manager: Class Setup

LABEL	DESCRIPTION
Interface	Select an interface from the drop-down list box for which you wish to set up classes.
Back	Click **Back** to go to the main **BW Manager** screen.
Add Child-Class	Click **Add Child-class** to add a sub-class.
Edit	Click **Edit** to configure the selected class. You cannot edit the root class.
Delete	Click **Delete** to delete the class and all its child-classes. You cannot delete the root class.
Statistics	Click **Statistics** to display the status of the selected class.

18.9.1 Bandwidth Manager Class Configuration

Configure a bandwidth management class in the **Class Configuration** screen. You must use the **Bandwidth Manager - Summary** screen to enable bandwidth management on an interface before you can configure classes for that interface.

To add a child class, click **BW Manager**, then **Class Setup**. Click the **Add Child-Class** button to open the following screen.



BW Manager- Class Configuration

Class Name	lan-3.3
BW Budget	0 (kbps)
Priority	3 (0-7)

□ Borrow bandwidth from parent class

Bandwidth Filter

□ Active

Service	None
Destination IP Address	
Destination Subnet Mask	
Destination Port	0
Source IP Address	
Source Subnet Mask	
Source Port	0
Protocol ID	0

Table 18-12 Bandwidth Manager: Class Configuration

The following table describes the labels in this screen.

Table 18-13 Bandwidth Manager: Class Configuration

LABEL	DESCRIPTION
Class Name	Use the auto-generated name or enter a descriptive name of up to 20 alphanumeric characters, including spaces.
BW Budget (kbps)	Specify the maximum bandwidth allowed for the class in kbps. The recommendation is a setting between 20 kbps and 20000 kbps for an individual class.
Priority	Enter a number between 0 and 7 to set the priority of this class. The higher the number, the higher the priority. The default setting is 3.
Borrow bandwidth from parent class	Select this option to allow a child-class to borrow bandwidth from its parent class if the parent class is not using up its bandwidth budget. Bandwidth borrowing is governed by the priority of the child-classes. That is, a child-class with the highest priority (7) is the first to borrow bandwidth from its parent class. Do not select this for the classes directly below the root class if you want to leave bandwidth available for other traffic types (see *section 18.6.1*) or you want to set the interface's speed to match what the next device in network can handle (see the **Speed** field description in *Table 18-9*).
Bandwidth Filter The Prestige uses a bandwidth filter to identify the traffic that belongs to a bandwidth class.	
Active	Select the check box to have the Prestige use this bandwidth filter when it performs bandwidth management.
Service	You can select a predefined service instead of configuring the **Destination Port**, **Source Port** and **Protocol ID** fields. SIP (Session Initiation Protocol) is a signaling protocol used in Internet telephony, instant messaging and other VoIP (Voice over IP) applications. Select **SIP** from the drop-down list box to configure this bandwidth filter for traffic that uses SIP. At the time of writing, SIP was the only predefined service. When you select **None**, the bandwidth class applies to all services unless you specify one by configuring the **Destination Port**, **Source Port** and **Protocol ID** fields.
Destination IP Address	Enter the destination IP address in dotted decimal notation. A blank destination IP address means any destination IP address.
Destination Subnet Mask	Enter the destination subnet mask. This field is N/A if you do not specify a **Destination IP Address**. Refer to the appendix for more information on IP subnetting.
Destination Port	Enter the port number of the destination. A blank destination port means any destination port.
Source IP Address	Enter the source IP address. A blank source IP address means any source IP address.
Source Subnet Mask	Enter the source subnet mask. This field is N/A if you do not specify a **Source IP Address**. Refer to the appendix for more information on IP subnetting.
Source Port	Enter the port number of the source. See the following table for some common services and port numbers. A blank source port means any source port number.
Protocol ID	Enter the protocol ID (service type) number, for example: 1 for ICMP, 6 for TCP or 17 for UDP. A blank protocol ID means any protocol number.
TOS (Type of Service)	TOS defines the DS(Differentiated Service) field in the IP header. Enter the new TOS value of the outgoing packet (between 0 and 255). 0 is the lowest priority.

Table 18-13 Bandwidth Manager: Class Configuration

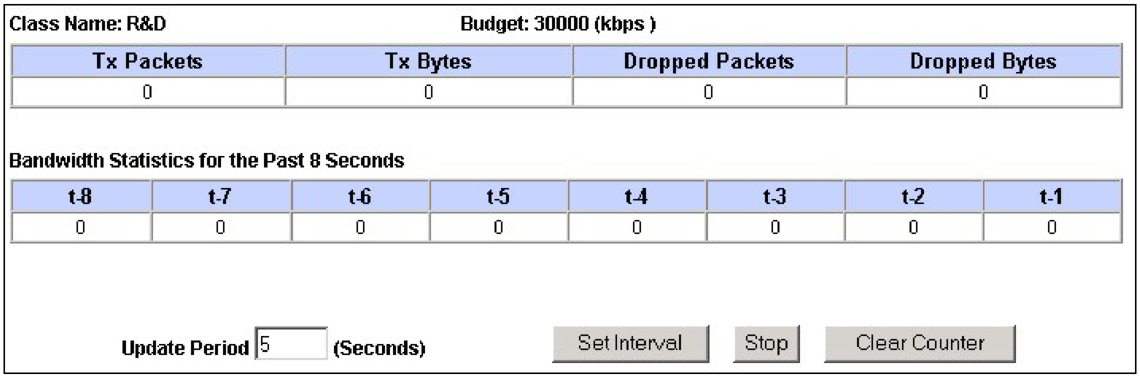
LABEL	DESCRIPTION
TOS Mask	The ToS mask is used to compare the specified (or entire) bits in the ToS IP header with the value specified in this rule. Enter the TOS Mask value between 0 (lowest priority) and 255.
Back	Click **Back** to go to the main **BW Manager** screen.
Apply	Click **Apply** to save your changes back to the Prestige.
Cancel	Click **Cancel** to begin configuring this screen afresh.

Table 18-14 Services and Port Numbers

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

18.9.2 Bandwidth Management Statistics

Use the **Bandwidth Management Statistics** screen to view network performance information. Click the **Statistics** button in the **Class Setup** screen to open the **Statistics** screen.



Class Name: R&D Budget: 30000 (kbps)

Tx Packets	Tx Bytes	Dropped Packets	Dropped Bytes
0	0	0	0

Bandwidth Statistics for the Past 8 Seconds

t-8	t-7	t-6	t-5	t-4	t-3	t-2	t-1
0	0	0	0	0	0	0	0

Update Period 5 (Seconds)

Table 18-15 Bandwidth Management Statistics

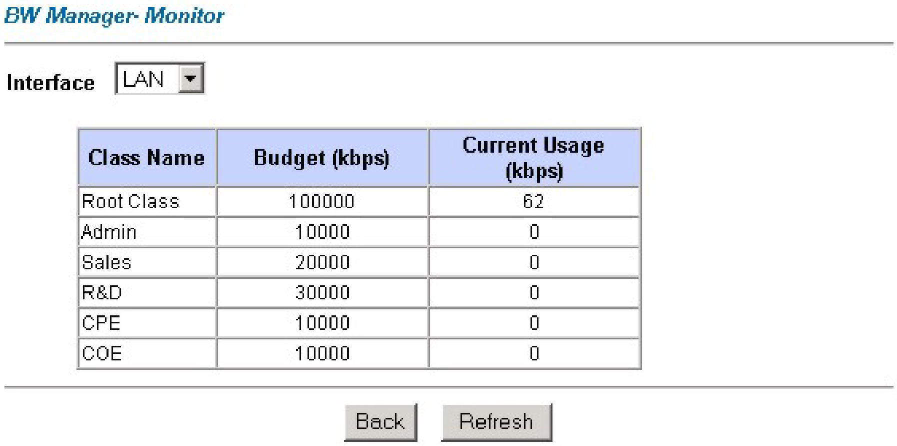
The following table describes the labels in this screen.

Table 18-16 Bandwidth Management Statistics

LABEL	DESCRIPTION
Class Name	This field displays the name of the class the statistics page is showing.
Budget (kbps)	This field displays the amount of bandwidth allocated to the class.
Tx Packets	This field displays the total number of packets transmitted.
Tx Bytes	This field displays the total number of bytes transmitted.
Dropped Packets	This field displays the total number of packets dropped.
Dropped Bytes	This field displays the total number of bytes dropped.
Bandwidth Statistics for the Past 8 Seconds (t-8 to t-1)	
This field displays the bandwidth statistics (in bps) for the past one to eight seconds. For example, t-1 means one second ago.	
Update Period (seconds)	Enter the time interval in seconds to define how often the information should be refreshed.
Set Interval	Click **Set Interval** to apply the new update period you entered in the **Update Period** field above.
Stop Update	Click **Stop Update** to stop the browser from refreshing bandwidth management statistics.
Clear Counter	Click **Clear Counter** to clear all of the bandwidth management statistics.

18.10 Bandwidth Monitor

To view the Prestige's bandwidth usage and allotments, click **BW Manager**, then **Monitor**. The screen appears as shown.



BW Manager- Monitor

Interface: LAN

Class Name	Budget (kbps)	Current Usage (kbps)
Root Class	100000	62
Admin	10000	0
Sales	20000	0
R&D	30000	0
CPE	10000	0
COE	10000	0

Table 18-17 Bandwidth Manager Monitor

The following table describes the labels in this screen.

Table 18-18 Bandwidth Manager Monitor

LABEL	DESCRIPTION
Interface	Select an interface from the drop-down list box to view the bandwidth usage of its bandwidth classes.

Table 18-18 Bandwidth Manager Monitor

LABEL	DESCRIPTION
Class Name	This field displays the name of the class.
Budget (kbps)	This field displays the amount of bandwidth allocated to the class.
Current Usage (kbps)	This field displays the amount of bandwidth that each class is using.
Back	Click **Back** to go to the main **BW Manager** screen.
Refresh	Click **Refresh** to update the page.

Part VII:

Maintenance

This part covers the maintenance screens.

Chapter 19 Maintenance

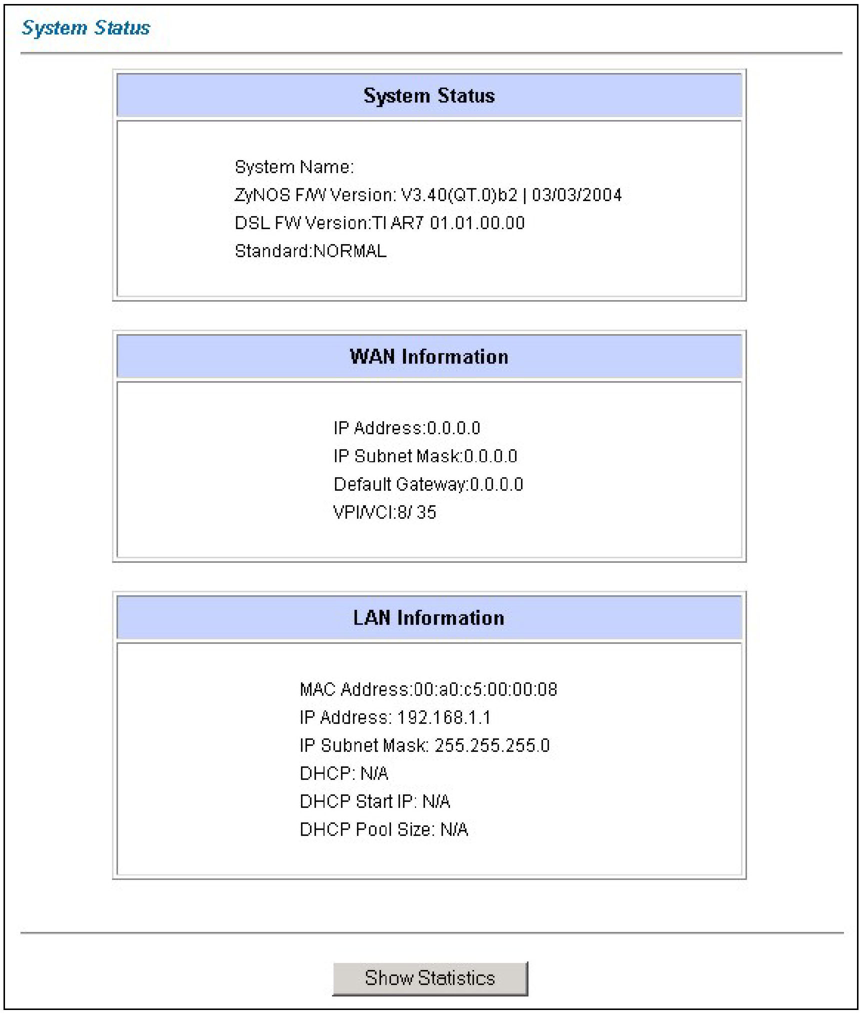
This chapter displays system information such as ZyNOS firmware, port IP addresses and port traffic statistics.

19.1 Maintenance Overview

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

19.2 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.



System Status

System Status

System Name:
ZyNOS F/W Version: V3.40(QT.0)b2 | 03/03/2004
DSL FW Version:TI AR7 01.01.00.00
Standard:NORMAL

WAN Information

IP Address:0.0.0.0
IP Subnet Mask:0.0.0.0
Default Gateway:0.0.0.0
VPI/VCI:8/ 35

LAN Information

MAC Address:00:a0:c5:00:00:08
IP Address: 192.168.1.1
IP Subnet Mask: 255.255.255.0
DHCP: N/A
DHCP Start IP: N/A
DHCP Pool Size: N/A

Figure 19-1 System Status

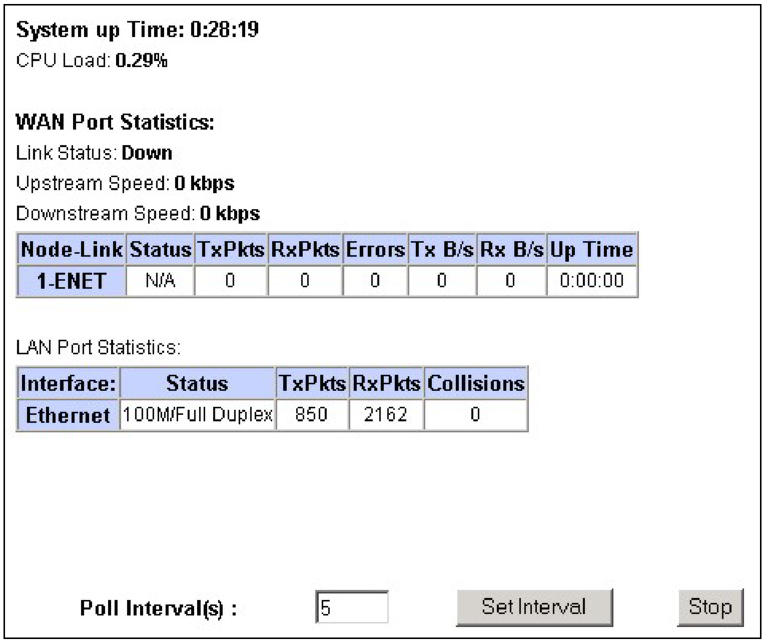
The following table describes the fields in this screen.

Table 19-1 System Status

LABEL	DESCRIPTION
System Status	
System Name	This is the name of your Prestige. It is for identification purposes.
ZyNOS Firmware Version	This is the ZyNOS firmware version and the date created. ZyNOS is ZyXEL's proprietary Network Operating System design.
DSL FW Version	This is the DSL firmware version associated with your Prestige.
Standard	This is the standard that your Prestige is using.
WAN Information	
IP Address	This is the WAN port IP address.
IP Subnet Mask	This is the WAN port IP subnet mask.
Default Gateway	This is the IP address of the default gateway, if applicable.
VPI/VCI	This is the Virtual Path Identifier and Virtual Channel Identifier that you entered in the first Wizard screen.
LAN Information	
MAC Address	This is the MAC (Media Access Control) or Ethernet address unique to your Prestige.
IP Address	This is the LAN port IP address.
IP Subnet Mask	This is the LAN port IP subnet mask.
DHCP	This is the WAN port DHCP role - **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.

19.2.1 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.



System up Time: 0:28:19

CPU Load: **0.29%**

WAN Port Statistics:

Link Status: **Down**

Upstream Speed: **0 kbps**

Downstream Speed: **0 kbps**

Node-Link	Status	TxPkts	RxPkts	Errors	Tx B/s	Rx B/s	Up Time
1-ENET	N/A	0	0	0	0	0	0:00:00

LAN Port Statistics:

Interface:	Status	TxPkts	RxPkts	Collisions
Ethernet	100M/Full Duplex	850	2162	0

Poll Interval(s) : 5

Figure 19-2 System Status: Show Statistics

The following table describes the fields in this screen.

Table 19-2 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.

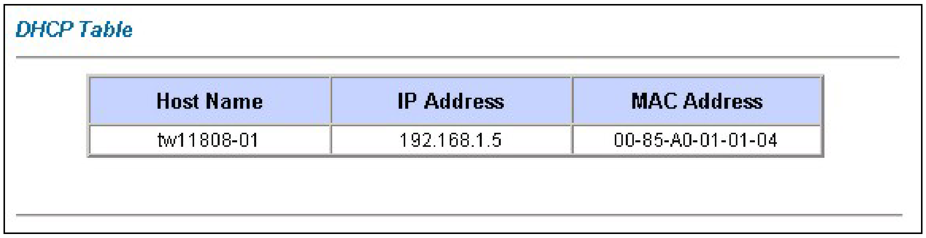
Table 19-2 System Status: Show Statistics

LABEL	DESCRIPTION
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.

19.3 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.



DHCP Table

Host Name	IP Address	MAC Address
tw11808-01	192.168.1.5	00-85-A0-01-01-04

Figure 19-3 DHCP Table

The following table describes the fields in this screen.

Table 19-3 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.

19.4 Diagnostic Screens

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

19.4.1 Diagnostic General Screen

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

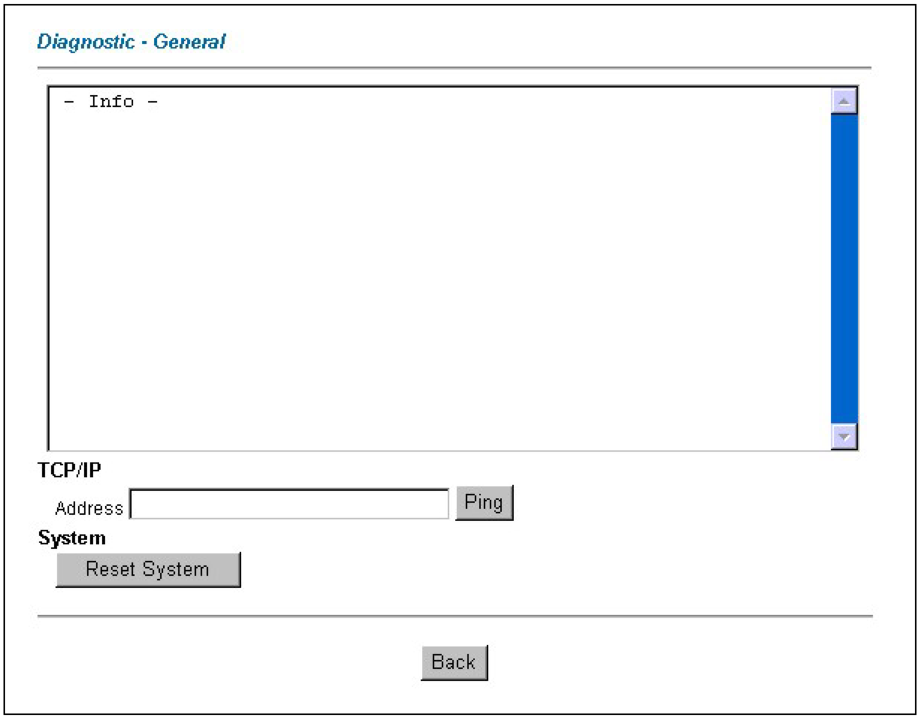


Figure 19-4 Diagnostic General

The following table describes the fields in this screen.

Table 19-4 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.

19.4.2 Diagnostic DSL Line Screen

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

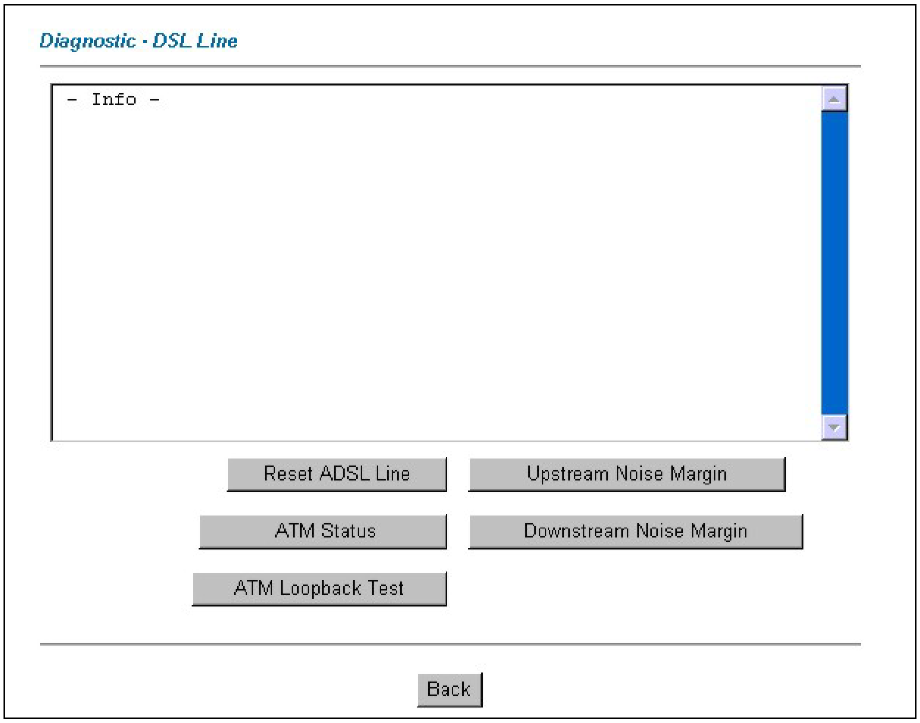


Figure 19-5 Diagnostic DSL Line

The following table describes the fields in this screen.

Table 19-5 Diagnostic DSL Line

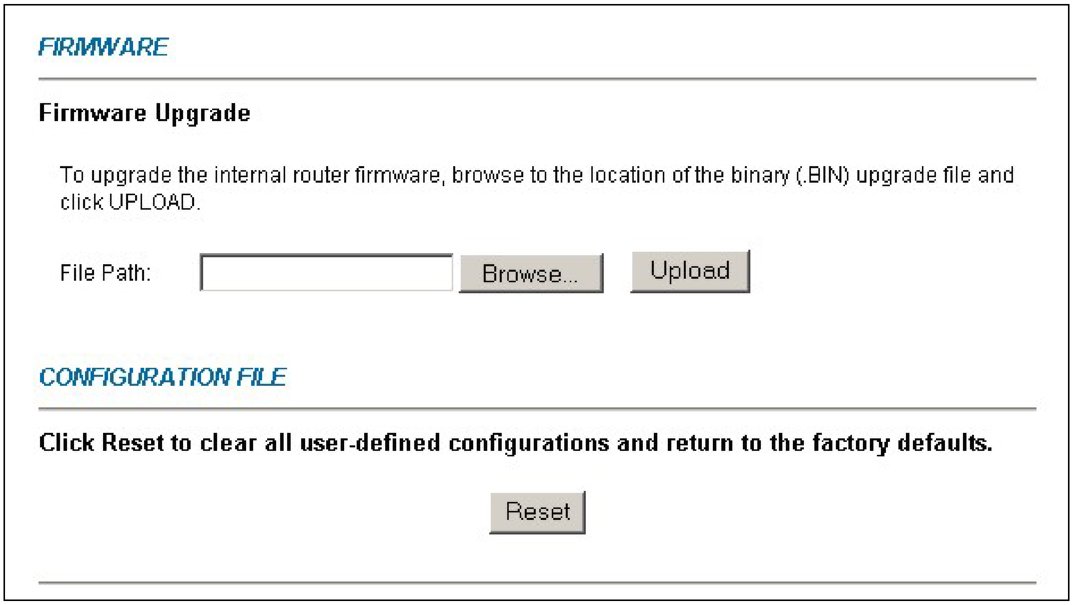
LABEL	DESCRIPTION
Reset ADSL Line	Click this button to reinitialize the ADSL line. The large text box above then displays the progress and results of this operation, for example: "Start to reset ADSL Loading ADSL modem F/W... Reset ADSL Line Successfully!"
ATM Status	Click this button to view ATM status.
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.

19.5 Firmware Screen

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

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

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



FIRMWARE

Firmware Upgrade

To upgrade the internal router firmware, browse to the location of the binary (.BIN) upgrade file and click UPLOAD.

File Path:

CONFIGURATION FILE

Click Reset to clear all user-defined configurations and return to the factory defaults.

Figure 19-6 Firmware Upgrade

The following table describes the labels in this screen.

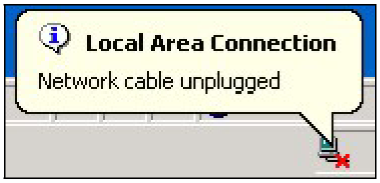
Table 19-6 Firmware Upgrade

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.

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.



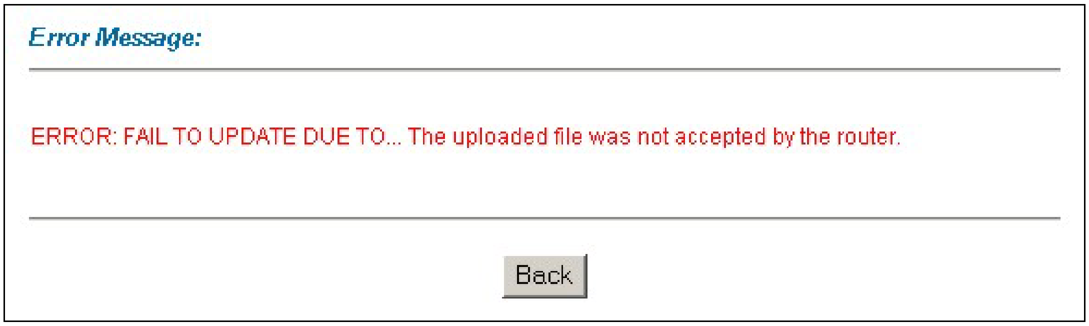
Local Area Connection

Network cable unplugged

Figure 19-7 Network Temporarily Disconnected

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

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



Error Message:

ERROR: FAIL TO UPDATE DUE TO... The uploaded file was not accepted by the router.

Figure 19-8 Error Message

Part VIII:

SMT General Configuration

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

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

Chapter 20
Introducing the SMT

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

20.1 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.

20.1.1 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.

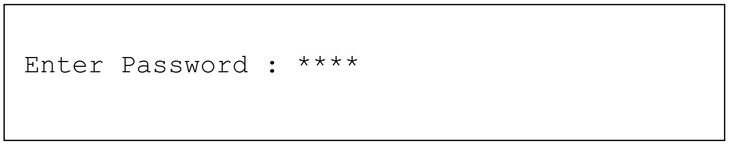
Please note that if there is no activity for longer than five minutes (default timeout period) after you log in, your Prestige will automatically log you out. You will then have to telnet into the Prestige again.

20.1.2 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.



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

Figure 20-1 Login Screen

20.1.3 Prestige SMT Menu Overview

We use the Prestige 660H-61 SMT menus in this guide as an example. The SMT menus vary slightly for different Prestige models.

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

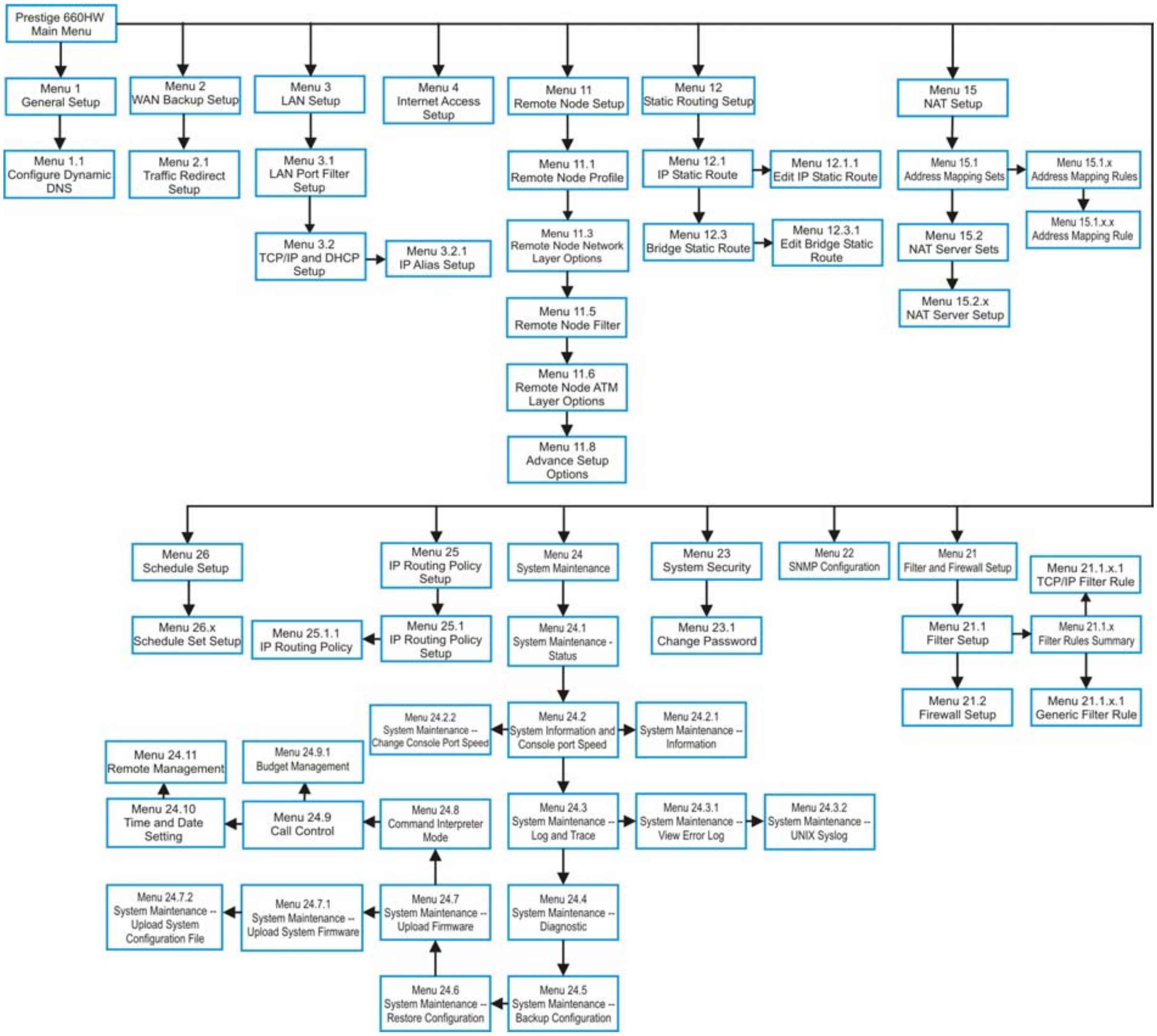

Prestige 660HW Main Menu
Menu 1 General Setup
Menu 1.1 Configure Dynamic DNS
Menu 2 WAN Backup Setup
Menu 2.1 Traffic Redirect Setup
Menu 3 LAN Setup
Menu 3.1 LAN Port Filter Setup
Menu 3.2 TCP/IP and DHCP Setup
Menu 3.2.1 IP Alias Setup
Menu 4 Internet Access Setup
Menu 11 Remote Node Setup
Menu 11.1 Remote Node Profile
Menu 11.3 Remote Node Network Layer Options
Menu 11.5 Remote Node Filter
Menu 11.6 Remote Node ATM Layer Options
Menu 11.8 Advance Setup Options
Menu 12 Static Routing Setup
Menu 12.1 IP Static Route
Menu 12.1.1 Edit IP Static Route
Menu 12.3 Bridge Static Route
Menu 12.3.1 Edit Bridge Static Route
Menu 15 NAT Setup
Menu 15.1 Address Mapping Sets
Menu 15.1.x Address Mapping Rules
Menu 15.1.x.x Address Mapping Rule
Menu 15.2 NAT Server Sets
Menu 15.2.x NAT Server Setup
Menu 26 Schedule Setup
Menu 26.x Schedule Set Setup
Menu 25 IP Routing Policy Setup
Menu 25.1 IP Routing Policy Setup
Menu 25.1.1 IP Routing Policy
Menu 24 System Maintenance
Menu 24.1 System Maintenance - Status
Menu 24.2 System Information and Console port Speed
Menu 24.2.1 System Maintenance -- Information
Menu 24.2.2 System Maintenance -- Change Console Port Speed
Menu 24.3 System Maintenance -- Log and Trace
Menu 24.3.1 System Maintenance -- View Error Log
Menu 24.3.2 System Maintenance -- UNIX Syslog
Menu 24.4 System Maintenance -- Diagnostic
Menu 24.5 System Maintenance -- Backup Configuration
Menu 24.6 System Maintenance -- Restore Configuration
Menu 24.7 System Maintenance -- Upload Firmware
Menu 24.7.1 System Maintenance -- Upload System Firmware
Menu 24.7.2 System Maintenance -- Upload System Configuration File
Menu 24.8 Command Interpreter Mode
Menu 24.9 Call Control
Menu 24.9.1 Budget Management
Menu 24.10 Time and Date Setting
Menu 24.11 Remote Management
Menu 23 System Security
Menu 23.1 Change Password
Menu 22 SNMP Configuration
Menu 21 Filter and Firewall Setup
Menu 21.1 Filter Setup
Menu 21.1.x Filter Rules Summary
Menu 21.1.x.1 TCP/IP Filter Rule
Menu 21.1.x.1 Generic Filter Rule
Menu 21.2 Firewall Setup

Figure 20-2 Prestige 660H-61 SMT Menu Overview

20.2 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.

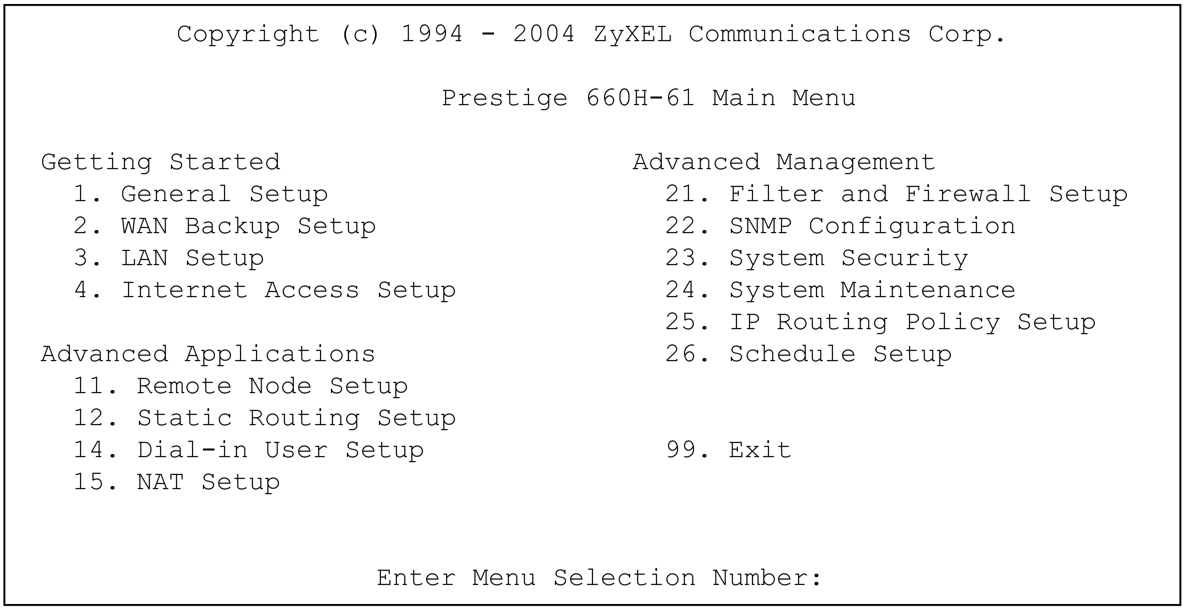
Table 20-1 Main Menu Commands

OPERATION	KEYSTROKE	DESCRIPTION
Move down to another menu	[ENTER]	To move forward to a submenu, type in the number of the desired submenu and press [ENTER].
Move up to a previous menu	[ESC]	Press [ESC] to move back to the previous menu.

Table 20-1 Main Menu Commands

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

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



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

                             Prestige 660H-61 Main Menu

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


                        Enter Menu Selection Number:
```

Figure 20-3 SMT Main Menu

20.2.1 System Management Terminal Interface Summary

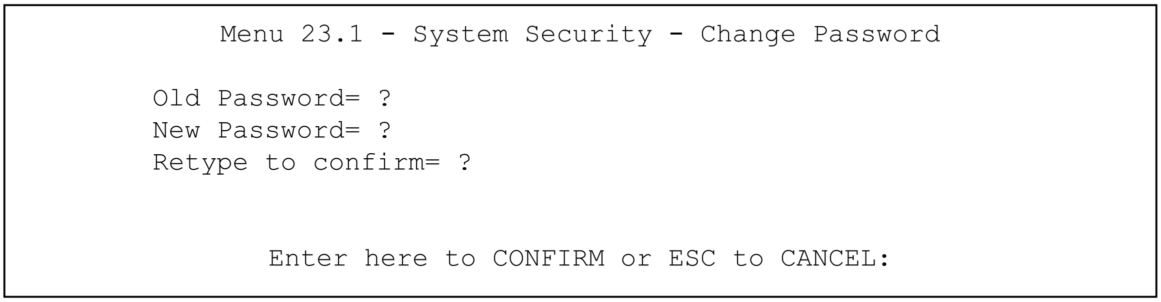
Table 20-2 Main Menu Summary

#	MENU TITLE	DESCRIPTION
1	General Setup	Use this menu to set up your general information.
2	WAN Backup Setup	Use this menu to setup traffic redirect and dial-back up.
3	LAN Setup	Use this menu to set up your LAN connection.
4	Internet Access Setup	A quick and easy way to set up an Internet connection.
11	Remote Node Setup	Use this menu to set up the Remote Node for LAN-to-LAN connection, including Internet connection.
12	Static Routing Setup	Use this menu to set up static routes.
14	Dial-in User Setup	Use this menu to set up local user profiles on the Prestige.
15	NAT Setup	Use this menu to specify inside servers when NAT is enabled.
21	Filter and Firewall Setup	Use this menu to configure filters, activate/deactivate the firewall and view the firewall log.
22	SNMP Configuration	Use this menu to set up SNMP related parameters.
23	System Security	Use this menu to 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.

20.3 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 Security**.
2. Enter 1 to display **Menu 23.1 - System Security - Change Password** as shown next.
3. Type your existing system password in the **Old Password** field, for example "1234", and press [ENTER].



```
                 Menu 23.1 - System Security - Change Password

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


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

Figure 20-4 Menu 23.1 Change Password

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

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

Chapter 21
Menu 1 General Setup

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

21.1 General Setup

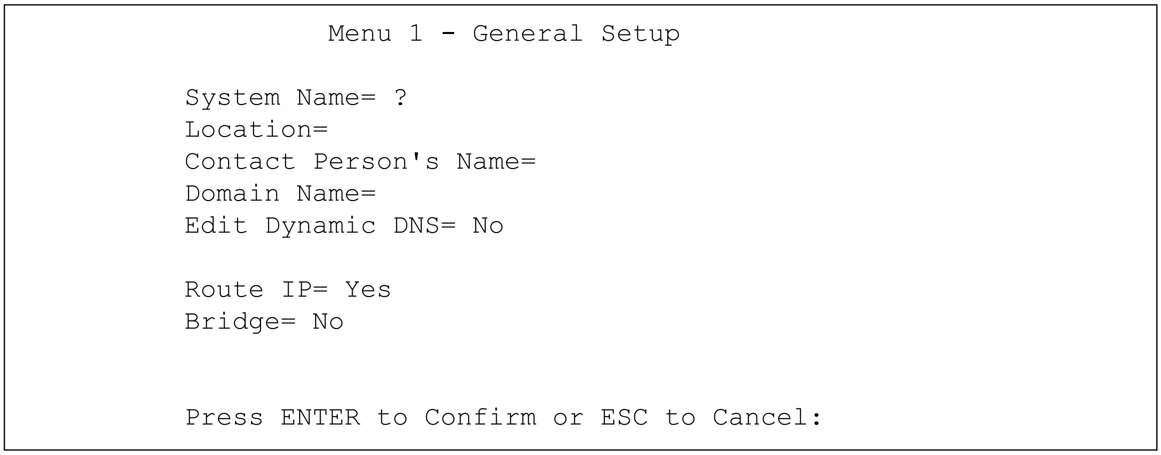
Menu 1 — General Setup contains administrative and system-related information (shown next). The **System Name** field is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

- 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.

21.2 Procedure To Configure Menu 1

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



```
                   Menu 1 - General Setup

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

          Route IP= Yes
          Bridge= No


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

Figure 21-1 Menu 1 General Setup

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

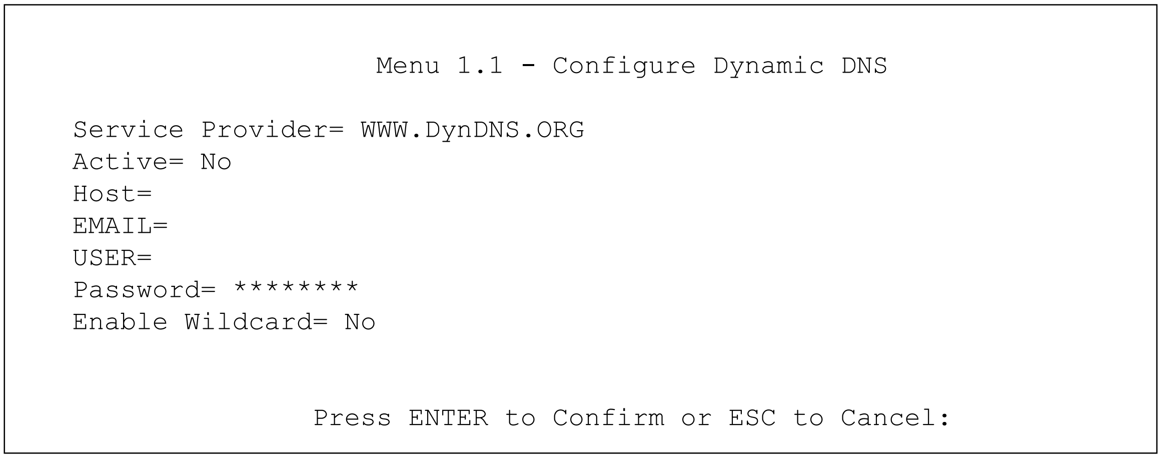
Table 21-1 Menu 1 General Setup

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

21.2.1 Procedure to Configure Dynamic DNS

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.



```
                    Menu 1.1 - Configure Dynamic DNS

    Service Provider= WWW.DynDNS.ORG
    Active= No
    Host=
    EMAIL=
    USER=
    Password= ********
    Enable Wildcard= No


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

Figure 21-2 Menu 1.1 Configure Dynamic DNS

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

Table 21-2 Menu 1.1 Configure Dynamic DNS

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

Chapter 22
Menu 2 WAN Backup Setup

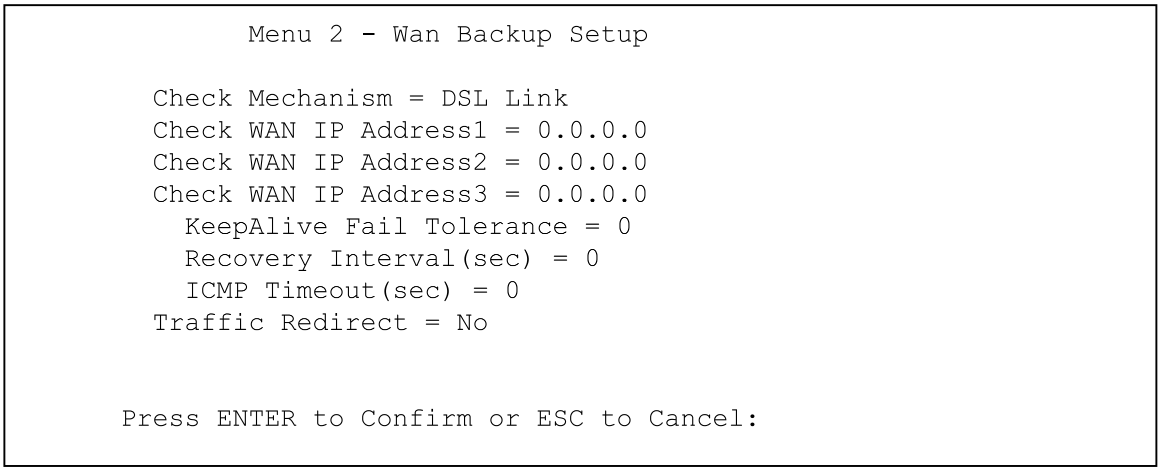
This chapter describes how to configure traffic redirect and dial-backup using menu 2 and 2.1.

22.1 Introduction to WAN Backup Setup

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

22.2 Configuring Dial Backup in Menu 2

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



```
               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:
```

Figure 22-1 Menu 2 WAN Backup Setup

The following table describes the fields in this menu.

Table 22-1 Menu 2 WAN Backup Setup

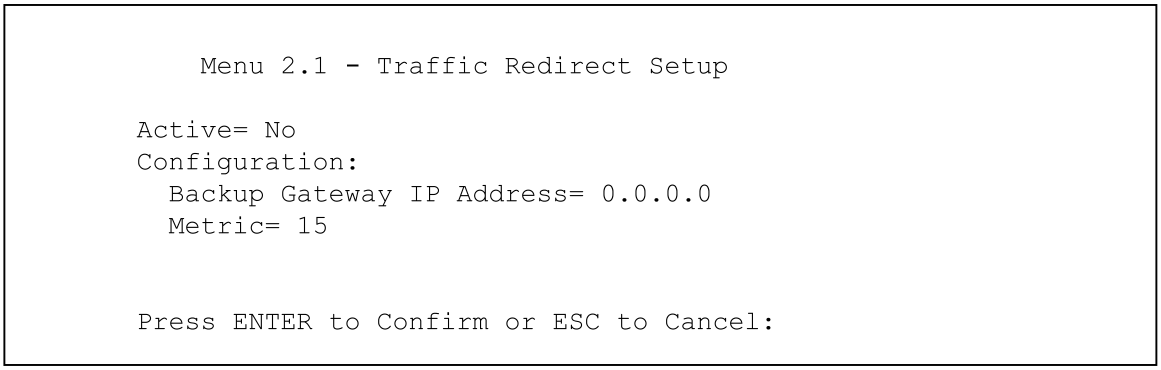
FIELD	DESCRIPTION
Check Mechanism	Press [SPACE BAR] and then press [ENTER] to select the method that the Prestige uses to check the DSL connection. Select **DSL Link** to have the Prestige check the DSL connection's physical layer. Select **ICMP** to have the Prestige periodically ping the IP addresses 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).

Table 22-1 Menu 2 WAN Backup Setup

FIELD	DESCRIPTION
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…" to save your configuration, or press [ESC] at any time to cancel.	

22.2.1 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**.



```
          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:
```

Figure 22-2 Menu 2.1Traffic Redirect Setup

The following table describes the fields in this menu.

Table 22-2 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.

