Prestige 324

Intelligent Broadband Sharing Gateway

User's Guide

Version 3.60
January 2003

ZyXEL
TOTAL INTERNET ACCESS SOLUTION

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

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

Information for Canadian Users

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

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

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

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

Caution

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

Note

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

Declaration of Conformity

We, the Manufacturer/Importer,

ZyXEL Communications Corp.

No. 6, Innovation Rd. II,

Science-Based Industrial Park,

Hsinchu, Taiwan, 300 R.O.C

declare that the product

Prestige 324

is in conformity with:

STANDARD	STANDARD ITEM	VERSION
EN 55022	Radio disturbance characteristics – Limits and method of measurement.	1998
EN 61000-3-2	Disturbance in supply system caused by household appliances and similar electrical equipment “Harmonics”.	1995
EN 61000-3-3	Disturbance in supply system caused by household appliances and similar electrical equipment “Voltage fluctuations”.	1995
EN 61000-4-2	Electrostatic discharge immunity test – Basic EMC Publication	1995
EN 61000-4-3	Radiated, radio-frequency, electromagnetic field immunity test	1996
EN 61000-4-4	Electrical fast transient / burst immunity test - Basic EMC Publication	1995
EN 61000-4-5	Surge immunity test	1995
EN 61000-4-6	Immunity to conducted disturbances, induced by radio-frequency fields	1996
EN 61000-4-8		1993
EN61000-4-11	Voltage dips, short interruptions and voltage variations immunity tests	1994

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind of character to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Online Registration

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

Customer Support

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

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

METHOD LOCATION	E-MAIL SUPPORT/SALES	TELEPHONE/FAX	WEB SITE/ FTP SITE	REGULAR MAIL
WORLDWIDE	Support@zyxel.com.tw Support@europe.zyxel.com Sales@zyxel.com.tw	+886-3-578-3942 +886-3-578-2439	www.zyxel.com www.europe.zyxel.com ftp.europe.zyxel.com	ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan
NORTH AMERICA	Support@zyxel.com Sales@zyxel.com	+1-714-632-0882 800-255-4101 +1-714-632-0858	www.zyxel.com ftp.zyxel.com	ZyXEL Communications Inc., 1650 Miraloma Avenue, Placentia, CA 92870, U.S.A.
SCANDINAVIA	Support@zyxel.dk Sales@zyxel.dk	+45-3955-0700 +45-3955-0707	www.zyxel.dk ftp.zyxel.dk	ZyXEL Communications A/S, Columbusvej 5, 2860 Soeborg, Denmark
GERMANY	Support@zyxel.de Sales@zyxel.de Sales@zyxel.com.my	+49-2405-6909-0 +49-2405-6909-99 +603-795-34-407	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen, Germany

Table of Contents

List of Figures

List of Diagrams

List of Charts

List of Tables

Preface

Congratulations on your purchase of the Prestige 324 Broadband Sharing Gateway with four-port switch.

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

Your Prestige is easy to install and to configure. The embedded web configurator is a convenient platform-independent GUI (Graphical User Interface) that allows you to access the Prestige's management settings.

All functions of the Prestige are also software configurable via the SMT (System Management Terminal) interface. The SMT is a menu-driven interface that you can access from a terminal emulator through the console port or through an Ethernet port using a telnet connection.

About This User's Manual

This manual is designed to guide you through the SMT configuration of your Prestige for its various applications.

Related Documentation

- Online HTML help

  The online HTML help shows you how to configure each screen in the embedded web configurator. Refer to this *User's Guide* for more background information on each feature.

- Supporting Disk

  More detailed information and examples can be found in the included disk (as well as on the zyxel.com web site).

- Quick Start Guide

  Our Quick Start Guide is designed to help you get up and running right away. It contains a detailed easy-to-follow connection diagram, default settings, handy checklists and information on setting up your network and configuring for Internet access.

- Packing List Card

  The Packing List Card lists all items that should have come in the package.

- ZyXEL Glossary and Web Site

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

Syntax Conventions

- Mouse action sequences are denoted using a comma. For example, click **Start**, **Settings**, **Control Panel**, **Network** means first you click **Start**, move the mouse pointer over **Settings**, then move the mouse pointer over **Control Panel** and finally click **Network**
- "Enter" means for you to type one or more characters and press the carriage return. "Select" or "Choose" means for you to select one from the predefined choices.
- The SMT menu titles and labels are in **Bold Times New Roman** font. The choices of a menu item are in **Bold Arial** font. A single keystroke is in Arial font and enclosed in square brackets, for instance, [ENTER] means the Enter, or carriage return, key; [ESC] means the escape key and [SPACE BAR] means the space bar. [UP] and [DOWN] are the up and down arrow keys.
- For brevity's sake, we will use "e.g." as shorthand for "for instance" and "i.e." for "that is" or "in other words" throughout this manual.
- The Prestige 324 may be referred to as the Prestige or the P324 in this manual. Occasionally, SMT screens may refer to the Prestige as a router.

Part I:

Getting Started

This section helps you connect, install and setup your Prestige to operate on your network and access the Internet.

Chapter 1
Getting to Know Your Prestige

This chapter introduces the main applications of the Prestige as well as a list of key features.

1.1 Intelligent