Table 22-2 Menu 2.1Traffic Redirect Setup

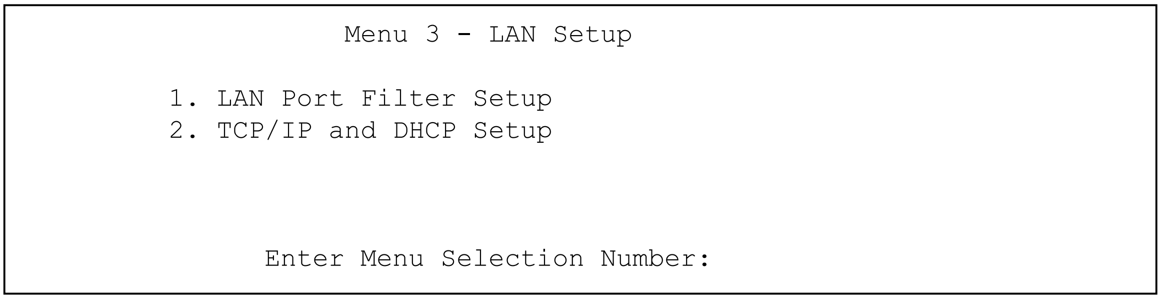
FIELD	DESCRIPTION
Metric	This field sets this route's priority among the routes the Prestige uses. The metric represents the "cost of transmission". A router determines the best route for transmission by choosing a path with the lowest "cost". RIP routing uses hop count as the measurement of cost, with a minimum of "1" for directly connected networks. The number must be between "1" and "15"; a number greater than "15" means the link is down. The smaller the number, the lower the "cost".
When you have completed this menu, press [ENTER] at the prompt “Press [ENTER] to confirm or [ESC] to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

Chapter 23
Menu 3 LAN Setup

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

23.1 LAN Setup

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

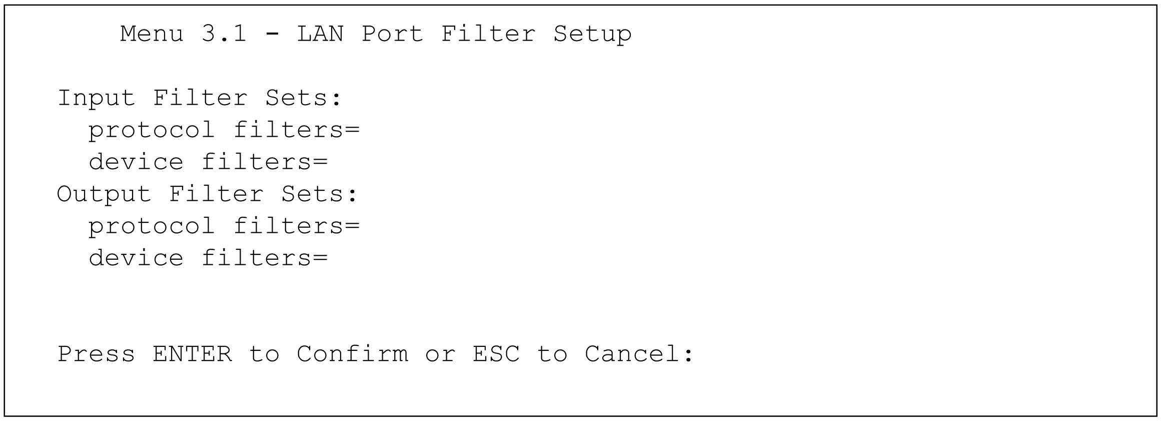


```
                    Menu 3 - LAN Setup

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



               Enter Menu Selection Number:
```

Figure 23-1 Menu 3 LAN Setup

23.1.1 General Ethernet Setup

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



```
       Menu 3.1 - LAN Port Filter Setup

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


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

Figure 23-2 Menu 3.1 LAN Port Filter Setup

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

23.2 Protocol Dependent Ethernet Setup

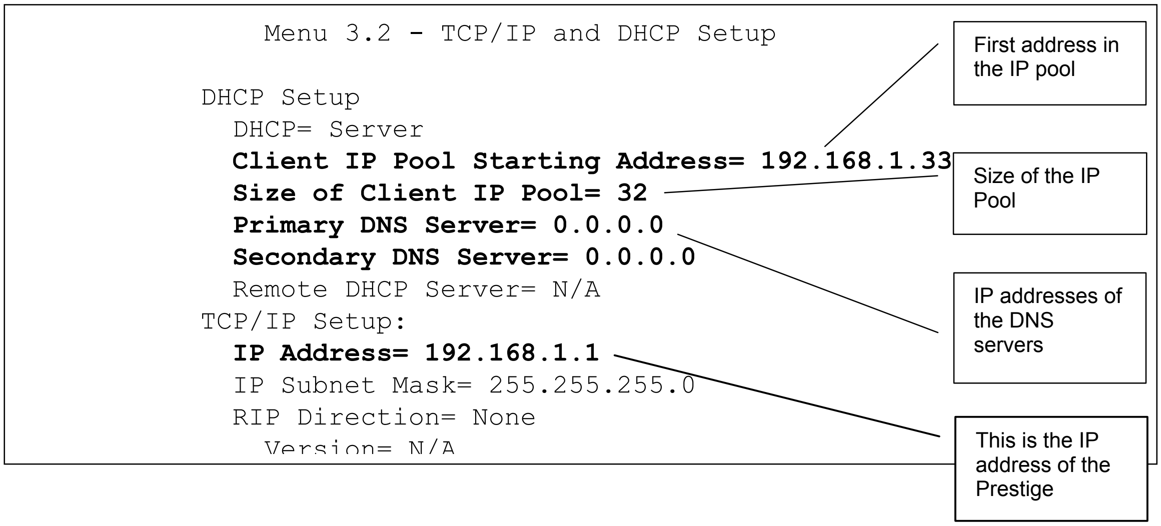
Depending on the protocols for your applications, you need to configure the respective Ethernet Setup, as outlined below.

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

23.3 TCP/IP Ethernet Setup and DHCP

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

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



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

            DHCP Setup
              DHCP= Server
              Client IP Pool Starting Address= 192.168.1.33
              Size of Client IP Pool= 32
              Primary DNS Server= 0.0.0.0
              Secondary DNS Server= 0.0.0.0
              Remote DHCP Server= N/A
            TCP/IP Setup:
              IP Address= 192.168.1.1
              IP Subnet Mask= 255.255.255.0
              RIP Direction= None
                Version= N/A
```

First address in the IP pool

Size of the IP Pool

IP addresses of the DNS servers

This is the IP address of the Prestige

Figure 23-3 Menu 3.2 TCP/IP and DHCP Ethernet Setup

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

Table 23-1 DHCP Ethernet Setup

FIELD	DESCRIPTION	EXAMPLE
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 is used, the following items need to be set:	**Server** (default)
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.	192.168.1.33
Size of Client IP Pool	This field specifies the size or count of the IP address pool.	32

Table 23-1 DHCP Ethernet Setup

FIELD	DESCRIPTION	EXAMPLE
Primary DNS Server Secondary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.	
Remote DHCP Server	If **Relay** is selected in the **DHCP** field above then enter the IP address of the actual remote DHCP server here.	

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

Table 23-2 TCP/IP Ethernet Setup

FIELD	DESCRIPTION	EXAMPLE
TCP/IP Setup		
IP Address	Enter the (LAN) IP address of your Prestige in dotted decimal notation	192.168.1.1
IP Subnet Mask	Your Prestige will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Prestige.	255.255.255.0
RIP Direction	Press [SPACE BAR] to select the RIP direction. Choices are **Both**, **In Only**, **Out Only** or **None**.	**Both** (default)
Version	Press [SPACE BAR] to select the RIP version. Choices are **RIP-1**, **RIP-2B** or **RIP-2M**.	**RIP-1** (default)
Multicast	IGMP (Internet Group Multicast Protocol) is a network-layer protocol used to establish membership in a Multicast group. The Prestige supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). Press the [SPACE BAR] to enable IP Multicasting or select **None** to disable it.	**None** (default)
IP Policies	Create policies using SMT menu 25 (see the *IP Policy Routing chapter*) and apply them on the Prestige LAN interface here. You can apply up to four IP Policy sets (from twelve) by entering their numbers separated by commas.	2,4,7,9
Edit IP Alias	The Prestige supports three logical LAN interfaces via its single physical Ethernet interface with the Prestige itself as the gateway for each LAN network. Press [SPACE BAR] to change **No** to **Yes** and press [ENTER] to display menu 3.2.1.	**No** (default)

Chapter 24
Internet Access

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

24.1 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.

24.2 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 *IP Policy Routing*) and apply them on the Prestige LAN and/or WAN interfaces using menus 3.2 (LAN) and 11.3 (WAN).

24.3 IP Alias

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

When you use IP alias, you can also configure firewall rules to control access between the LAN's logical networks (subnets).

☞ **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.

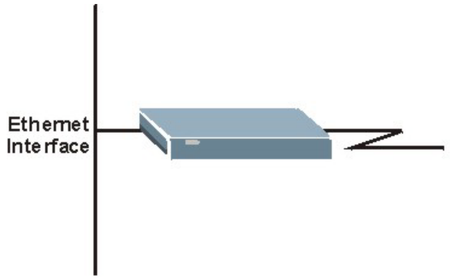


Figure 24-1 Physical Network

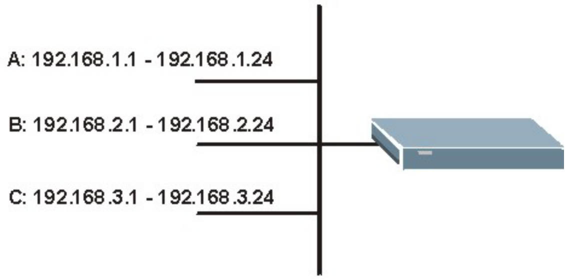
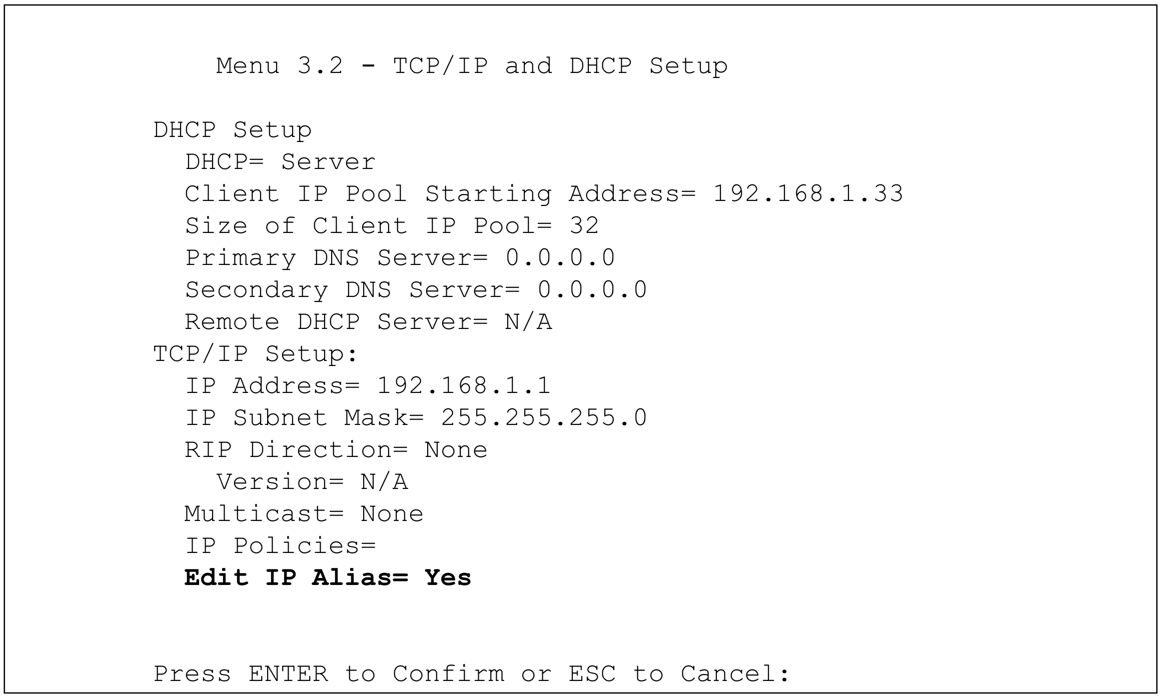

A: 192.168.1.1 - 192.168.1.24
B: 192.168.2.1 - 192.168.2.24
C: 192.168.3.1 - 192.168.3.24

Figure 24-2 Partitioned Logical Networks

Use menu 3.2.1 to configure IP Alias on your Prestige.

24.4 IP Alias Setup

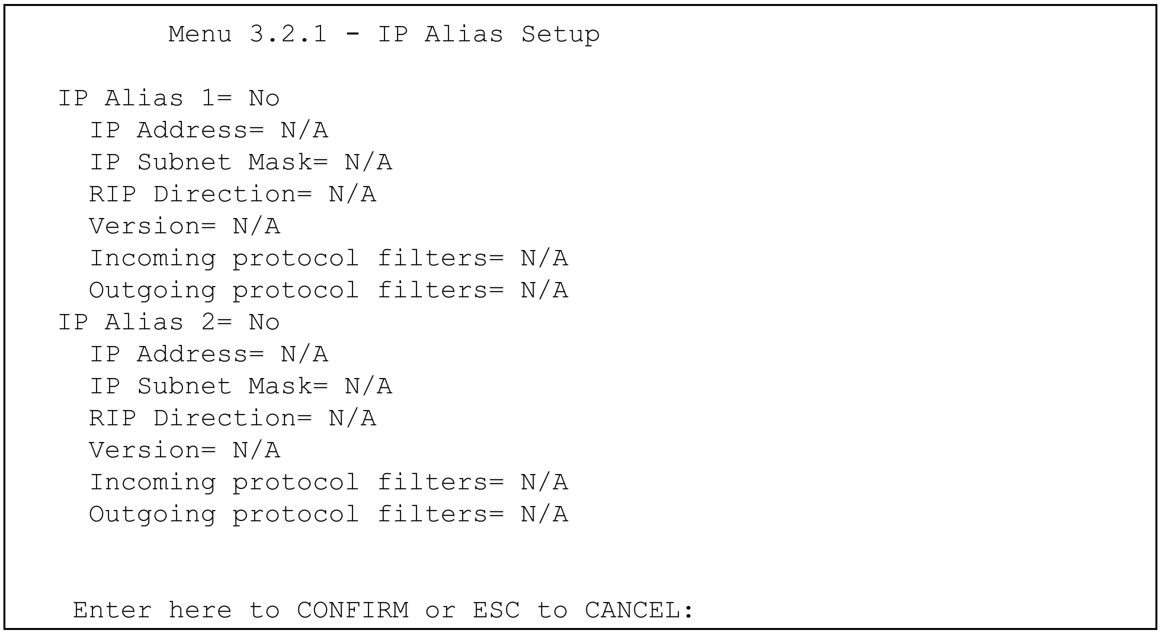
Use menu 3.2 to configure the first network. Move the cursor to **Edit IP Alias** field and press [SPACEBAR] to choose **Yes** and press [ENTER] to configure the second and third network.



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

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


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

Figure 24-3 Menu 3.2 TCP/IP and DHCP Setup

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



```
          Menu 3.2.1 - IP Alias Setup

   IP Alias 1= No
     IP Address= N/A
     IP Subnet Mask= N/A
     RIP Direction= N/A
     Version= N/A
     Incoming protocol filters= N/A
     Outgoing protocol filters= N/A
   IP Alias 2= No
     IP Address= N/A
     IP Subnet Mask= N/A
     RIP Direction= N/A
     Version= N/A
     Incoming protocol filters= N/A
     Outgoing protocol filters= N/A


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

Figure 24-4 Menu 3.2.1 IP Alias Setup

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

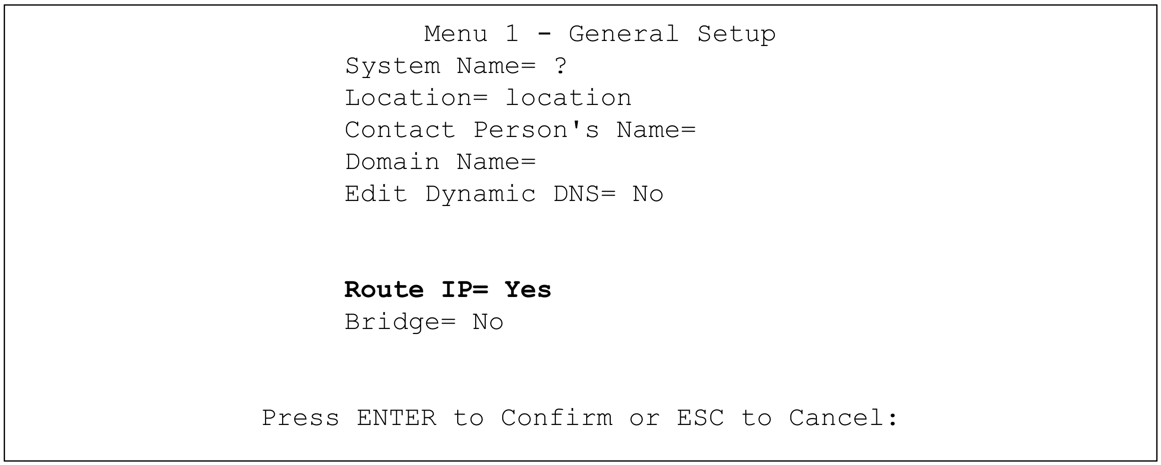
Table 24-1 Menu 3.2.1 IP Alias Setup

FIELD	DESCRIPTION	EXAMPLE
IP Alias	Choose **Yes** to configure the LAN network for the Prestige.	**Yes**
IP Address	Enter the IP address of your Prestige in dotted decimal notation	192.168.2.1
IP Subnet Mask	Your Prestige will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Prestige	255.255.255.0
RIP Direction	Press [SPACE BAR] to select the RIP direction. Choices are **None**, **Both**, **In Only** or **Out Only**.	**None**
Version	Press [SPACE BAR] to select the RIP version. Choices are **RIP-1**, **RIP-2B** or **RIP-2M**.	**RIP-1**
Incoming Protocol Filters	Enter the filter set(s) you wish to apply to the incoming traffic between this node and the Prestige.	
Outgoing Protocol Filters	Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the Prestige.	
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.		

24.5 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].



```
                         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:
```

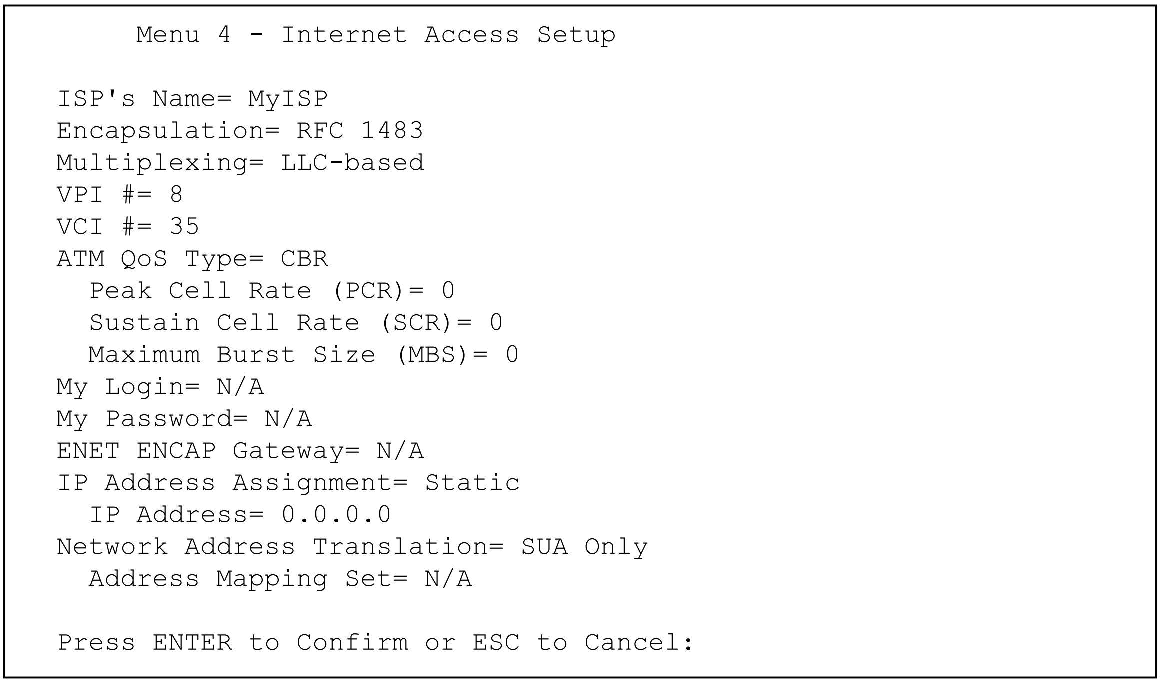
Figure 24-5 Menu 1 General Setup

24.6 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 *Compact Guide* to record your Internet account information. Note that if you are using PPPoA or PPPoE encapsulation, then the only ISP information you need is a login name and password. You only need to know the Ethernet Encapsulation Gateway IP address if you are using ENET ENCAP encapsulation.

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



```
     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:
```

Figure 24-6 Menu 4 Internet Access Setup

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

Table 24-2 Menu 4 Internet Access Setup

FIELD	DESCRIPTION	EXAMPLE
ISP's Name	Enter the name of your Internet Service Provider. This information is for identification purposes only.	MyIsp
Encapsulation	Press [SPACE BAR] to select the method of encapsulation used by your ISP. Choices are **PPPoE**, **PPPoA**, **RFC 1483** or **ENET ENCAP**.	ENET ENCAP
Multiplexing	Press [SPACE BAR] to select the method of multiplexing used by your ISP. Choices are **VC-based** or **LLC-based**.	LLC-based
VPI #	Enter the Virtual Path Identifier (VPI) assigned to you.	8
VCI #	Enter the Virtual Channel Identifier (VCI) assigned to you.	32
ATM QoS Type	Press [SPACE BAR] and select **CBR** (Continuous Bit Rate) to specify fixed (always-on) bandwidth. Select **UBR** (Unspecified Bit Rate) for applications that are non-time sensitive, such as e-mail. Select **VBR** (Variable Bit Rate) for bursty traffic and bandwidth sharing with other applications.	UBR
Peak Cell Rate (PCR)	This is the maximum rate at which the sender can send cells. Type the PCR.	0
Sustain Cell Rate (SCR)= 0	Sustained Cell Rate is the mean cell rate of a bursty, on-off traffic source that can be sent at the peak rate, and a parameter for burst-traffic. Type the SCR; it must be less than the PCR.	0
Maximum Burst Size (MBS)= 0	Refers to the maximum number of cells that can be sent at the peak rate. Type the MBS. The MBS must be less than 65535.	0
My Login	Configure the **My Login** and **My Password** fields for PPPoA and PPPoE encapsulation only. Enter the login name that your ISP gives you. If you are using PPPoE encapsulation**,** then this field must be of the form user@domain where domain identifies your PPPoE service name.	N/A
My Password	Enter the password associated with the login name above.	N/A
ENET ENCAP Gateway	Enter the gateway IP address supplied by your ISP when you are using **ENET ENCAP** encapsulation.	N/A
Idle Timeout	This value specifies the number of idle seconds that elapse before the Prestige automatically disconnects the PPPoE session.	0
IP Address Assignment	Press [SPACE BAR] to select **Static** or **Dynamic** address assignment.	Dynamic
IP Address	Enter the IP address supplied by your ISP if applicable.	N/A
Network Address Translation	Press [SPACE BAR] to select **None**, **SUA Only** or **Full Feature**. Please see the *NAT Chapter* for more details on the SUA (Single User Account) feature.	SUA Only
Address Mapping Set	Type the numbers of mapping sets (1-8) to use with NAT. See the *NAT* chapter for details.	N/A
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

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

Chapter 25 Remote Node Configuration

This chapter covers remote node configuration.

25.1 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.

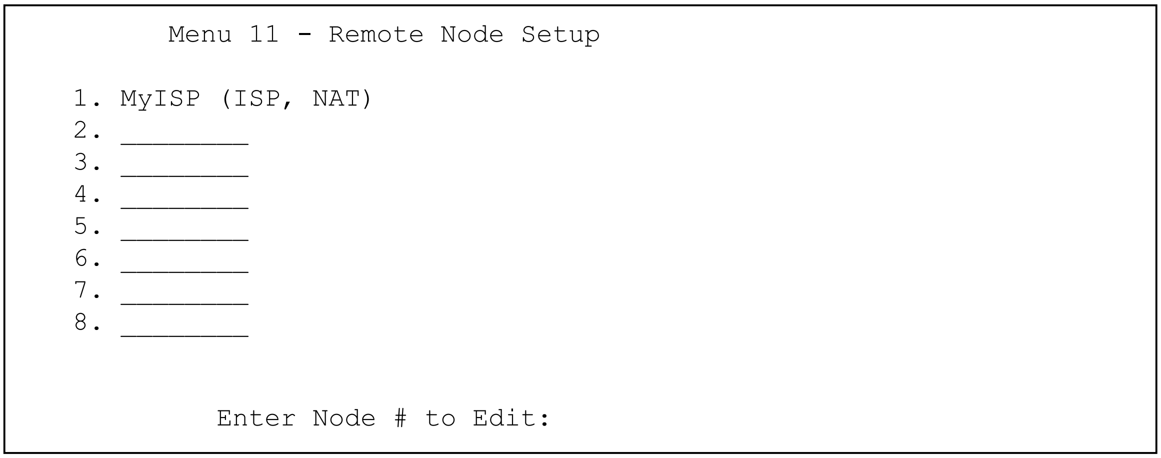
25.2 Remote Node Setup

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

25.2.1 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.



```
        Menu 11 - Remote Node Setup

   1. MyISP (ISP, NAT)
   2. ________
   3. ________
   4. ________
   5. ________
   6. ________
   7. ________
   8. ________


           Enter Node # to Edit:
```

Figure 25-1 Menu 11 Remote Node Setup

25.2.2 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.

Scenario 1. One VC, Multiple Protocols

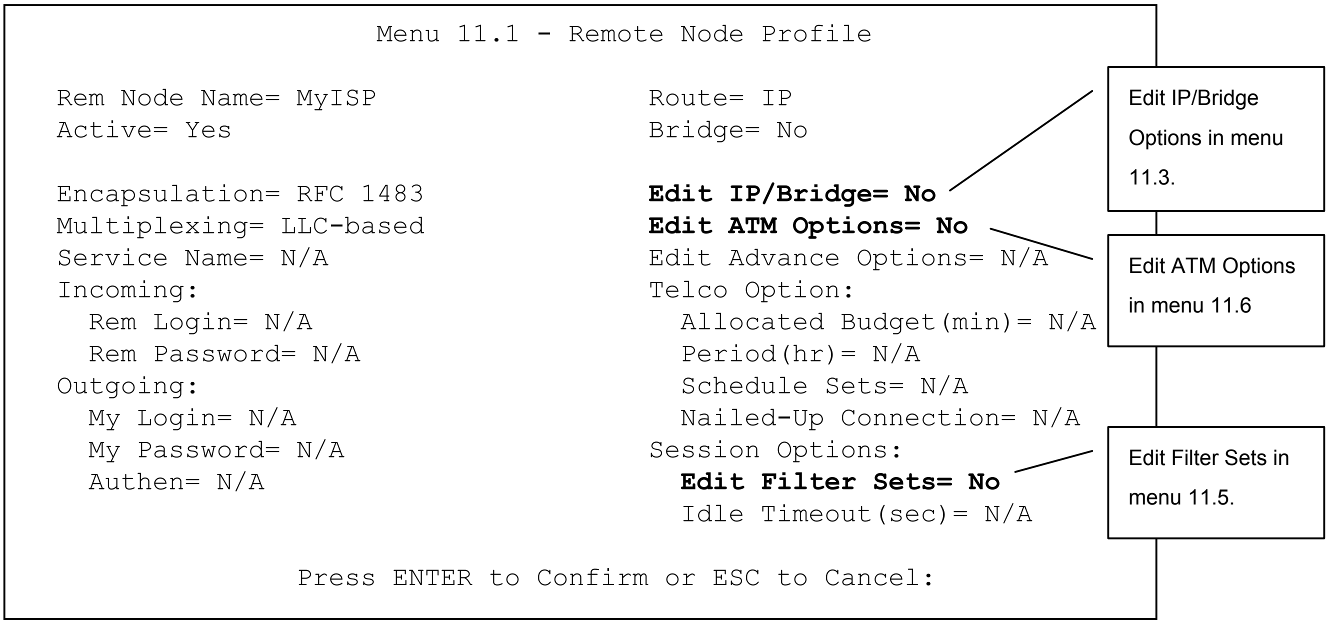
PPPoA (RFC-2364) encapsulation with **VC-based** multiplexing is the best combination because no extra protocol identifying headers are needed. The **PPP** protocol already contains this information.

Scenario 2. One VC, One Protocol (IP)

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

Scenario 3. Multiple VCs

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



```
                    Menu 11.1 - Remote Node Profile

  Rem Node Name= MyISP                    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:
```

Edit IP/Bridge Options in menu 11.3.

Edit ATM Options in menu 11.6

Edit Filter Sets in menu 11.5.

Figure 25-2 Menu 11.1 Remote Node Profile

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

Table 25-1 Menu 11.1 Remote Node Profile

FIELD	DESCRIPTION	EXAMPLE
Rem Node Name	Type a unique, descriptive name of up to eight characters for this node.	MyIsp
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** to activate or **No** to deactivate this node. Inactive nodes are displayed with a minus sign “–“ in SMT menu 11.	**Yes**
Encapsulation	**PPPoA** refers to RFC-2364 (PPP Encapsulation over ATM Adaptation Layer 5). 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**).	**ENET ENCAP**
Multiplexing	Press [SPACE BAR] and then [ENTER] to select the method of multiplexing that your ISP uses, either **VC-based** or **LLC-based**.	**LLC-based**
Service Name	When using **PPPoE** encapsulation, type the name of your PPPoE service here.	N/A
Incoming:		
Rem Login	Type the login name that this remote node will use to call your Prestige. The login name and the **Rem Password** will be used to authenticate this node.	
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.	

Table 25-1 Menu 11.1 Remote Node Profile

FIELD	DESCRIPTION	EXAMPLE
My Password	Type the password assigned by your ISP when the Prestige calls this remote node.	
Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are: **CHAP**/**PAP** – Your Prestige will accept either **CHAP** or **PAP** when requested by this remote node. **CHAP** – accept **CHAP** (Challenge Handshake Authentication Protocol) only. **PAP** – accept PAP (Password Authentication Protocol) only.	
Route	This field determines the protocol used in routing. Options are **IP** and **None.**	**IP**
Bridge	When bridging is enabled, your Prestige will forward any packet that it does not route to this remote node; otherwise, the packets are discarded. Select **Yes** to enable and **No** to disable.	**No**
Edit IP/Bridge	Press [SPACE BAR] to select **Yes** and press [ENTER] to display **Menu 11.3 – Remote Node Network Layer Options**.	**No**
Edit ATM Options	Press [SPACE BAR] to select **Yes** and press [ENTER] to display **Menu 11.6 – Remote Node ATM Layer Options**.	**No**
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**.	**No**
Telco Option		
Allocated Budget (min)	This sets a ceiling for outgoing call time for this remote node. The default for this field is 0 meaning no budget control.	
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 the *Call Schedule Setup* chapter.	
Nailed up Connection	This field is only applicable for **PPPoE** and **PPPoA** encapsulation. This field specifies if you want to make the connection to this remote node a nailed-up connection. More details are given earlier in this section.	
Session Options		
Edit Filter Sets	Use [SPACE BAR] to choose **Yes** and press [ENTER] to open menu 11.5 to edit the filter sets. See the *Remote Node Filter* section for more details.	**No** (default)
Idle Timeout (sec)	Type the number of seconds (0-9999) that can elapse when the Prestige is idle (there is no traffic going to the remote node), before the Prestige automatically disconnects the remote node. 0 means that the session will not timeout.	
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.		

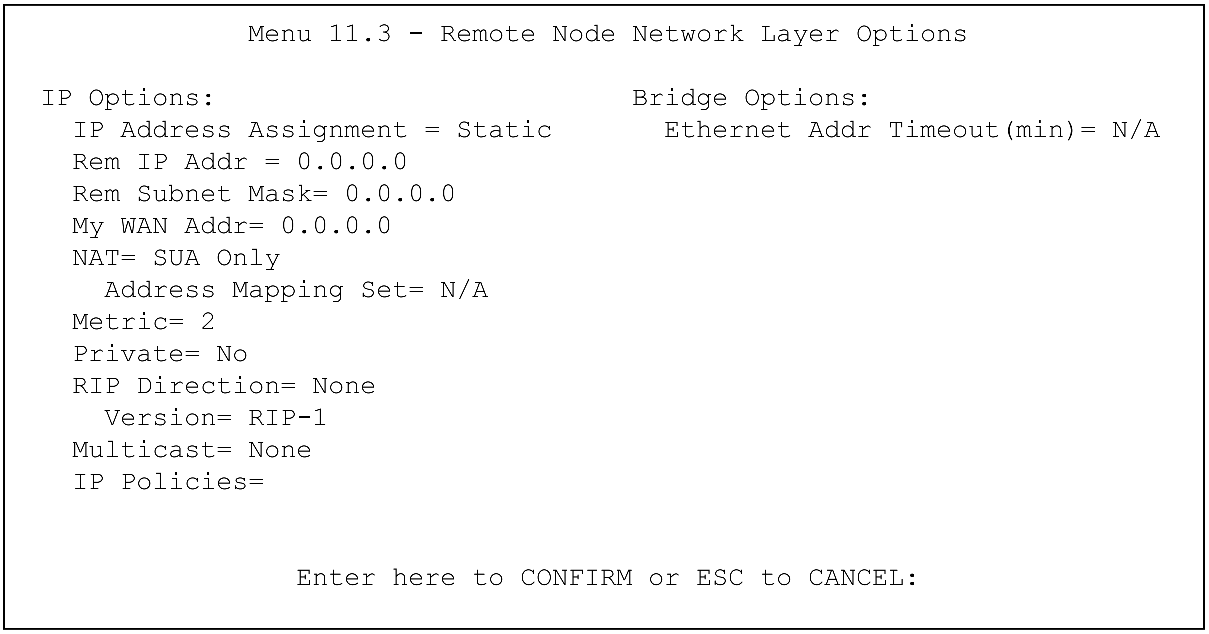
25.2.3 Outgoing Authentication Protocol

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.

25.3 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.**



```
               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:
```

Figure 25-3 Menu 11.3 Remote Node Network Layer Options

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

Table 25-2 Menu 11.3 Remote Node Network Layer Options

FIELD	DESCRIPTION	EXAMPLE
IP Address Assignment	Press [SPACE BAR] and then [ENTER] to select **Dynamic** if the remote node is using a dynamically assigned IP address or **Static** if it is using a static (fixed) IP address. You will only be able to configure this in the ISP node (also the one you configure in menu 4), all other nodes are set to **Static**.	**Dynamic**
Rem IP Addr	This is the IP address you entered in the previous menu.	

Table 25-2 Menu 11.3 Remote Node Network Layer Options

FIELD	DESCRIPTION	EXAMPLE
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 section *28.3.1*). Select **None** to disable NAT.	**SUA Only**
Address Mapping Set	When **Full Feature** is selected in the **NAT** field, configure address mapping sets in menu 15.1. Select one of the NAT server sets (2-10) in menu 15.2 (see the *NAT* chapter for details) and type that number here. When **SUA Only** is selected in the NAT field, the SMT uses NAT server set 1 in menu 15.2 (see the *NAT* chapter for details).	2
Metric	The metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the cost measurement, with a minimum of 1 for directly connected networks. Type a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.	2
Private	This determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and not included in RIP broadcast. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.	**No**
RIP Direction	Press [SPACE BAR] and then [ENTER] to select the RIP Direction. Options are **Both**, **In Only**, **Out Only** or **None**.	**None**
Version	Press [SPACE BAR] and then [ENTER] to select the RIP version. Options are **RIP-1**, **RIP-2B** or **RIP-2M**.	**RIP-1**
Multicast	**IGMP-v1** sets IGMP to version 1, **IGMP-v2** sets IGMP to version 2 and **None** disables IGMP.	**None**
IP Policies	You can apply up to four IP Policy sets (from 12) by typing in their numbers separated by commas. Configure the filter sets in menu 25 first (see the *IP Policy Routing* chapter) and then apply them here.	3, 4, 5, 6
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

25.3.1 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 *LAN and WAN IP Addresses* figure in the web configurator chapter on LAN setup for a brief review of what a WAN IP is. **My WAN Addr** indicates the local Prestige WAN IP (172.16.0.1 in the following figure) while **Rem IP Addr** indicates the peer WAN IP (172.16.0.2 in the following figure).

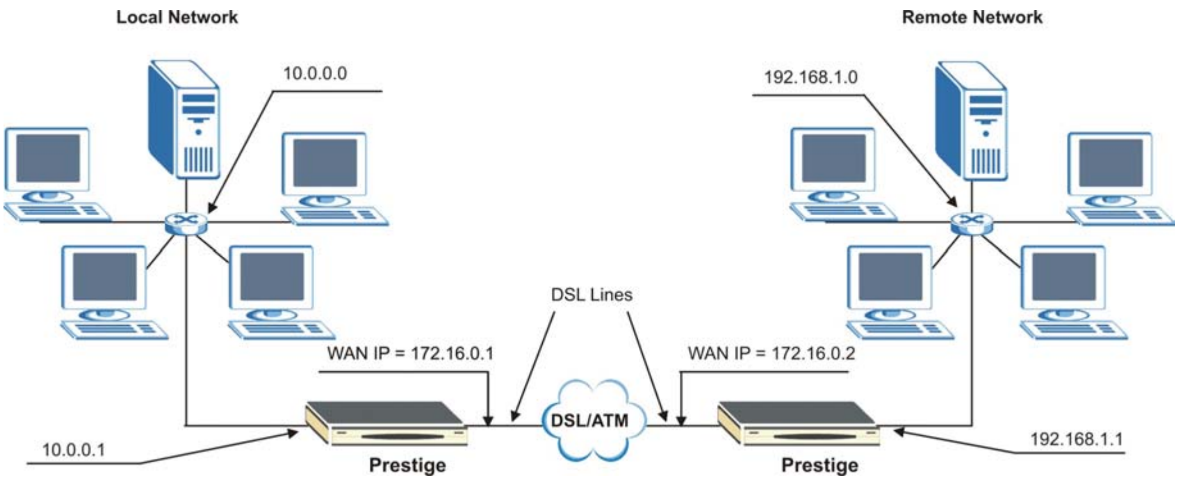


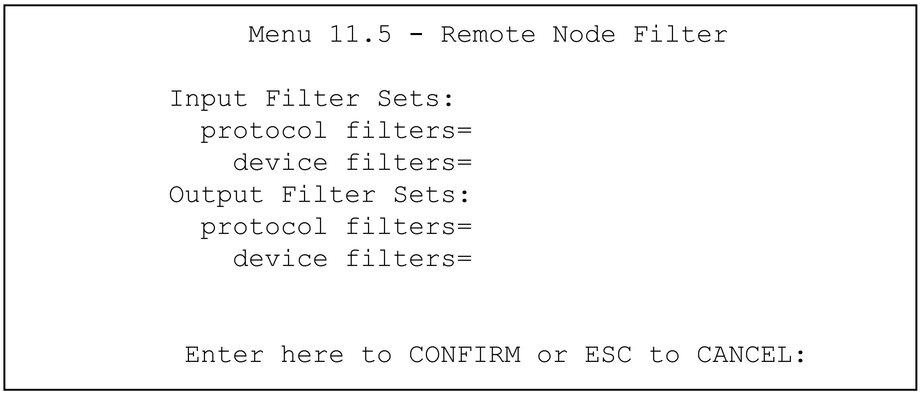
Figure 25-4 Sample IP Addresses for a TCP/IP LAN-to-LAN Connection

25.4 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**.

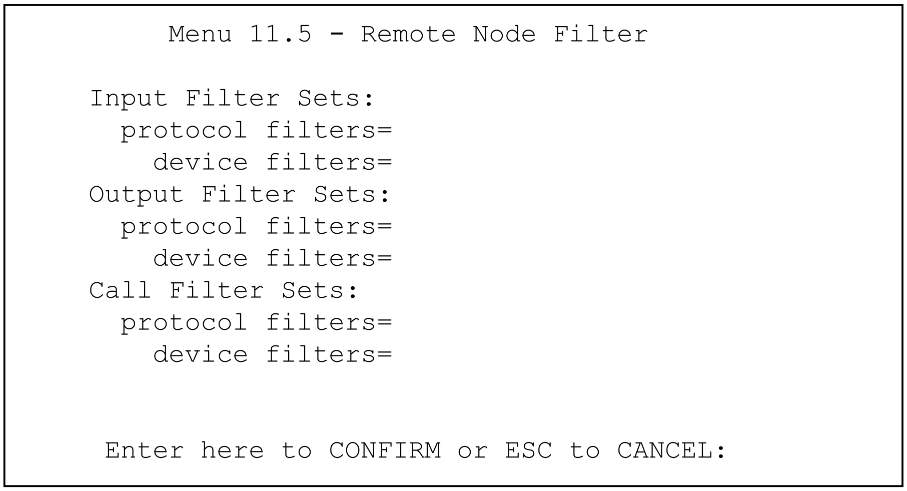
Use **Menu 11.5 – Remote Node Filter** to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the Prestige and also to prevent certain packets from triggering calls. You can specify up to 4 filter sets separated by comma, for example, 1, 5, 9, 12, in each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



```
                 Menu 11.5 - Remote Node Filter

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


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

Figure 25-5 Menu 11.5 Remote Node Filter (RFC 1483 or ENET Encapsulation)



```
          Menu 11.5 - Remote Node Filter

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


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

Figure 25-6 Menu 11.5 Remote Node Filter (PPPoA or PPPoE Encapsulation)

25.5 Editing ATM Layer Options

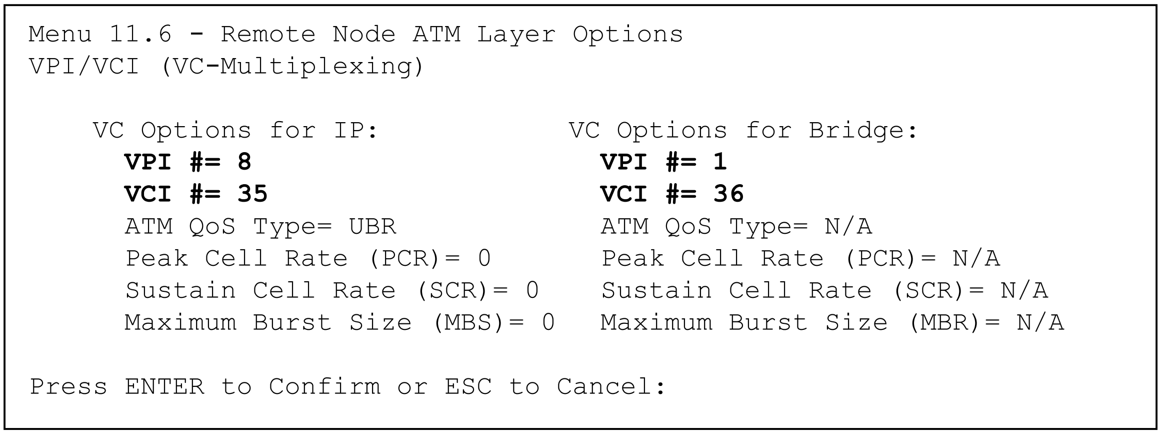
Follow the steps shown next to edit **Menu 11.6 – Remote Node ATM Layer Options**.

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.

25.5.1 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.

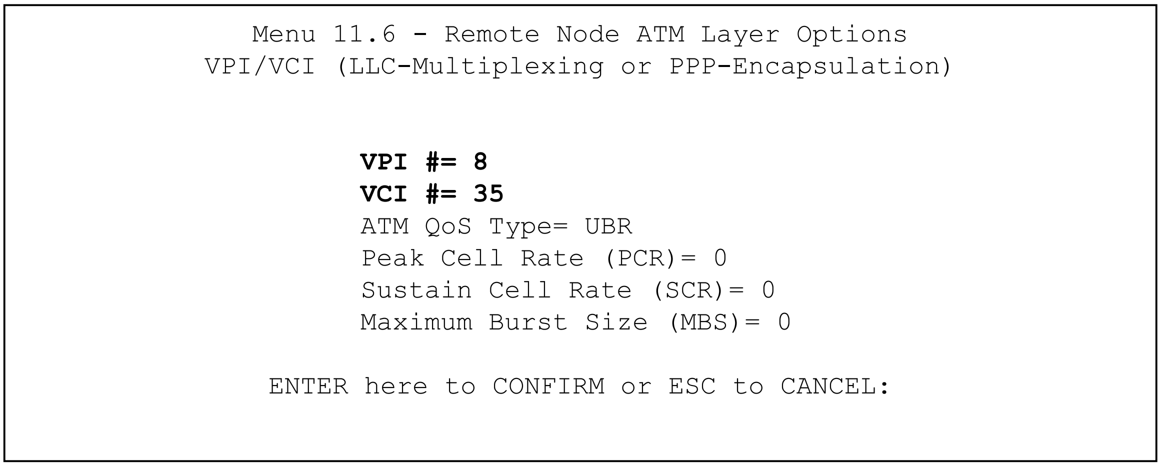


```
Menu 11.6 - Remote Node ATM Layer Options
VPI/VCI (VC-Multiplexing)

    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:
```

Figure 25-7 Menu 11.6 for VC-based Multiplexing

25.5.2 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.



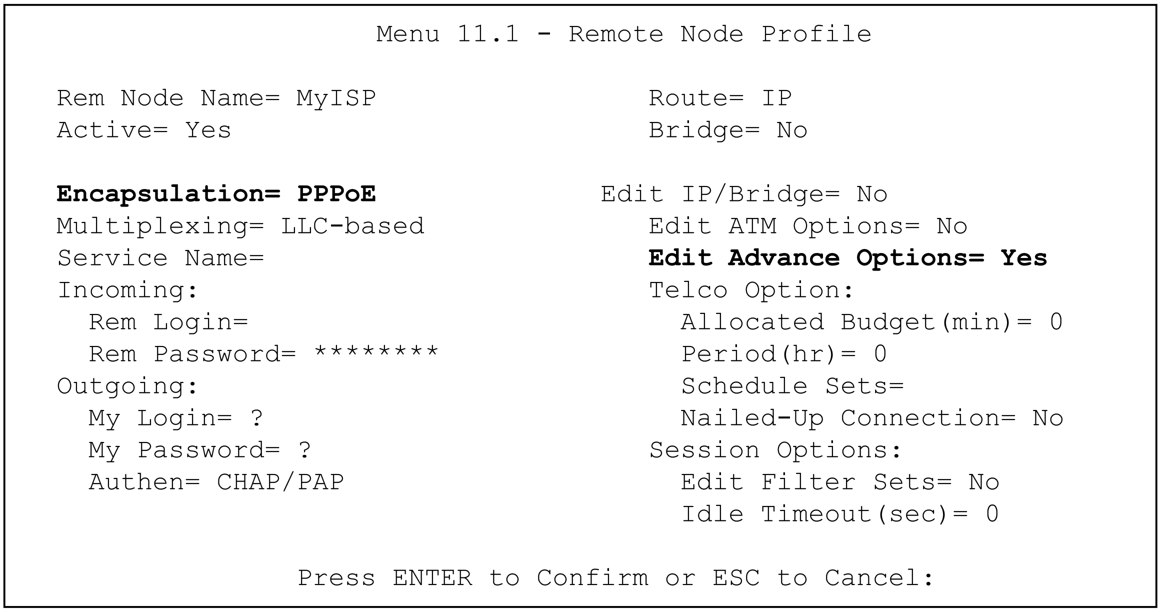
```
               Menu 11.6 - Remote Node ATM Layer Options
            VPI/VCI (LLC-Multiplexing or PPP-Encapsulation)


                      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:
```

Figure 25-8 Menu 11.6 for LLC-based Multiplexing or PPP Encapsulation

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

25.5.3 Advance Setup Options

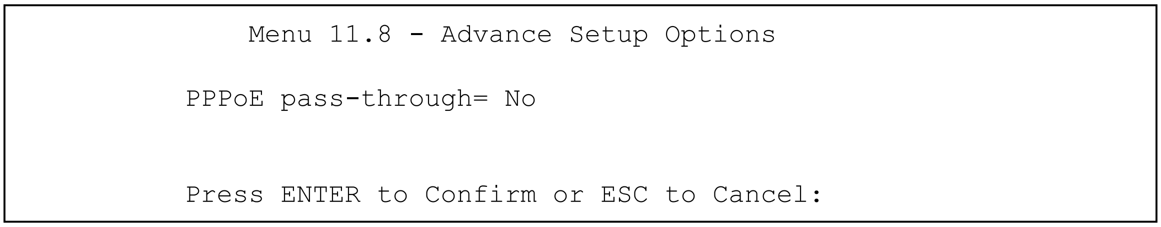
In menu 11.1, select **PPPoE** in the **Encapsulation** field.



```
                       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:
```

Figure 25-9 Menu 11.1 Remote Node Profile

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**.



```
                Menu 11.8 - Advance Setup Options

            PPPoE pass-through= No


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

Figure 25-10 Menu 11.8 Advance Setup Options

The following table describes the fields in this menu.

Table 25-3 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] to cancel and go back to the previous screen.	

Chapter 26
Static Route Setup

This chapter shows how to setup IP static routes.

26.1 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.

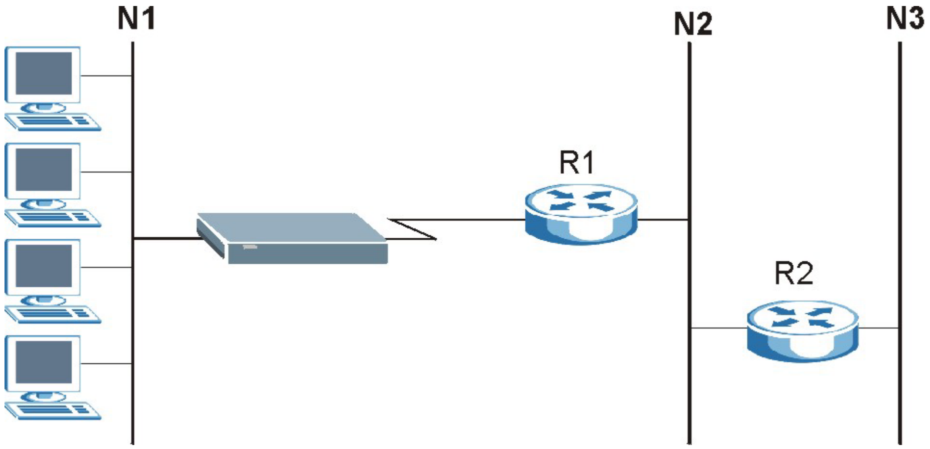
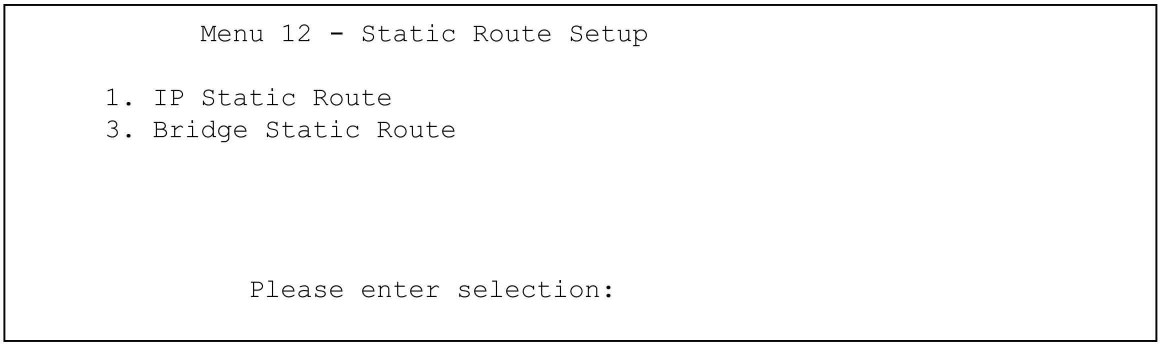


Figure 26-1 Sample Static Routing Topology

26.2 Configuration

Follow the steps below to configure a static route.

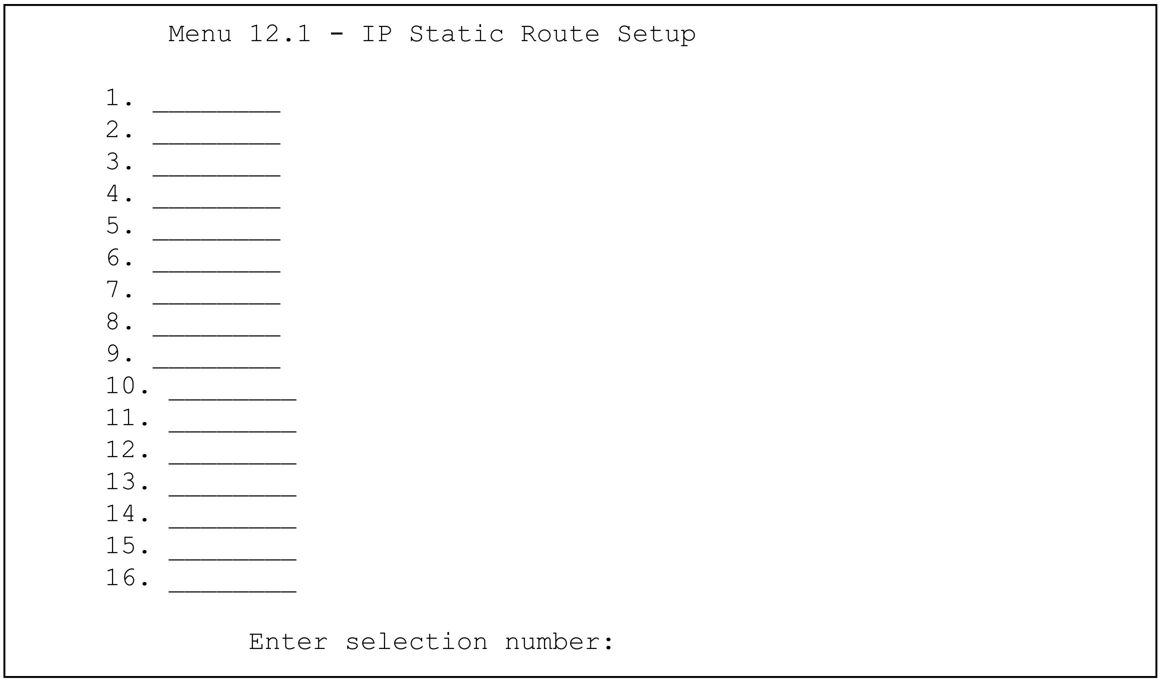
1. To configure an IP static route, use **Menu 12 – Static Route Setup** (shown next).



```
            Menu 12 - Static Route Setup

      1. IP Static Route
      3. Bridge Static Route




               Please enter selection:
```

Figure 26-2 Menu 12 Static Route Setup

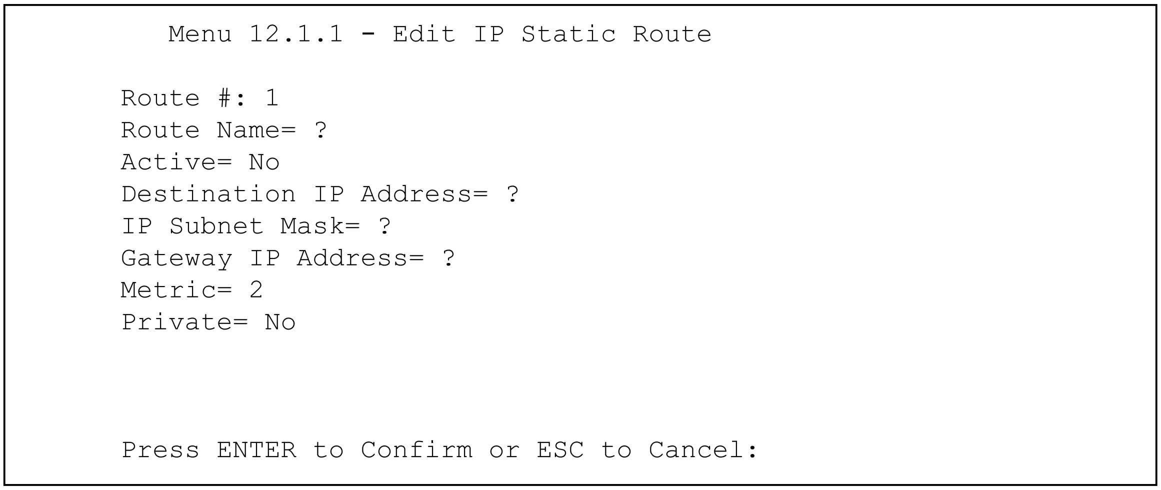
2. From menu 12, select 1 to open **Menu 12.1 — IP Static Route Setup** (shown next).



```
          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:
```

Figure 26-3 Menu 12.1 IP Static Route Setup

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



```
          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:
```

Figure 26-4 Menu12.1.1 Edit IP Static Route

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

Table 26-1 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. Follow the discussion on *IP Subnet Mask* in this manual.
Gateway IP Address	Type the IP address of the gateway. The gateway is an immediate neighbor of your Prestige that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your Prestige; over WAN, the gateway must be the IP address of one of the remote nodes.
Metric	Metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Type a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Private	This parameter determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and is not included in RIP broadcasts. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

Chapter 27
Bridging Setup

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

27.1 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.

27.2 Bridge Ethernet Setup

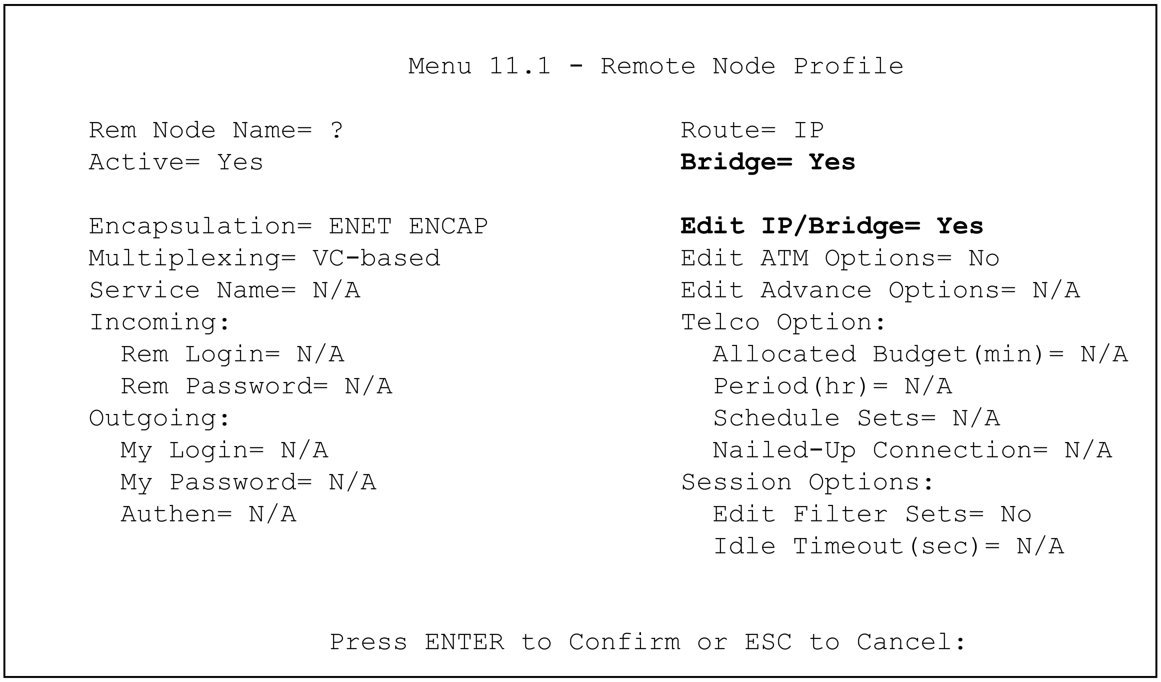
Basically, all non-local packets are bridged to the WAN. Your Prestige does not support IPX.

27.2.1 Remote Node Bridging Setup

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

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

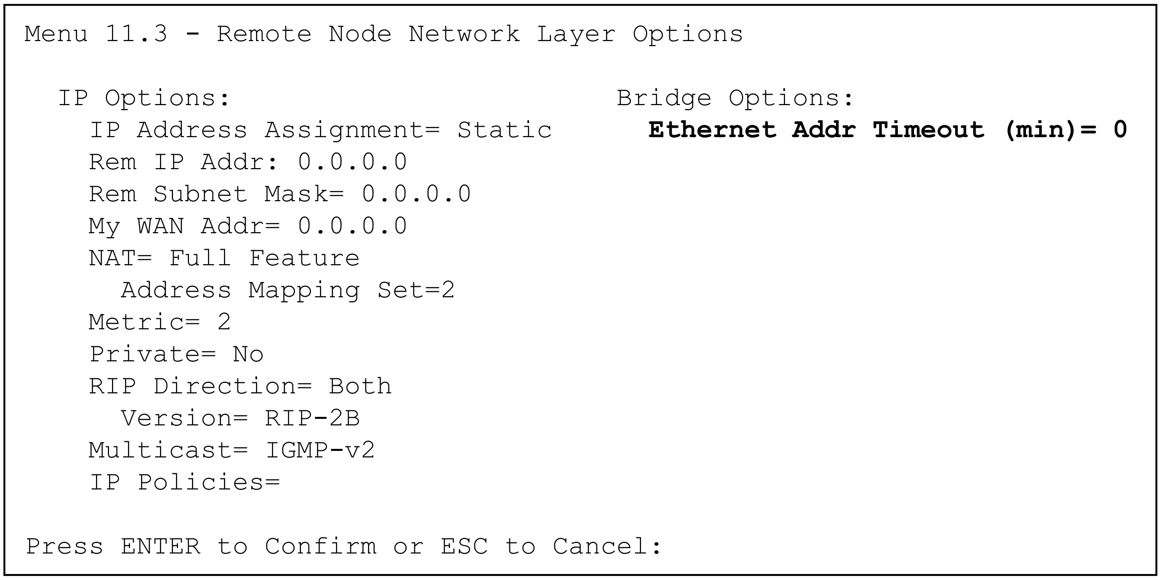
1. In menu 11.1, make sure the **Bridge** field is set to **Yes**.



```
                    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:
```

Figure 27-1 Menu 11.1 Remote Node Profile

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



```
Menu 11.3 - Remote Node Network Layer Options

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

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

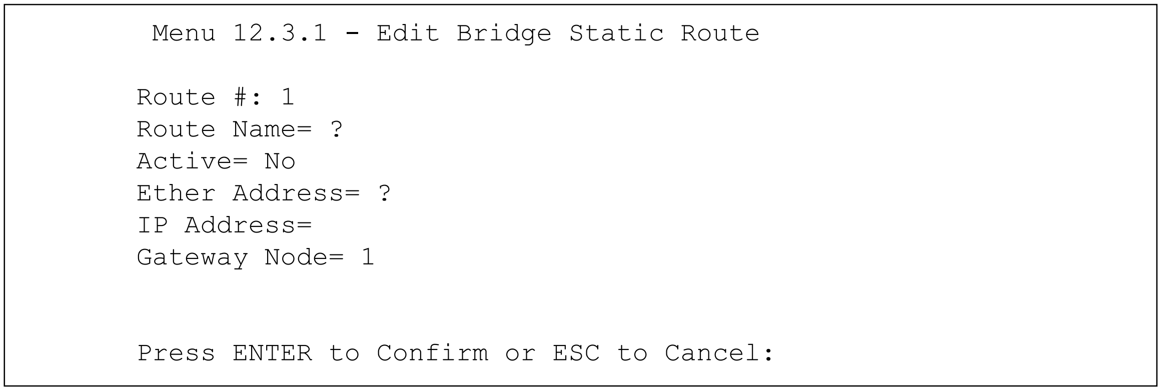
Figure 27-2 Menu 11.3 Remote Node Network Layer Options

Table 27-1 Remote Node Network Layer Options: Bridge Fields

FIELD	DESCRIPTION
Bridge (menu 11.1)	Make sure this field is set to **Yes**.
Edit IP/Bridge (menu 11.1)	Press [SPACE BAR] to select **Yes** and press [ENTER] to display menu 11.3.
Ethernet Addr Timeout (min.) (menu 11.3)	Type the time (in minutes) for the Prestige to retain the Ethernet Address information in its internal tables while the line is down. If this information is retained, your Prestige will not have to recompile the tables when the line comes back up.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

27.2.2 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.



```
         Menu 12.3.1 - Edit Bridge Static Route

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


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

Figure 27-3 Menu 12.3.1 Edit Bridge Static Route

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

Table 27-2 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] to cancel and go back to the previous screen.	

Chapter 28 Network Address Translation (NAT)

This chapter discusses how to configure NAT on the Prestige.

28.1 Using NAT

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

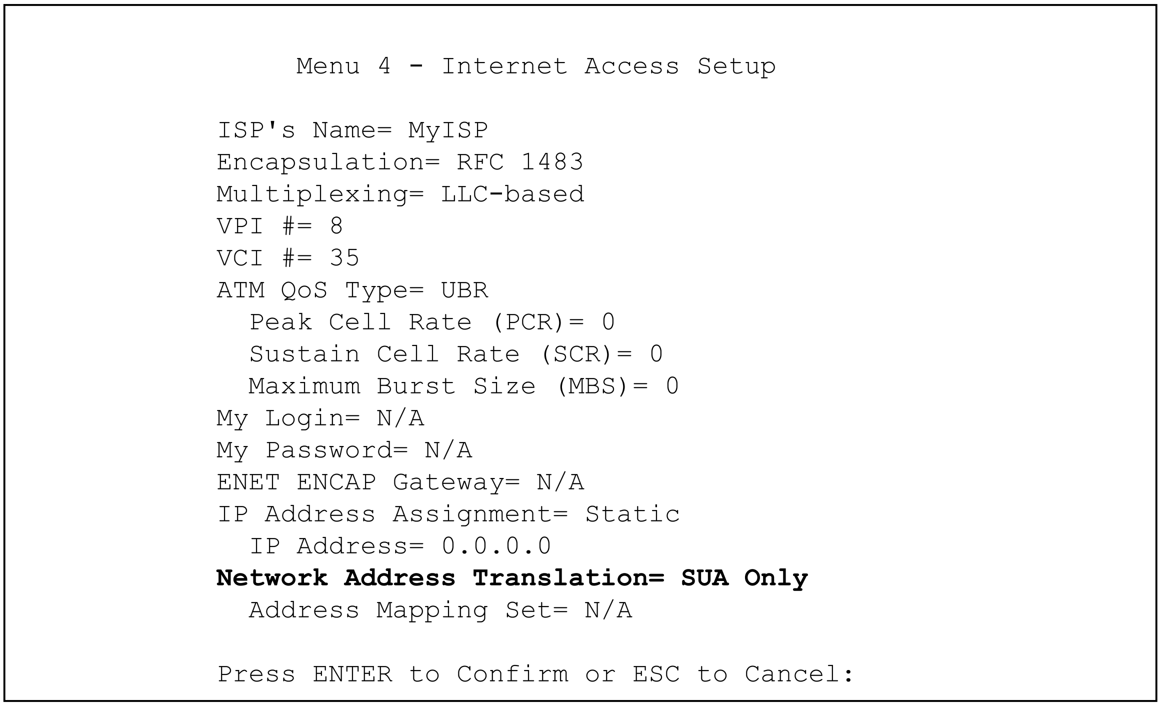
28.1.1 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. See *section 28.3.1* for a detailed description of the NAT set for SUA. The Prestige also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types.

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

28.2 Applying NAT

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

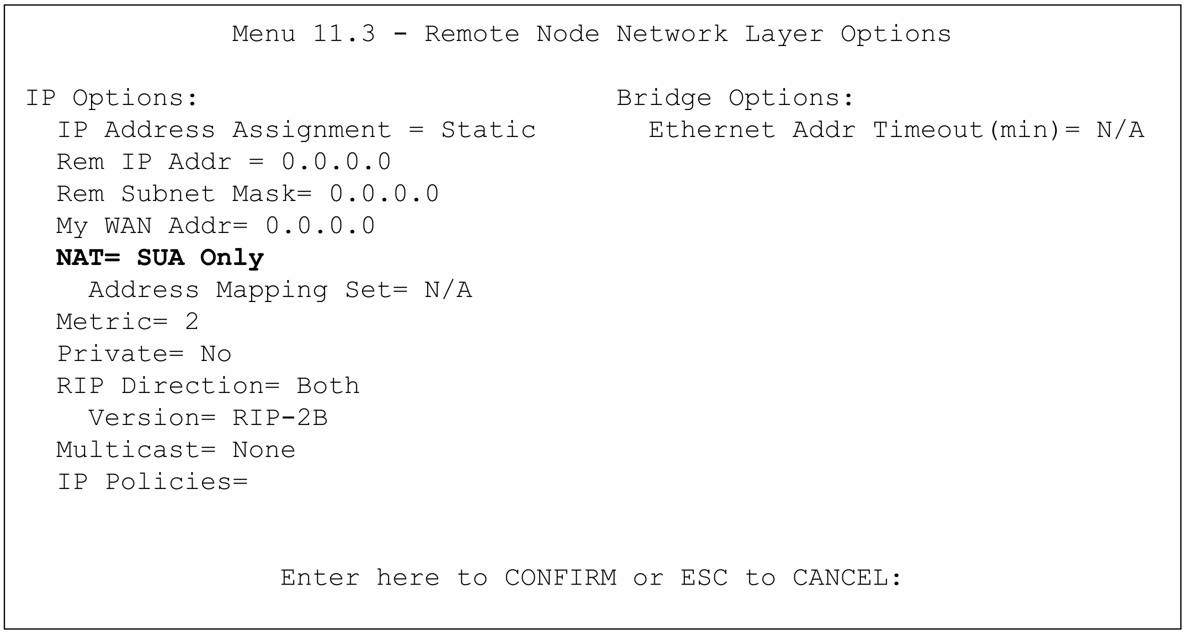


```
     Menu 4 - Internet Access Setup

ISP's Name= MyISP
Encapsulation= 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:
```

Figure 28-1 Applying NAT in Menus 4

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.**



```
              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:
```

Figure 28-2 Applying NAT in Menus 11.3

The following table describes the options for Network Address Translation.

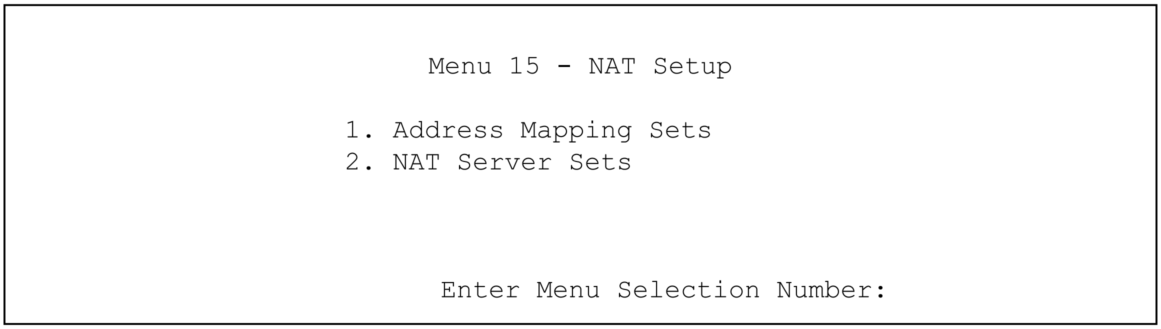
Table 28-1 Applying NAT in Menus 4 and 11.3

FIELD	DESCRIPTION	EXAMPLE
NAT	Press [SPACE BAR] and then [ENTER] to select **Full Feature** if you have multiple public WAN IP addresses for your Prestige. The SMT uses the address mapping set that you configure and enter in the **Address Mapping Set** field (menu 15.1 - see section *28.3.1*).	**Full Feature**
	Select **None** to disable NAT.	**None**
	When you select **SUA Only**, the SMT uses Address Mapping Set 255 (menu 15.1 - see section *28.3.1*). Choose **SUA Only** if you have just one public WAN IP address for your Prestige.	**SUA Only**

28.3 NAT Setup

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

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

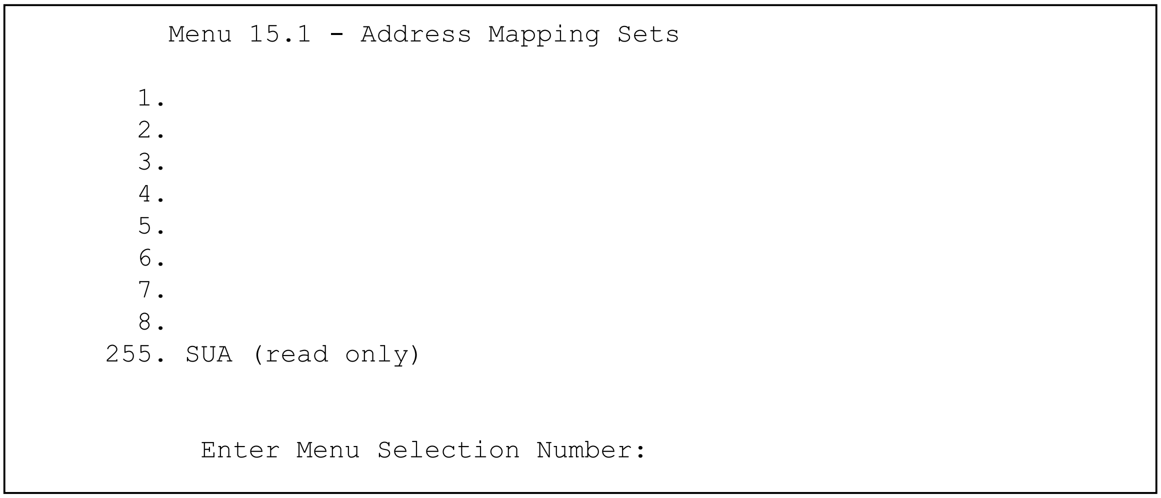


```
                         Menu 15 - NAT Setup

                    1. Address Mapping Sets
                    2. NAT Server Sets



                          Enter Menu Selection Number:
```

Figure 28-3 Menu 15 NAT Setup

28.3.1 Address Mapping Sets

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

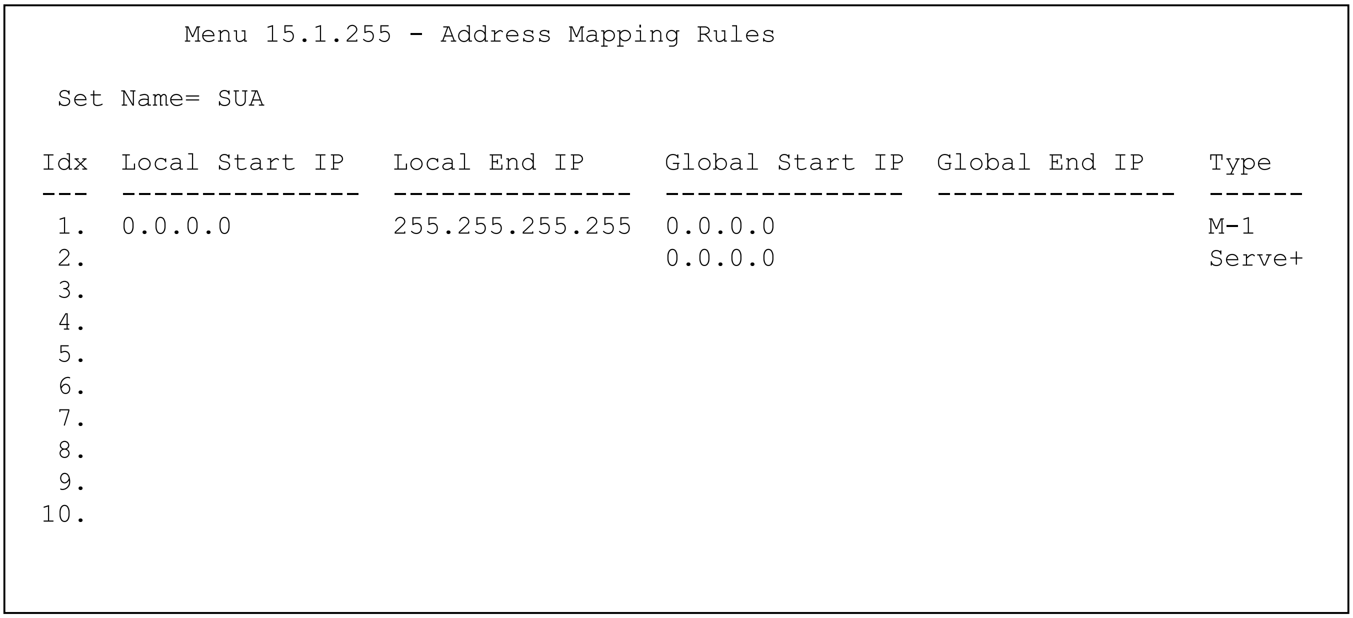


```
          Menu 15.1 - Address Mapping Sets

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


            Enter Menu Selection Number:
```

Figure 28-4 Menu 15.1 Address Mapping Sets

SUA Address Mapping Set

Enter 255 to display the next screen (see also *section 28.1.1)*. The fields in this menu cannot be changed.



```
        Menu 15.1.255 - Address Mapping Rules

  Set Name= SUA

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

Figure 28-5 Menu 15.1.255 SUA Address Mapping Rules

The following table explains the fields in this menu.

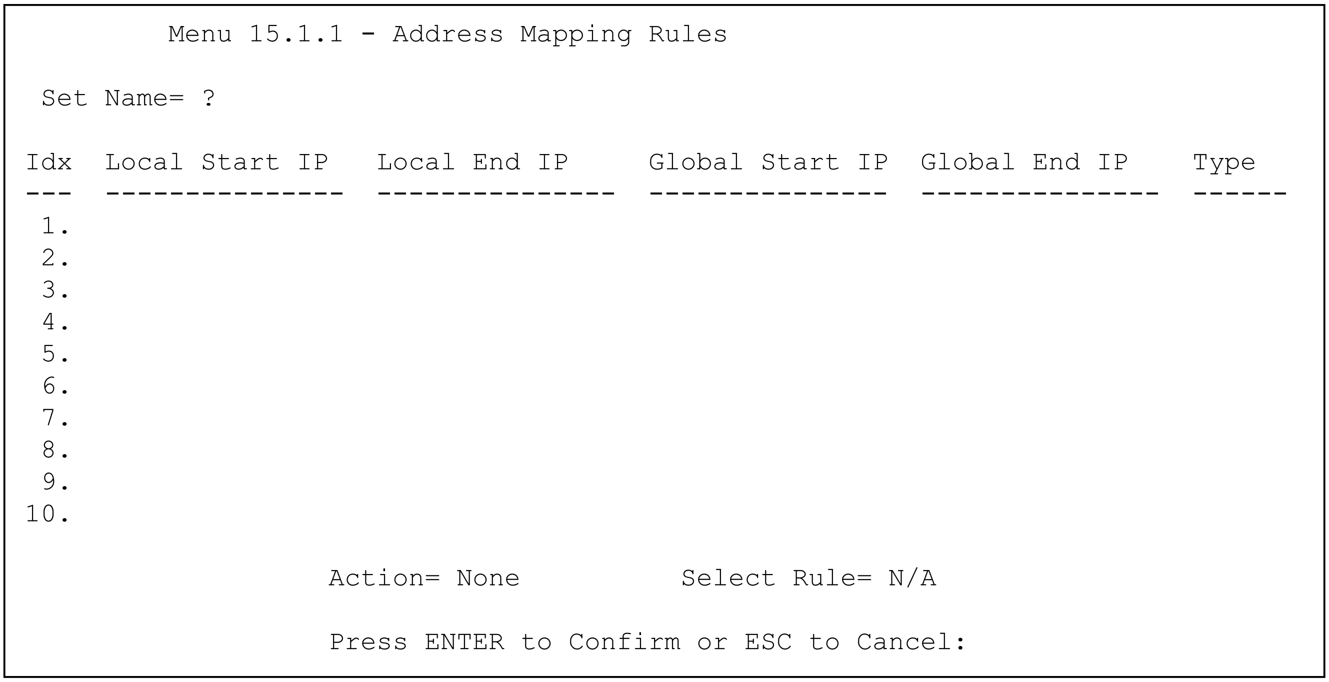
Menu 15.1.255 is read-only.

Table 28-2 SUA Address Mapping Rules

FIELD	DESCRIPTION	EXAMPLE
Set Name	This is the name of the set you selected in menu 15.1 or enter the name of a new set you want to create.	SUA
Idx	This is the index or rule number.	1
Local Start IP	**Local Start IP** is the starting local IP address (ILA).	0.0.0.0
Local End IP	**Local End IP** is the ending local IP address (ILA). If the rule is for all local IPs, then the Start IP is 0.0.0.0 and the End IP is 255.255.255.255.	255.255.255.255
Global Start IP	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global Start IP**.	0.0.0.0
Global End IP	This is the ending global IP address (IGA).	
Type	These are the mapping types. **Server** allows us to specify multiple servers of different types behind NAT to this machine. See later for some examples.	Server
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

User-Defined Address Mapping Sets

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



```
        Menu 15.1.1 - Address Mapping Rules

 Set Name= ?

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

                  Action= None          Select Rule= N/A

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

Figure 28-6 Menu 15.1.1 First Set

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

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

Ordering Your Rules

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

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

Table 28-3 Menu 15.1.1 First Set

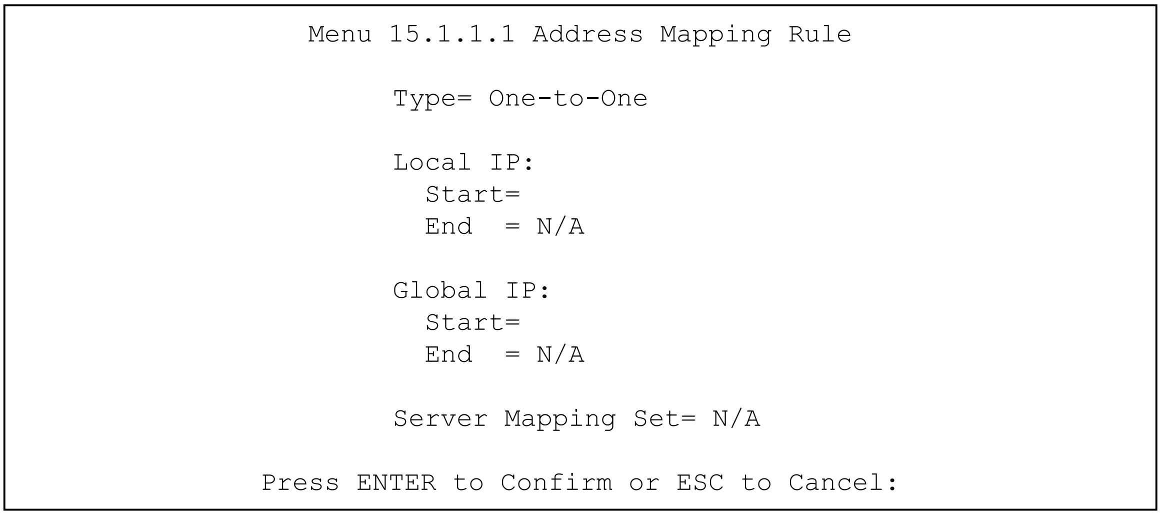
FIELD	DESRIPTION	EXAMPLE
Set Name	Enter a name for this set of rules. This is a required field. If this field is left blank, the entire set will be deleted.	NAT_SET

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

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

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

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



```
                    Menu 15.1.1.1 Address Mapping Rule

                          Type= One-to-One

                          Local IP:
                            Start=
                            End  = N/A

                          Global IP:
                            Start=
                            End  = N/A

                          Server Mapping Set= N/A

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

Figure 28-7 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set

The following table explains the fields in this menu.

Table 28-4 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set

FIELD	DESCRIPTION	EXAMPLE
Type	Press [SPACE BAR] and then [ENTER] to select from a total of five types. These are the mapping types discussed in the chapter on NAT web configurator screens. **Server** allows you to specify multiple servers of different types behind NAT to this computer. See *section 28.5.3* for an example.	**One-to-One**
Local IP	Only local IP fields are **N/A** for server; Global IP fields MUST be set for **Server**.	
Start	This is the starting local IP address (ILA).	0.0.0.0
End	This is the ending local IP address (ILA). If the rule is for all local IPs, then put the Start IP as 0.0.0.0 and the End IP as 255.255.255.255. This field is **N/A** for One-to-One and Server types.	N/A

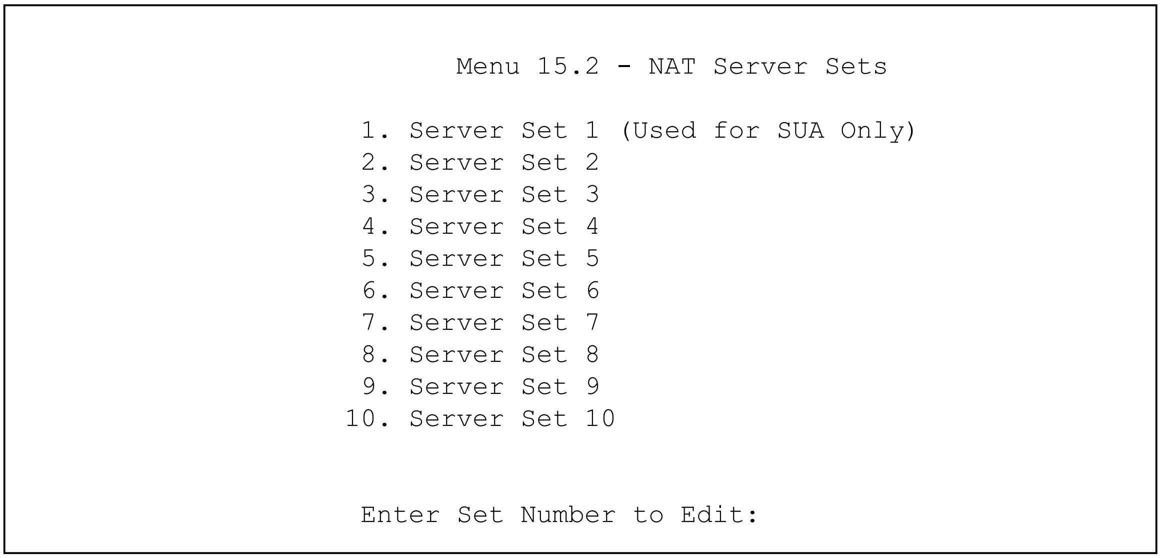
Table 28-4 Menu 15.1.1.1 Editing/Configuring an Individual Rule in a Set

FIELD	DESCRIPTION	EXAMPLE
Global IP		
Start	This is the starting inside global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global IP Start**. Note that **Global IP Start** can be set to 0.0.0.0 only if the types are **Many-to-One** or **Server**.	0.0.0.0
End	This is the ending inside global IP address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server types**.	N/A
Server Mapping Set	Only available when **Type** is set to **Server**. Type a number from 1 to 10 to choose a server set from menu 15.2.	
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to confirm or ESC to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.		

28.4 Configuring a Server behind NAT

Follow these steps to configure a server behind NAT:

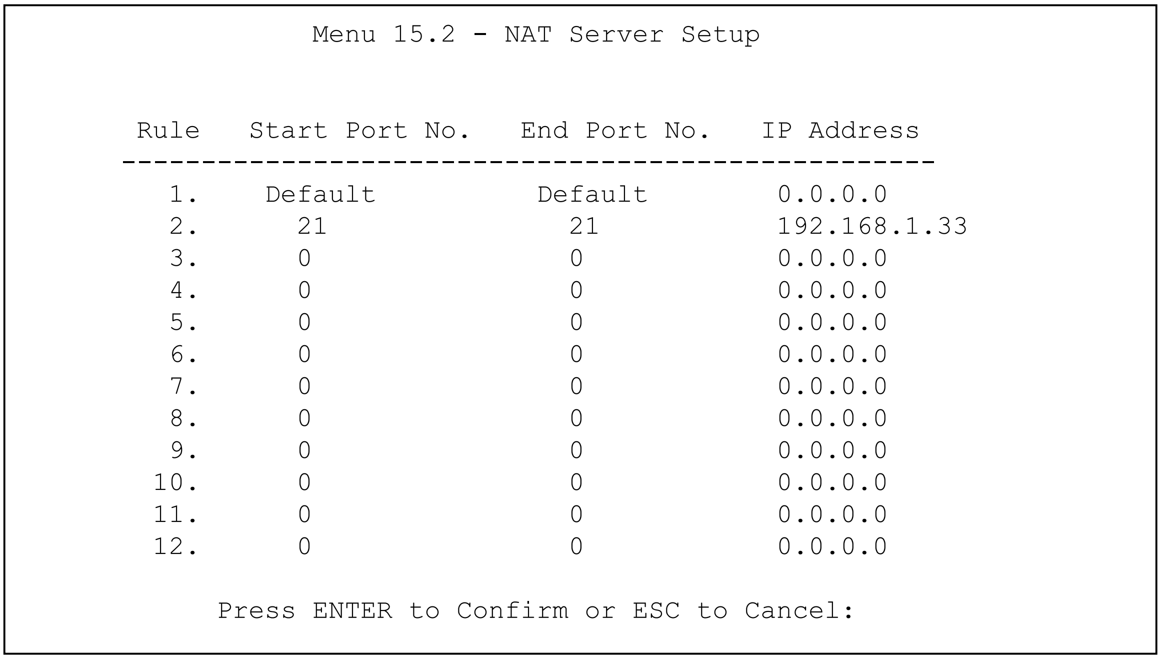
1. Enter 15 in the main menu to go to **Menu 15 - NAT Setup**.
2. Enter 2 to display **Menu 15.2 - NAT Server Sets** as shown next.



```
                        Menu 15.2 - NAT Server Sets

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


                  Enter Set Number to Edit:
```

Figure 28-8 Menu 15.2 NAT Server Setup

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



```
                   Menu 15.2 - NAT Server Setup


          Rule   Start Port No.   End Port No.   IP Address
         ---------------------------------------------------
            1.     Default          Default        0.0.0.0
            2.       21               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:
```

Figure 28-9 Menu 15.2.1 NAT Server Setup

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.

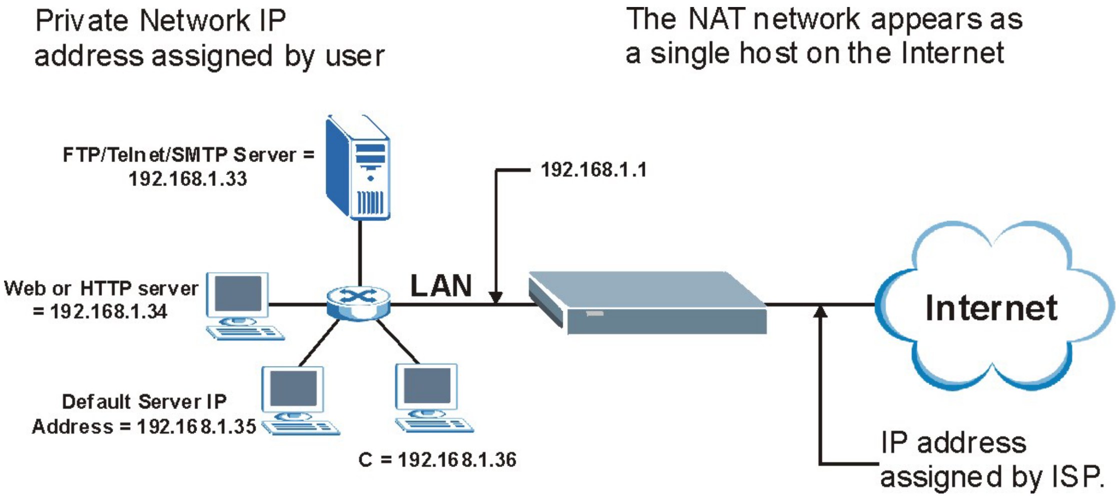

Private Network IP address assigned by user
The NAT network appears as a single host on the Internet
FTP/Telnet/SMTP Server = 192.168.1.33
192.168.1.1
Web or HTTP server = 192.168.1.34
LAN
Internet
Default Server IP Address = 192.168.1.35
C = 192.168.1.36
IP address assigned by ISP.

Figure 28-10 Multiple Servers Behind NAT Example

28.5 General NAT Examples

The following are some examples of NAT configuration.

28.5.1 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.

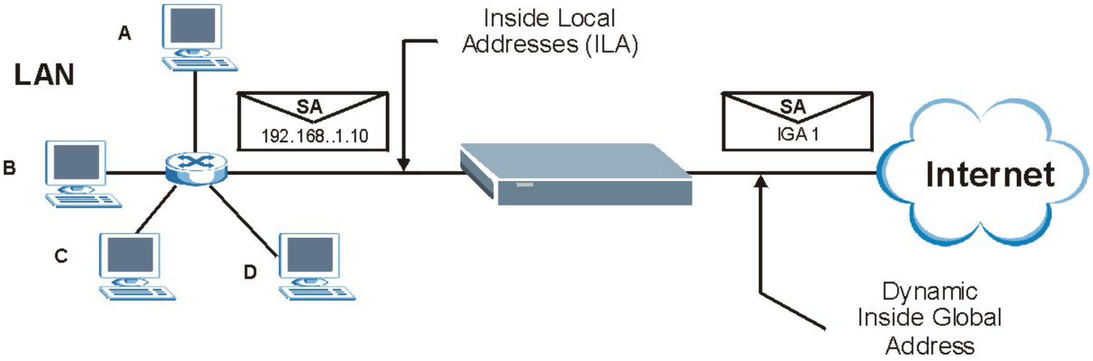
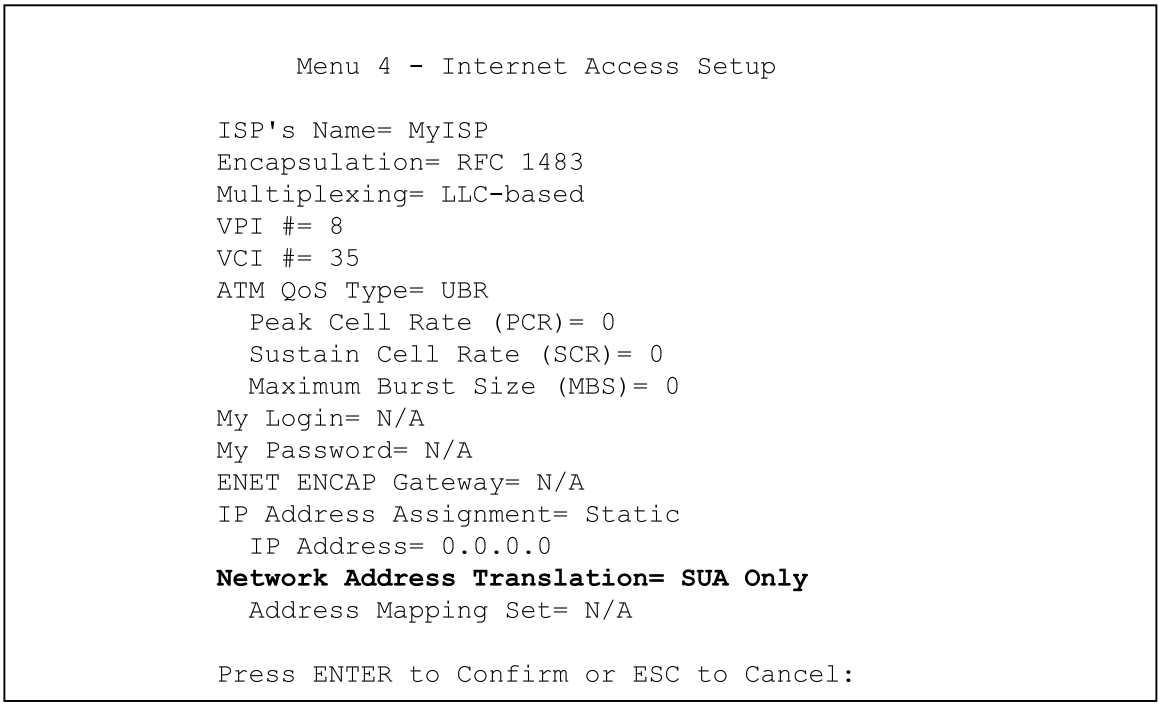


Figure 28-11 NAT Example 1



```
              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:
```

Figure 28-12 Menu 4 Internet Access & NAT Example

From menu 4, choose the **SUA Only** option from the **Network Address Translation** field. This is the Many-to-One mapping discussed in *section 28.5*. The **SUA Only** read-only option from the **Network Address Translation** field in menus 4 and 11.3 is specifically pre-configured to handle this case.

28.5.2 Example 2: Internet Access with an Inside Server

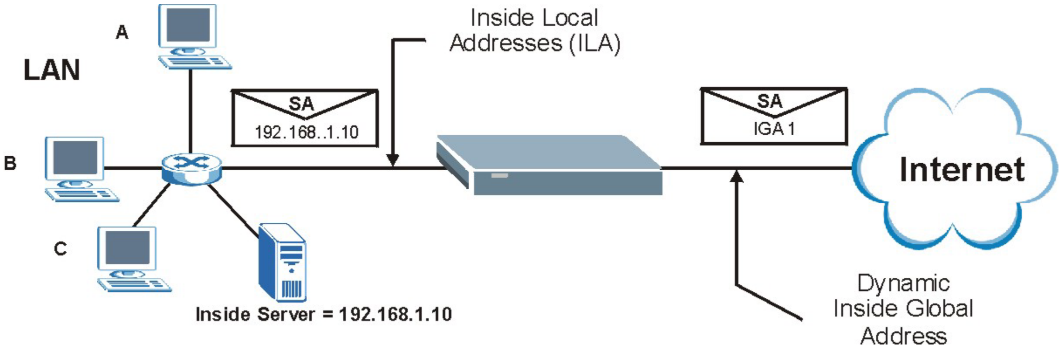
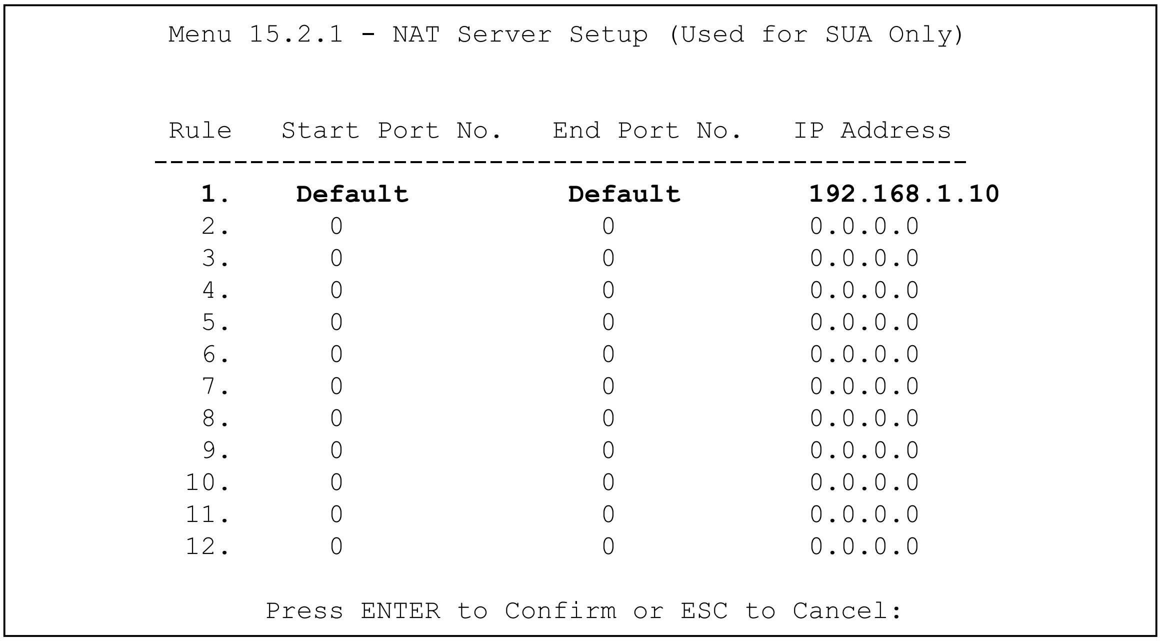


Figure 28-13 NAT Example 2

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



```
          Menu 15.2.1 - NAT Server Setup (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:
```

Figure 28-14 Menu 15.2.1 Specifying an Inside Server

28.5.3 Example 3: Multiple Public IP Addresses With Inside Servers

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

Map the first IGA to the first inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).

Map the second IGA to our second inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).

Map the other outgoing LAN traffic to IGA3 (**Many : 1** mapping).

You also map your third IGA to the web server and mail server on the LAN. Type **Server** allows you to specify multiple servers, of different types, to other computers behind NAT on the LAN.

The example situation looks somewhat like this:

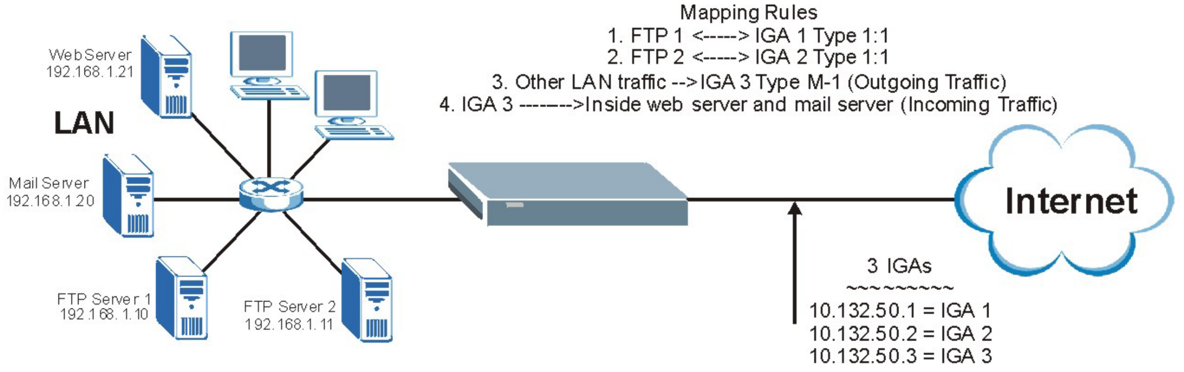
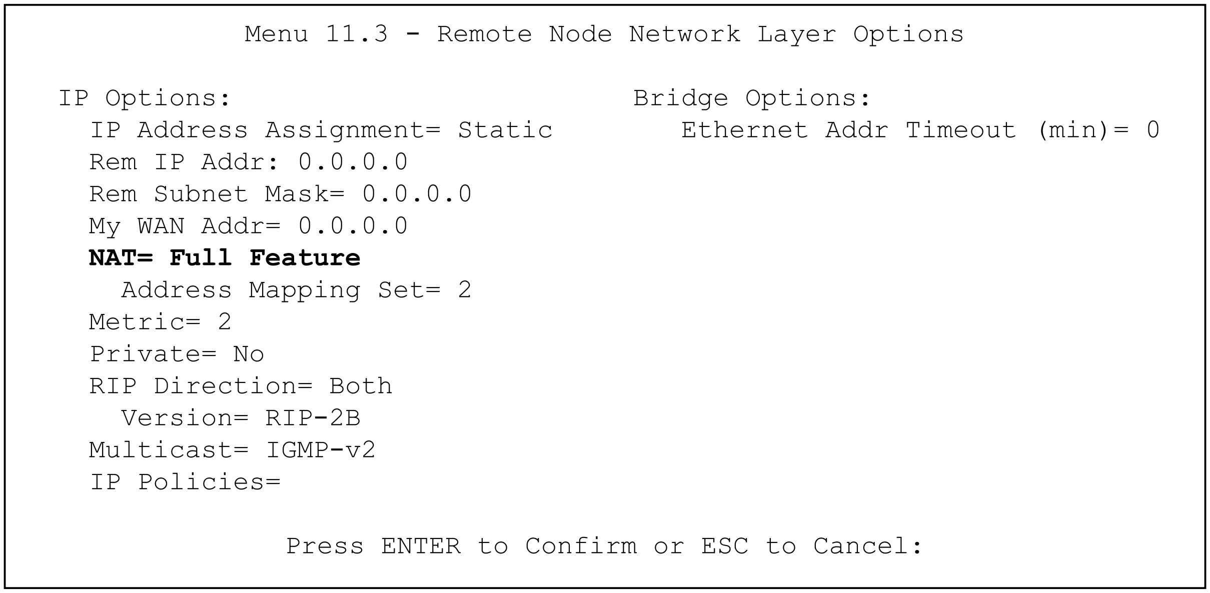


Figure 28-15 NAT Example 3

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 28-16.*

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 28-17).*
5. Repeat the previous step for rules 2 to 4 as outlined above.

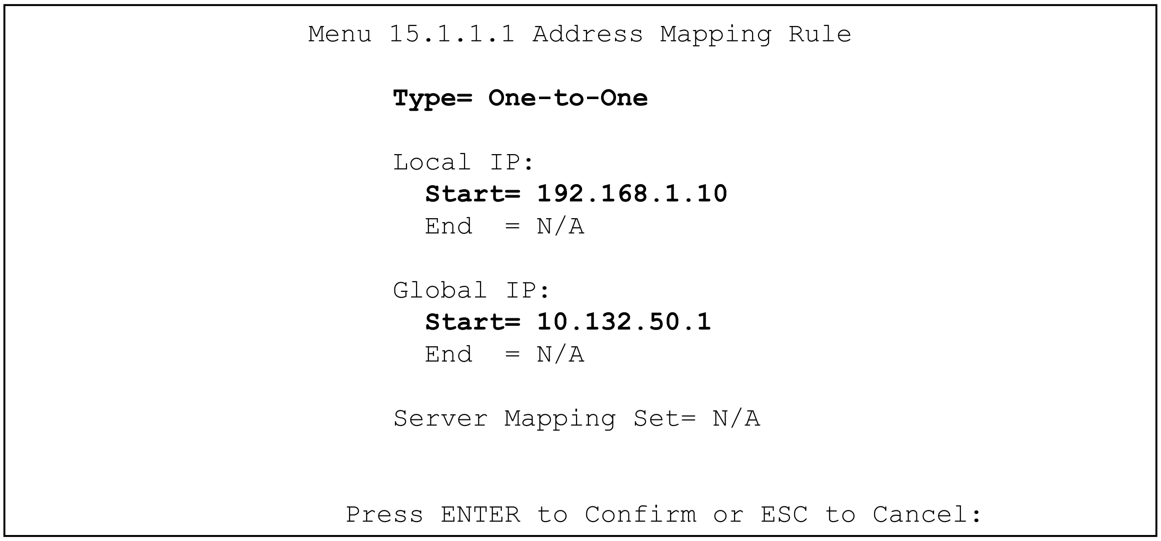
When finished, menu 15.1.1 should look like as shown in Figure 28-18.



```
              Menu 11.3 - Remote Node Network Layer Options

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

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

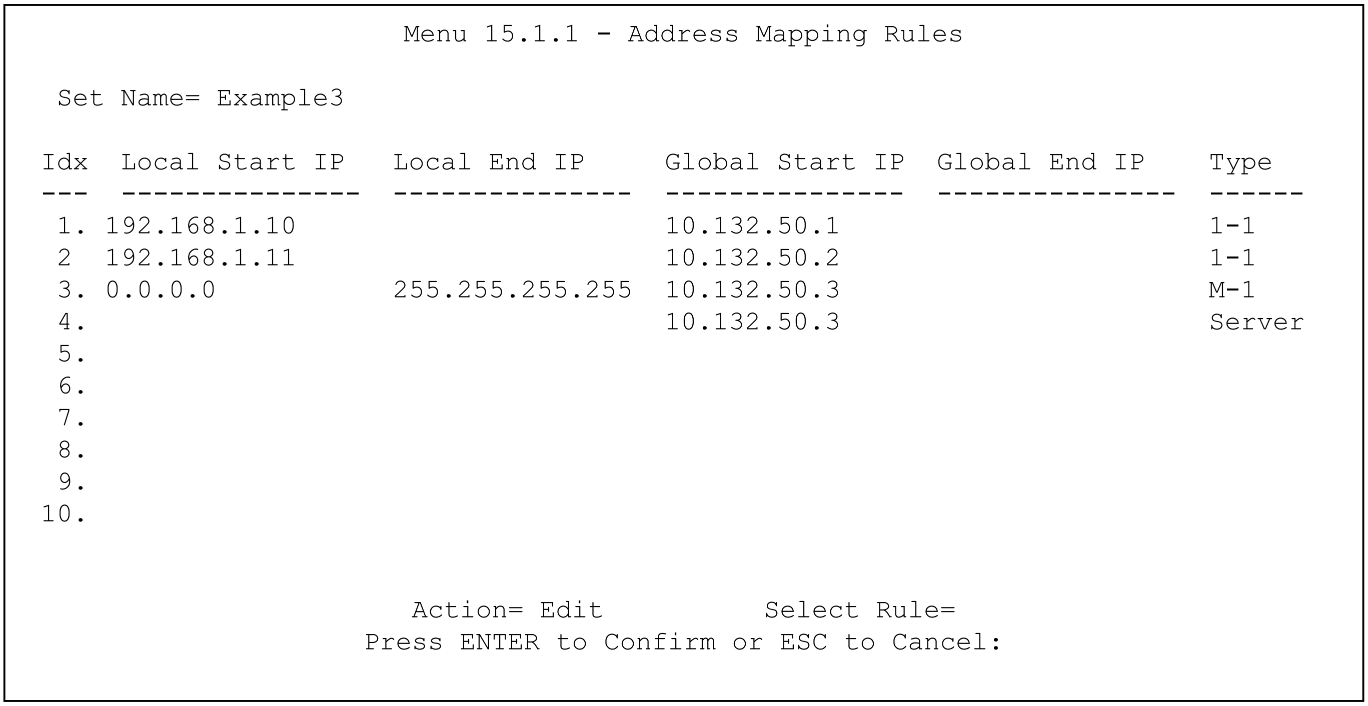
Figure 28-16 Example 3: Menu 11.3

The following figures show how to configure the first rule



```
                   Menu 15.1.1.1 Address Mapping Rule

                        Type= One-to-One

                        Local IP:
                          Start= 192.168.1.10
                          End  = N/A

                        Global IP:
                          Start= 10.132.50.1
                          End  = N/A

                        Server Mapping Set= N/A


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

Figure 28-17 Example 3: Menu 15.1.1.1



```
                       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:
```

Figure 28-18 Example 3: Final Menu 15.1.1

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.

```
                    Menu 15.2.1 - NAT Server Setup


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

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

Example 3: Menu 15.2.1

28.5.4 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.

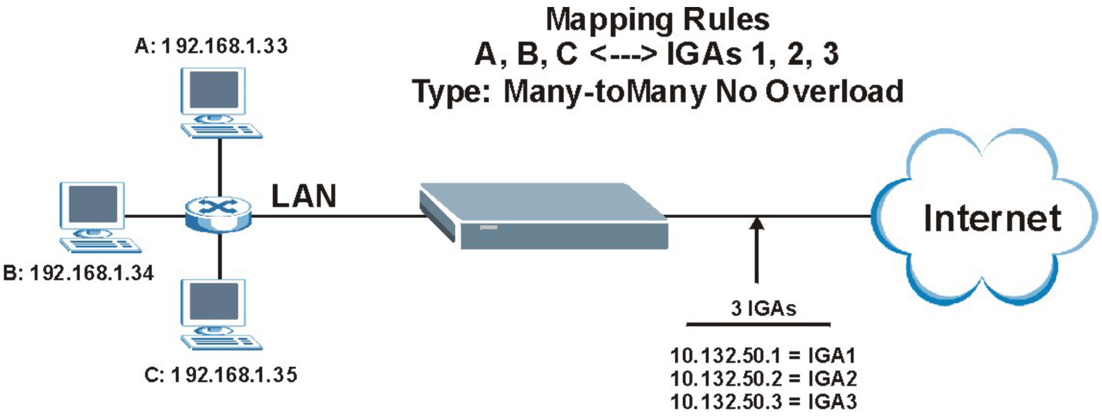
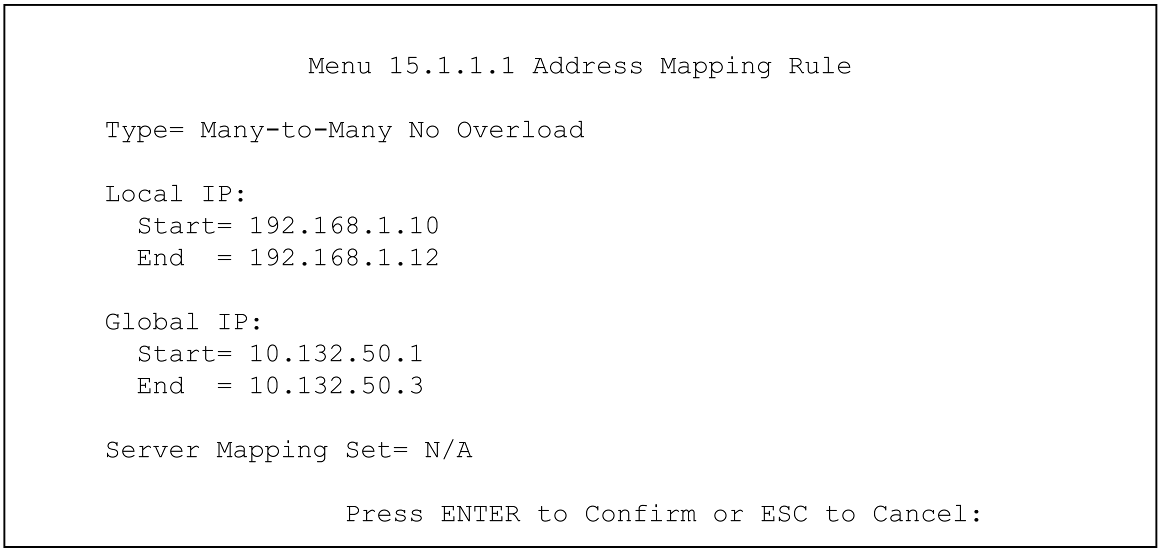


Figure 28-19 NAT Example 4

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

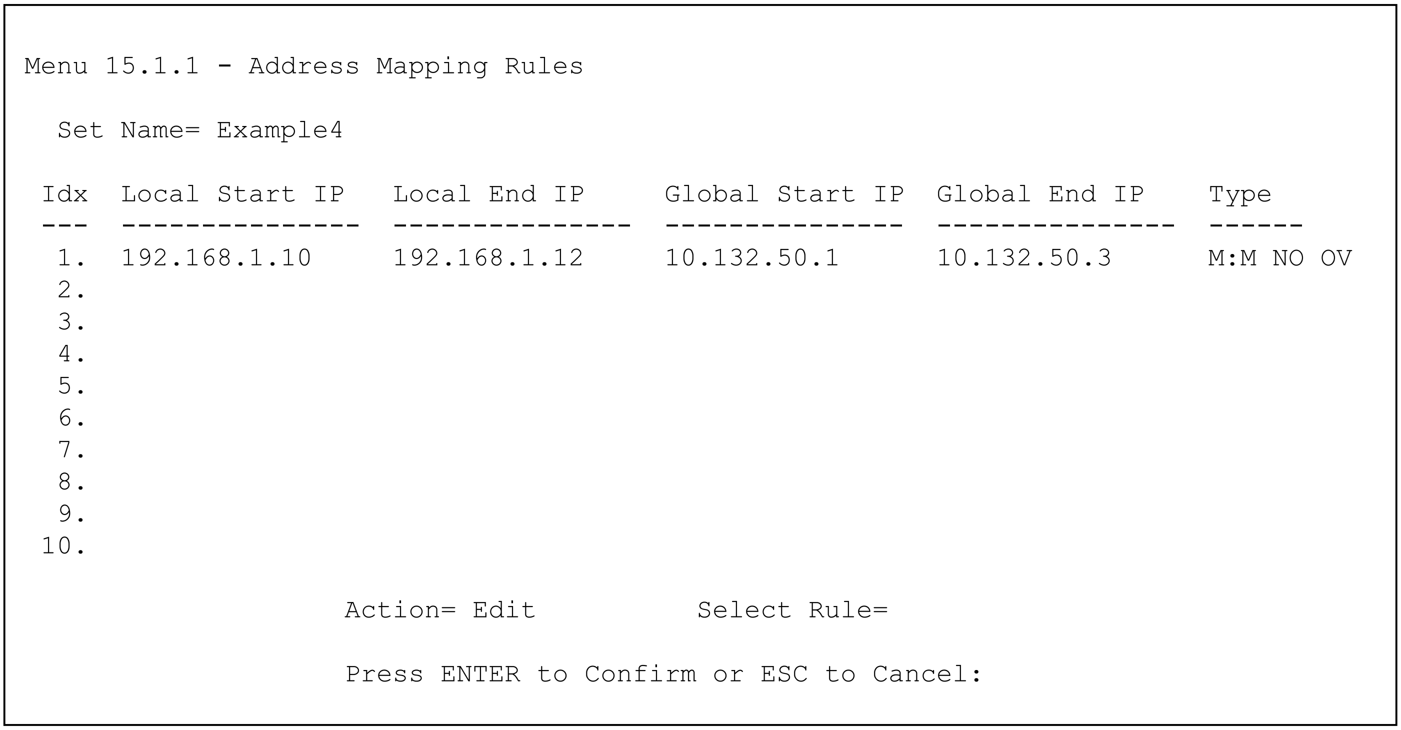
Follow the steps outlined in example 3 to configure these two menus as follows.



```
                   Menu 15.1.1.1 Address Mapping Rule

      Type= Many-to-Many No Overload

      Local IP:
        Start= 192.168.1.10
        End  = 192.168.1.12

      Global IP:
        Start= 10.132.50.1
        End  = 10.132.50.3

      Server Mapping Set= N/A

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

Figure 28-20 Example 4: Menu 15.1.1.1 Address Mapping Rule

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



```
Menu 15.1.1 - Address Mapping Rules

  Set Name= Example4

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

                    Action= Edit          Select Rule=

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

Figure 28-21 Example 4: Menu 15.1.1 Address Mapping Rules

Chapter 29
Enabling the Firewall

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

29.1 Remote Management and the Firewall

When SMT menu 24.11 is configured to allow management (see the *Remote Management* chapter) and the firewall is enabled:

- The firewall blocks remote management from the WAN unless you configure a firewall rule to allow it.
- The firewall allows remote management from the LAN.

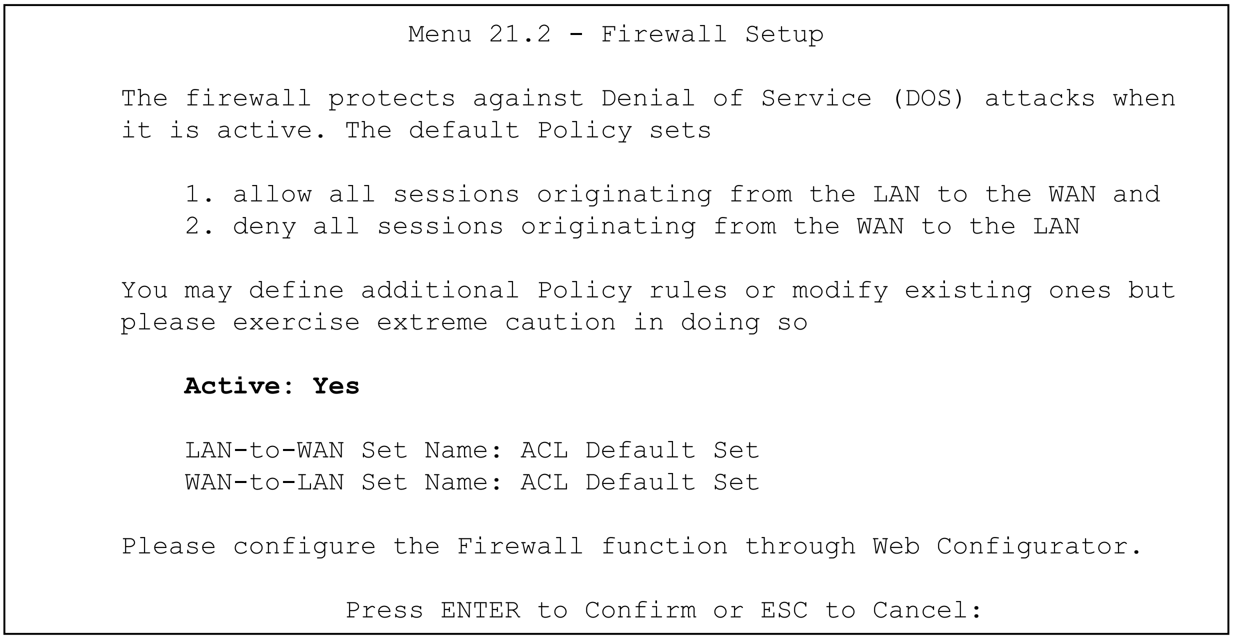
29.2 Access Methods

The web configurator is, by far, the most comprehensive firewall configuration tool your Prestige has to offer. For this reason, it is recommended that you configure your firewall using the web configurator, see the following chapters for instructions. SMT screens allow you to activate the firewall and view firewall logs.

29.3 Enabling the Firewall

From the main menu enter 21 to go to **Menu 21 - Filter Set and Firewall Configuration** to display the screen shown next**.**

Enter option 2 in this menu to bring up the following screen. Press [SPACE BAR] and then [ENTER] to select **Yes** in the **Active** field to activate the firewall. The firewall must be active to protect against Denial of Service (DoS) attacks. Additional rules may be configured using the web configurator.



```
                         Menu 21.2 - Firewall Setup

       The firewall protects against Denial of Service (DOS) attacks when
       it is active. The default Policy sets

           1. allow all sessions originating from the LAN to the WAN and
           2. deny all sessions originating from the WAN to the LAN

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

           Active: Yes

           LAN-to-WAN Set Name: ACL Default Set
           WAN-to-LAN Set Name: ACL Default Set

       Please configure the Firewall function through Web Configurator.

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

Figure 29-1 Menu 21.2 Firewall Setup

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

Part IX:

SMT Advanced Management

This part discusses filtering setup, SNMP, system security, system information and diagnosis, firmware and configuration file maintenance, system maintenance, remote management, IP Policy Routing, call scheduling and Internal SPTGEN for configuration of multiple Prestiges.

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

Chapter 30 Filter Configuration

This chapter shows you how to create and apply filters.

30.1 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.

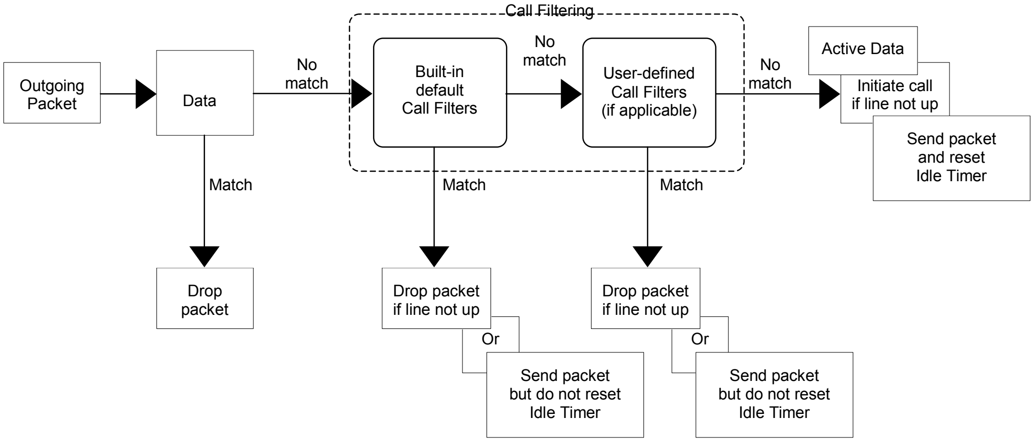

Call Filtering
Outgoing Packet
Data
No match
Built-in default Call Filters
No match
User-defined Call Filters (if applicable)
No match
Active Data
Initiate call if line not up
Send packet and reset Idle Timer
Match
Match
Match
Drop packet
Drop packet if line not up
Or
Send packet but do not reset Idle Timer
Drop packet if line not up
Or
Send packet but do not reset Idle Timer

Figure 30-1 Outgoing Packet Filtering Process

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

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

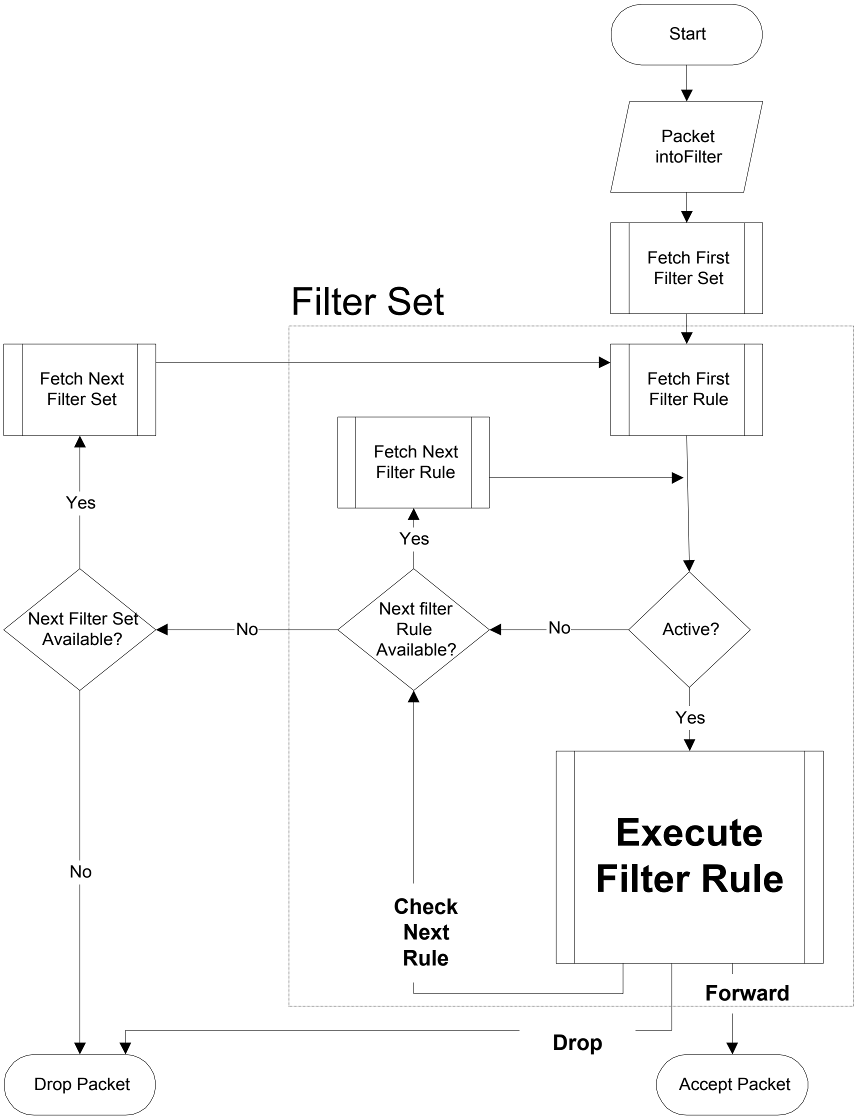


Figure 30-2 Filter Rule Process

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

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

The Filter Structure of the Prestige

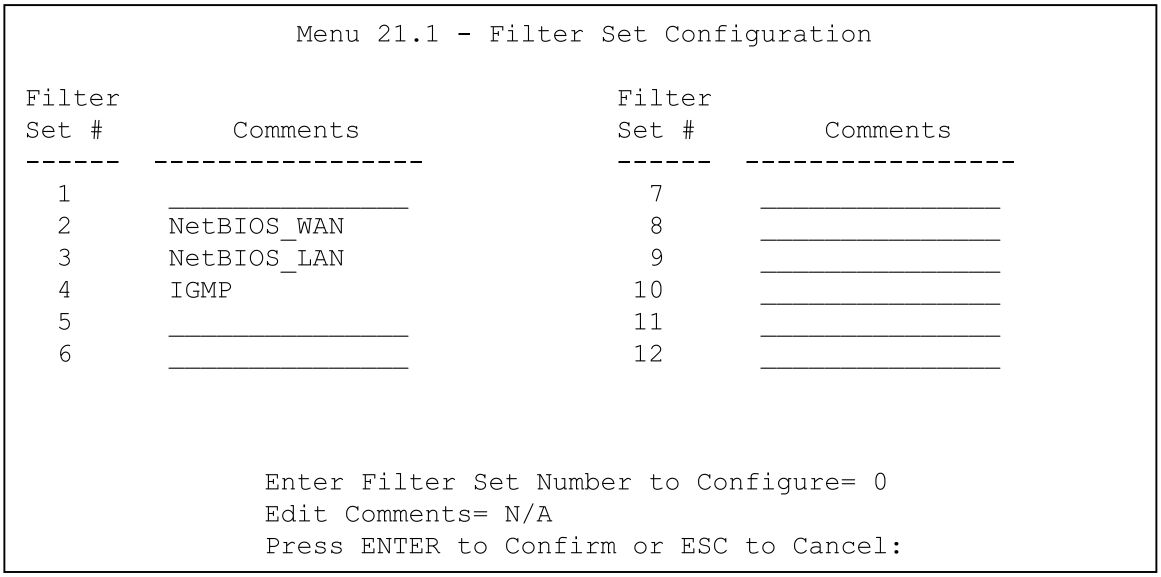
A filter set consists of one or more filter rules. Usually, you would group related rules, for example, all the rules for NetBIOS, into a single set and give it a descriptive name. You can configure up to twelve filter sets with six rules in each set, for a total of 72 filter rules in the system.

30.2 Configuring a Filter Set for the Prestige

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

Enter 21 in the main menu to display **Menu 21 – Filter and Firewall Setup**.

Enter 1 to display Menu 21.1 – Filter Set Configuration as shown next.



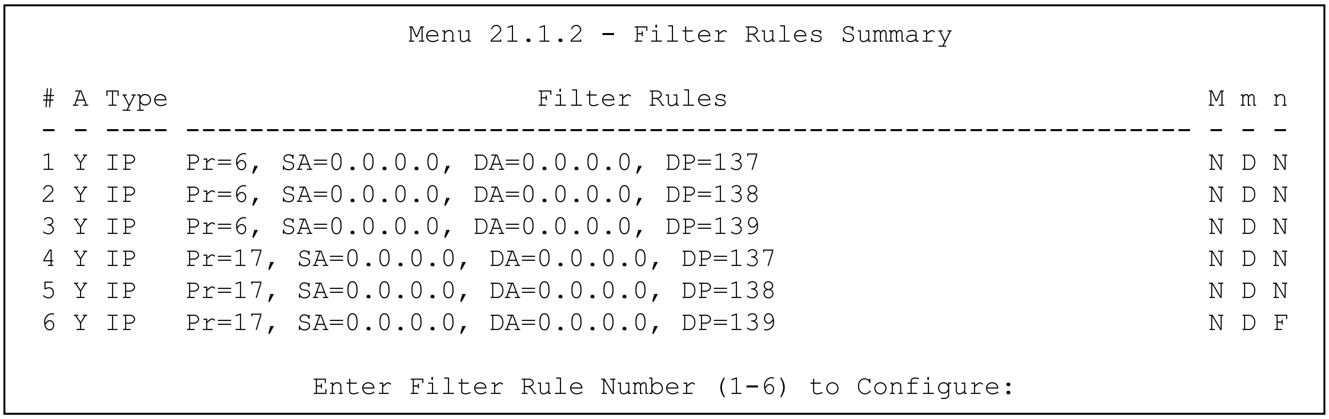
```
                  Menu 21.1 - Filter Set Configuration

 Filter                                Filter
 Set #       Comments                  Set #       Comments
 ------  -----------------             ------  -----------------
   1      _______________                7      _______________
   2      NetBIOS_WAN                    8      _______________
   3      NetBIOS_LAN                    9      _______________
   4      IGMP                          10      _______________
   5      _______________               11      _______________
   6      _______________               12      _______________



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

Figure 30-3 Menu 21 Filter Set Configuration

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

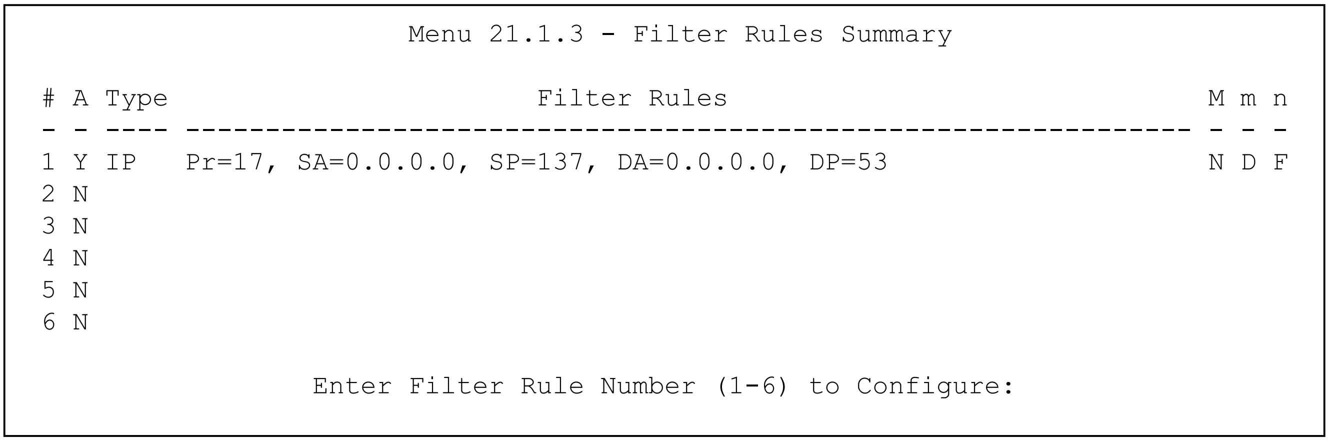
Step 2. Type a descriptive name or comment in the **Edit Comments** field and press [ENTER].

Step 3. Press [ENTER] at the message "`Press ENTER to confirm…`" to display **Menu 21.1.1 – Filter Rules Summary** (that is, if you selected filter set 1 in menu 21.1).



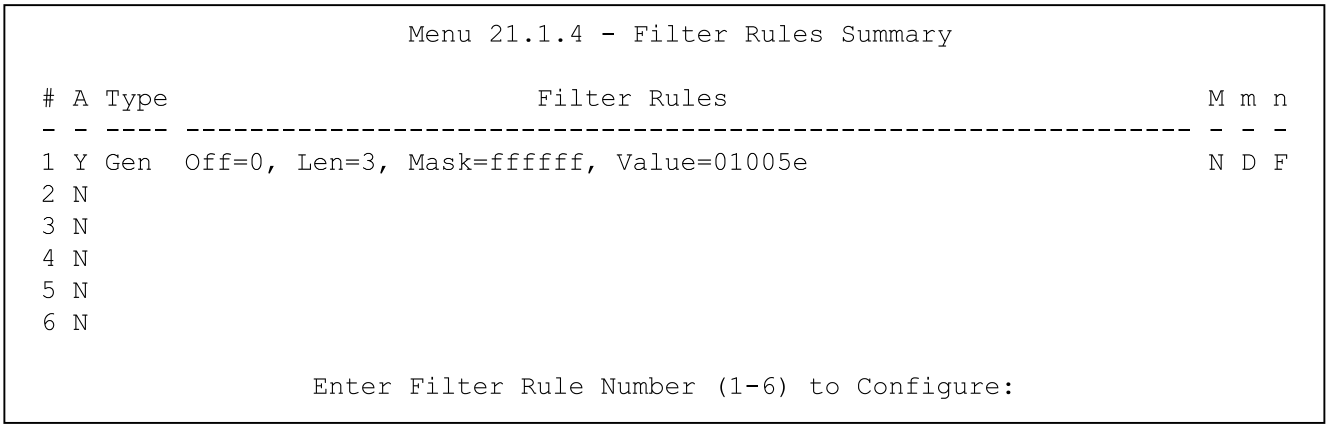
```
                        Menu 21.1.2 - Filter Rules Summary

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

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

Figure 30-4 NetBIOS_WAN Filter Rules Summary



```
                       Menu 21.1.3 - Filter Rules Summary

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

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

Figure 30-5 NetBIOS_LAN Filter Rules Summary



```
                       Menu 21.1.4 - Filter Rules Summary

# A Type                       Filter Rules                                  M m n
- - ---- --------------------------------------------------------------- - - -
1 Y Gen  Off=0, Len=3, Mask=ffffff, Value=01005e                         N D F
2 N
3 N
4 N
5 N
6 N

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

Figure 30-6 IGMP Filter Rules Summary

30.3 Filter Rules Summary Menus

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

Table 30-1 Abbreviations Used in the Filter Rules Summary Menu

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

Table 30-1 Abbreviations Used in the Filter Rules Summary Menu

FIELD	DESCRIPTION
m	Action Matched. "F" means to forward the packet immediately and skip checking the remaining rules. "D" means to drop the packet. "N" means to check the next rule.
n	Action Not Matched. "F" means to forward the packet immediately and skip checking the remaining rules. "D" means to drop the packet. "N" means to check the next rule.

The protocol dependent filter rules abbreviation are listed as follows:

Table 30-2 Rule Abbreviations Used

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

30.4 Configuring a Filter Rule

To configure a filter rule, type its number in **Menu 21.1.x – Filter Rules Summary** and press [ENTER] to open menu 21.1.x.1 for the rule.

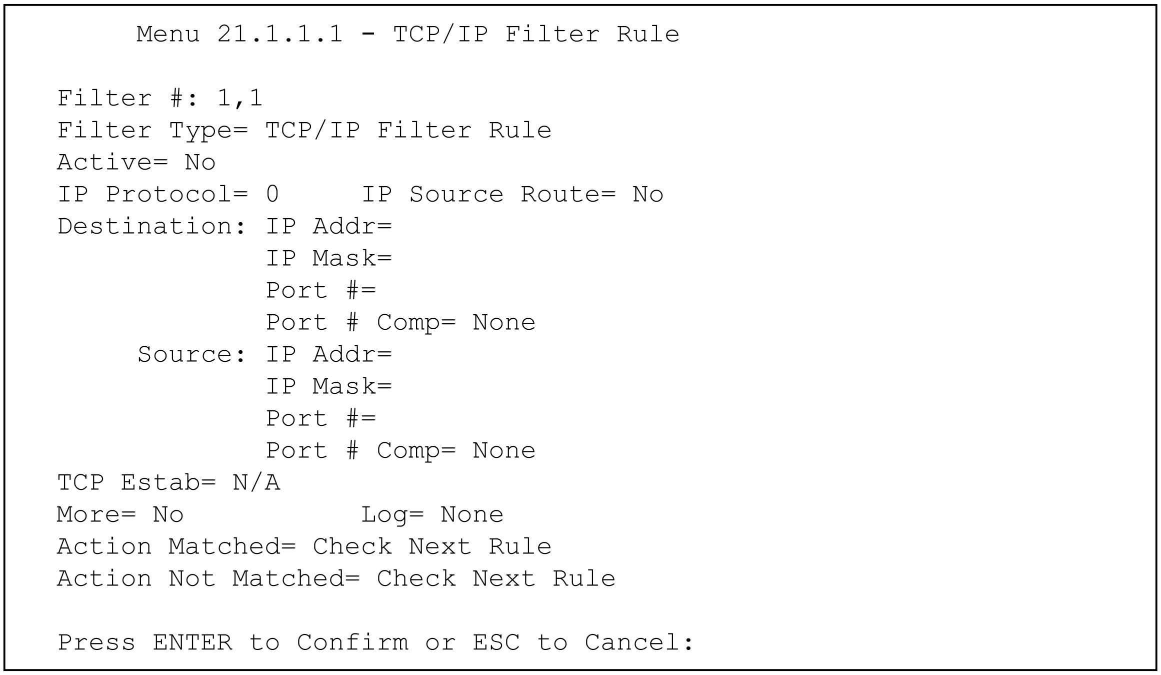
There are two types of filter rules: **TCP/IP** and **Generic**. Depending on the type of rule, the parameters for each type will be different. Use [SPACE BAR] to select the type of rule that you want to create in the **Filter Type** field and press [ENTER] to open the respective menu.

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

30.4.1 TCP/IP Filter Rule

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

To configure TCP/IP rules, select TCP/IP Filter Rule from the **Filter Type** field and press [ENTER] to open **Menu 21.1.x.1 – TCP/IP Filter Rule**, as shown next.



```
          Menu 21.1.1.1 - TCP/IP Filter Rule

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

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

Figure 30-7 Menu 21.1.x.1 TCP/IP Filter Rule

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

Table 30-3 Menu 21.1.x.1 TCP/IP Filter Rule

FIELD	DESCRIPTION	EXAMPLE
Filter #	This is the filter set, filter rule coordinates, for instance, 2, 3 refers to the second filter set and the third filter rule of that set.	1,1
Filter Type	Use [SPACE BAR] and then [ENTER] to choose a rule. Parameters displayed for each type will be different. Choices are **TCP/IP Filter Rule** or **Generic Filter Rule**.	**TCP/IP Filter Rule**
Active	Select **Yes** to activate or **No** to deactivate the filter rule.	**No** (default)
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 O matches ANY protocol.	0 to 255
IP Source Route	IP Source Route is an optional header that dictates the route an IP packet takes from its source to its destination. If **Yes**, the rule applies to any packet with an IP source route. The majority of IP packets do not have source route.	**No** (default)
Destination:		
IP Addr	Type the destination IP address of the packet you want to filter. This field is ignored if it is 0.0.0.0.	IP address
IP Mask	Type the IP mask to apply to the Destination: IP Addr field.	IP mask
Port #	Type the destination port of the packets you want to filter. The field range is 0 to 65535. A 0 field is ignored.	0 to 65535

Table 30-3 Menu 21.1.x.1 TCP/IP Filter Rule

FIELD	DESCRIPTION	EXAMPLE
Port # Comp	Select the comparison to apply to the destination port in the packet against the value given in **Destination: Port #.** Choices are **None**, **Less**, **Greater**, **Equal** or **Not Equal**.	**None**
Source:		
IP Addr	Type the source IP Address of the packet you want to filter. A 0.0.0.0 field is ignored.	IP address
IP Mask	Type the IP mask to apply to the **Source: IP Addr** field.	IP mask
Port #	Type the source port of the packets you want to filter. The range of this field is 0 to 65535. A 0 field is ignored.	0 to 65535
Port # Comp	Select the comparison to apply to the source port in the packet against the value given in **Source: Port #** field. Choices are **None**, **Less**, **Greater**, **Equal** or **Not Equal**.	**None**
TCP Estab	This applies only when the IP Protocol field is 6, TCP. If **Yes**, the rule matches packets that want to establish TCP connection(s) (SYN=1 and ACK=0); else it is ignored.	**No** (default)
More	If **Yes**, a matching packet is passed to the next filter rule before an action is taken or else the packet is disposed of according to the action fields. If **More** is **Yes**, then **Action Matched** and **Action Not Matched** will be N/A.	**No** (default)
Log	Select the logging option from the following: **None** – No packets will be logged. **Action Matched** – Only packets that match the rule parameters will be logged. **Action Not Matched** – Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.	**None**
Action Matched	Select the action for a matching packet. Choices are **Check Next Rule**, **Forward** or **Drop**.	**Check Next Rule** (default)
Action Not Matched	Select the action for a packet not matching the rule. Choices are **Check Next Rule**, **Forward** or **Drop**.	**Check Next Rule** (default)
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

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

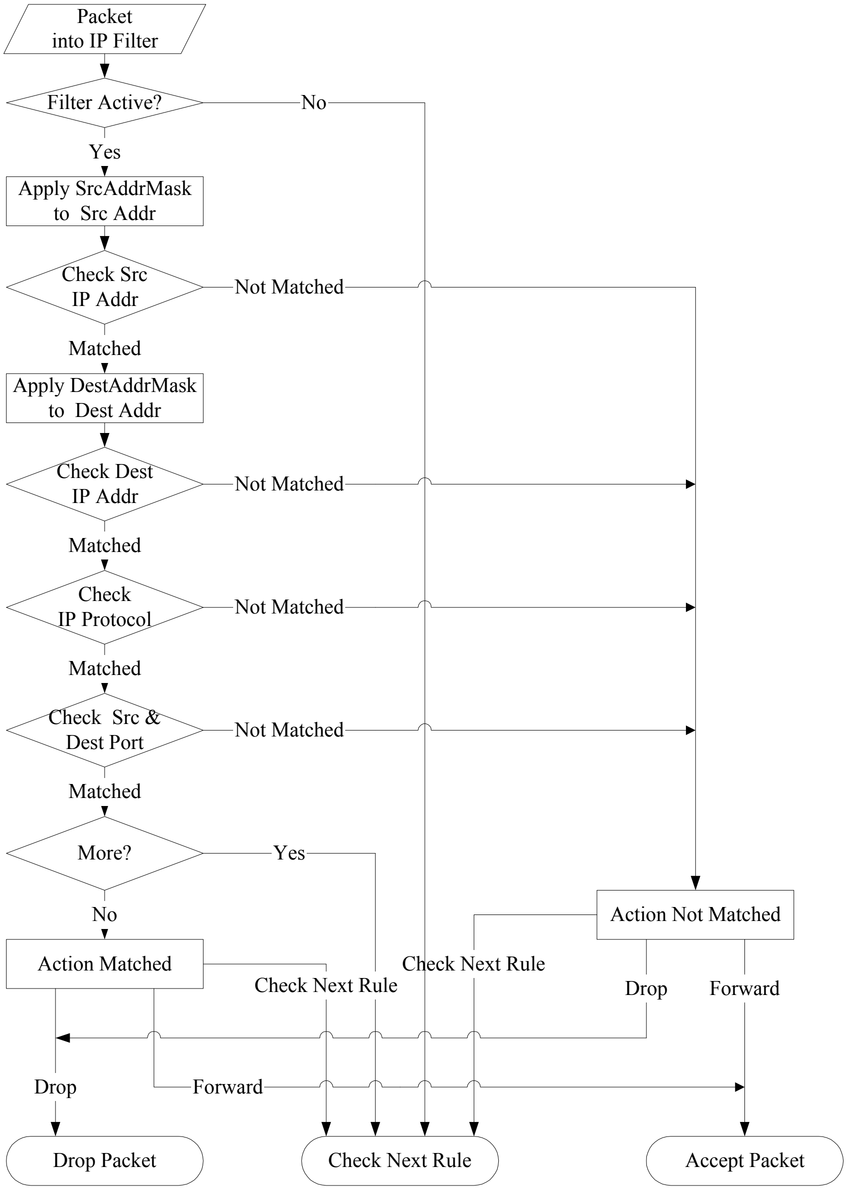


Figure 30-8 Executing an IP Filter

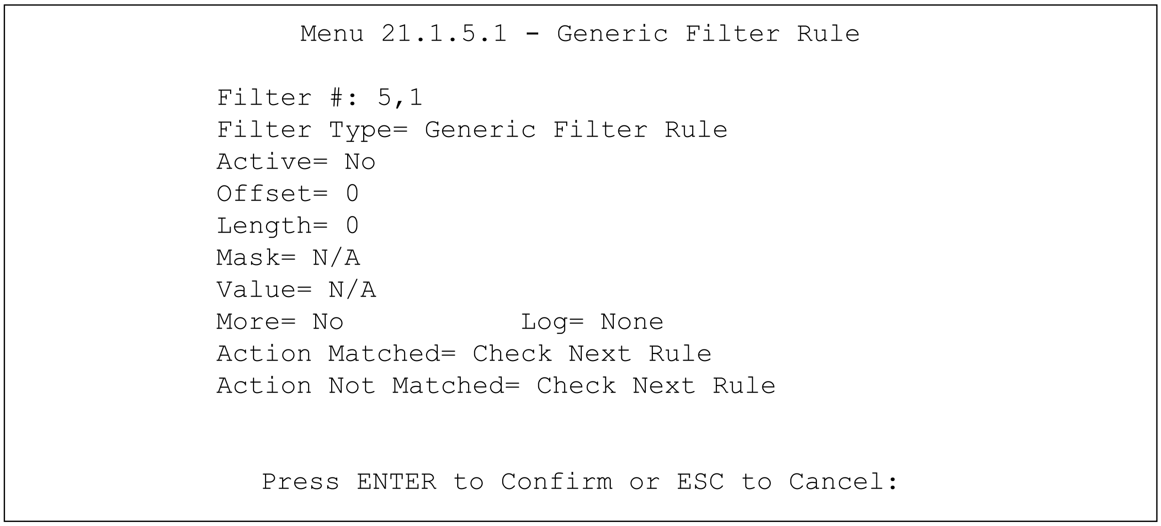
30.4.2 Generic Filter Rule

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

For generic rules, the Prestige treats a packet as a byte stream as opposed to an IP packet. You specify the portion of the packet to check with the **Offset** (from 0) and the **Length** fields, both in bytes. The Prestige applies the Mask (bit-wise ANDing) to the data portion before comparing the result against the Value to determine a match. The **Mask** and **Value** fields are specified in hexadecimal numbers.

Note that it takes two hexadecimal digits to represent a byte, so if the length is 4, the value in either field will take 8 digits, for example, FFFFFFFF.

To configure a generic rule select an empty filter set in menu 21, for example 5. Select **Generic Filter Rule** in the **Filter Type** field and press [ENTER] to open **Menu 21.1.5.1 – Generic Filter Rule**, as shown in the following figure.



```
                 Menu 21.1.5.1 - Generic Filter Rule

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


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

Figure 30-9 Menu 21.1.5.1 Generic Filter Rule

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

Table 30-4 Menu 21.1.5.1 Generic Filter Rule

FIELD	DESCRIPTION	EXAMPLE
Filter #	This is the filter set, filter rule coordinates, for instance, 2, 3 refers to the second filter set and the third rule of that set.	5,1
Filter Type	Press [SPACE BAR] and then [ENTER] to select a type of rule. Parameters displayed below each type will be different. Choices are **Generic Filter Rule** or **TCP/IP Filter Rule**.	**Generic Filter Rule**
Active	Select **Yes** to turn on or **No** to turn off the filter rule.	**No** (default)
Offset	Type the starting byte of the data portion in the packet that you want to compare. The range for this field is from 0 to 255.	0 (default)
Length	Type the byte count of the data portion in the packet that you want to compare. The range for this field is 0 to 8.	0 (default)
Mask	Type the mask (in Hexadecimal) to apply to the data portion before comparison.	
Value	Type the value (in Hexadecimal) to compare with the data portion.	
More	If **Yes**, a matching packet is passed to the next filter rule before an action is taken or else the packet is disposed of according to the action fields. If **More** is **Yes**, then **Action Matched** and **Action Not Matched** will be **N/A**.	**No** (default)

Table 30-4 Menu 21.1.5.1 Generic Filter Rule

FIELD	DESCRIPTION	EXAMPLE
Log	Select the logging option from the following: **None** – No packets will be logged. **Action Matched** – Only matching packets and rules will be logged. **Action Not Matched** – Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.	**None**
Action Matched	Select the action for a matching packet. Choices are **Check Next Rule**, **Forward** or **Drop**.	**Check Next Rule** (default)
Action Not Matched	Select the action for a packet not matching the rule. Choices are **Check Next Rule**, **Forward** or **Drop**.	**Check Next Rule** (default)
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

30.5 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.

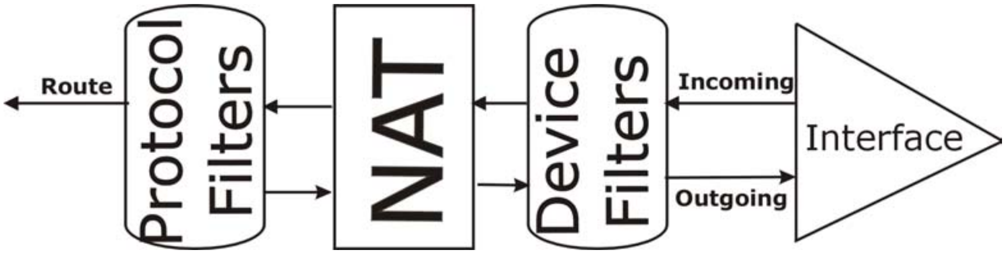


Figure 30-10 Protocol and Device Filter Sets

30.6 Example Filter

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

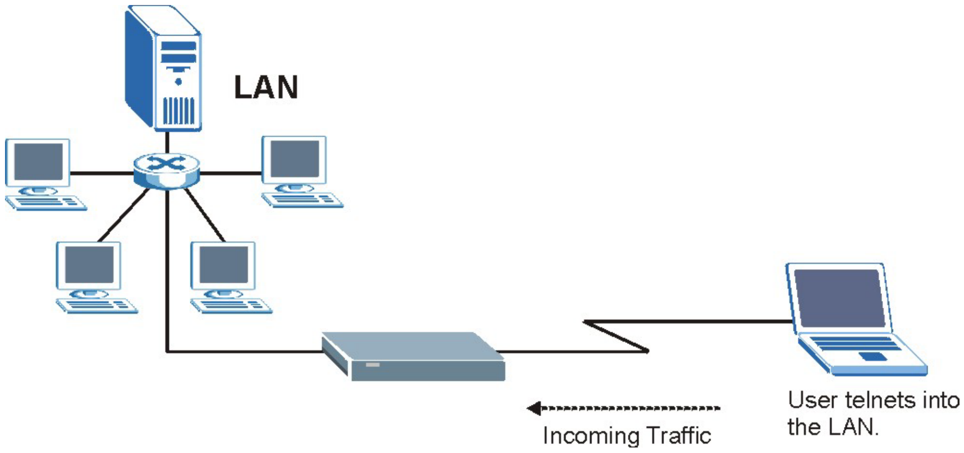
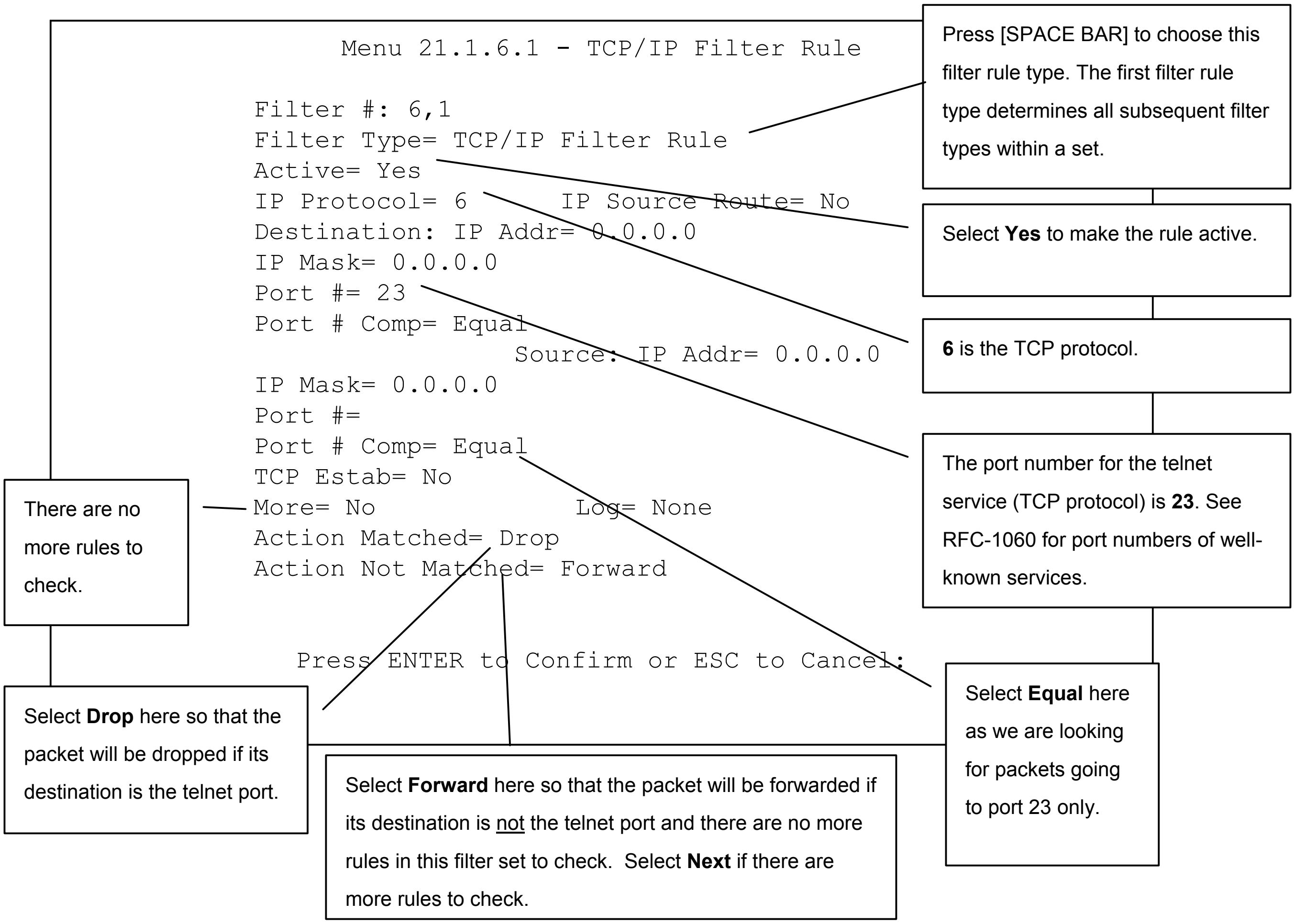


Figure 30-11 Sample Telnet Filter

1. Enter 1 in the menu 21 to display **Menu 21.1 — Filter Set Configuration**.
2. Enter the index number of the filter set you want to configure (in this case 6).
3. Type a descriptive name or comment in the **Edit Comments** field (for example, TELNET_WAN) and press [ENTER].
4. Press [ENTER] at the message "Press [ENTER] to confirm or [ESC] to cancel" to open **Menu 21.1.6 — Filter Rules Summary**.
5. Type 1 to configure the first filter rule. Make the entries in this menu as shown next.
6. When you press [ENTER] to confirm, the following screen appears. Note that there is only one filter rule in this set.



```
                    Menu 21.1.6.1 - TCP/IP Filter Rule

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


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

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

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

6 is the TCP protocol.

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

There are no more rules to check.

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

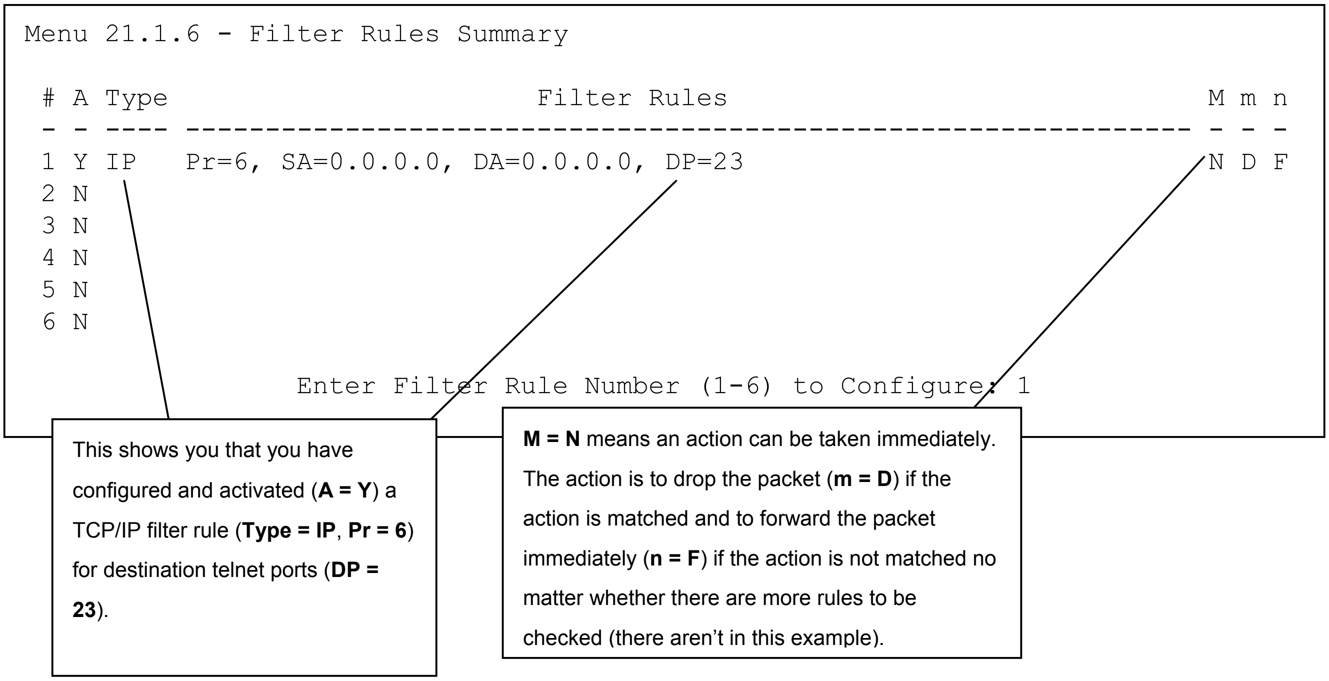
Select **Forward** here so that the packet will be forwarded if its destination is not the telnet port and there are no more rules in this filter set to check. Select **Next** if there are more rules to check.

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

Figure 30-12 Menu 21.1.6.1 Sample Filter

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.



```
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).

Figure 30-13 Menu 21.1.6.1 Sample Filter Rules Summary

30.7 Applying Filters and Factory Defaults

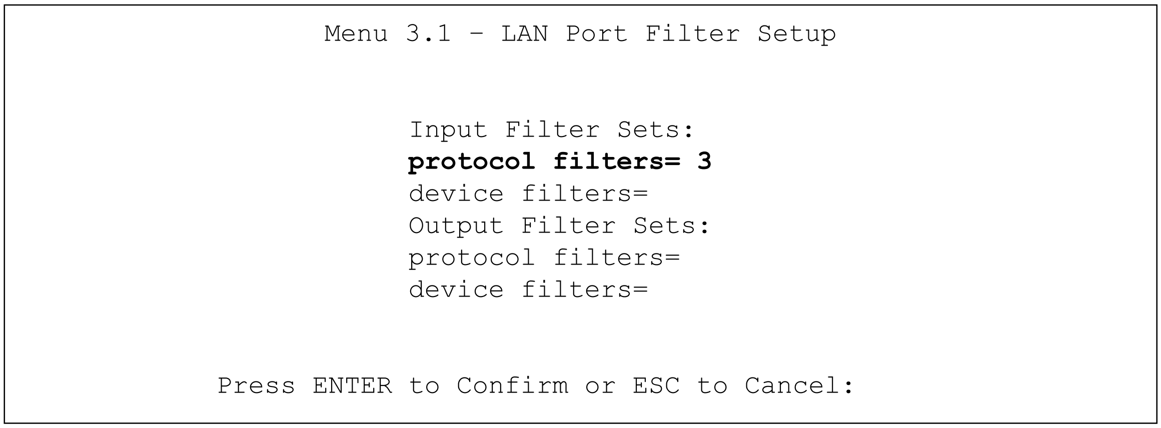
This section shows you where to apply the filter(s) after you design it (them). Sets of factory default filter rules have been configured in menu 21 (but have not been applied) to filter traffic.

Table 30-5 Filter Sets Table

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

30.7.1 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.

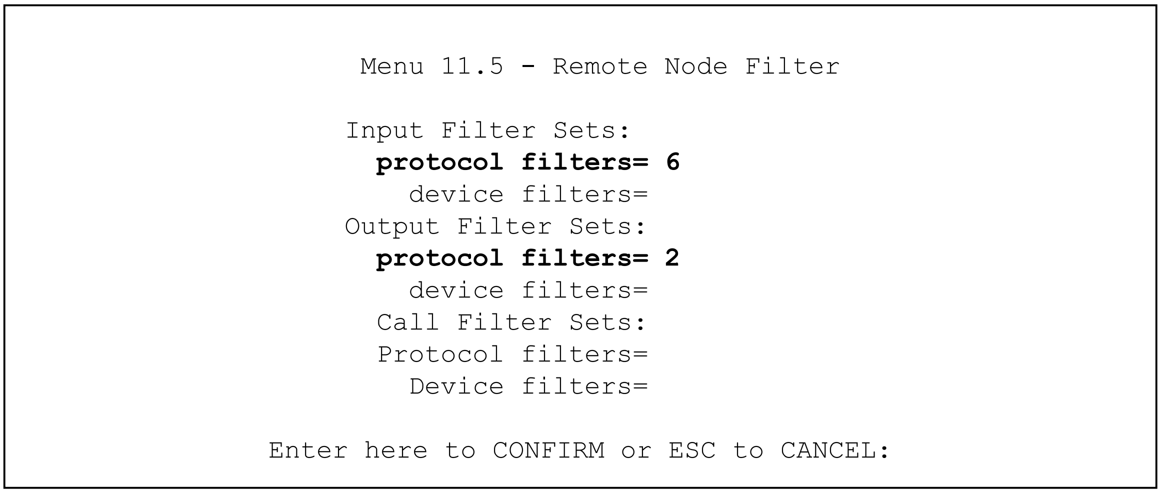


```
                Menu 3.1 - LAN Port Filter Setup


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


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

Figure 30-14 Filtering Ethernet Traffic

30.7.2 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.



```
                  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:
```

Figure 30-15 Filtering Remote Node Traffic

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

Chapter 31
SNMP Configuration

This chapter explains SNMP Configuration menu 22.

31.1 About SNMP

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

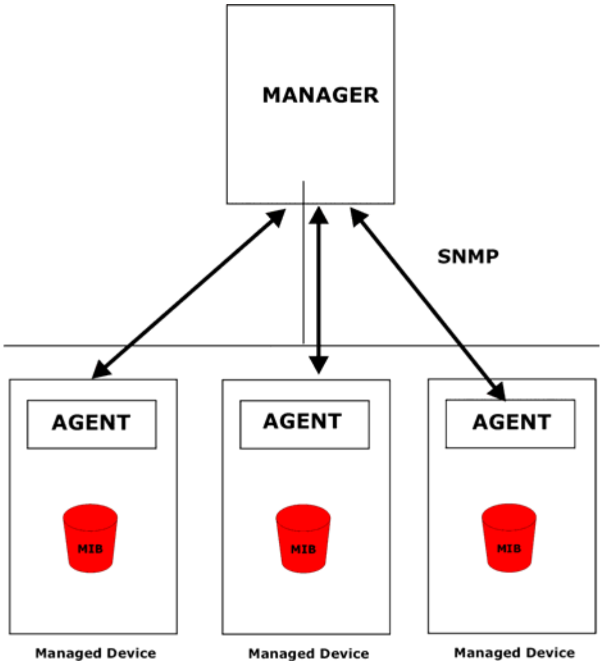


Figure 31-1 SNMP Management Model

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

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

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

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

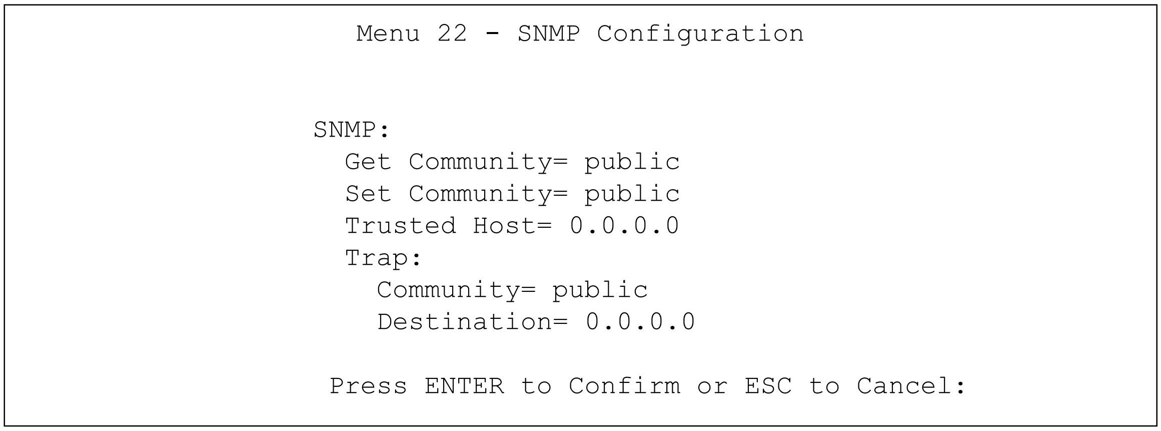
- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed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

31.2 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.

31.3 SNMP Configuration

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



```
                        Menu 22 - SNMP Configuration


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

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

Figure 31-2 Menu 22 SNMP Configuration

The following table describes the SNMP configuration parameters.

Table 31-1 Menu 22 SNMP Configuration

FIELD	DESCRIPTION	EXAMPLE
SNMP:		
Get Community	Type the **Get Community**, which is the password for the incoming Get- and GetNext requests from the management station.	public
Set Community	Type the **Set** community, which is the password for incoming Set requests from the management station.	public
Trusted Host	If you enter a trusted host, your Prestige will only respond to SNMP messages from this address. A blank (default) field means your Prestige will respond to all SNMP messages it receives, regardless of source.	0.0.0.0
Trap:		

Table 31-1 Menu 22 SNMP Configuration

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

31.4 SNMP Traps

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

Table 31-2 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 31-3 Ports and Permanent Virtual Circuits

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

Chapter 32
System Security

This chapter describes how to configure the system security on the Prestige.

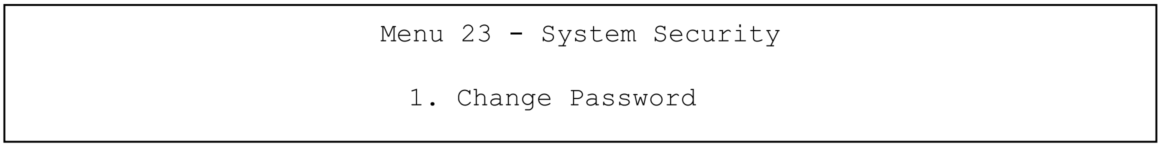
32.1 System Security

You can configure the system password..

32.1.1 System Password

Enter 23 in the main menu to display **Menu 23 – System Security**.

You should change the default password. If you forget your password you have to restore the default configuration file. Refer to the section on changing the system password in the *Introducing the SMT* chapter and the section on resetting the Prestige in the *Introducing the Web Configurator* chapter.



```
                         Menu 23 - System Security

                            1. Change Password
```

Figure 32-1 Menu 23 – System Security

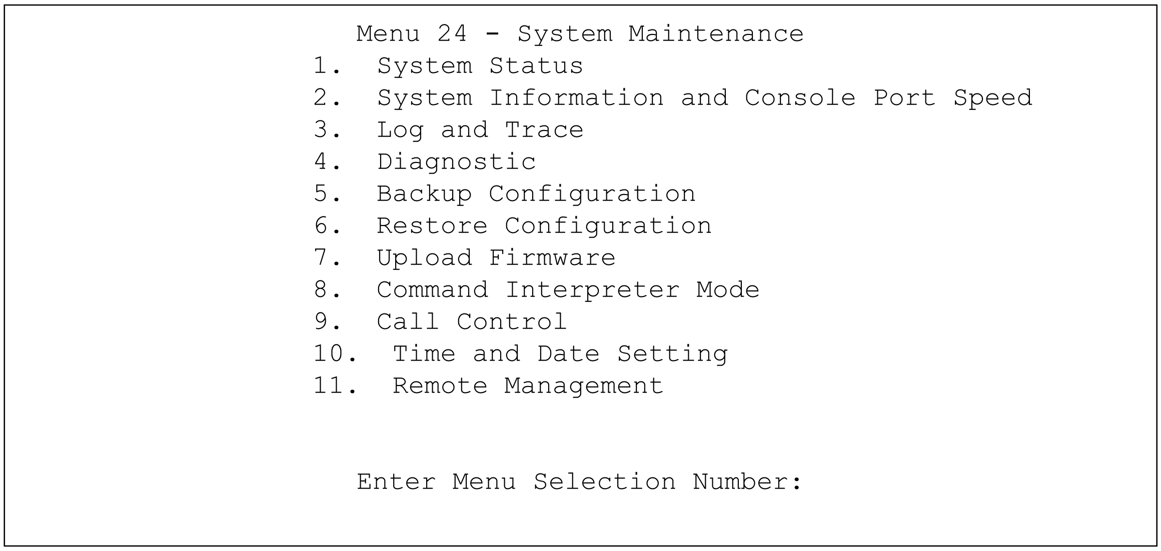
Chapter 33 System Information and Diagnosis

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

33.1 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.



```
                         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:
```

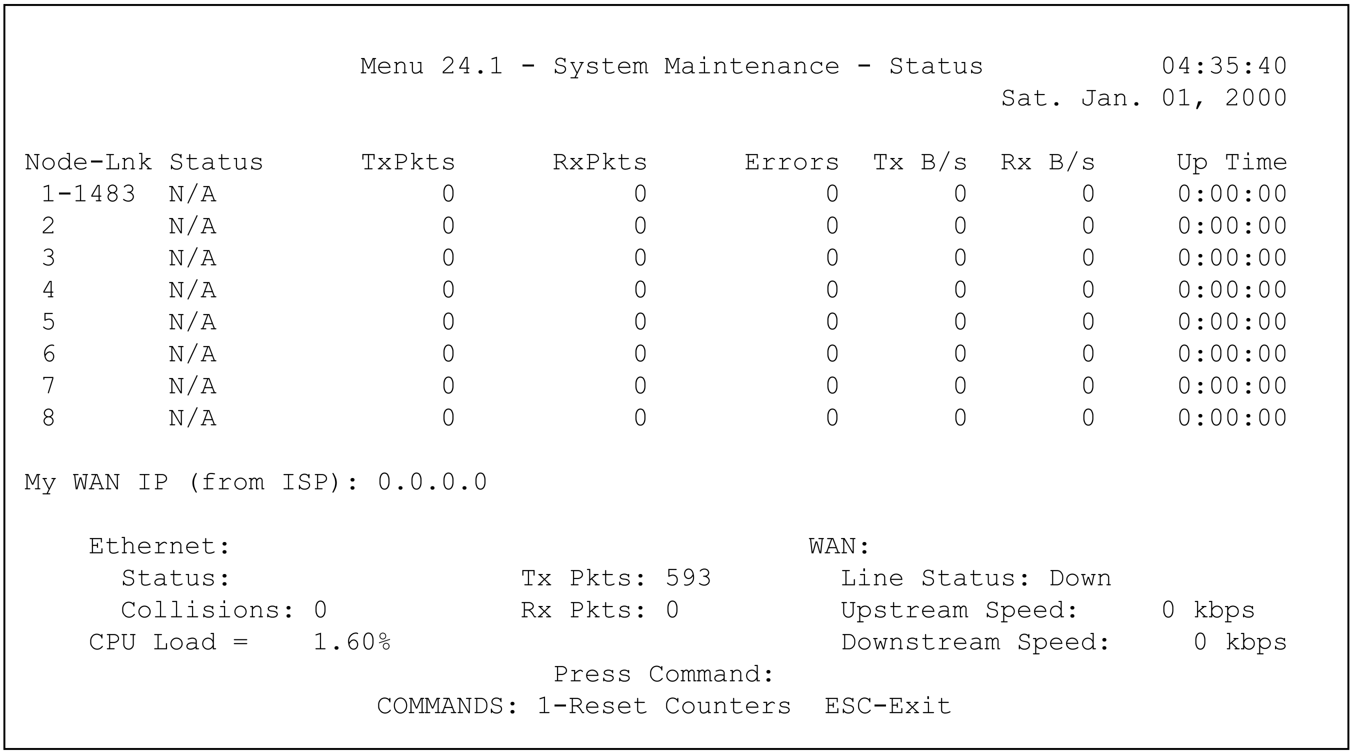
Figure 33-1 Menu 24 System Maintenance

33.2 System Status

The first selection, System Status gives you information on the status and statistics of the ports, as shown next (see *Figure 33-2*). System Status is a tool that can be used to monitor your Prestige. Specifically, it gives you information on your ADSL telephone line status, number of packets sent and received.

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

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



```
                    Menu 24.1 - System Maintenance - Status           04:35:40
                                                                Sat. Jan. 01, 2000

Node-Lnk Status      TxPkts      RxPkts      Errors  Tx B/s  Rx B/s      Up Time
 1-1483  N/A              0           0           0       0       0      0:00:00
 2       N/A              0           0           0       0       0      0:00:00
 3       N/A              0           0           0       0       0      0:00:00
 4       N/A              0           0           0       0       0      0:00:00
 5       N/A              0           0           0       0       0      0:00:00
 6       N/A              0           0           0       0       0      0:00:00
 7       N/A              0           0           0       0       0      0:00:00
 8       N/A              0           0           0       0       0      0:00:00

My WAN IP (from ISP): 0.0.0.0

    Ethernet:                                        WAN:
      Status:                Tx Pkts: 593              Line Status: Down
      Collisions: 0          Rx Pkts: 0                Upstream Speed:     0 kbps
    CPU Load =    1.60%                                Downstream Speed:     0 kbps
                                   Press Command:
                     COMMANDS: 1-Reset Counters  ESC-Exit
```

Figure 33-2 Menu 24.1 System Maintenance : Status

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

Table 33-1 Menu 24.1 System Maintenance : Status

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

Table 33-1 Menu 24.1 System Maintenance : Status

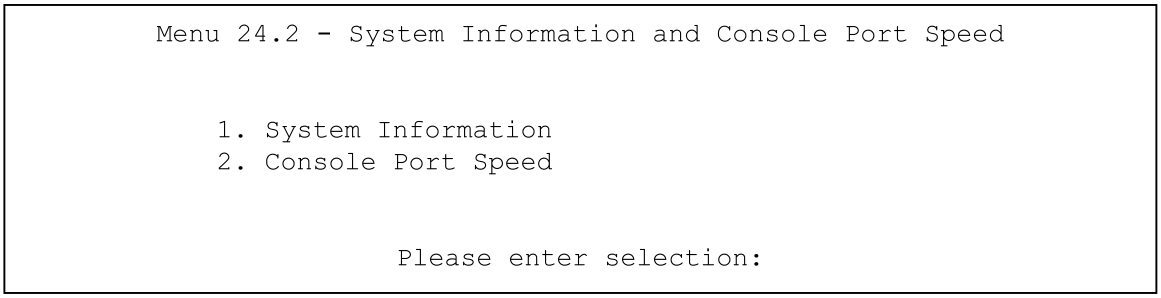
FIELD	DESCRIPTION
Upstream Speed	This shows the upstream transfer rate in kbps.
Downstream Speed	This shows the downstream transfer rate in kbps.
CPU Load	This specifies the percentage of CPU utilization.

33.3 System Information

To get to the System Information:

4. Enter 24 to display **Menu 24 — System Maintenance**.
5. 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:



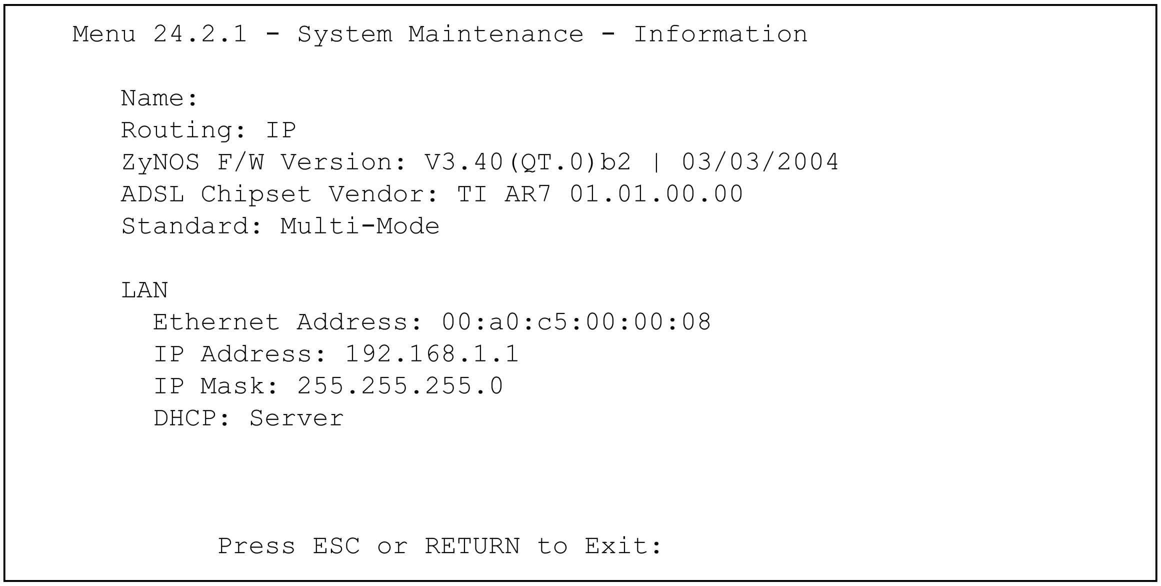
```
          Menu 24.2 - System Information and Console Port Speed


              1. System Information
              2. Console Port Speed


                           Please enter selection:
```

Figure 33-3 Menu 24.2 System Information and Console Port Speed

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

33.3.1 System Information

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



```
Menu 24.2.1 - System Maintenance - Information

   Name:
   Routing: IP
   ZyNOS F/W Version: V3.40(QT.0)b2 | 03/03/2004
   ADSL Chipset Vendor: TI AR7 01.01.00.00
   Standard: Multi-Mode

   LAN
     Ethernet Address: 00:a0:c5:00:00:08
     IP Address: 192.168.1.1
     IP Mask: 255.255.255.0
     DHCP: Server



         Press ESC or RETURN to Exit:
```

Figure 33-4 Menu 24.2.1 System Maintenance : Information

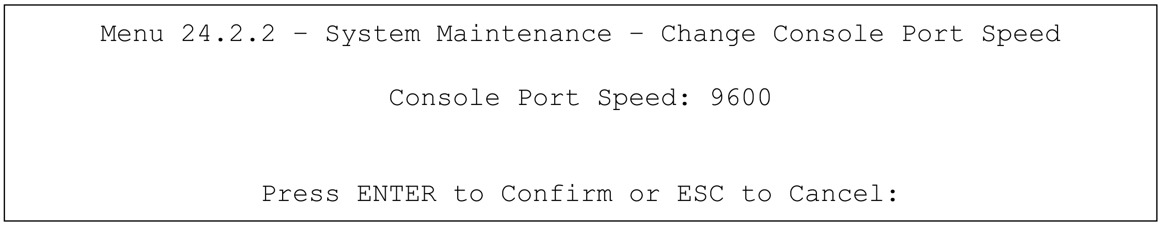
The following table describes the fields in this menu.

Table 33-2 Menu 24.2.1 System Maintenance : Information

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

33.3.2 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.



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

                        Console Port Speed: 9600


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

Figure 33-5 Menu 24.2.2 System Maintenance : Change Console Port Speed

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

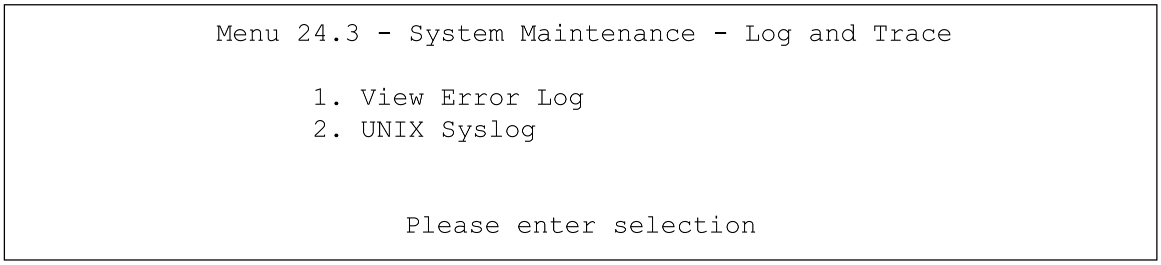
33.4 Log and Trace

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

33.4.1 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:

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

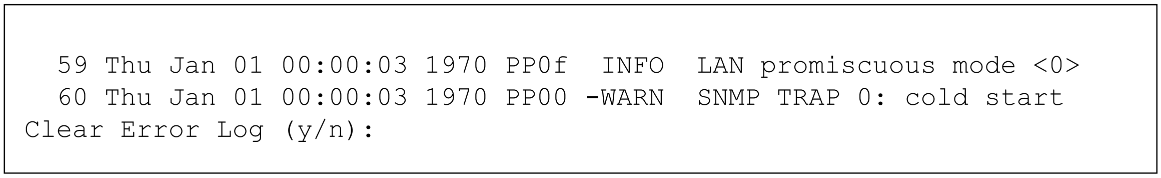


```
             Menu 24.3 - System Maintenance - Log and Trace

                   1. View Error Log
                   2. UNIX Syslog


                         Please enter selection
```

Figure 33-6 Menu 24.3 System Maintenance : Log and Trace

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

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

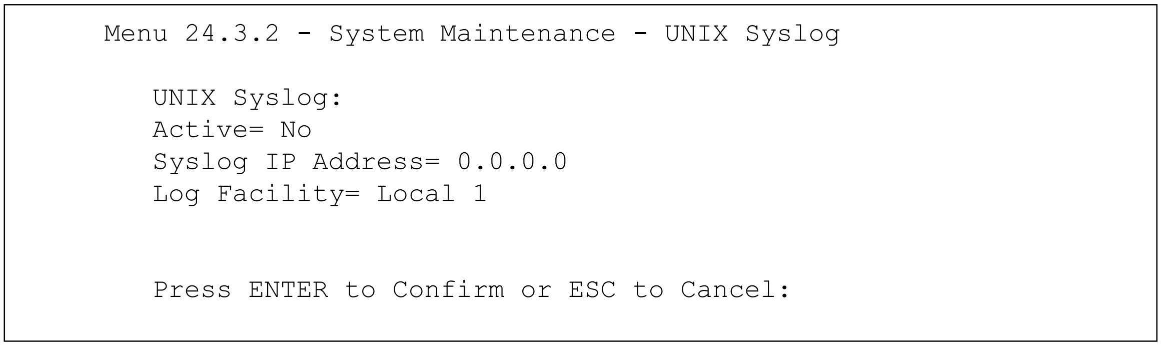


```
  59 Thu Jan 01 00:00:03 1970 PP0f  INFO  LAN promiscuous mode <0>
  60 Thu Jan 01 00:00:03 1970 PP00 -WARN  SNMP TRAP 0: cold start
Clear Error Log (y/n):
```

Figure 33-7 Sample Error and Information Messages

33.4.2 Syslog and Accounting

The Prestige uses the UNIX 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.



```
      Menu 24.3.2 - System Maintenance - UNIX Syslog

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


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

Figure 33-8 Menu 24.3.2 System Maintenance: Syslog and Accounting

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

Table 33-3 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.

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

```
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
```

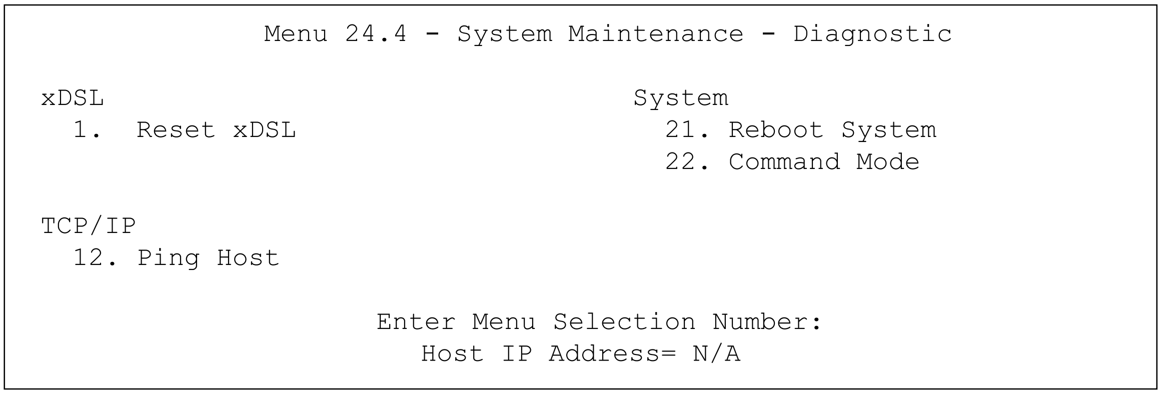
2 - Packet Triggered
SdcmdSyslogSend (SYSLOG_PKTTRI, SYSLOG_NOTICE, String);
String = Packet trigger: Protocol=xx Data=xxxxxxxxxx…..x
Protocol: (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG)
Data: We will send forty-eight Hex characters to the server
Jul 19 11:28:39 192.168.102.2 ZYXEL: Packet Trigger: Protocol=1, Data=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a6b6c6d6e6f7071727374 Jul 19 11:28:56 192.168.102.2 ZYXEL: Packet Trigger: Protocol=1, Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600220008cd40000020405b4 Jul 19 11:29:06 192.168.102.2 ZYXEL: Packet Trigger: Protocol=1, Data=450000282401400 01f06ac12c0a86614ca849a7b0427001700195b451d143013500400007760 0000
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

33.5 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**.



```
              Menu 24.4 - System Maintenance - Diagnostic

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


TCP/IP
  12. Ping Host

                     Enter Menu Selection Number:
                        Host IP Address= N/A
```

Figure 33-9 Menu 24.4 System Maintenance: Diagnostic

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

Table 33-4 Menu 24.4 System Maintenance: 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 34 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.

34.1 Filename Conventions

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

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

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

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

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

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

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

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

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

Table 34-1 Filename Conventions

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

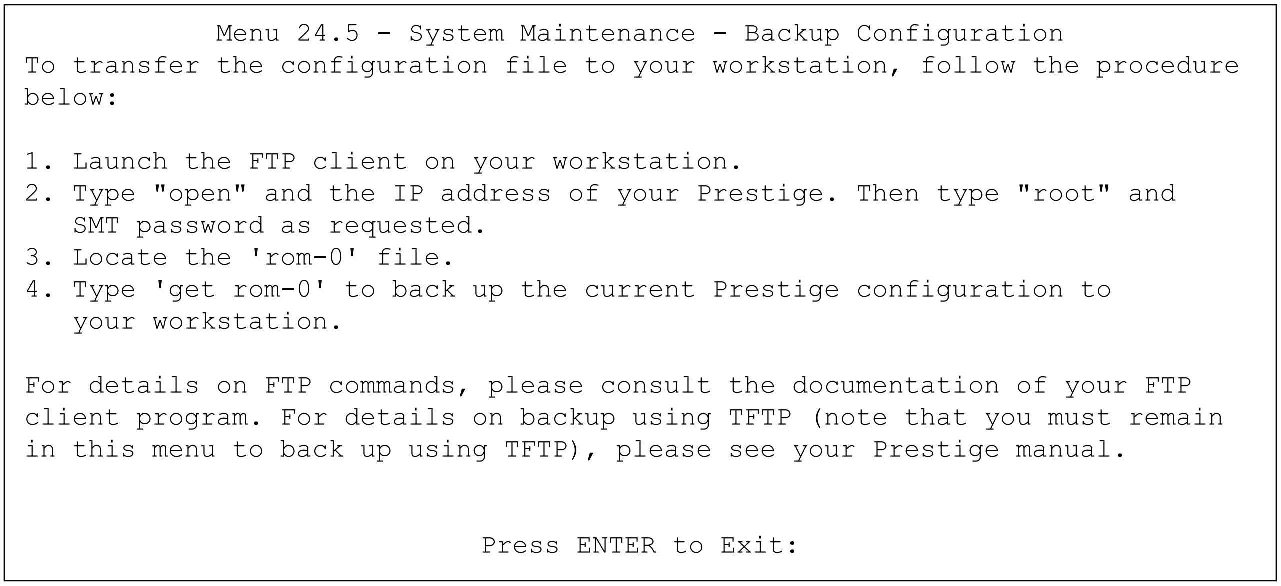
34.2 Backup Configuration

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.

34.2.1 Backup Configuration

Follow the instructions as shown in the next screen.



```
             Menu 24.5 - System Maintenance - Backup Configuration
To transfer the configuration file to your workstation, follow the procedure
below:

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

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


                            Press ENTER to Exit:
```

Figure 34-1 Telnet in Menu 24.5

34.2.2 Using the FTP Command from the Command Line

3. Launch the FTP client on your computer.

4. Enter "open", followed by a space and the IP address of your Prestige.

5. Press [ENTER] when prompted for a username.

6. Enter your password as requested (the default is "1234").

7. Enter "bin" to set transfer mode to binary.

8. 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.

9. Enter "quit" to exit the ftp prompt.

34.2.3 Example of FTP Commands from the Command Line

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

Figure 34-2 FTP Session Example

34.2.4 GUI-based FTP Clients

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

Table 34-2 General Commands for GUI-based FTP Clients

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

34.2.5 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.

34.2.6 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.

34.2.7 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.

34.2.8 GUI-based TFTP Clients

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

Table 34-3 General Commands for GUI-based TFTP Clients

COMMAND	DESCRIPTION
Host	Enter the IP address of the Prestige. 192.168.1.1 is the Prestige's default IP address when shipped.
Send/Fetch	Use "Send" to upload the file to the Prestige and "Fetch" to back up the file on your computer.
Local File	Enter the path and name of the firmware file (*.bin extension) or configuration file (*.rom extension) on your computer.

Table 34-3 General Commands for GUI-based TFTP Clients

COMMAND	DESCRIPTION
Remote File	This is the filename on the Prestige. The filename for the firmware is "ras" and for the configuration file, is "rom-0".
Binary	Transfer the file in binary mode.
Abort	Stop transfer of the file.

Refer to *section 34.2.5* to read about configurations that disallow TFTP and FTP over WAN.

34.3 Restore Configuration

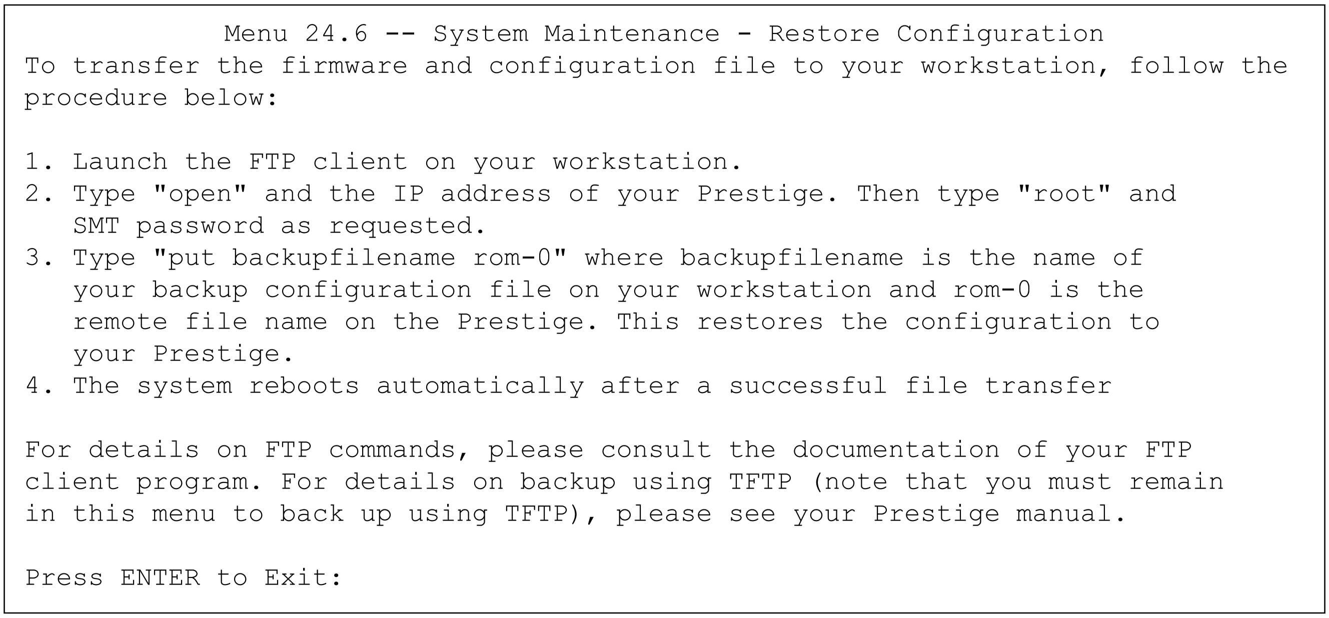
This section shows you how to restore a previously saved configuration. Note that this function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

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

WARNING!
Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR Prestige.

34.3.1 Restore Using FTP

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



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

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

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

Press ENTER to Exit:
```

Figure 34-3 Telnet into Menu 24.6

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.

34.3.2 Restore Using FTP Session Example

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

Figure 34-4 Restore Using FTP Session Example

Refer to *section 34.2.5* to read about configurations that disallow TFTP and FTP over WAN.

34.4 Uploading Firmware and Configuration Files

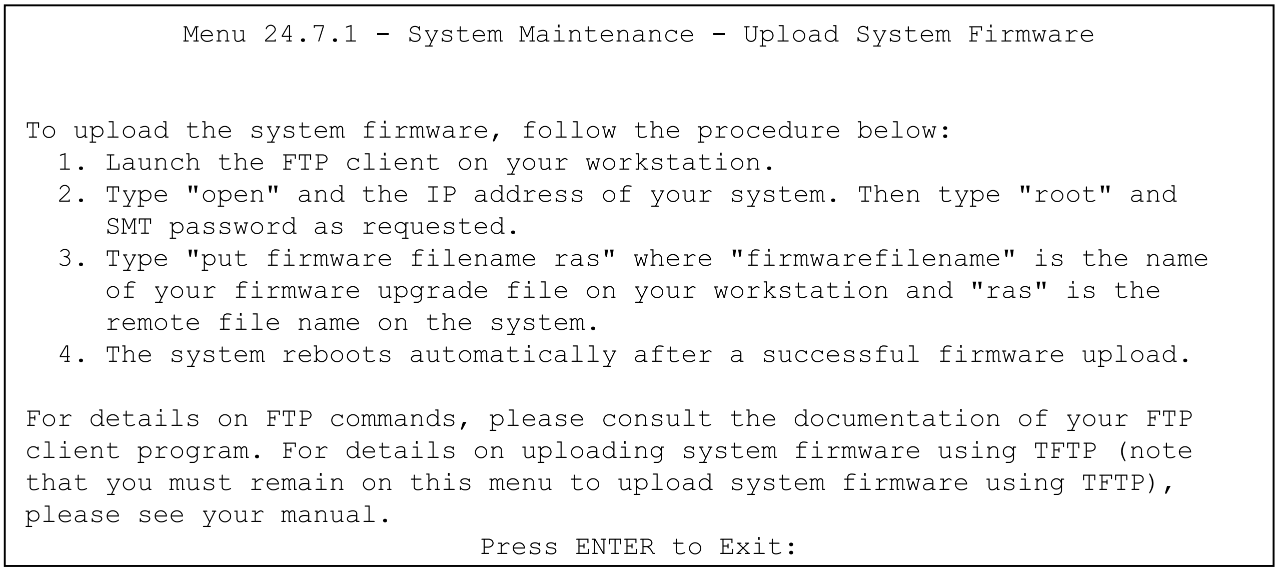
This section shows you how to upload firmware and configuration files. You can upload configuration files by following the procedure in the previous *Restore Configuration* section or by following the instructions in **Menu 24.7.2 – System Maintenance – Upload System Configuration File**.

☞ **WARNING!**
Do not interrupt the file transfer process as this may PERMANENTLY DAMAGE YOUR Prestige.

34.4.1 Firmware File Upload

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

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

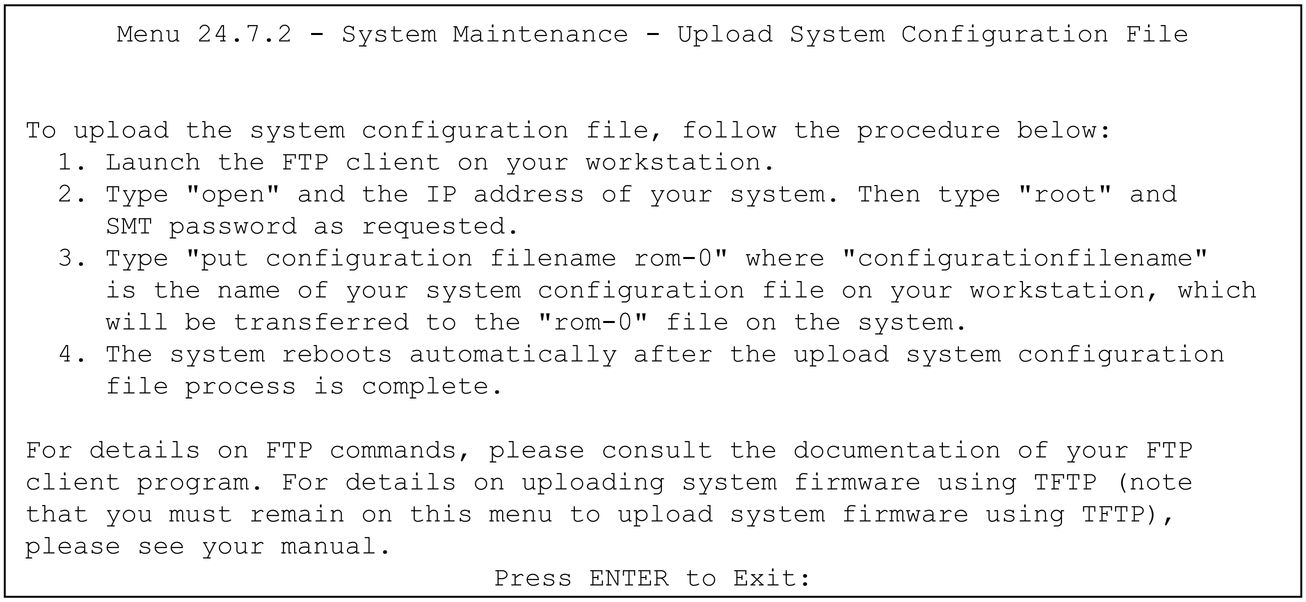


```
          Menu 24.7.1 - System Maintenance - Upload System Firmware


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

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

Figure 34-5 Telnet Into Menu 24.7.1 Upload System Firmware

34.4.2 Configuration File Upload

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



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


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

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

Figure 34-6 Telnet Into Menu 24.7.2 System Maintenance

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

34.4.3 FTP File Upload Command from the DOS Prompt Example

1. Launch the FTP client on your computer.
2. Enter “open”, followed by a space and the IP address of your Prestige.

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

The Prestige automatically restarts after a successful file upload.

34.4.4 FTP Session Example of Firmware File Upload

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

Figure 34-7 FTP Session Example of Firmware File Upload

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

Refer to *section 34.2.5* to read about configurations that disallow TFTP and FTP over WAN.

34.4.5 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 "command 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.

34.4.6 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).

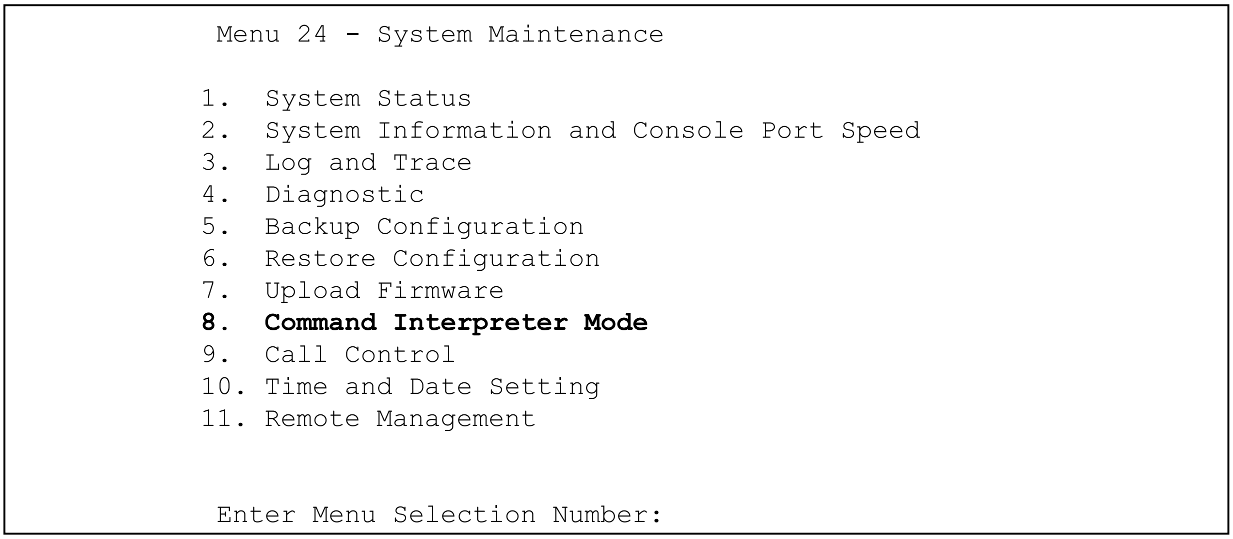
Commands that you may see in GUI-based TFTP clients are listed earlier in this chapter.

Chapter 35
System Maintenance

This chapter leads you through SMT menus 24.8 to 24.10.

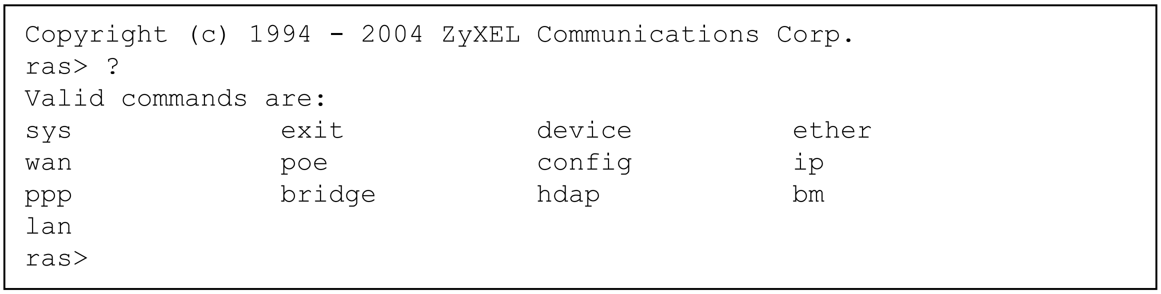
35.1 Command Interpreter Mode

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



```
             Menu 24 - System Maintenance

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


             Enter Menu Selection Number:
```

Figure 35-1 Command Mode in Menu 24



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

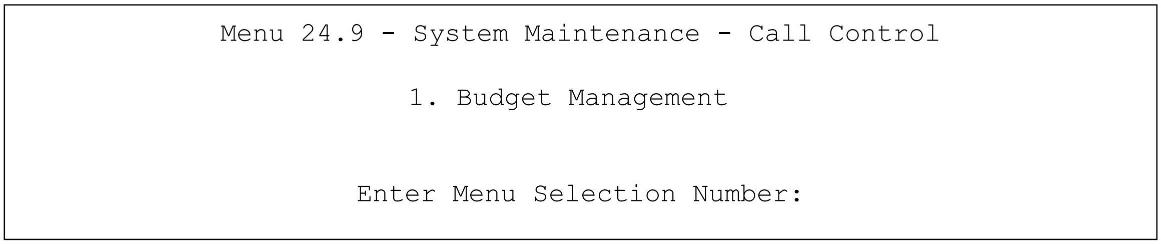
Figure 35-2 Valid Commands

35.2 Call Control Support

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

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

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

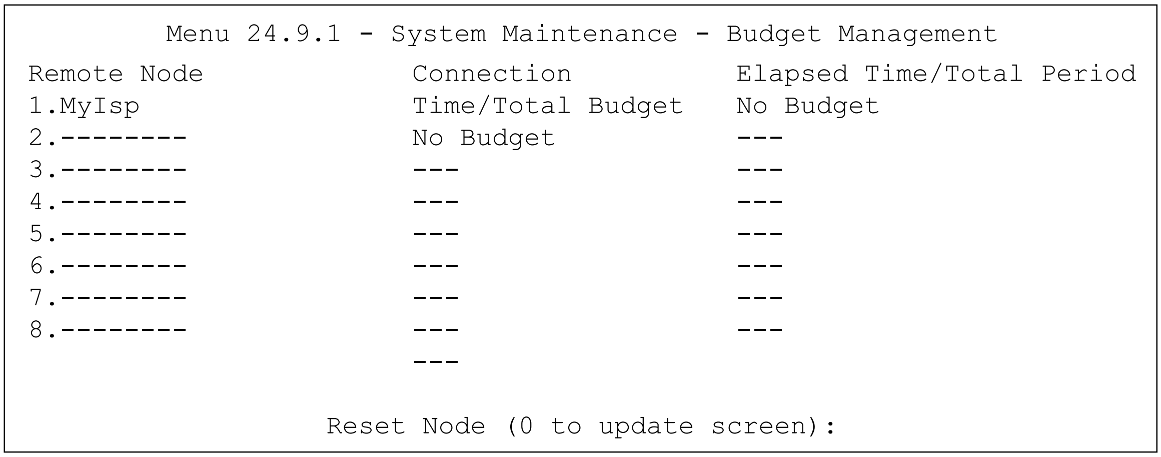


```
            Menu 24.9 - System Maintenance - Call Control

                        1. Budget Management


                     Enter Menu Selection Number:
```

Figure 35-3 Menu 24.9 System Maintenance : Call Control

35.2.1 Budget Management

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



```
         Menu 24.9.1 - System Maintenance - Budget Management
Remote Node              Connection          Elapsed Time/Total Period
1.MyIsp                  Time/Total Budget   No Budget
2.--------               No Budget           ---
3.--------               ---                 ---
4.--------               ---                 ---
5.--------               ---                 ---
6.--------               ---                 ---
7.--------               ---                 ---
8.--------               ---                 ---
                         ---

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

Figure 35-4 Menu 24.9.1 System Maintenance: Budget Management

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

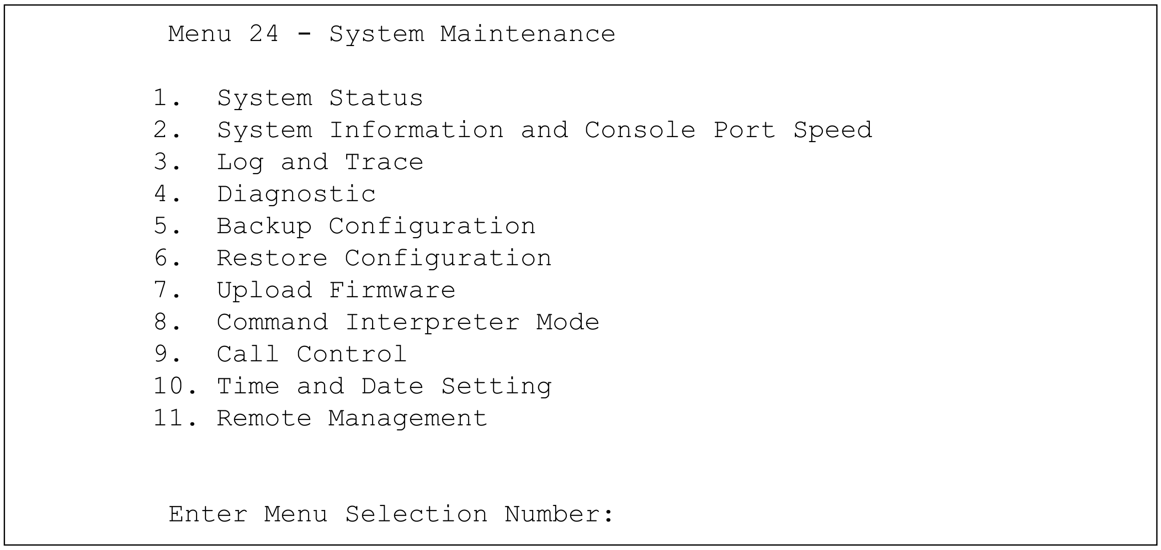
Table 35-1 Menu 24.9.1 System Maintenance: Budget Management

FIELD	DESCRIPTION	EXAMPLE
Remote Node	Enter the index number of the remote node you want to reset (just one in this case)	1
Connection Time/Total Budget	This is the total connection time that has gone by (within the allocated budget that you set in menu 11.1.	5/10 means that 5 minutes out of a total allocation of 10 minutes have lapsed.
Elapsed Time/Total Period	The period is the time cycle in hours that the allocation budget is reset (see menu 11.1.) The elapsed time is the time used up within this period.	0.5/1 means that 30 minutes out of the 1 hour time period has lapsed.
Enter "0" to update the screen or press [ESC] to return to the previous screen.		

35.3 Time and Date Setting

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

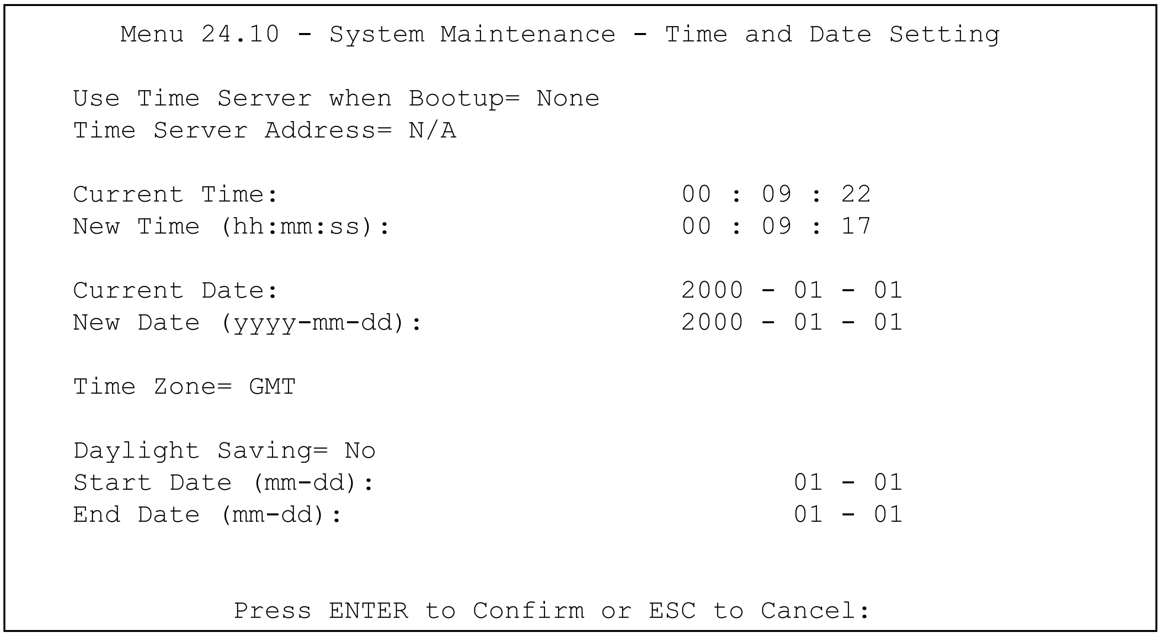
Select menu 24 in the main menu to open **Menu 24 System Maintenance**, as shown next.



```
          Menu 24 - System Maintenance

         1.  System Status
         2.  System Information 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 35-5 Menu 24 System Maintenance

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



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

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

    Current Time:                        00 : 09 : 22
    New Time (hh:mm:ss):                 00 : 09 : 17

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

    Time Zone= GMT

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


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

Figure 35-6 Menu 24.10 System Maintenance: Time and Date Setting

Table 35-2 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 New Time	This field displays an updated time only when you reenter this menu. Enter the new time in hour, minute and second format.
Current Date New Date	This field displays an updated date only when you re-enter this menu. Enter the new date in year, month and day format.
Time Zone	Press [SPACE BAR] and then [ENTER] to set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Saving	If you use daylight savings time, then choose **Yes**.
Start Date	If using daylight savings time, enter the month and day that it starts on.
End Date	If using daylight savings time, enter the month and day that it ends on
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.	

35.3.1 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 36 Remote Management

This chapter covers remote management (SMT menu 24.11).

36.1 Remote Management Overview

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

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

36.2 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**.

36.2.1 Remote Management Setup

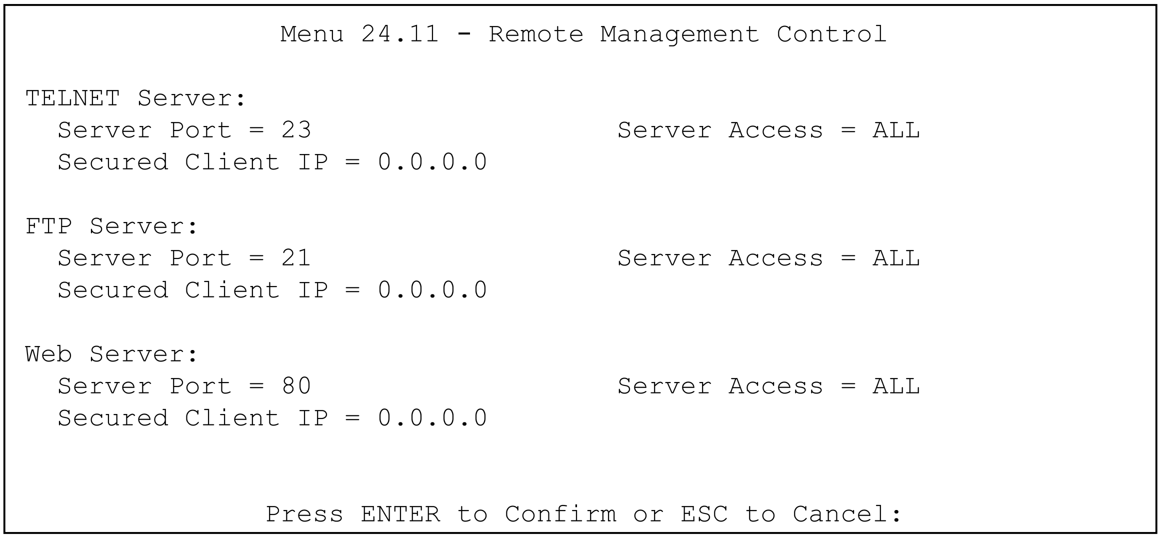
You may manage your Prestige from a remote location via:

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

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

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

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



```
                  Menu 24.11 - Remote Management Control

TELNET Server:
  Server Port = 23                    Server Access = ALL
  Secured Client IP = 0.0.0.0

FTP Server:
  Server Port = 21                    Server Access = ALL
  Secured Client IP = 0.0.0.0

Web Server:
  Server Port = 80                    Server Access = ALL
  Secured Client IP = 0.0.0.0


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

Figure 36-1 Menu 24.11 Remote Management Control

The following table describes the fields in this menu.

Table 36-1 Menu 24.11 Remote Management Control

FIELD	DESCRIPTION	EXAMPLE
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.	23
Access	Select the access interface (if any) by pressing the [SPACE BAR]. Choices are: **LAN only**, **WAN only**, **All** or **Disable**. The default is **LAN only**.	**LAN only**
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.	0.0.0.0
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.		

36.2.2 Remote Management Limitations

Remote management over LAN or WAN will not work when:

- A filter in menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a Telnet, FTP or Web service.
- You have disabled that service in menu 24.11.
- The IP address in the **Secured Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the Prestige will disconnect the session immediately.
- There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.
- There is a firewall rule that blocks it.

36.3 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.

36.4 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 37
IP Policy Routing

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

37.1 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.

37.2 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.

37.3 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.

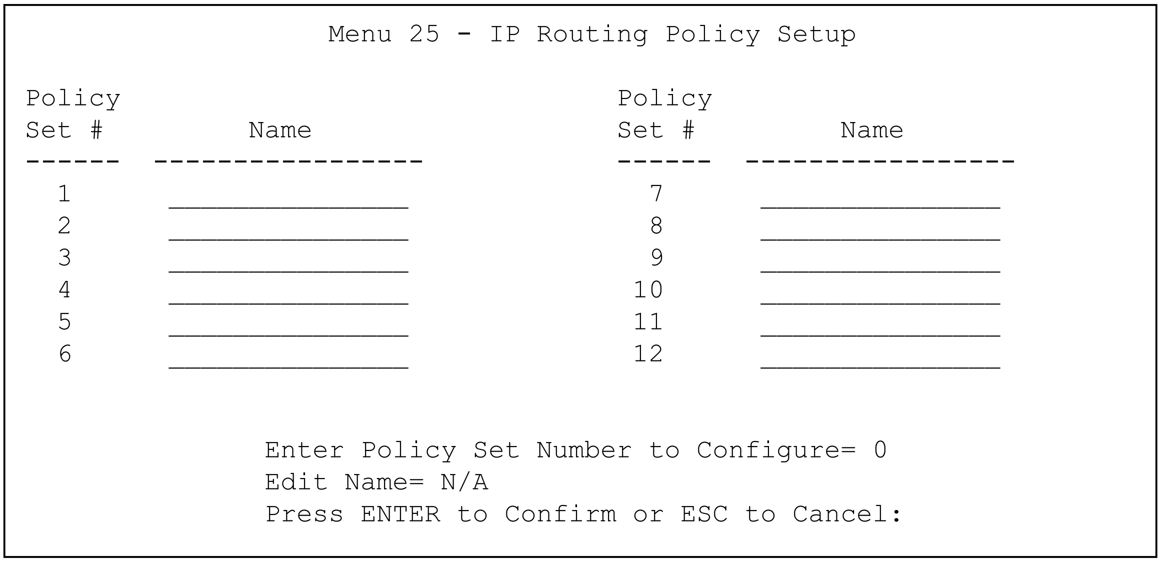
The actions that can be taken include:

- 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.

37.4 IP Routing Policy Setup

Menu 25 shows all the policies defined.



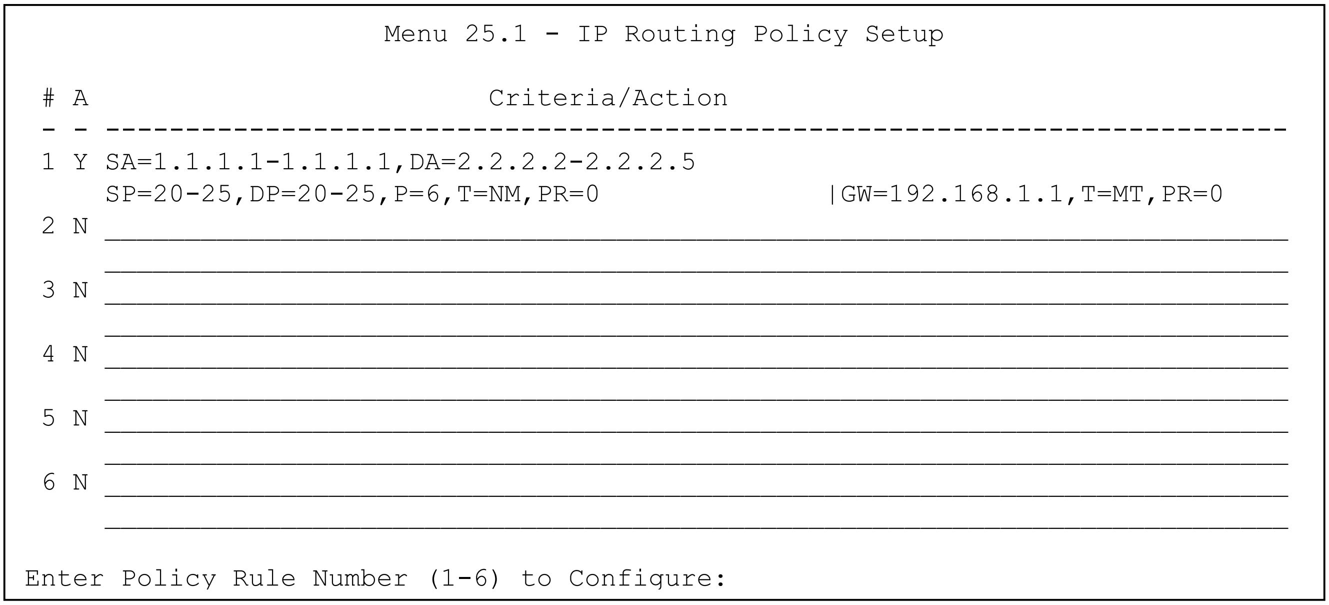
```
                    Menu 25 - IP Routing Policy Setup

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


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

Figure 37-1 Menu 25 IP Routing Policy Setup

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.



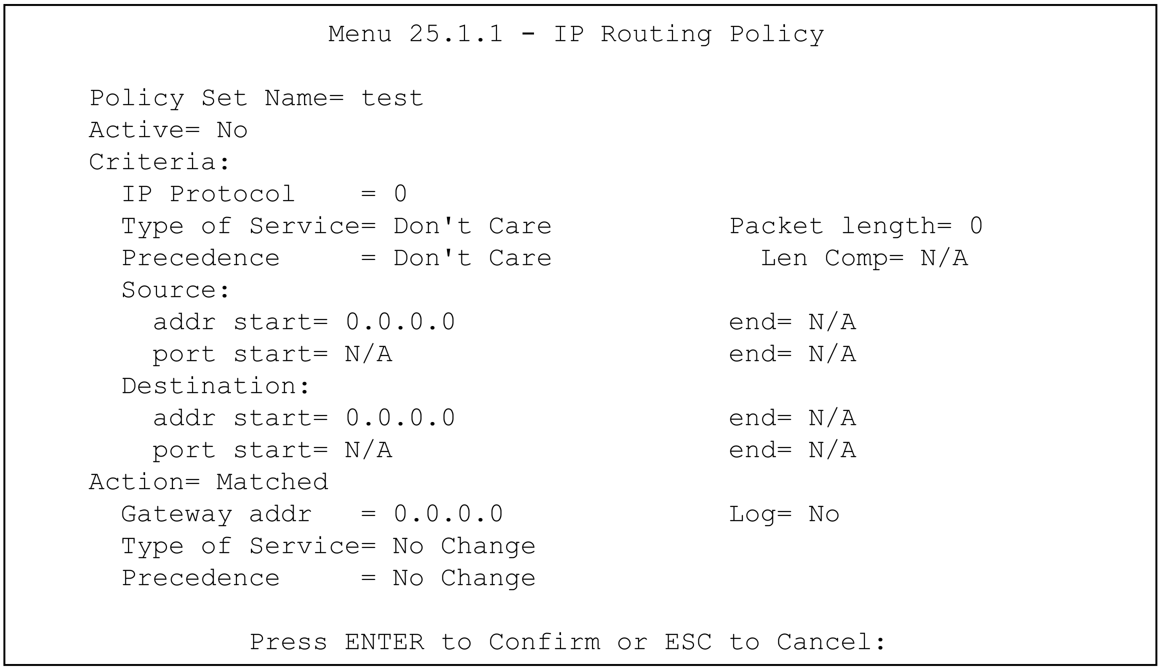
```
                         Menu 25.1 - IP Routing Policy Setup

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

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

Figure 37-2 Menu 25.1 IP Routing Policy Setup

Table 37-1 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.



```
                   Menu 25.1.1 - IP Routing Policy

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

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

Figure 37-3 Menu 25.1.1 IP Routing Policy

The following table describes the fields in this menu.

Table 37-2 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**.
Gateway addr	Defines the outgoing gateway address. The gateway must be on the same subnet as the Prestige if it is on the LAN, otherwise, the gateway must be the IP address of a remote node. The default gateway is specified as 0.0.0.0.
Type of Service	Set the new TOS value of the outgoing packet. Prioritize incoming network traffic by choosing **No Change**, **Normal**, **Min Delay**, **Max Thruput**, **Max Reliable** or **Min Cost**.
Precedence	Set the new outgoing packet precedence value. Values are **0** to **7** or **No Change**.
Log	Press [SPACE BAR] and then [ENTER] to select **Yes** to make an entry in the system log when a policy is executed.
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.	

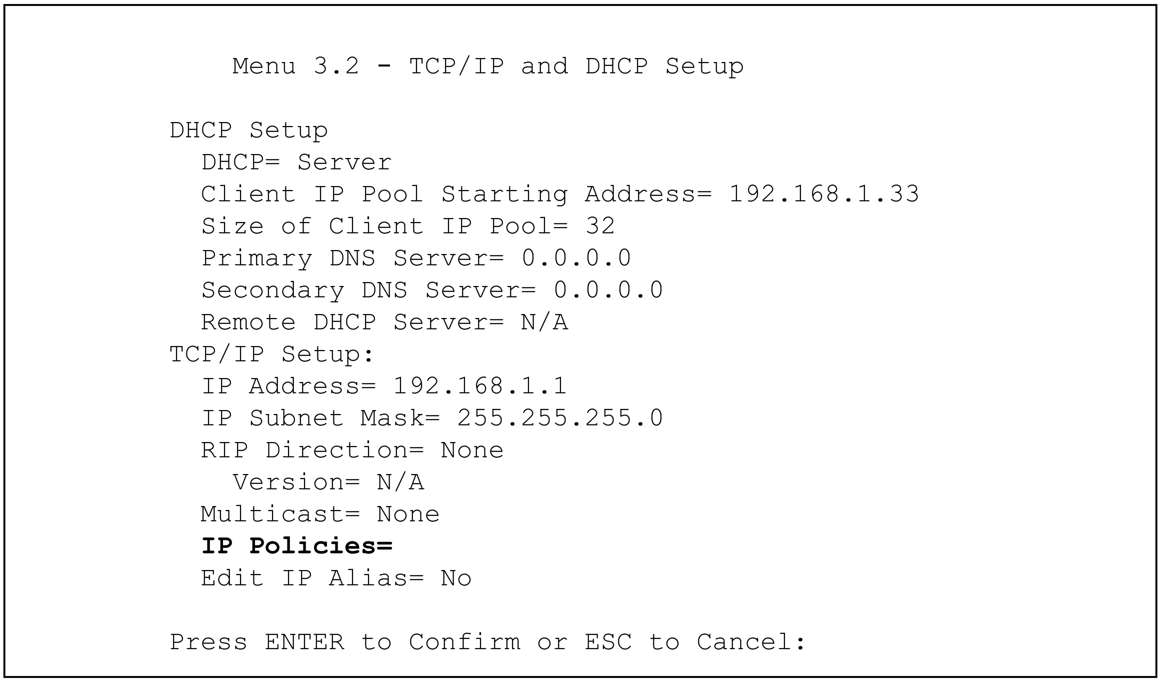
37.5 Applying an IP Policy

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

37.5.1 Ethernet IP Policies

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

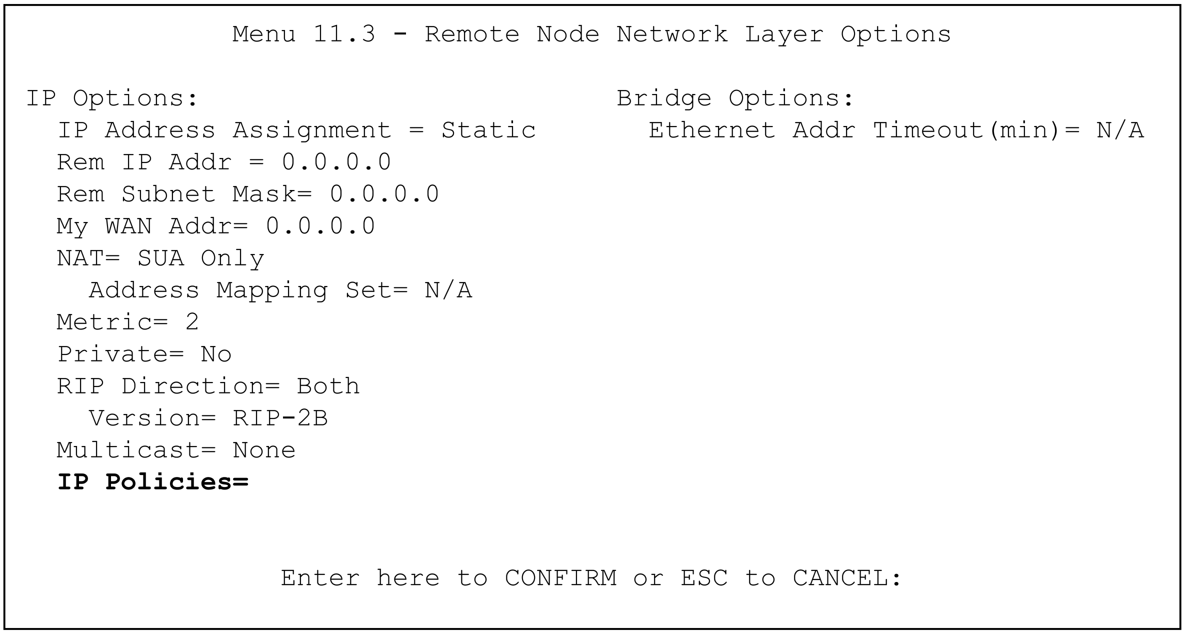
You can choose up to four IP policy sets (from 12) by typing their numbers separated by commas, for example, 2, 4, 7, 9.



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

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

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

Figure 37-4 Menu 3.2 TCP/IP and DHCP Ethernet Setup

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



```
              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:
```

Figure 37-5 Menu 11.3 Remote Node Network Layer Options

37.6 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.

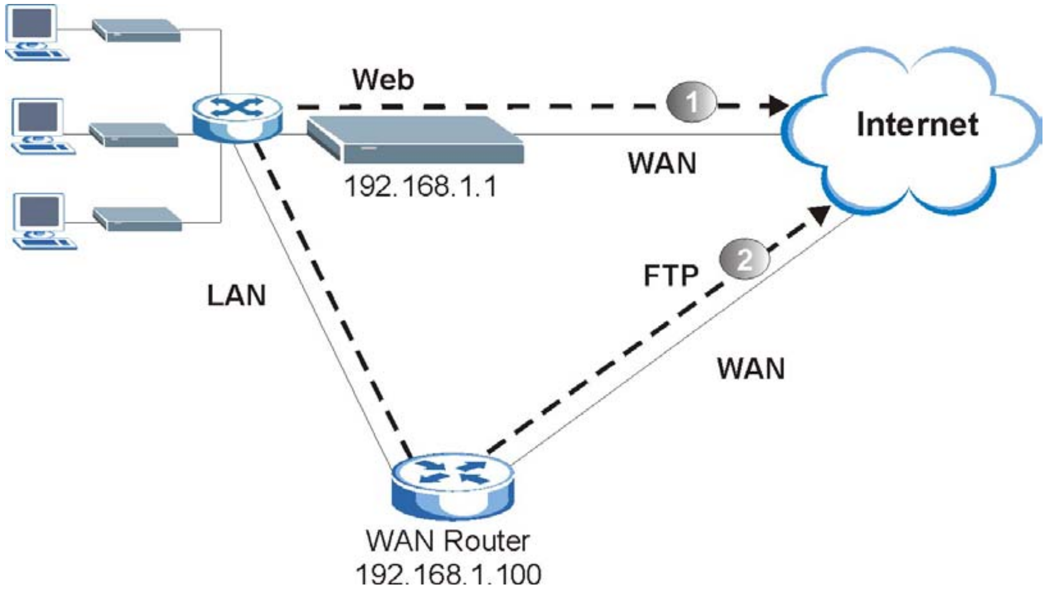
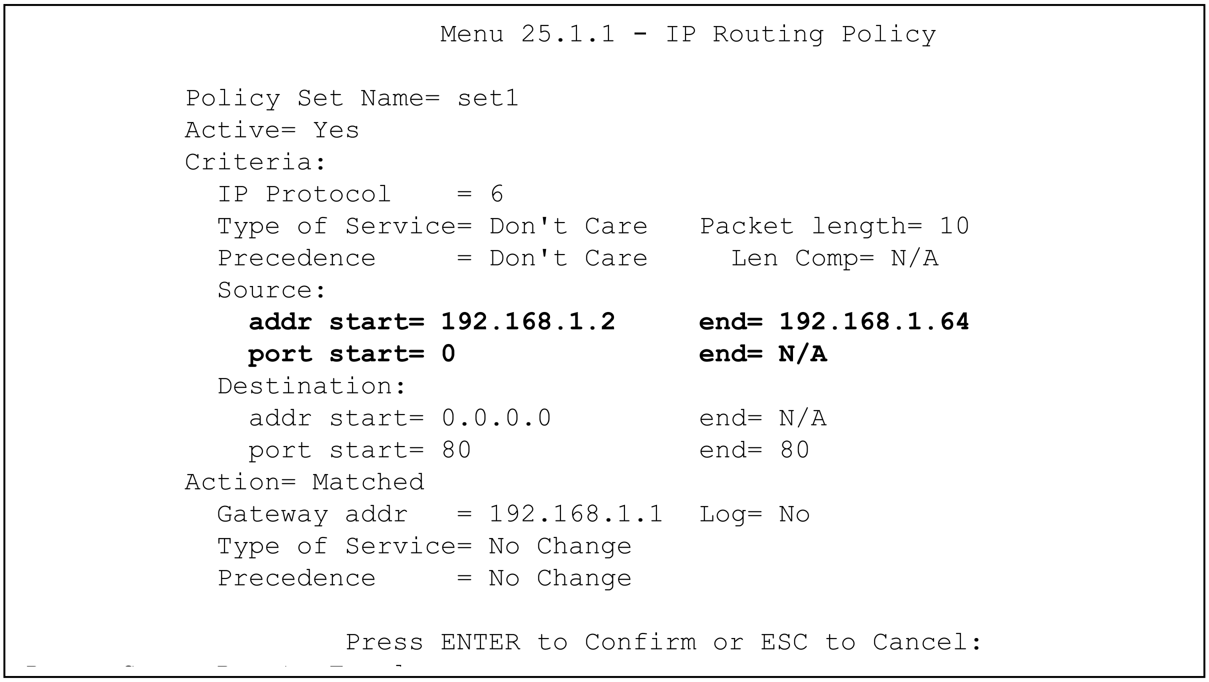


Figure 37-6 Example of IP Policy Routing

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

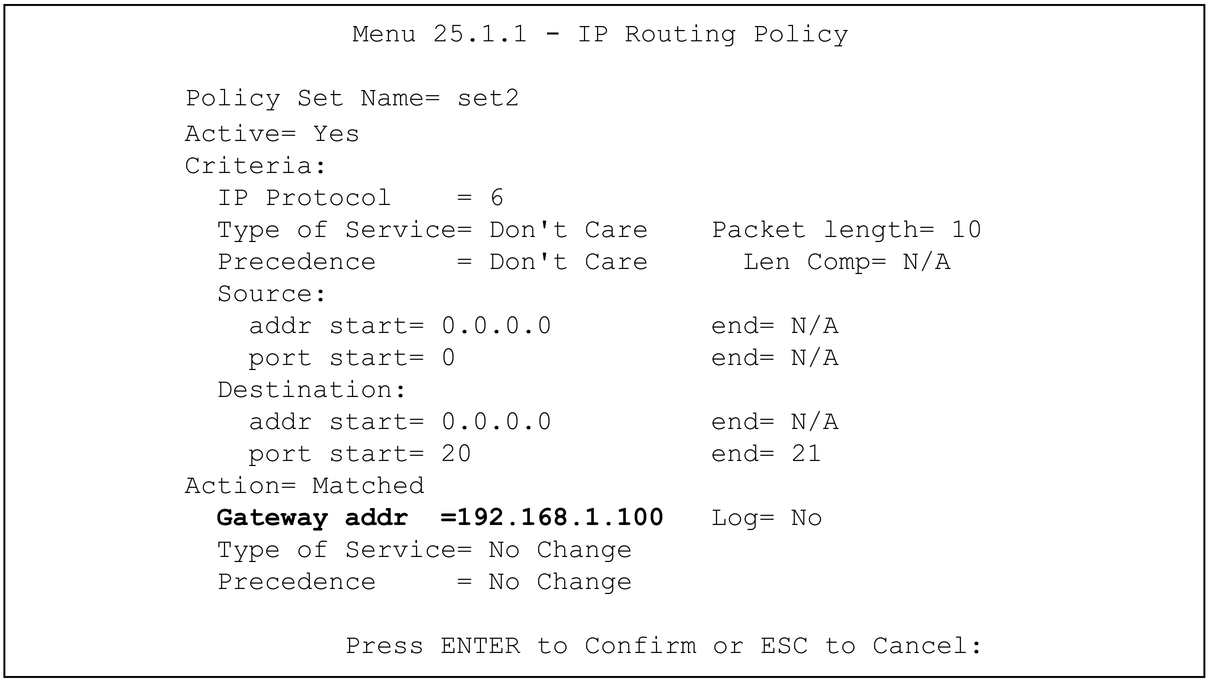
1. Create a routing policy set in menu 25.
2. Create a rule for this set in **Menu 25.1.1 — IP Routing Policy** as shown next.



```
                           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= 192.168.1.2      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:
```

Figure 37-7 IP Routing Policy Example

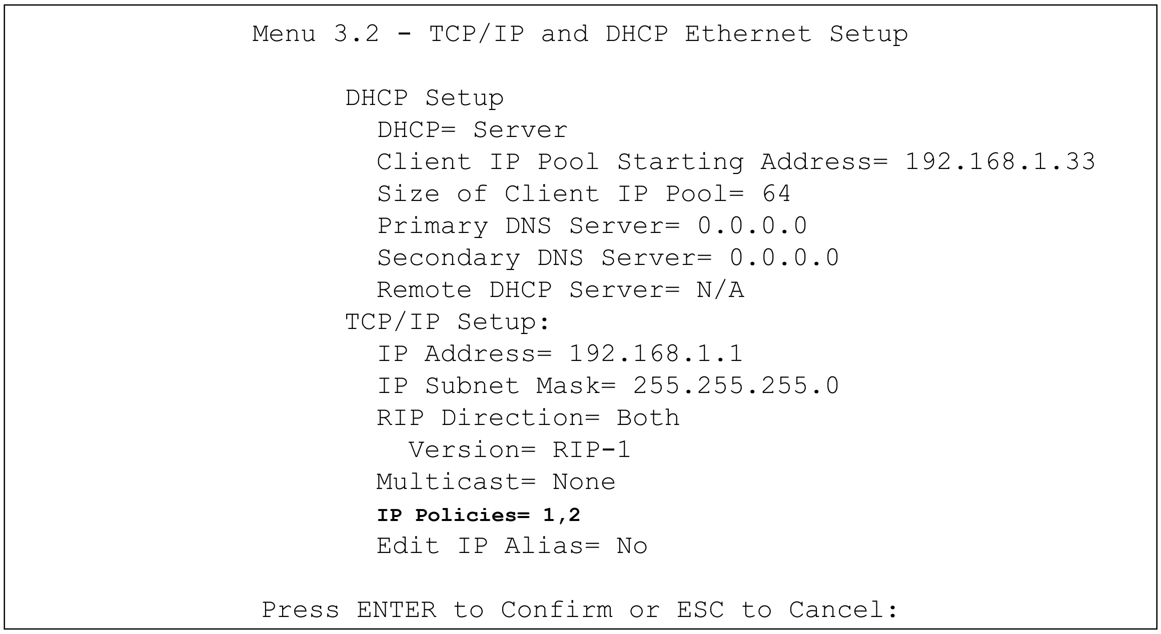
3. Check **Menu 25.1 — IP Routing Policy Setup** to see if the rule is added correctly.
4. Create another policy set in menu 25.
5. Create a rule in menu 25.1 for this set to route packets from any host (IP=0.0.0.0 means any host) with protocol TCP and port FTP access through another gateway (192.168.1.100).



```
                     Menu 25.1.1 - IP Routing Policy

           Policy Set Name= set2
           Active= Yes
           Criteria:
             IP Protocol    = 6
             Type of Service= Don't Care    Packet length= 10
             Precedence     = Don't Care      Len Comp= N/A
             Source:
               addr start= 0.0.0.0          end= N/A
               port start= 0                end= N/A
             Destination:
               addr start= 0.0.0.0          end= N/A
               port start= 20               end= 21
           Action= Matched
             Gateway addr  =192.168.1.100   Log= No
             Type of Service= No Change
             Precedence     = No Change

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

Figure 37-8 IP Routing Policy Example

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.



```
                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:
```

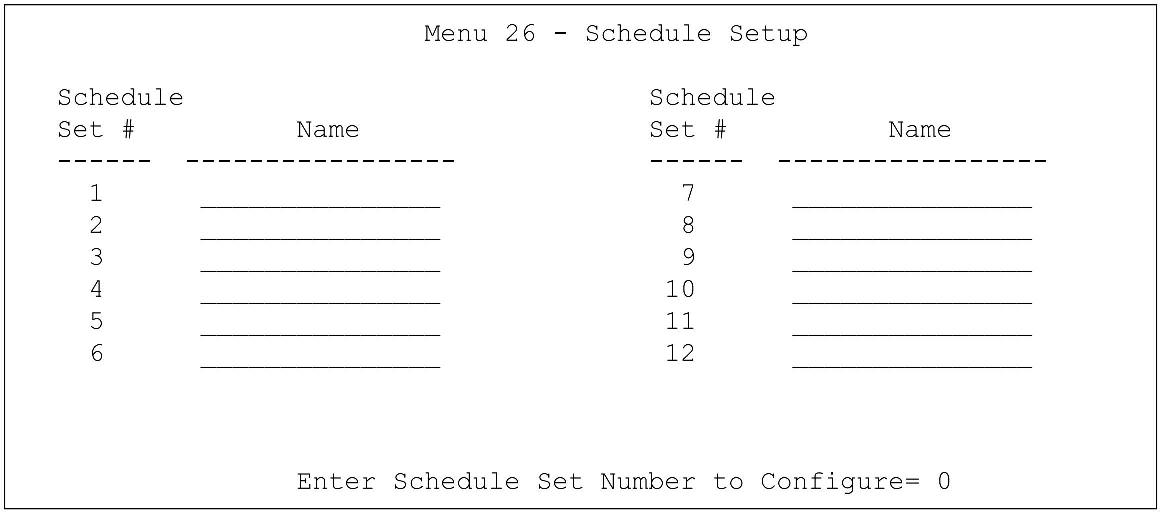
Figure 37-9 Applying IP Policies Example

Chapter 38
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.

38.1 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.



```
                       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
```

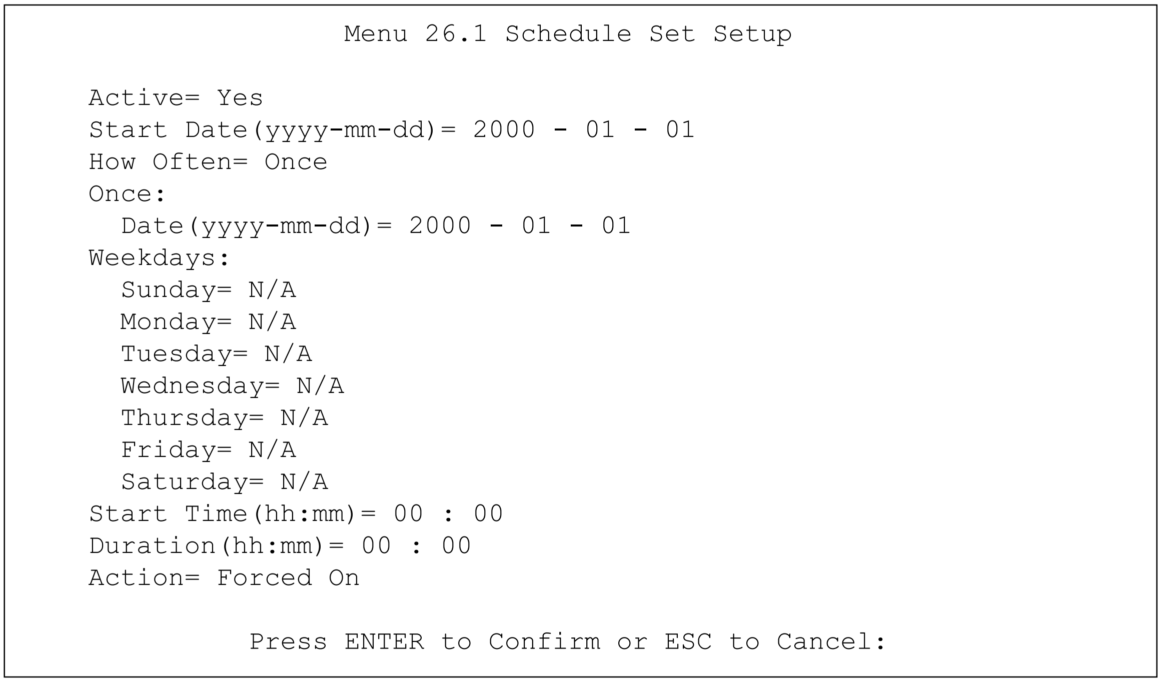
Figure 38-1 Menu 26 Schedule Setup

Lower numbered sets take precedence over higher numbered sets thereby avoiding scheduling conflicts. For example, if sets 1, 2 ,3 and 4 in are applied in the remote node then set 1 will take precedence over set 2, 3 and 4 as the Prestige, by default, applies the lowest numbered set first. Set 2 will take precedence over set 3 and 4, and so on.

You can design up to 12 schedule sets but you can only apply up to four schedule sets for a remote node.

To delete a schedule set, enter the set number and press **[SPACE BAR]** and then **[ENTER]** (or delete) in the **Edit Name** field.

To setup a schedule set, select the schedule set you want to setup from menu 26 (1-12) and press [ENTER] to see **Menu 26.1 — Schedule Set Setup** as shown next.



```
                     Menu 26.1 Schedule Set Setup

     Active= Yes
     Start Date(yyyy-mm-dd)= 2000 - 01 - 01
     How Often= Once
     Once:
       Date(yyyy-mm-dd)= 2000 - 01 - 01
     Weekdays:
       Sunday= N/A
       Monday= N/A
       Tuesday= N/A
       Wednesday= N/A
       Thursday= N/A
       Friday= N/A
       Saturday= N/A
     Start Time(hh:mm)= 00 : 00
     Duration(hh:mm)= 00 : 00
     Action= Forced On

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

Figure 38-2 Menu 26.1 Schedule Set Setup

If a connection has been already established, your Prestige will not drop it. Once the connection is dropped manually or it times out, then that remote node can't be triggered up until the end of the **Duration**.

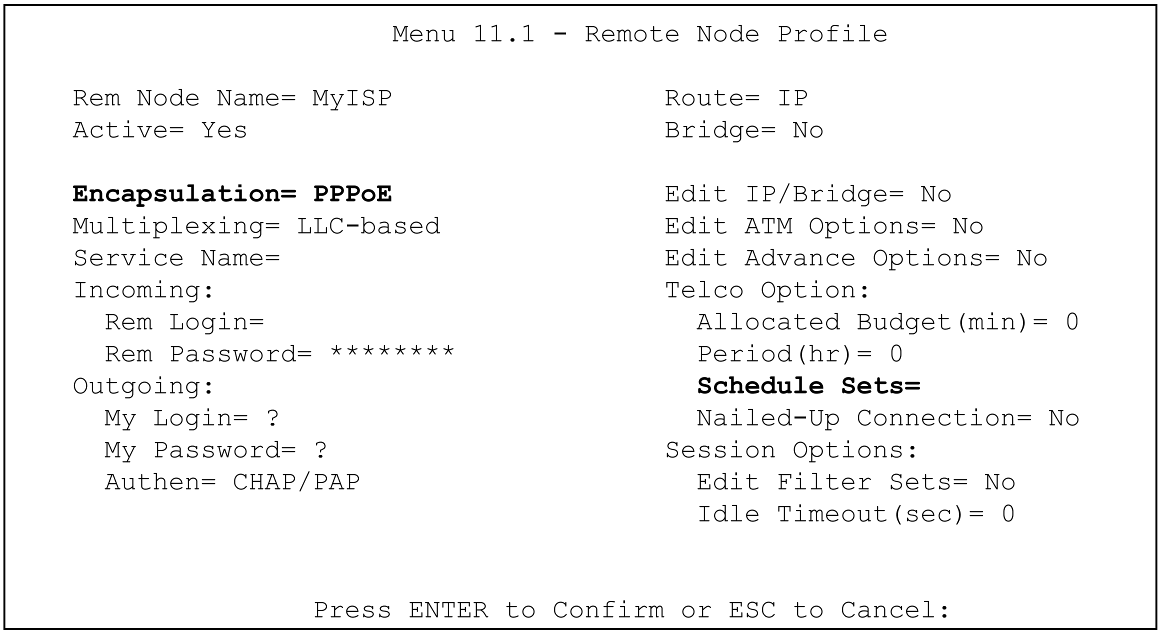
Table 38-1 Menu 26.1 Schedule Set Setup

FIELD	DESCRIPTION	EXAMPLE
Active	Press [SPACE BAR] to select **Yes** or **No**. Choose **Yes** and press [ENTER] to activate the schedule set.	**Yes**
Start Date	Enter the start date when you wish the set to take effect in year -month-date format. Valid dates are from the present to 2036-February-5.	2000-01-01
How Often	Should this schedule set recur weekly or be used just once only? Press the [SPACE BAR] and then [ENTER] to select **Once** or **Weekly**. Both these options are mutually exclusive. If **Once** is selected, then all weekday settings are **N/A**. When **Once** is selected, the schedule rule deletes automatically after the scheduled time elapses.	**Once**
Once: Date	If you selected **Once** in the **How Often** field above, then enter the date the set should activate here in year-month-date format.	2000-01-01
Weekday: Day	If you selected **Weekly** in the **How Often** field above, then select the day(s) when the set should activate (and recur) by going to that day(s) and pressing [SPACE BAR] to select **Yes**, then press [ENTER].	**Yes** **No** **N/A**
Start Time	Enter the start time when you wish the schedule set to take effect in hour-minute format.	09:00
Duration	Enter the maximum length of time this connection is allowed in hour-minute format.	08:00

Table 38-1 Menu 26.1 Schedule Set Setup

FIELD	DESCRIPTION	EXAMPLE
Action	**Forced On** means that the connection is maintained whether or not there is a demand call on the line and will persist for the time period specified in the **Duration** field. **Forced Down** means that the connection is blocked whether or not there is a demand call on the line. **Enable Dial-On-Demand** means that this schedule permits a demand call on the line. **Disable Dial-On-Demand** means that this schedule prevents a demand call on the line.	**Forced On**
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to confirm or ESC to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

Once your schedule sets are configured, you must then apply them to the desired remote node(s). Enter 11 from the **Main Menu** and then enter the target remote node index. Using [SPACE BAR], select **PPPoE** or **PPPoA** in the **Encapsulation** field and then press [ENTER] to make the schedule sets field available as shown next.



```
                        Menu 11.1 - Remote Node Profile

    Rem Node Name= 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= No
    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:
```

Figure 38-3 Applying Schedule Set(s) to a Remote Node (PPPoE)

You can apply up to four schedule sets, separated by commas, for one remote node. Change the schedule set numbers to your preference(s).

Chapter 39
Internal SPTGEN

39.1 Internal SPTGEN Overview

Internal SPTGEN (System Parameter Table Generator) is a configuration text file useful for efficient configuration of multiple Prestiges. Internal SPTGEN lets you configure, save and upload multiple menus at the same time using just one configuration text file – eliminating the need to navigate and configure individual SMT menus for each Prestige.

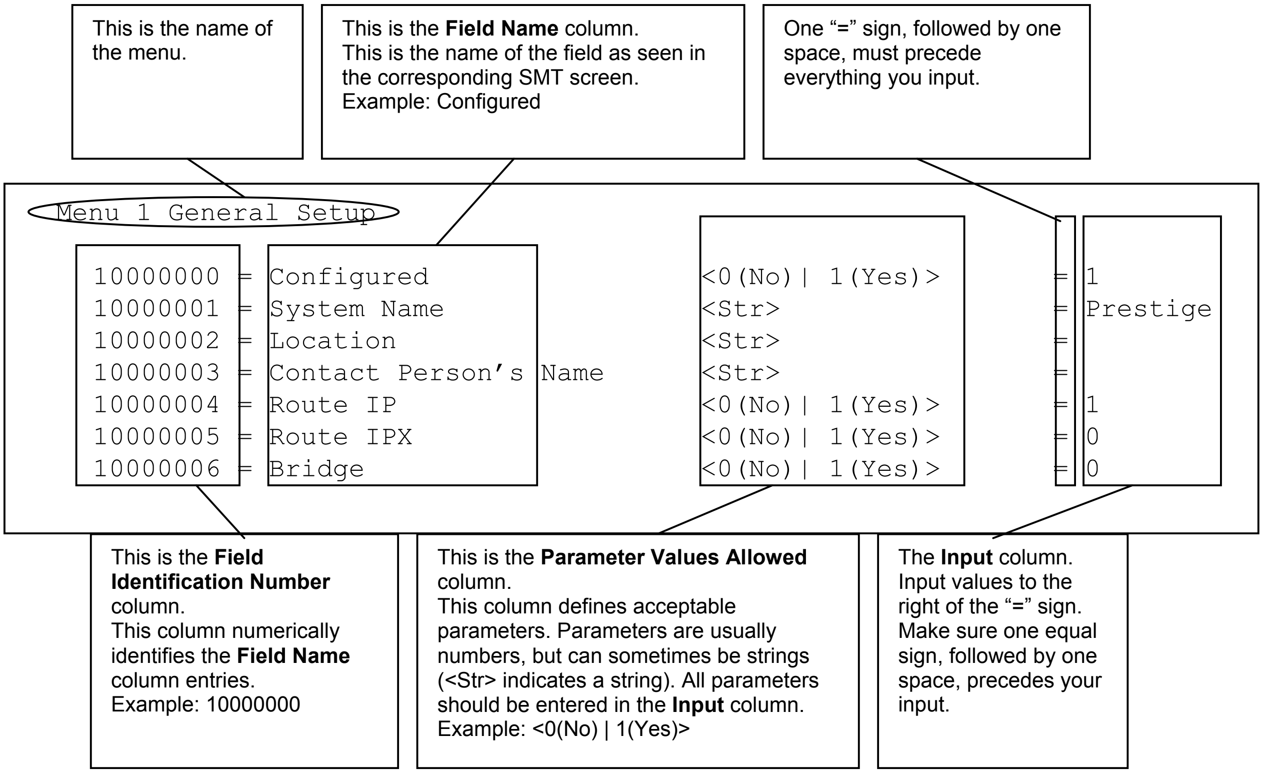
39.2 The Configuration Text File Format

All Internal SPTGEN text files conform to the following format:

<field identification number = field name = parameter values allowed = input>,

where `<input>` is your input conforming to `<parameter values allowed>`.

The figure shown next is an example of an Internal SPTGEN text file.



This is the name of the menu.

This is the **Field Name** column.
This is the name of the field as seen in the corresponding SMT screen.
Example: Configured

One "=" sign, followed by one space, must precede everything you input.

```
Menu 1 General Setup

10000000 = Configured                    <0(No)| 1(Yes)>       = 1
10000001 = System Name                   <Str>                 = Prestige
10000002 = Location                      <Str>                 =
10000003 = Contact Person's Name         <Str>                 =
10000004 = Route IP                      <0(No)| 1(Yes)>       = 1
10000005 = Route IPX                     <0(No)| 1(Yes)>       = 0
10000006 = Bridge                        <0(No)| 1(Yes)>       = 0
```

This is the **Field Identification Number** column.
This column numerically identifies the **Field Name** column entries.
Example: 10000000

This is the **Parameter Values Allowed** column.
This column defines acceptable parameters. Parameters are usually numbers, but can sometimes be strings (<Str> indicates a string). All parameters should be entered in the **Input** column.
Example: <0(No) | 1(Yes)>

The **Input** column.
Input values to the right of the "=" sign.
Make sure one equal sign, followed by one space, precedes your input.

Figure 39-1 Configuration Text File Format: Column Descriptions

☞ **DO NOT alter or delete any field except parameters in the** Input **column.**

For more text file examples, refer to the *Example Internal SPTGEN Screens Appendix*.

39.2.1 Internal SPTGEN File Modification - Important Points to Remember

- Each parameter you enter must be preceded by one "="sign and one space.
- Some parameters are dependent on others. For example, if you disable the **Configured** field in menu 1 (see *Figure 39-1*), then you disable every field in this menu.
- If you enter a parameter that is invalid in the **Input** column, the Prestige will not save the configuration and the command line will display the **Field Identification Number**. *Figure 39-2*, shown next, is an example of what the Prestige displays if you enter a value other than "0" or "1" in the **Input** column of **Field Identification Number** 1000000 (refer to *Figure 39-1*).

```
field value is not legal error:-1
ROM-t is not saved, error Line ID:10000000
reboot to get the original configuration
Bootbase Version: V2.02 | 2/22/2001 13:33:11
RAM: Size = 8192 Kbytes
FLASH: Intel 8M *2
```

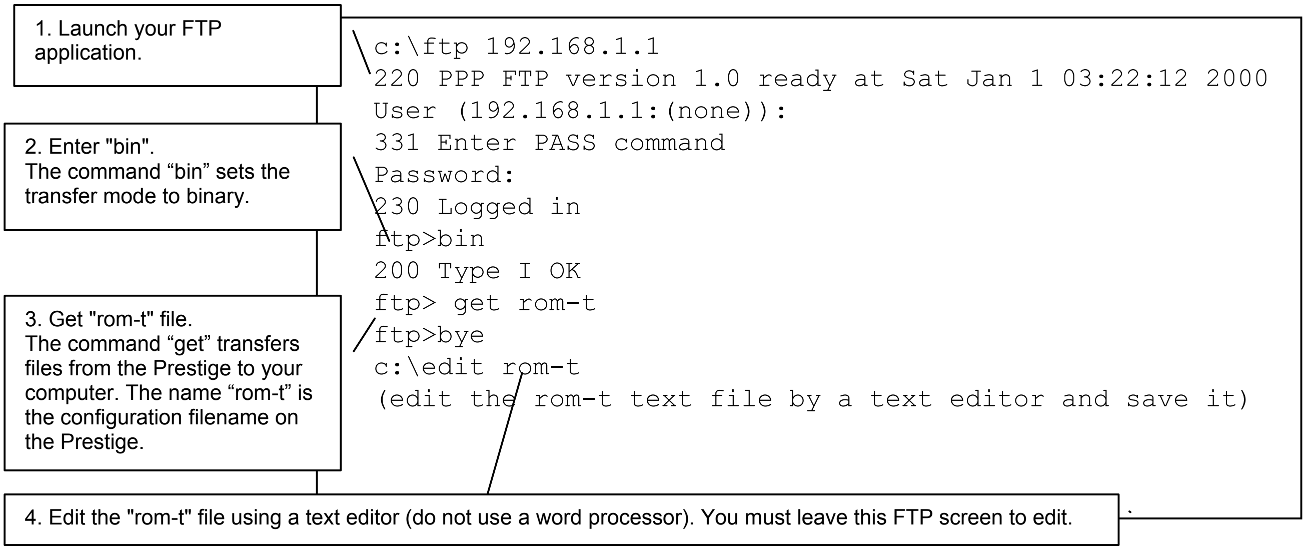
Figure 39-2 Invalid Parameter Entered: Command Line Example

The Prestige will display the following if you enter parameter(s) that *are* valid.

```
Please wait for the system to write SPT text file(ROM-t)...
Bootbase Version: V2.02 | 2/22/2001 13:33:11
RAM: Size = 8192 Kbytes
FLASH: Intel 8M *2
```

Figure 39-3 Valid Parameter Entered: Command Line Example

39.3 Internal SPTGEN FTP Download Example



1. Launch your FTP application.

2. Enter "bin".
The command "bin" sets the transfer mode to binary.

3. Get "rom-t" file.
The command "get" transfers files from the Prestige to your computer. The name "rom-t" is the configuration filename on the Prestige.

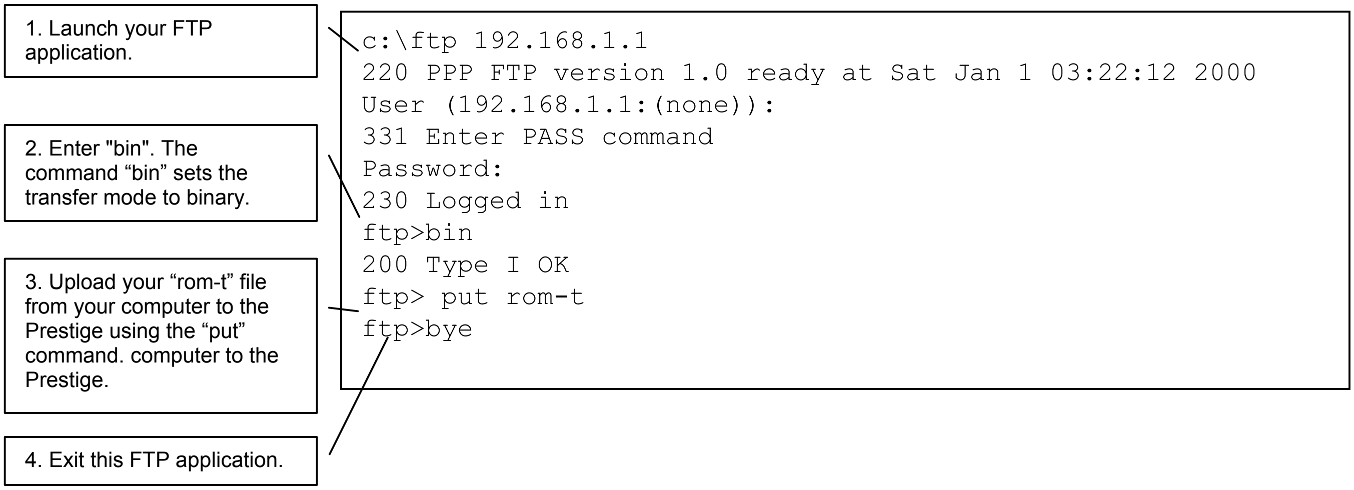
4. Edit the "rom-t" file using a text editor (do not use a word processor). You must leave this FTP screen to edit.

```
c:\ftp 192.168.1.1
220 PPP FTP version 1.0 ready at Sat Jan 1 03:22:12 2000
User (192.168.1.1:(none)):
331 Enter PASS command
Password:
230 Logged in
ftp>bin
200 Type I OK
ftp> get rom-t
ftp>bye
c:\edit rom-t
(edit the rom-t text file by a text editor and save it)
```

Figure 39-4 Internal SPTGEN FTP Download Example

You can rename your "rom-t" file when you save it to your computer but it must be named "rom-t" when you upload it to your Prestige.

39.4 Internal SPTGEN FTP Upload Example



1. Launch your FTP application.

2. Enter "bin". The command “bin” sets the transfer mode to binary.

3. Upload your “rom-t” file from your computer to the Prestige using the “put” command. computer to the Prestige.

4. Exit this FTP application.

```
c:\ftp 192.168.1.1
220 PPP FTP version 1.0 ready at Sat Jan 1 03:22:12 2000
User (192.168.1.1:(none)):
331 Enter PASS command
Password:
230 Logged in
ftp>bin
200 Type I OK
ftp> put rom-t
ftp>bye
```

Figure 39-5 Internal SPTGEN FTP Upload Example

Part X:

Appendices and Index

This part contains additional background information and an index or key terms.

Appenidx A Troubleshooting

This chapter covers potential problems and the corresponding remedies.

Problems Starting Up the Prestige

Chart A-1 Troubleshooting the Start-Up of Your Prestige

PROBLEM	CORRECTIVE ACTION
None of the LEDs turn on when I turn on the Prestige.	Make sure that the Prestige's power 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.

Problems with the LAN LED

Chart A-2 Troubleshooting the LAN LED

PROBLEM	CORRECTIVE ACTION
The LAN LEDs do not turn on.	Check your Ethernet cable connections and type (refer to the *Compact Guide* for details). Check for faulty Ethernet cables.
	Make sure your computer's Ethernet Card is working properly.

Problems with the DSL LED

Chart A-3 Troubleshooting the DSL LED

PROBLEM	CORRECTIVE ACTION
The xDSL 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 the *Maintenance* chapter (web configurator) or the System Information and Diagnosis chapter (SMT).

Problems with the LAN Interface

Chart A-4 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 *Chart A-2 Troubleshooting the LAN LED*. 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 *Chart A-2 Troubleshooting the LAN LED*. Make sure that the IP address and the subnet mask of the Prestige and the computers are on the same subnet.

Problems with the WAN Interface

Chart A-5 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 PPoA 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 the *WAN Setup* chapter (web configurator) or the *Internet Access* chapter (SMT).

Problems with Internet Access

Chart A-6 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 *Chart A-3 Troubleshooting the DSL LED*. Verify your WAN settings. Refer to the *WAN Setup* chapter (web configurator) or the *Internet Access* chapter (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 the *Menu 1 General Setup* chapter for details. For wireless stations, check that both the Prestige and wireless station(s) are using the same ESSID, channel and WEP keys (if WEP encryption is activated).
Internet connection disconnects.	Check the schedule rules. Refer to the *Call Scheduling* chapter (SMT). If you use PPPoA or PPPoE encapsulation, check the idle time-out setting. Refer to the *WAN* chapter (web configurator) or the *Remote Node Configuration* chapter (SMT). Contact your ISP.

Problems with the Password

Chart A-7 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 the *Introducing the Web Configurator* chapter). This restores all of the factory defaults including the password.

Problems with the Web Configurator

Chart A-8 Troubleshooting the Web Configurator

PROBLEM	CORRECTIVE ACTION
I cannot access the web configurator.	Refer to *Chart A-7 Troubleshooting the Password*. 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). You must also configure a firewall rule to allow access from the WAN. Refer to the chapters on remote management and firewall 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.

Problems with Remote Management

Chart A-9 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 the *Firmware and Configuration File Management* chapter (SMT) 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 *Chart A-4 Troubleshooting the LAN Interface* for instructions on checking your LAN connection.
	Refer to the *Problems with the WAN Interface* section for instructions on checking your WAN connection.
	See also the *Problems with the Web Configurator* section.

Appenidx B
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.)

Chart B-1 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

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.

Chart B-2 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 bits; each bit of the mask corresponds to a bit of the IP address. If a bit in the subnet mask 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.

Chart B-3 "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.

Chart B-4 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

Chart B-4 Alternative Subnet Mask Notation

SUBNET MASK IP ADDRESS	SUBNET MASK "1" BITS	LAST OCTET BIT VALUE
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.

	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.

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.

Chart B-5 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

Chart B-6 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

Chart B-6 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
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).

Chart B-7 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	

Chart B-8 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	

Chart B-9 Subnet 3

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128

Chart B-9 Subnet 3

	NETWORK NUMBER	LAST OCTET BIT VALUE
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	

Chart B-10 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.

Chart B-11 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.

Chart B-12 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

Chart B-12 Class C Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
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 *Chart B-1*) available for subnetting.

The following table is a summary for class "B" subnet planning.

Chart B-13 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

Appenidx C
PPPoE

PPPoE in Action

An ADSL modem bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your PC to an ATM PVC (Permanent Virtual Circuit) that connects to a xDSL Access Concentrator where the PPP session terminates (see the next figure). One PVC can support any number of PPP sessions from your LAN. PPPoE provides access control and billing functionality in a manner similar to dial-up services using PPP.

Benefits of PPPoE

PPPoE offers the following benefits:

1. It provides you with a familiar dial-up networking (DUN) user interface.
2. It lessens the burden on the carriers of provisioning virtual circuits all the way to the ISP on multiple switches for thousands of users. For GSTN (PSTN and ISDN), the switching fabric is already in place.
3. It allows the ISP to use the existing dial-up model to authenticate and (optionally) to provide differentiated services.

Traditional Dial-up Scenario

The following diagram depicts a typical hardware configuration where the PCs use traditional dial-up networking.

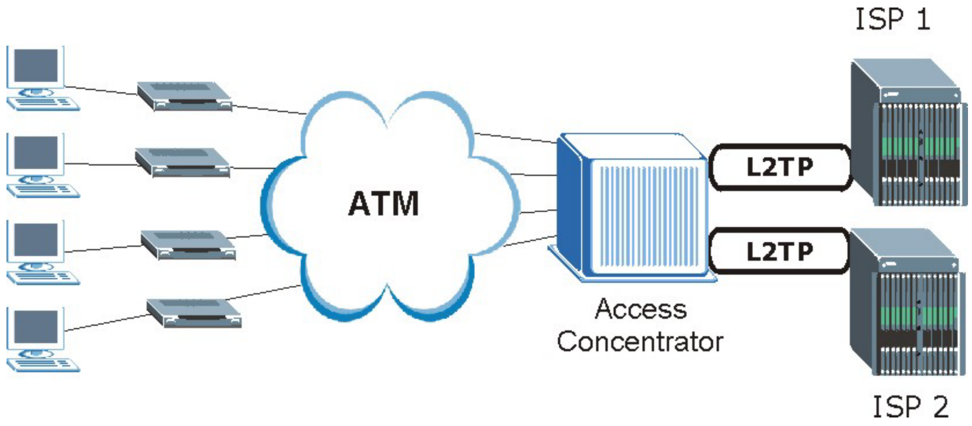


Diagram C-1 Single-PC per Router Hardware Configuration

How PPPoE Works

The PPPoE driver makes the Ethernet appear as a serial link to the PC and the PC runs PPP over it, while the modem bridges the Ethernet frames to the Access Concentrator (AC). Between the AC and an ISP, the AC is acting as a L2TP (Layer 2 Tunneling Protocol) LAC (L2TP Access Concentrator) and tunnels the PPP frames to the ISP. The L2TP tunnel is capable of carrying multiple PPP sessions.

With PPPoE, the VC (Virtual Circuit) is equivalent to the dial-up connection and is between the modem and the AC, as opposed to all the way to the ISP. However, the PPP negotiation is between the PC and the ISP.

Prestige as a PPPoE Client

When using the Prestige as a PPPoE client, the 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 PCs.

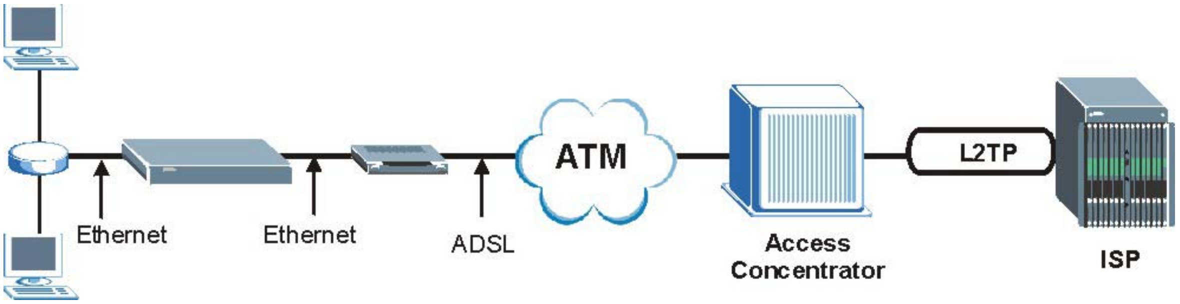


Diagram C-2 Prestigce as a PPPoE Client

Appenidx D
Virtual Circuit Topology

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

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

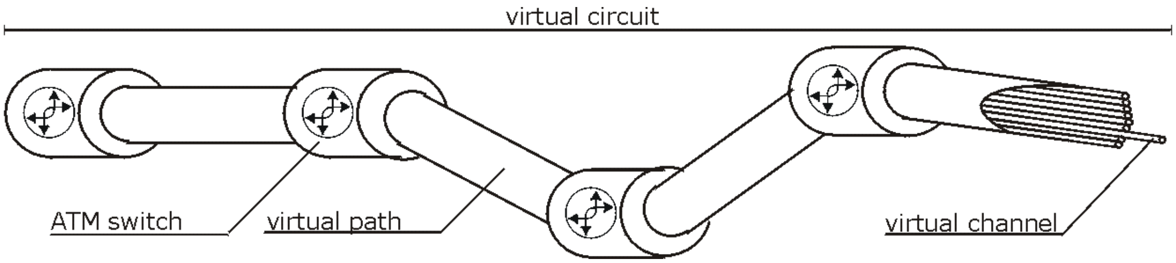


Diagram D-1 Virtual Circuit Topology

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

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

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

Appenidx E
Example Internal SPTGEN Screens

This appendix covers Prestige Internal SPTGEN screens.

Abbreviations Used in the Example Internal SPTGEN Screens Table

ABBREVIATION	MEANING
FIN	Field Identification Number (not seen in SMT screens)
FN	Field Name
PVA	Parameter Values Allowed
INPUT	An example of what you may enter
*	Applies to the Prestige.

The following are Internal SPTGEN screens associated with the SMT screens of your Prestige.

Example Internal SPTGEN Screens Table

/ Menu 1 General Setup (SMT Menu 1)			
FIN	FN	PVA	INPUT
10000000 =	Configured	<0(No) | 1(Yes)>	= 0
10000001 =	System Name	<Str>	= Prestige
10000002 =	Location	<Str>	=
10000003 =	Contact Person's Name	<Str>	=
10000004 =	Route IP	<0(No) | 1(Yes)>	= 1
10000006 =	Bridge	<0(No) | 1(Yes)>	= 0

/ Menu 3.1 General Ethernet Setup (SMT menu 3.1)			
FIN	FN	PVA	INPUT
30100001 =	Input Protocol filters Set 1		= 2
30100002 =	Input Protocol filters Set 2		= 256
30100003 =	Input Protocol filters Set 3		= 256
30100004 =	Input Protocol filters Set 4		= 256
30100005 =	Input device filters Set 1		= 256
30100006 =	Input device filters Set 2		= 256
30100007 =	Input device filters Set 3		= 256
30100008 =	Input device filters Set 4		= 256
30100009 =	Output protocol filters Set 1		= 256
30100010 =	Output protocol filters Set 2		= 256
30100011 =	Output protocol filters Set 3		= 256
30100012 =	Output protocol filters Set 4		= 256
30100013 =	Output device filters Set 1		= 256
30100014 =	Output device filters Set 2		= 256
30100015 =	Output device filters Set 3		= 256
30100016 =	Output device filters Set 4		= 256
/ Menu 3.2 TCP/IP and DHCP Ethernet Setup (SMT Menu 3.2)			
FIN	FN	PVA	INPUT
30200001 =	DHCP	<0(None) | 1(Server) | 2(Relay)>	= 0
30200002 =	Client IP Pool Starting Address		= 192.168.1.33
30200003 =	Size of Client IP Pool		= 32
30200004 =	Primary DNS Server		= 0.0.0.0
30200005 =	Secondary DNS Server		= 0.0.0.0
30200006 =	Remote DHCP Server		= 0.0.0.0
30200008 =	IP Address		= 172.21.2.200
30200009 =	IP Subnet Mask		= 16
30200010 =	RIP Direction	<0(None) | 1(Both) | 2(In Only) | 3(Out Only)>	= 0
30200011 =	Version	<0(Rip-1) | 1(Rip-2B) |2(Rip-2M)>	= 0

The valid parameters for a set are 1-12. Type "256" if you do not want to select a set.

This value must be between 1-254.

This value must be between 0-32.

30200012 =	Multicast	<0(IGMP-v2) | 1(IGMP-v1) | 2(None)>	= 2
30200013 =	IP Policies Set 1 (1~12)		= 256
30200014 =	IP Policies Set 2 (1~12)		= 256
30200015 =	IP Policies Set 3 (1~12)		= 256
30200016 =	IP Policies Set 4 (1~12)		= 256
/ Menu 3.2.1 IP Alias Setup (SMT Menu 3.2.1)			
FIN	FN	PVA	INPUT
30201001 =	IP Alias 1	<0(No) | 1(Yes)>	= 0
30201002 =	IP Address		= 0.0.0.0
30201003 =	IP Subnet Mask		= 0
30201004 =	RIP Direction	<0(None) | 1(Both) | 2(In Only) | 3(Out Only)>	= 0
30201005 =	Version	<0(Rip-1) | 1(Rip-2B) |2(Rip-2M)>	= 0
30201006 =	IP Alias #1 Incoming protocol filters Set 1		= 256
30201007 =	IP Alias #1 Incoming protocol filters Set 2		= 256
30201008 =	IP Alias #1 Incoming protocol filters Set 3		= 256
30201009 =	IP Alias #1 Incoming protocol filters Set 4		= 256
30201010 =	IP Alias #1 Outgoing protocol filters Set 1		= 256
30201011 =	IP Alias #1 Outgoing protocol filters Set 2		= 256
30201012 =	IP Alias #1 Outgoing protocol filters Set 3		= 256
30201013 =	IP Alias #1 Outgoing protocol filters Set 4		= 256
30201014 =	IP Alias 2 <0(No) | 1(Yes)>		= 0
30201015 =	IP Address		= 0.0.0.0
30201016 =	IP Subnet Mask		= 0

This value must be between 0-32.

30201017 =	RIP Direction	<0(None) | 1(Both) | 2(In Only) | 3(Out Only)>	= 0
30201018 =	Version	<0(Rip-1) | 1(Rip-2B) |2(Rip-2M)>	= 0
30201019 =	IP Alias #2 Incoming protocol filters Set 1		= 256
30201020 =	IP Alias #2 Incoming protocol filters Set 2		= 256
30201021 =	IP Alias #2 Incoming protocol filters Set 3		= 256
30201022 =	IP Alias #2 Incoming protocol filters Set 4		= 256
30201023 =	IP Alias #2 Outgoing protocol filters Set 1		= 256
30201024 =	IP Alias #2 Outgoing protocol filters Set 2		= 256
30201025 =	IP Alias #2 Outgoing protocol filters Set 3		= 256
30201026 =	IP Alias #2 Outgoing protocol filters Set 4		= 256
*/ Menu 3.5 Wireless LAN Setup (SMT Menu 3.5)			
30500001 =	ESSID		Wireless
30500002 =	Hide ESSID	<0(No) | 1(Yes)>	= 0
30500003 =	Channel ID	<1|2|3|4|5|6|7|8|9|10|11|12|13>	= 1
30500004 =	RTS Threshold	<0 ~ 2432>	= 2432
30500005 =	FRAG. Threshold	<256 ~ 2432>	= 2432
30500006 =	WEP	<0(DISABLE) | 1(64-bit WEP) | 2(128-bit WEP)>	= 0
30500007 =	Default Key	<1|2|3|4>	= 0
30500008 =	WEP Key1		=
30500009 =	WEP Key2		=
30500010 =	WEP Key3		=

30500011 =	WEP Key4		=
*/ MENU 3.5.1 WLAN MAC ADDRESS FILTER (SMT MENU 3.5.1)			
30501001 =	Mac Filter Active	<0(No) | 1(Yes)>	= 0
30501002 =	Filter Action	<0(Allow) | 1(Deny)>	= 0
30501003 =	Address 1		= 00:00:00:00:00:00
30501004 =	Address 2		= 00:00:00:00:00:00
30501005 =	Address 3		= 00:00:00:00:00:00
Continued	…		…
30501034 =	Address 32		= 00:00:00:00:00:00
/ Menu 4 Internet Access Setup (SMT Menu 4)			
FIN	FN	PVA	INPUT
40000000 =	Configured	<0(No) | 1(Yes)>	= 1
40000001 =	ISP	<0(No) | 1(Yes)>	= 1
40000002 =	Active	<0(No) | 1(Yes)>	= 1
40000003 =	ISP's Name		= ChangeMe
40000004 =	Encapsulation	<2(PPPOE) | 3(RFC 1483)| 4(PPPoA)| 5(ENET ENCAP)>	= 2
40000005 =	Multiplexing	<1(LLC-based) | 2(VC-based)	= 1
40000006 =	VPI #		= 0
40000007 =	VCI #		= 35
40000008 =	Service Name	<Str>	= any
40000009 =	My Login	<Str>	= test@p
40000010 =	My Password	<Str>	= 1234

This value must be between 0-32.

This value must be between 0-655355.

40000011 =	Single User Account	<0(No) | 1(Yes)>	= 1
40000012 =	IP Address Assignment	<0(Static)| 1(Dynamic)>	= 1
40000013 =	IP Address		= 0.0.0.0
40000014 =	Remote IP address		= 0.0.0.0
40000015 =	Remote IP subnet mask		= 0
40000016 =	ISP incoming protocol filter set 1		= 6
40000017 =	ISP incoming protocol filter set 2		= 256
40000018 =	ISP incoming protocol filter set 3		= 256
40000019 =	ISP incoming protocol filter set 4		= 256
40000020 =	ISP outgoing protocol filter set 1		= 256
40000021 =	ISP outgoing protocol filter set 2		= 256
40000022 =	ISP outgoing protocol filter set 3		= 256
40000023 =	ISP outgoing protocol filter set 4		= 256
40000024 =	ISP PPPoE idle timeout		= 0
40000025 =	Route IP	<0(No) | 1(Yes)>	= 1
40000026 =	Bridge	<0(No) | 1(Yes)>	= 0
40000027 =	ATM QoS Type	<0(CBR) | (1 (UBR)>	= 1
40000028 =	Peak Cell Rate (PCR)		= 0
40000029 =	Sustain Cell Rate (SCR)		= 0
40000030 =	Maximum Burst Size(MBS)		= 0
40000031=	RIP Direction	<0(None) | 1(Both) | 2(In Only) | 3(Out Only)>	= 0
40000032=	RIP Version	<0(Rip-1) | 1(Rip-2B) |2(Rip-2M)>	= 0
40000033=	Nailed-up Connection	<0(No) |1(Yes)>	= 0

This value must be between 0-32.

/ Menu 12.1.1 IP Static Route Setup (SMT Menu 12.1.1)			
FIN	FN	PVA	INPUT
120101001 =	IP Static Route set #1, Name	<Str>	=
120101002 =	IP Static Route set #1, Active	<0(No) |1(Yes)>	= 0
120101003 =	IP Static Route set #1, Destination IP address		= 0.0.0.0
120101004 =	IP Static Route set #1, Destination IP subnetmask		= 0
120101005 =	IP Static Route set #1, Gateway		= 0.0.0.0
120101006 =	IP Static Route set #1, Metric		= 0
120101007 =	IP Static Route set #1, Private	<0(No) |1(Yes)>	= 0
/ Menu 12.1.2 IP Static Route Setup (SMT Menu 12.1.2)			
FIN	FN	PVA	INPUT
120102001 =	IP Static Route set #2, Name		=
120102002 =	IP Static Route set #2, Active	<0(No) |1(Yes)>	= 0
120102003 =	IP Static Route set #2, Destination IP address		= 0.0.0.0
120102004 =	IP Static Route set #2, Destination IP subnetmask		= 0
120102005 =	IP Static Route set #2, Gateway		= 0.0.0.0
120102006 =	IP Static Route set #2, Metric		= 0
120102007 =	IP Static Route set #2, Private	<0(No) |1(Yes)>	= 0
/ Menu 12.1.3 IP Static Route Setup (SMT Menu 12.1.3)			
FIN	FN	PVA	INPUT
120103001 =	IP Static Route set #3, Name	<Str>	=
120103002 =	IP Static Route set #3, Active	<0(No) |1(Yes)>	= 0
120103003 =	IP Static Route set #3, Destination IP address		= 0.0.0.0
120103004 =	IP Static Route set #3, Destination IP subnetmask		= 0
120103005 =	IP Static Route set #3, Gateway		= 0.0.0.0
120103006 =	IP Static Route set #3, Metric		= 0
120103007 =	IP Static Route set #3, Private	<0(No) |1(Yes)>	= 0
/ Menu 12.1.4 IP Static Route Setup (SMT Menu 12.1.4)			

This value must be between 0-8.

This value must be between 0-32.

FIN	FN	PVA	INPUT
120104001 =	IP Static Route set #4, Name	<Str>	=
120104002 =	IP Static Route set #4, Active	<0(No) |1(Yes)>	= 0
120104003 =	IP Static Route set #4, Destination IP address		= 0.0.0.0
120104004 =	IP Static Route set #4, Destination IP subnetmask		= 0
120104005 =	IP Static Route set #4, Gateway		= 0.0.0.0
120104006 =	IP Static Route set #4, Metric		= 0
120104007 =	IP Static Route set #4, Private	<0(No) |1(Yes)>	= 0
/ Menu 12.1.5 IP Static Route Setup (SMT Menu 12.1.5)			
FIN	FN	PVA	INPUT
120105001 =	IP Static Route set #5, Name	<Str>	=
120105002 =	IP Static Route set #5, Active	<0(No) |1(Yes)>	= 0
120105003 =	IP Static Route set #5, Destination IP address		= 0.0.0.0
120105004 =	IP Static Route set #5, Destination IP subnetmask		= 0
120105005 =	IP Static Route set #5, Gateway		= 0.0.0.0
120105006 =	IP Static Route set #5, Metric		= 0
120105007 =	IP Static Route set #5, Private	<0(No) |1(Yes)>	= 0
/ Menu 12.1.6 IP Static Route Setup (SMT Menu 12.1.6)			
FIN	FN	PVA	INPUT
120106001 =	IP Static Route set #6, Name	<Str>	=
120106002 =	IP Static Route set #6, Active	<0(No) |1(Yes)>	= 0
120106003 =	IP Static Route set #6, Destination IP address		= 0.0.0.0
120106004 =	IP Static Route set #6, Destination IP subnetmask		= 0
120106005 =	IP Static Route set #6, Gateway		= 0.0.0.0
120106006 =	IP Static Route set #6, Metric		= 0
120106007 =	IP Static Route set #6, Private	<0(No) |1(Yes)>	= 0
/ Menu 12.1.7 IP Static Route Setup (SMT Menu 12.1.7)			
FIN	FN	PVA	INPUT

120107001 =	IP Static Route set #7, Name	<Str>	=
120107002 =	IP Static Route set #7, Active	<0(No) |1(Yes)>	= 0
120107003 =	IP Static Route set #7, Destination IP address		= 0.0.0.0
120107004 =	IP Static Route set #7, Destination IP subnetmask		= 0
120107005 =	IP Static Route set #7, Gateway		= 0.0.0.0
120107006 =	IP Static Route set #7, Metric		= 0
120107007 =	IP Static Route set #7, Private	<0(No) |1(Yes)>	= 0
/ Menu 12.1.8 IP Static Route Setup (SMT Menu 12.1.8)			
FIN	FN	PVA	INPUT
120108001 =	IP Static Route set #8, Name	<Str>	=
120108002 =	IP Static Route set #8, Active	<0(No) |1(Yes)>	= 0
120108003 =	IP Static Route set #8, Destination IP address		= 0.0.0.0
120108004 =	IP Static Route set #8, Destination IP subnetmask		= 0
120108005 =	IP Static Route set #8, Gateway		= 0.0.0.0
120108006 =	IP Static Route set #8, Metric		= 0
120108007 =	IP Static Route set #8, Private	<0(No) |1(Yes)>	= 0

*/ Menu 12.1.9 IP Static Route Setup (SMT Menu 12.1.9)			
FIN	FN	PVA	INPUT
120109001 =	IP Static Route set #9, Name	<Str>	=
120109002 =	IP Static Route set #9, Active	<0(No) |1(Yes)>	= 0
120109003 =	IP Static Route set #9, Destination IP address		= 0.0.0.0
120109004 =	IP Static Route set #9, Destination IP subnetmask		= 0
120109005 =	IP Static Route set #9, Gateway		= 0.0.0.0
120109006 =	IP Static Route set #9, Metric		= 0
120109007 =	IP Static Route set #9, Private	<0(No) |1(Yes)>	= 0
*/ Menu 12.1.10 IP Static Route Setup (SMT Menu 12.1.10)			
FIN	FN	PVA	INPUT

120110001 =	IP Static Route set #10, Name		=
120110002 =	IP Static Route set #10, Active	<0(No) |1(Yes)>	= 0
120110003 =	IP Static Route set #10, Destination IP address		= 0.0.0.0
120110004 =	IP Static Route set #10, Destination IP subnetmask	This value must be between 0-32.	= 0
120110005 =	IP Static Route set #10, Gateway		= 0.0.0.0
120110006 =	IP Static Route set #10, Metric	This value must be between 0-8.	= 0
120110007 =	IP Static Route set #10, Private	<0(No) |1(Yes)>	= 0
*/ Menu 12.1.11 IP Static Route Setup (SMT Menu 12.1.11)			
FIN	FN	PVA	INPUT
120111001 =	IP Static Route set #11, Name	<Str>	=
120111002 =	IP Static Route set #11, Active	<0(No) |1(Yes)>	= 0
120111003 =	IP Static Route set #11, Destination IP address		= 0.0.0.0
120111004 =	IP Static Route set #11, Destination IP subnetmask		= 0
120111005 =	IP Static Route set #11, Gateway		= 0.0.0.0
120111006 =	IP Static Route set #11, Metric		= 0
120111007 =	IP Static Route set #11, Private	<0(No) |1(Yes)>	= 0
*/ Menu 12.1.12 IP Static Route Setup (SMT Menu 12.1.12)			
FIN	FN	PVA	INPUT
120112001 =	IP Static Route set #12, Name	<Str>	=
120112002 =	IP Static Route set #12, Active	<0(No) |1(Yes)>	= 0
120112003 =	IP Static Route set #12, Destination IP address		= 0.0.0.0
120112004 =	IP Static Route set #12, Destination IP subnetmask		= 0
120112005 =	IP Static Route set #12, Gateway		= 0.0.0.0
120112006 =	IP Static Route set #12, Metric		= 0
120112007 =	IP Static Route set #12, Private	<0(No) |1(Yes)>	= 0
*/ Menu 12.1.13 IP Static Route Setup (SMT Menu 12.1.13)			
FIN	FN	PVA	INPUT
120113001 =	IP Static Route set #13, Name	<Str>	=

120113002 =	IP Static Route set #13, Active	<0(No) |1(Yes)>	= 0
120113003 =	IP Static Route set #13, Destination IP address		= 0.0.0.0
120113004 =	IP Static Route set #13, Destination IP subnetmask		= 0
120113005 =	IP Static Route set #13, Gateway		= 0.0.0.0
120113006 =	IP Static Route set #13, Metric		= 0
120113007 =	IP Static Route set #13, Private	<0(No) |1(Yes)>	= 0
*/ Menu 12.1.14 IP Static Route Setup (SMT Menu 12.1. 14)			
FIN	FN	PVA	INPUT
120114001 =	IP Static Route set #14, Name	<Str>	=
120114002 =	IP Static Route set #14, Active	<0(No) |1(Yes)>	= 0
120114003 =	IP Static Route set #14, Destination IP address		= 0.0.0.0
120114004 =	IP Static Route set #14, Destination IP subnetmask		= 0
120114005 =	IP Static Route set #14, Gateway		= 0.0.0.0
120114006 =	IP Static Route set #14, Metric		= 0
120114007 =	IP Static Route set #14, Private	<0(No) |1(Yes)>	= 0
*/ Menu 12.1.15 IP Static Route Setup (SMT Menu 12.1. 15)			
FIN	FN	PVA	INPUT
120115001 =	IP Static Route set #15, Name	<Str>	=
120115002 =	IP Static Route set #15, Active	<0(No) |1(Yes)>	= 0
120115003 =	IP Static Route set #15, Destination IP address		= 0.0.0.0
120115004 =	IP Static Route set #15, Destination IP subnetmask		= 0
120115005 =	IP Static Route set #15, Gateway		= 0.0.0.0
120115006 =	IP Static Route set #15, Metric		= 0
120115007 =	IP Static Route set #15, Private	<0(No) |1(Yes)>	= 0
*/ Menu 12.1.16 IP Static Route Setup (SMT Menu 12.1. 16)			
FIN	FN	PVA	INPUT
120116001 =	IP Static Route set #16, Name	<Str>	=
120116002 =	IP Static Route set #16, Active	<0(No) |1(Yes)>	= 0

120116003 =	IP Static Route set #16, Destination IP address		= 0.0.0.0
120116004 =	IP Static Route set #16, Destination IP subnetmask		= 0
120116005 =	IP Static Route set #16, Gateway		= 0.0.0.0
120116006 =	IP Static Route set #16, Metric		= 0
120116007 =	IP Static Route set #16, Private	<0(No) |1(Yes)>	= 0

/ Menu 15 SUA Server Setup (SMT Menu 15)

FIN	FN	PVA	INPUT
150000001 =	SUA Server IP address for default port		= 0.0.0.0
150000002 =	SUA Server #2 Active	<0(No) | 1(Yes)>	= 0
150000003 =	SUA Server #2 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000004 =	SUA Server #2 Port Start		= 0
150000005 =	SUA Server #2 Port End		= 0
150000006 =	SUA Server #2 Local IP address		= 0.0.0.0
150000007 =	SUA Server #3 Active	<0(No) | 1(Yes)>	= 0
150000008 =	SUA Server #3 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000009 =	SUA Server #3 Port Start		= 0
150000010 =	SUA Server #3 Port End		= 0
150000011 =	SUA Server #3 Local IP address		= 0.0.0.0
150000012 =	SUA Server #4 Active	<0(No) | 1(Yes)>	= 0
150000013 =	SUA Server #4 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000014 =	SUA Server #4 Port Start		= 0
150000015 =	SUA Server #4 Port End		= 0
150000016 =	SUA Server #4 Local IP address		= 0.0.0.0
150000017 =	SUA Server #5 Active	<0(No) | 1(Yes)>	= 0
150000018 =	SUA Server #5 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000019 =	SUA Server #5 Port Start		= 0
150000020 =	SUA Server #5 Port End		= 0
150000021 =	SUA Server #5 Local IP address		= 0.0.0.0
150000022 =	SUA Server #6 Active	<0(No) | 1(Yes)> = 0	= 0

150000023 =	SUA Server #6 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000024 =	SUA Server #6 Port Start		= 0
150000025 =	SUA Server #6 Port End		= 0
150000026 =	SUA Server #6 Local IP address		= 0.0.0.0
150000027 =	SUA Server #7 Active	<0(No) | 1(Yes)>	= 0
150000028 =	SUA Server #7 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0.0.0.0
150000029 =	SUA Server #7 Port Start		= 0
150000030 =	SUA Server #7 Port End		= 0
150000031 =	SUA Server #7 Local IP address		= 0.0.0.0
150000032 =	SUA Server #8 Active	<0(No) | 1(Yes)>	= 0
150000033 =	SUA Server #8 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000034 =	SUA Server #8 Port Start		= 0
150000035 =	SUA Server #8 Port End		= 0
150000036 =	SUA Server #8 Local IP address		= 0.0.0.0
150000037 =	SUA Server #9 Active	<0(No) | 1(Yes)>	= 0
150000038 =	SUA Server #9 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000039 =	SUA Server #9 Port Start		= 0
150000040 =	SUA Server #9 Port End		= 0
150000041 =	SUA Server #9 Local IP address		= 0.0.0.0
150000042	= SUA Server #10 Active	<0(No) | 1(Yes)>	= 0
150000043 =	SUA Server #10 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000044 =	SUA Server #10 Port Start		= 0
150000045 =	SUA Server #10 Port End		= 0
150000046 =	SUA Server #10 Local IP address		= 0.0.0.0
150000047 =	SUA Server #11 Active	<0(No) | 1(Yes)>	= 0
150000048 =	SUA Server #11 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0
150000049 =	SUA Server #11 Port Start		= 0
150000050 =	SUA Server #11 Port End		= 0
150000051 =	SUA Server #11 Local IP address		= 0.0.0.0
150000052 =	SUA Server #12 Active	<0(No) | 1(Yes)>	= 0
150000053 =	SUA Server #12 Protocol	<0(All)|6(TCP)|17(UDP)>	= 0

150000054 =	SUA Server #12 Port Start		= 0
150000055 =	SUA Server #12 Port End		= 0
150000056 =	SUA Server #12 Local IP address		= 0.0.0.0
/ Menu 21 Filter set #1 (SMT Menu 21)			
FIN	FN	PVA	INPUT
210100001 =	Filter Set 1, Name	<Str>	=

You may configure up to 12 filter sets with SMT menus; one with Internal SPTGEN.

/ Menu 21.1.1.1 Filter set #1, rule #1 (SMT Menu 21.1.1.1)			
FIN	FN	PVA	INPUT
210101001 =	IP Filter Set 1,Rule 1 Type	<2(TCP/IP)>	= 2
210101002 =	IP Filter Set 1,Rule 1 Active	<0(No)|1(Yes)>	= 1
210101003 =	IP Filter Set 1,Rule 1 Protocol		= 6
210101004 =	IP Filter Set 1,Rule 1 Dest IP address		= 0.0.0
210101005 =	IP Filter Set 1,Rule 1 Dest Subnet Mask		= 0
210101006 =	IP Filter Set 1,Rule 1 Dest Port		= 137
210101007 =	IP Filter Set 1,Rule 1 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210101008 =	IP Filter Set 1,Rule 1 Src IP address		= 0.0.0.0
210101009 =	IP Filter Set 1,Rule 1 Src Subnet Mask		= 0
210101010 =	IP Filter Set 1,Rule 1 Src Port		= 0
210101011 =	IP Filter Set 1,Rule 1 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210101013 =	IP Filter Set 1,Rule 1 Act Match	<1(check next)|2(forward)|3(drop)>	= 3
210101014 =	IP Filter Set 1,Rule 1 Act Not Match	<1(check next)|2(forward)|3(drop)>	= 1
/ Menu 21.1.1.2 set #1, rule #2 (SMT Menu 21.1.1.2)			
FIN	FN	PVA	INPUT
210102001 =	IP Filter Set 1,Rule 2 Type	<2(TCP/IP)>	= 2
210102002 =	IP Filter Set 1,Rule 2 Active	<0(No)|1(Yes)>	= 1
210102003 =	IP Filter Set 1,Rule 2 Protocol		= 6

You may change this type using SMT menus only.

This value must be between 0-255.

This value must be between 0-65535.

<table>
<tr><td>210102004 =</td><td>IP Filter Set 1,Rule 2 Dest IP address</td><td></td><td>= 0.0.0.0</td></tr>
<tr><td>210102005 =</td><td>IP Filter Set 1,Rule 2 Dest Subnet Mask</td><td></td><td>= 0</td></tr>
<tr><td>210102006 =</td><td>IP Filter Set 1,Rule 2 Dest Port</td><td></td><td>= 138</td></tr>
<tr><td>210102007 =</td><td>IP Filter Set 1,Rule 2 Dest Port Comp</td><td><0(none)|1(equal)|2(not equal)|3(less)|4(greater)></td><td>= 1</td></tr>
<tr><td>210102008 =</td><td>IP Filter Set 1,Rule 2 Src IP address</td><td></td><td>= 0.0.0.0</td></tr>
<tr><td>210102009 =</td><td>IP Filter Set 1,Rule 2 Src Subnet Mask</td><td></td><td>= 0</td></tr>
<tr><td>210102010 =</td><td>IP Filter Set 1,Rule 2 Src Port</td><td></td><td>= 0</td></tr>
<tr><td>210102011 =</td><td>IP Filter Set 1,Rule 2 Src Port Comp</td><td><0(none)|1(equal)|2(not equal)|3(less)|4(greater)></td><td>= 0</td></tr>
<tr><td>210102013 =</td><td>IP Filter Set 1,Rule 2 Act Match</td><td><1(check next)|2(forward)|3(drop)></td><td>= 3</td></tr>
<tr><td>210102014 =</td><td>IP Filter Set 1,Rule 2 Act Not Match</td><td><1(check next)|2(forward)|3(drop)></td><td>= 1</td></tr>
<tr><td colspan="4">/ Menu 21.1.1.3 set #1, rule #3 (SMT Menu 21.1.1.3)</td></tr>
<tr><td>FIN</td><td>FN</td><td>PVA</td><td>INPUT</td></tr>
<tr><td>210103001 =</td><td>IP Filter Set 1,Rule 3 Type</td><td><2(TCP/IP)></td><td>= 2</td></tr>
<tr><td>210103002 =</td><td>IP Filter Set 1,Rule 3 Active</td><td><0(No)|1(Yes)></td><td>= 1</td></tr>
<tr><td>210103003 =</td><td>IP Filter Set 1,Rule 3 Protocol</td><td></td><td>= 6</td></tr>
<tr><td>210103004 =</td><td>IP Filter Set 1,Rule 3 Dest IP address</td><td></td><td>= 0.0.0.0</td></tr>
<tr><td>210103005 =</td><td>IP Filter Set 1,Rule 3 Dest Subnet Mask</td><td></td><td>= 0</td></tr>
<tr><td>210103006 =</td><td>IP Filter Set 1,Rule 3 Dest Port</td><td></td><td>= 139</td></tr>
<tr><td>210103007 =</td><td>IP Filter Set 1,Rule 3 Dest Port Comp</td><td><0(none)|1(equal)|2(not equal)|3(less)|4(greater)></td><td>= 1</td></tr>
<tr><td>210103008 =</td><td>IP Filter Set 1,Rule 3 Src IP address</td><td></td><td>= 0.0.0.0</td></tr>
<tr><td>210103009 =</td><td>IP Filter Set 1,Rule 3 Src Subnet Mask</td><td></td><td>= 0</td></tr>
<tr><td>210103010 =</td><td>IP Filter Set 1,Rule 3 Src Port</td><td></td><td>= 0</td></tr>
</table>

210103011 =	IP Filter Set 1,Rule 3 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210103013 =	IP Filter Set 1,Rule 3 Act Match	<1(check next)|2(forward)|3(drop)	= 3
210103014 =	IP Filter Set 1,Rule 3 Act Not Match	<1(check next)|2(forward)|3(drop)	= 1
/ Menu 21.1.1.4 set #1, rule #4 (SMT Menu 21.1.1.4)			
FIN	FN	PVA	INPUT
210104001 =	IP Filter Set 1,Rule 4 Type	<2(TCP/IP)>	= 2
210104002 =	IP Filter Set 1,Rule 4 Active	<0(No)|1(Yes)>	= 1
210104003 =	IP Filter Set 1,Rule 4 Protocol		= 17
210104004 =	IP Filter Set 1,Rule 4 Dest IP address		= 0.0.0.0
210104005 =	IP Filter Set 1,Rule 4 Dest Subnet Mask		= 0
210104006 =	IP Filter Set 1,Rule 4 Dest Port		= 137
210104007 =	IP Filter Set 1,Rule 4 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210104008 =	IP Filter Set 1,Rule 4 Src IP address		= 0.0.0.0
210104009 =	IP Filter Set 1,Rule 4 Src Subnet Mask		= 0
210104010 =	IP Filter Set 1,Rule 4 Src Port		= 0
210104011 =	IP Filter Set 1,Rule 4 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210104013 =	IP Filter Set 1,Rule 4 Act Match	<1(check next) |2(forward) | 3(drop)	= 3
210104014 =	IP Filter Set 1,Rule 4 Act Not Match	<1(check next)|2(forward)|3(drop)	= 1
/ Menu 21.1.1.5 set #1, rule #5 (SMT Menu 21.1.1.5)			
FIN	FN	PVA	INPUT
210105001 =	IP Filter Set 1,Rule 5 Type	<2(TCP/IP)>	= 2
210105002 =	IP Filter Set 1,Rule 5 Active	<0(No)|1(Yes)>	= 1

210105003 =	IP Filter Set 1,Rule 5 Protocol		= 17
210105004 =	IP Filter Set 1,Rule 5 Dest IP address		= 0.0.0.0
210105005 =	IP Filter Set 1,Rule 5 Dest Subnet Mask		= 0
210105006 =	IP Filter Set 1,Rule 5 Dest Port		= 138
210105007 =	IP Filter Set 1,Rule 5 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210105008 =	IP Filter Set 1,Rule 5 Src IP Address		= 0.0.0.0
210105009 =	IP Filter Set 1,Rule 5 Src Subnet Mask		= 0
210105010 =	IP Filter Set 1,Rule 5 Src Port		= 0
210105011 =	IP Filter Set 1,Rule 5 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210105013 =	IP Filter Set 1,Rule 5 Act Match	<1(check next)|2(forward)|3(drop)>	= 3
210105014 =	IP FILTER SET 1,RULE 5 ACT NOT MATCH	<1(CHECK NEXT)|2(FORWARD)|3(DROP)>	= 1
/ Menu 21.1.1.6 set #1, rule #6 (SMT Menu 21.1.1.6)			
FIN	FN	PVA	INPUT
210106001 =	IP Filter Set 1,Rule 6 Type	<2(TCP/IP)>	= 2
210106002 =	IP Filter Set 1,Rule 6 Active	<0(No)|1(Yes)>	= 1
210106003 =	IP Filter Set 1,Rule 6 Protocol		= 17
210106004 =	IP Filter Set 1,Rule 6 Dest IP address		= 0.0.0.0
210106005 =	IP Filter Set 1,Rule 6 Dest Subnet Mask		= 0
210106006 =	IP Filter Set 1,Rule 6 Dest Port		= 139
210106007 =	IP Filter Set 1,Rule 6 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210106008 =	IP Filter Set 1,Rule 6 Src IP address		= 0.0.0.0
210106009 =	IP Filter Set 1,Rule 6 Src Subnet Mask		= 0

210106010 =	IP Filter Set 1,Rule 6 Src Port		= 0
210106011 =	IP Filter Set 1,Rule 6 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210106013 =	IP Filter Set 1,Rule 6 Act Match	<1(check next)|2(forward)|3(drop)>	= 3
210106014 =	IP Filter Set 1,Rule 6 Act Not Match	<1(check next)|2(forward)|3(drop)>	= 2

/ Menu 21.1 filter set #2, (SMT Menu 21.1)			
FIN	FN	PVA	INPUT
210200001 =	Filter Set 2, Nam	<Str>	= NetBIOS_WAN

/ Menu 21.1.2.1 Filter set #2, rule #1 (SMT Menu 21.1.2.1)			
FIN	FN	PVA	INPUT
210201001 =	IP Filter Set 2, Rule 1 Type	<0(none)|2(TCP/IP)>	= 2
210201002 =	IP Filter Set 2, Rule 1 Active	<0(No)|1(Yes)>	= 1
210201003 =	IP Filter Set 2, Rule 1 Protocol		= 6
210201004 =	IP Filter Set 2, Rule 1 Dest IP address		= 0.0.0.0
210201005 =	IP Filter Set 2, Rule 1 Dest Subnet Mask		= 0
210201006 =	IP Filter Set 2, Rule 1 Dest Port		= 137
210201007 =	IP Filter Set 2, Rule 1 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210201008 =	IP Filter Set 2, Rule 1 Src IP address		= 0.0.0.0
210201009 =	IP Filter Set 2, Rule 1 Src Subnet Mask		= 0
210201010 =	IP Filter Set 2, Rule 1 Src Port		= 0
210201011 =	IP Filter Set 2, Rule 1 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210201013 =	IP Filter Set 2, Rule 1 Act Match	<1(check next)|2(forward)|3(drop)>	= 3

210201014 =	IP Filter Set 2, Rule 1 Act Not Match	<1(check next)|2(forward)|3(drop)>	= 1
/ Menu 21.1.2.2 Filter set #2, rule #2 (SMT Menu 21.1.2.2)			
FIN	FN	PVA	INPUT
210202001 =	IP Filter Set 2, Rule 2 Type	<0(none)|2(TCP/IP)>	= 2
210202002 =	IP Filter Set 2, Rule 2 Active	<0(No)|1(Yes)>	= 1
210202003 =	IP Filter Set 2, Rule 2 Protocol		= 6
210202004 =	IP Filter Set 2, Rule 2 Dest IP address		= 0.0.0.0
210202005 =	IP Filter Set 2, Rule 2 Dest Subnet Mask		= 0
210202006 =	IP Filter Set 2, Rule 2 Dest Port		= 138
210202007 =	IP Filter Set 2, Rule 2 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210202008 =	IP Filter Set 2, Rule 2 Src IP address		= 0.0.0.0
210202009 =	IP Filter Set 2, Rule 2 Src Subnet Mask		= 0
210202010 =	IP Filter Set 2,Rule 2 Src Port		= 0
210202011 =	IP Filter Set 2, Rule 2 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210202013 =	IP Filter Set 2, Rule 2 Act Match	<1(check next)|2(forward)|3(drop)>	= 3
210202014 =	IP Filter Set 2, Rule 2 Act Not Match	<1(check next)|2(forward)|3(drop)>	= 1
/ Menu 21.1.2.3 Filter set #2, rule #3 (SMT Menu 21.1.2.3)			
FIN	FN	PVA	INPUT
210203001 =	IP Filter Set 2, Rule 3 Type	<0(none)|2(TCP/IP)>	= 2
210203002 =	IP Filter Set 2, Rule 3 Active	<0(No)|1(Yes)>	= 1
210203003 =	IP Filter Set 2, Rule 3 Protocol		= 6
210203004 =	IP Filter Set 2, Rule 3 Dest IP address		= 0.0.0.0
210203005 =	IP Filter Set 2, Rule 3 Dest Subnet Mask		= 0

210203006 =	IP Filter Set 2, Rule 3 Dest Port		= 139
210203007 =	IP Filter Set 2, Rule 3 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210203008 =	IP Filter Set 2, Rule 3 Src IP address		= 0.0.0.0
210203009 =	IP Filter Set 2,Rule 3 Src Subnet Mask		= 0
210203010 =	IP Filter Set 2, Rule 3 Src Port		= 0
210203011 =	IP Filter Set 2, Rule 3 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210203013 =	IP Filter Set 2, Rule 3 Act Match	<1(check next)|2(forward)|3(drop)>	= 3
210203014 =	IP Filter Set 2,Rule 3 Act Not Match	<1(check next)|2(forward)|3(drop)>	= 1
/ Menu 21.1.2.4 Filter set #2, rule #4 (SMT Menu 21.1.2.4)			
FIN	FN	PVA	INPUT
210204001 =	IP Filter Set 2, Rule 4 Type	<0(none)|2(TCP/IP)>	= 2
210204002 =	IP Filter Set 2, Rule 4 Active		<0(No)|1(Yes)> = 1
210204003 =	IP Filter Set 2, Rule 4 Protocol		= 17
210204004 =	IP Filter Set 2, Rule 4 Dest IP address		= 0.0.0.0
210204005 =	IP Filter Set 2, Rule 4 Dest Subnet Mask		= 0
210204006 =	IP Filter Set 2, Rule 4 Dest Port		= 137
210204007 =	IP Filter Set 2, Rule 4 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210204008 =	IP Filter Set 2, Rule 4 Src IP address		= 0.0.0.0
210204009 =	IP Filter Set 2, Rule 4 Src Subnet Mask		= 0
210204010 =	IP Filter Set 2, Rule 4 Src Port		= 0
210204011 =	IP Filter Set 2, Rule 4 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0

210204013 =	IP Filter Set 2, Rule 4 Act Match	<1(check next)|2(forward)|3(drop)>	= 3
210204014 =	IP Filter Set 2, Rule 4 Act Not Match	<1(check next)|2(forward)|3(drop)>	= 1
/ Menu 21.1.2.5 Filter set #2, rule #5 (SMT Menu 21.1.2.5)			
FIN	FN	PVA	INPUT
210205001 =	IP Filter Set 2, Rule 5 Type	<0(none)|2(TCP/IP)>	= 2
210205002 =	IP Filter Set 2, Rule 5 Active	<0(No)|1(Yes)>	= 1
210205003 =	IP Filter Set 2,Rule 5 Protocol		= 17
210205004 =	IP Filter Set 2, Rule 5 Dest IP address		= 0.0.0.0
210205005 =	IP Filter Set 2, Rule 5 Dest Subnet Mask		= 0
210205006 =	IP Filter Set 2, Rule 5 Dest Port		= 138
210205007 =	IP Filter Set 2, Rule 5 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210205008 =	IP Filter Set 2, Rule 5 Src IP address		= 0.0.0.0
210205009 =	IP Filter Set 2, Rule 5 Src Subnet Mask		= 0
210205010 =	IP Filter Set 2, Rule 5 Src Port		= 0
210205011 =	IP Filter Set 2, Rule 5 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210205013 =	IP Filter Set 2, Rule 5 Act Match	<1(check next)|2(forward)|3(drop)>	= 3
210205014 =	IP Filter Set 2, Rule 5 Act Not Match	<1(check next)|2(forward)|3(drop)>	= 1
/ Menu 21.1.2.6 Filter set #2, rule #6 (SMT Menu 21.1.2.5)			
FIN	FN	PVA	INPUT
210206001 =	IP Filter Set 2, Rule 6 Type	<0(none)|2(TCP/IP)>	= 2
210206002 =	IP Filter Set 2, Rule 6 Active	<0(No)|1(Yes)>	= 1
210206003 =	IP Filter Set 2, Rule 6 Protocol		= 17

210206004 =	IP Filter Set 2, Rule 6 Dest IP address		= 0.0.0.0
210206005 =	IP Filter Set 2, Rule 6 Dest Subnet Mask		= 0
210206006 =	IP Filter Set 2, Rule 6 Dest Port		= 139
210206007 =	IP Filter Set 2, Rule 6 Dest Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 1
210206008 =	IP Filter Set 2, Rule 6 Src IP address		= 0.0.0.0
210206009 =	IP Filter Set 2, Rule 6 Src Subnet Mask		= 0
210206010 =	IP Filter Set 2, Rule 6 Src Port		= 0
210206011 =	IP Filter Set 2, Rule 6 Src Port Comp	<0(none)|1(equal)|2(not equal)|3(less)|4(greater)>	= 0
210206013 =	IP Filter Set 2,Rule 6 Act Match	<1(check next)|2(forward)|3(drop)>	= 3
210206014 =	IP Filter Set 2,Rule 6 Act Not Match	<1(check next)|2(forward)|3(drop)>	= 2
*/ Menu 23.1 System Password Setup (SMT Menu 23.1)			
FIN	FN	PVA	INPUT
230000000 =	System Password		= 1234
*/ Menu 23.2 System security: radius server (SMT Menu 23.2)			
FIN	FN	PVA	INPUT
230200001 =	Authentication Server Configured	<0(No) | 1(Yes)>	= 1
230200002 =	Authentication Server Active	<0(No) | 1(Yes)>	= 1
230200003 =	Authentication Server IP Address		= 192.168.1.32
230200004 =	Authentication Server Port		= 1822
230200005 =	Authentication Server Shared Secret		= 111111111111111 1111111111111111
230200006 =	Accounting Server Configured	<0(No) | 1(Yes)>	= 1
230200007 =	Accounting Server Active	<0(No) | 1(Yes)>	= 1

230200008 =	Accounting Server IP Address		= 192.168.1.44
230200009 =	Accounting Server Port		= 1823
230200010 =	Accounting Server Shared Secret		= 1234
*/ Menu 23.4 System security: IEEE802.1x (SMT Menu 23.4)			
FIN	FN	PVA	INPUT
230400002 =	ReAuthentication Timer (in second)		= 555
230400003 =	Idle Timeout (in second)		= 999
230400004 =	Authentication Databases	<0(Local User Database Only)|1(RADIUS Only)|2(Local,RADIUS)|3(RADIUS,Local)>	= 1
/ Menu 24.11 Remote Management Control (SMT Menu 24.11)			
FIN	FN	PVA	INPUT
241100001 =	TELNET Server Port		= 23
241100002 =	TELNET Server Access	<0(all)|1(none)|2(Lan)|3(Wan)>	= 0
241100003 =	TELNET Server Secured IP address		= 0.0.0.0
241100004 =	FTP Server Port		= 21
241100005 =	FTP Server Access	<0(all)|1(none)|2(Lan)|3(Wan)>	= 0
241100006 =	FTP Server Secured IP address		= 0.0.0.0
241100007 =	WEB Server Port		= 80
241100008 =	WEB Server Access	<0(all)|1(none)|2(Lan) |3(Wan)>	= 0
241100009 =	WEB Server Secured IP address		= 0.0.0.0

These values must be between 0-65535.

This value must be between 0-65535.

Command Examples

The following are example Internal SPTGEN screens associated with the Prestige's command interpreter commands.

/ci command (for annex a): wan adsl opencmd			
FIN	FN	PVA	INPUT
990000001 =	ADSL OPMD	<0(glite)|1(t1.413)|2(gdmt)|3(multimode)>	= 3
/ci command (for annex B): wan adsl opencmd			
FIN	FN	PVA	INPUT

990000001 =	ADSL OPMD	<0(etsi)|1(normal)|2(gdmt)|3(multimode)>	= 3

Appenidx F
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.

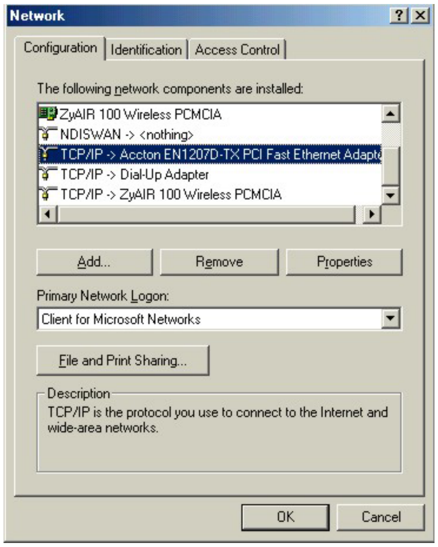
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

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.



The following network components are installed:

- ZyAIR 100 Wireless PCMCIA
- NDISWAN -> <nothing>
- TCP/IP -> Accton EN1207D-TX PCI Fast Ethernet Adapte
- TCP/IP -> Dial-Up Adapter
- TCP/IP -> ZyAIR 100 Wireless PCMCIA

Primary Network Logon: Client for Microsoft Networks

Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

Installing Components

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

If you need the adapter:

a. In the **Network** window, click **Add**.

b. Select **Adapter** and then click **Add**.

c. Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

a. In the **Network** window, click **Add**.

b. Select **Protocol** and then click **Add**.

c. Select **Microsoft** from the list of **manufacturers**.

d. Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

a. Click **Add**.

b. Select **Client** and then click **Add**.

c. Select **Microsoft** from the list of manufacturers.

d. Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.

e. Restart your computer so the changes you made take effect.

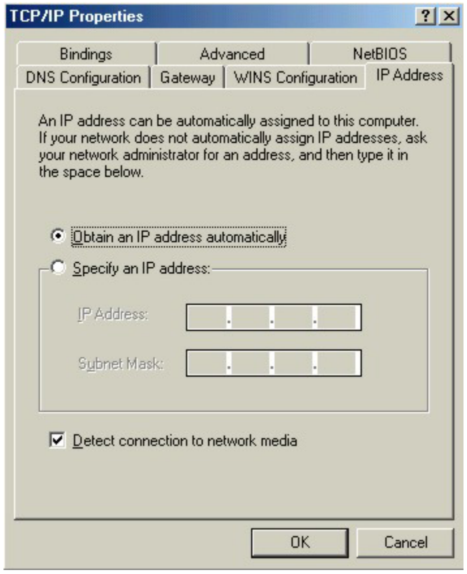
Configuring

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.



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

IP Address: . . .

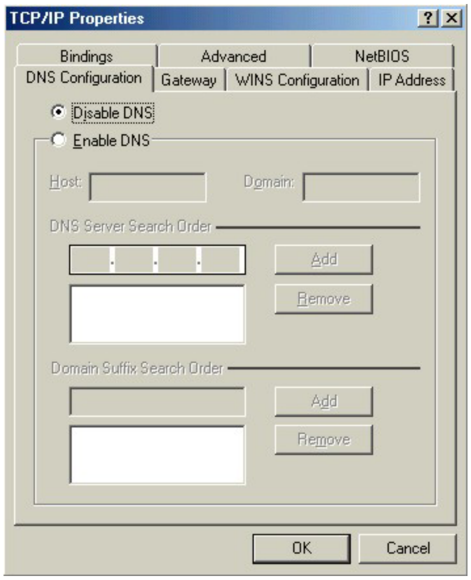
Subnet Mask: . . .

☑ Detect connection to network media

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

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

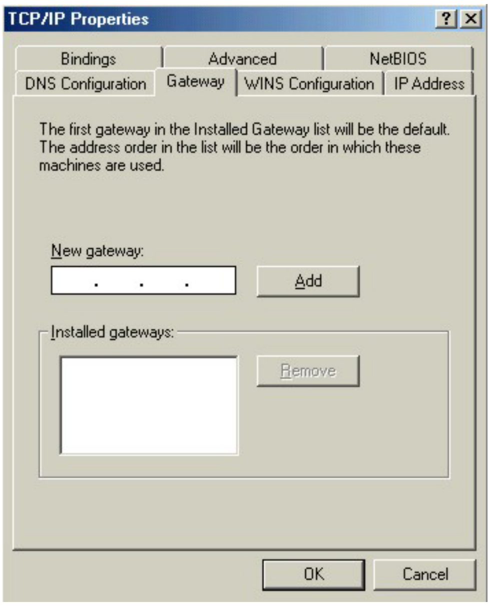
   -If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).



4. Click the **Gateway** tab.

   -If you do not know your gateway's IP address, remove previously installed gateways.

   -If you have a gateway IP address, type it in the **New gateway field** and click **Add**.


The first gateway in the Installed Gateway list will be the default. The address order in the list will be the order in which these machines are used.

5. Click **OK** to save and close the **TCP/IP Properties** window.

6. Click **OK** to close the **Network** window. Insert the Windows CD if prompted.

7. Turn on your Prestige and restart your computer when prompted.

Verifying Settings

1. Click **Start** and then **Run**.

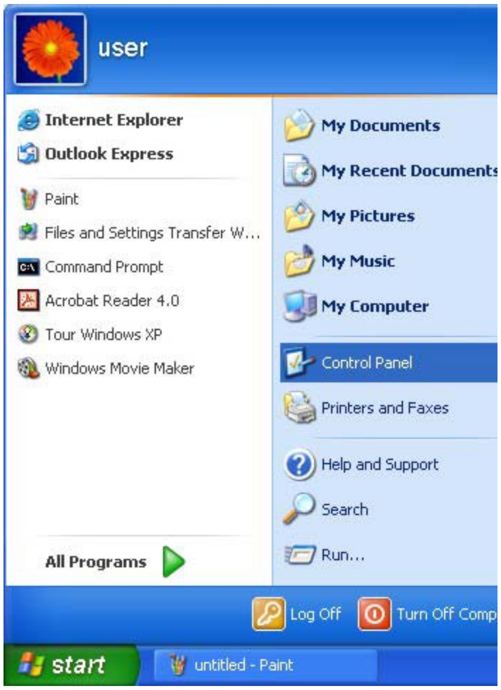
2. In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.

3. Select your network adapter. You should see your computer's IP address, subnet mask and

default gateway.

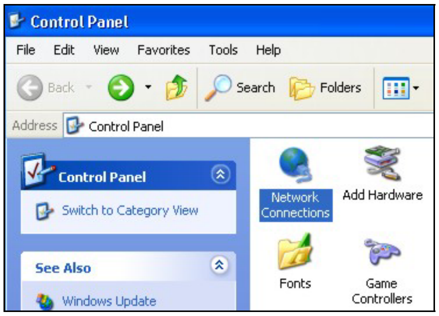
Windows 2000/NT/XP

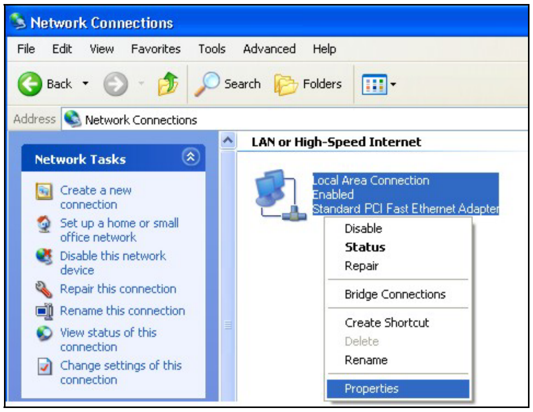
1. For Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.



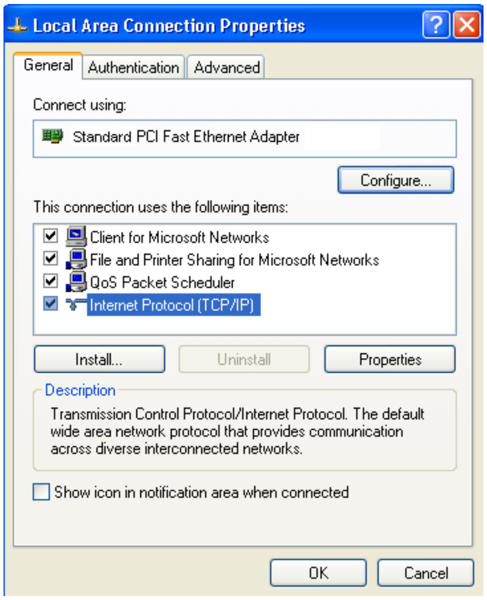
2. For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.

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





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



Local Area Connection Properties

Connect using:

Standard PCI Fast Ethernet Adapter

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

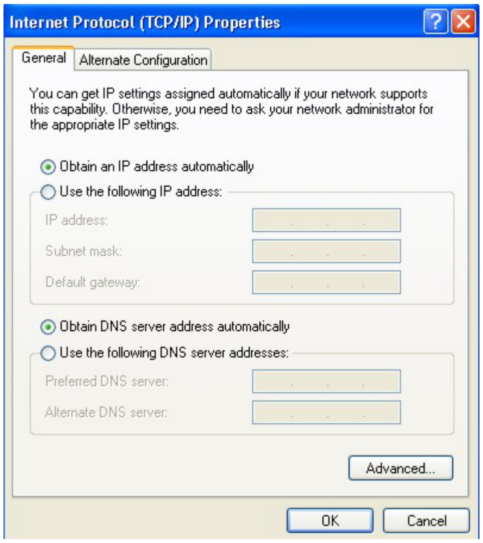
□ Show icon in notification area when connected

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**.



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

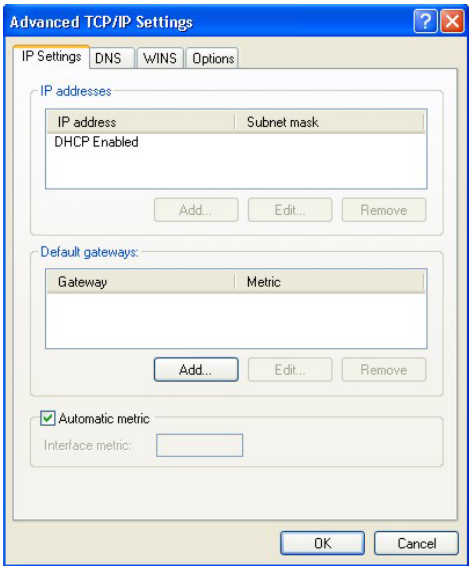
● Obtain an IP address automatically
○ Use the following IP address:

IP address: . . .
Subnet mask: . . .
Default gateway: . . .

● Obtain DNS server address automatically
○ Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

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



IP address	Subnet mask
DHCP Enabled	

Gateway	Metric

☑ Automatic metric

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.

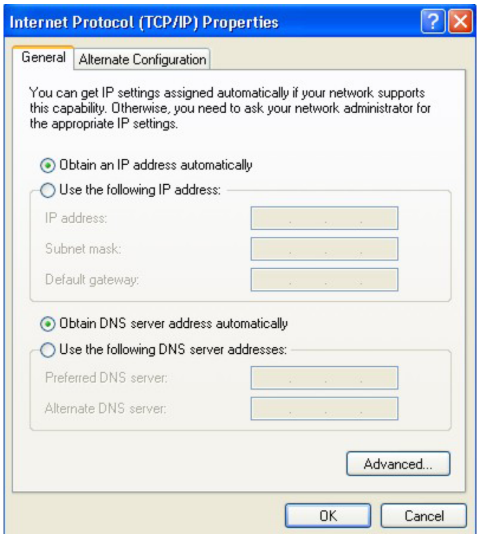
-Click **OK** when finished.

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.



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

8. Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9. Click **OK** to close the **Local Area Connection Properties** window.

10. Turn on your Prestige and restart your computer (if prompted).

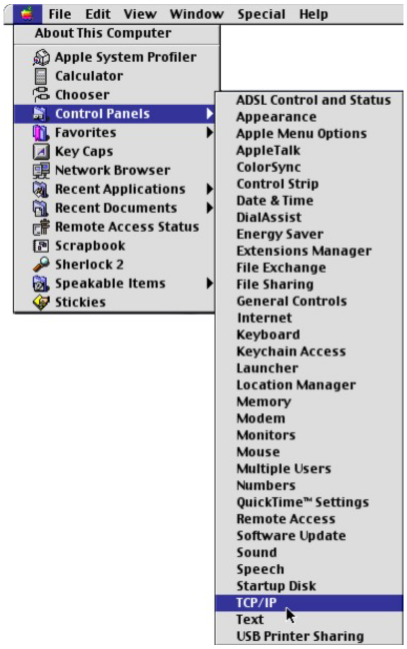
Verifying Settings

1. Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

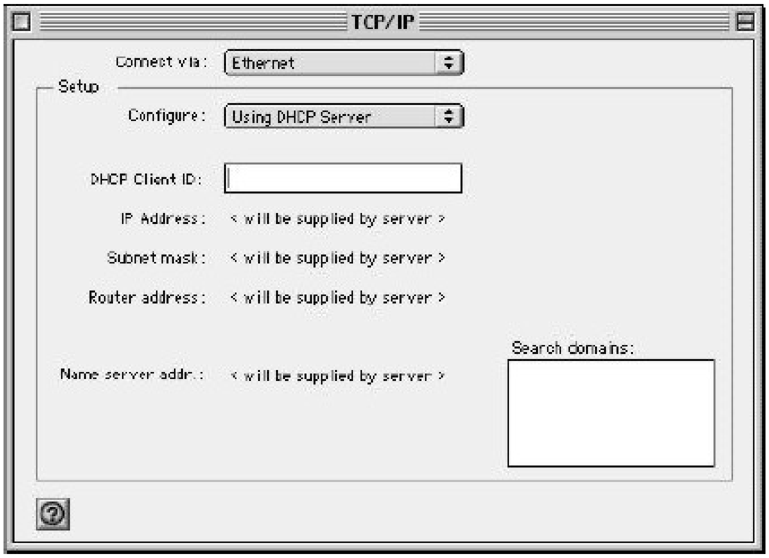
2. In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

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



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



TCP/IP

Connect via: Ethernet

Setup

Configure: Using DHCP Server

DHCP Client ID:

IP Address: < will be supplied by server >

Subnet mask: < will be supplied by server >

Router address: < will be supplied by server >

Name server addr.: < will be supplied by server >

Search domains:

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.

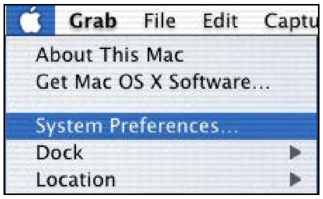
   -Type the IP address of your Prestige in the **Router address** box.
5. Close the **TCP/IP Control Panel**.
6. Click **Save** if prompted, to save changes to your configuration.
7. Turn on your Prestige and restart your computer (if prompted).

Verifyin 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.

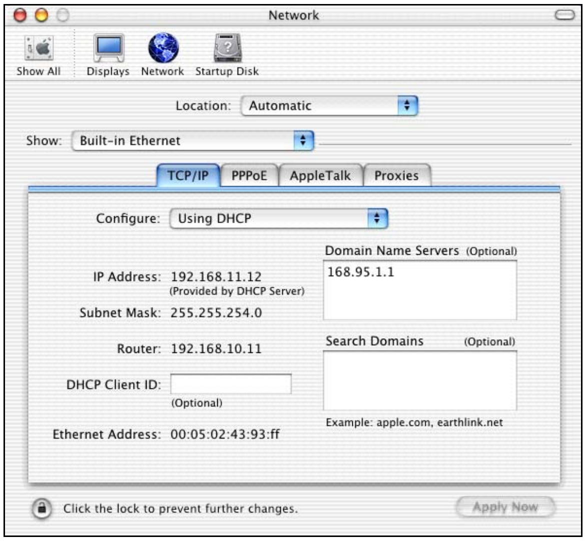


2. Click **Network** in the icon bar.

   - Select **Automatic** from the **Location** list.

   - Select **Built-in Ethernet** from the **Show** list.

   - Click the **TCP/IP** tab.



Location: Automatic

Show: Built-in Ethernet

Configure: Using DHCP

IP Address: 192.168.11.12
(Provided by DHCP Server)

Subnet Mask: 255.255.254.0

Router: 192.168.10.11

DHCP Client ID:
(Optional)

Ethernet Address: 00:05:02:43:93:ff

Domain Name Servers (Optional)
168.95.1.1

Search Domains (Optional)

Example: apple.com, earthlink.net

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

4. For statically assigned settings, do the following:

   -From the **Configure** box, select **Manually**.

   -Type your IP address in the **IP Address** box.

   -Type your subnet mask in the **Subnet mask** box.

   -Type the IP address of your Prestige in the **Router address** box.

5. Click **Apply Now** and close the window.

6. Turn on your Prestige and restart your computer (if prompted).

Verifying Settings

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

Appenidx G
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.

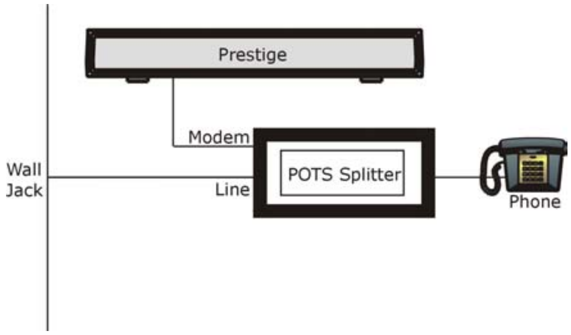


Diagram G-1 Connecting a POTS Splitter

Step 1. Connect the side labeled "Phone" to your telephone.

Step 2. Connect the side labeled "Modem" to your Prestige.

Step 3. Connect the side labeled "Line" to the telephone wall jack.

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.

Step 1. Connect a phone cable from the wall jack to the single jack end of the Y- Connector.

Step 2. Connect a cable from the double jack end of the Y-Connector to the "wall side" of the microfilter.

Step 3. Connect another cable from the double jack end of the Y-Connector to the Prestige.

Step 4. Connect the "phone side" of the microfilter to your telephone as shown in the following figure.

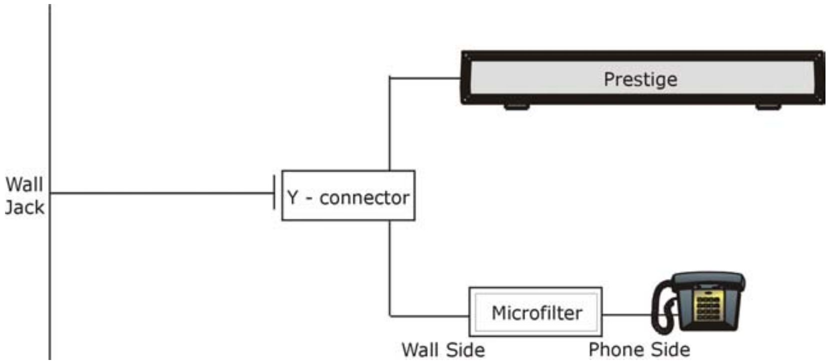


Diagram G-2 Connecting a Microfilter

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.

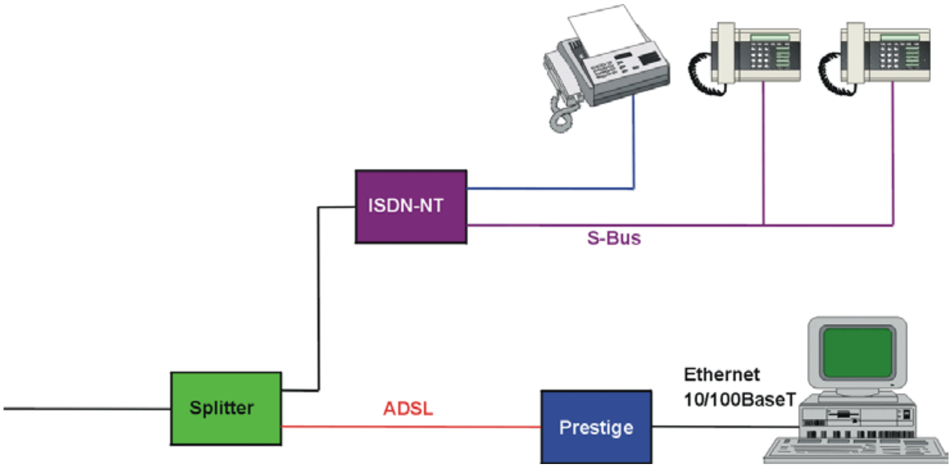


Diagram G-3 Prestige with ISDN

Appenidx H
Log Descriptions

This appendix provides descriptions of example log messages1.

Chart H-1 System Maintenance Logs

LOG MESSAGE	DESCRIPTION
`Time calibration is successful`	The router has adjusted its time based on information from the time server.
`Time calibration failed`	The router failed to get information from the time server.
`DHCP client gets %s`	A DHCP client got a new IP address from the DHCP server.
`DHCP client IP expired`	A DHCP client's IP address has expired.
`DHCP server assigns %s`	The DHCP server assigned an IP address to a client.
`SMT Login Successfully`	Someone has logged on to the router's SMT interface.
`SMT Login Fail`	Someone has failed to log on to the router's SMT interface.
`WEB Login Successfully`	Someone has logged on to the router's web configurator interface.
`WEB Login Fail`	Someone has failed to log on to the router's web configurator interface.
`TELNET Login Successfully`	Someone has logged on to the router via telnet.
`TELNET Login Fail`	Someone has failed to log on to the router via telnet.
`FTP Login Successfully`	Someone has logged on to the router via ftp.
`FTP Login Fail`	Someone has failed to log on to the router via ftp.

Chart H-2 UPnP Logs

LOG MESSAGE	DESCRIPTION
`UPnP pass through Firewall`	UPnP packets can pass through the firewall.

For the content filtering logs “(Destination)” means the destination IP address or domain name.

1 At the time of writing, the Prestige did not support the generation of all of the logs shown here.

Chart H-3 Content Filtering Logs

MESSAGE	NOTE	DESCRIPTION
`(Destination) Keyword Blocking`	Web Block	The Prestige blocked access to an address or domain name that had a forbidden keyword.
`(Destination) Contains ActiveX`	Web Block	The Prestige blocked access to an IP address or domain name that contains ActiveX because the content filter is set to forbid ActiveX.
`(Destination) Contains Java applet`	Web Block	The Prestige blocked access to an IP address or domain name that contains a Java applet because the content filter is set to forbid Java applets.
`(Destination) Contains cookie`	Web Block	The Prestige blocked access to an IP address or domain name that contains a cookie because the content filter is set to forbid cookies.
`(Destination) Proxy mode detected`	Web Block	The Prestige blocked access to an IP address or domain name that contains a proxy because the content filter is set to forbid proxies.
`(Destination)`	Web Forward	The Prestige allowed access to an address or domain name when content filtering was turned off according to its schedule.

The attack logs may include the protocol (Protocol) of the packet (for example TCP or UDP) that triggered the log.

Chart H-4 Attack Logs

LOG MESSAGE	DESCRIPTION
`attack (Protocol)`	The firewall detected an attack. The log may also display the protocol (for example TCP or UDP).
`land Protocol)`	The firewall detected a land attack. The log may also display the protocol (for example TCP or UDP).
`icmp echo ICMP (type:%d, code:%d)`	The firewall detected an ICMP echo attack. See the section on ICMP messages for type and code details.
`syn flood TCP`	The firewall detected a TCP syn flood attack.
`ports scan TCP`	The firewall detected a TCP port scan attack.
`teardrop (Protocol)`	The firewall detected a teardrop attack.
`illegal command TCP`	The firewall detected a TCP SMTP illegal command attack.
`NetBIOS TCP`	The firewall detected a TCP NetBIOS attack.
`ip spoofing - no routing entry (Protocol)`	The firewall detected an IP spoofing attack while the Prestige did not have a default route. The log may also display the protocol (for example TCP or UDP).
`vulnerability ICMP (type:%d, code:%d)`	The firewall detected an ICMP vulnerability attack; see the section on ICMP messages for type and code details.
`traceroute ICMP (type:%d, code:%d)`	The firewall detected an ICMP traceroute attack; see the section on ICMP messages for type and code details.

Access logs may include the following information:

- (Protocol) is the protocol of the packet (for example TCP or UDP) that triggered the log.
- (Direction) is the direction in which the packet was traveling (for example LAN to WAN or WAN to LAN)
- (Rule) is the number of the firewall rule that caused the log.

Chart H-5 Access Logs

LOG MESSAGE	DESCRIPTION
`Firewall default policy (Protocol, Direction)`	Access matched the default policy and the Prestige blocked or forwarded it according to the configuration of the default firewall policy.
`Firewall rule match (Protocol, Direction, Rule)`	Access matched a firewall rule and the Prestige blocked or forwarded it according to the rule’s configuration.
`Firewall rule NOT match: (Protocol, Direction, Rule)`	Access did not match a firewall rule and the Prestige logged it.
`dest port (Protocol, Direction)`	Access did not match a firewall rule’s destination port and the Prestige logged it.
`src port (Protocol, Direction)`	Access did not match a firewall rule’s source port and the Prestige logged it.
`dest IP (Protocol, Direction)`	Access did not match a firewall rule’s destination IP address and the Prestige logged it.
`src IP (Protocol, Direction)`	Access did not match a firewall rule’s source IP address and the Prestige logged it.
`protocol (Protocol, Direction)`	Access did not match a firewall rule’s protocol and the Prestige logged it.
`Triangle route packet forwarded (Protocol)`	The firewall allowed a triangle route session to pass through.
`ICMP Source Quench`	The Prestige sent or received an ICMP source quench packet to tell a host to slow down data transmission.
`ICMP Time Exceed`	The Prestige sent or received an ICMP Time Exceed packet because a packet with zero Time To Live (TTL) was dropped.
`ICMP Destination Unreachable`	The Prestige sent or received an ICMP Destination Unreachable packet when a packet was dropped because the target port was not open.
`Packet without a NAT table entry blocked (Protocol)`	The router blocked a packet that did not have a corresponding NAT table entry.
`Out of order TCP handshake packet blocked (Protocol)`	The router blocked a TCP handshake packet that came out of the proper order
`Unsupported/out-of-order ICMP (Protocol)`	The Prestige generates this log after it drops an ICMP packet due to one of the following two reasons: 1. The Prestige does not support the ICMP packet's protocol. 2. The ICMP packet is an echo reply for which there was no corresponding echo request.

Chart H-5 Access Logs

LOG MESSAGE	DESCRIPTION
Router reply ICMP packet	The router sent an ICMP response packet. This packet automatically bypasses the firewall.
Remote access denied	The router blocked a remote access attempt.

Chart H-6 TCP Reset Logs

LOG MESSAGE	DESCRIPTION
Firewall sent TCP reset packets	The firewall sent out TCP reset packets.

Chart H-7 ICMP Notes

TYPE	CODE	DESCRIPTION
0		Echo Reply
	0	Echo reply message
3		Destination Unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because it was set to Don't Fragment (DF)
	5	Source route failed
4		Source Quench
	0	A gateway may discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host
	2	Redirect datagrams for the Type of Service and Network
	3	Redirect datagrams for the Type of Service and Host
8		Echo
	0	Echo message
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded

Chart H-7 ICMP Notes

TYPE	CODE	DESCRIPTION
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

Appenidx I Index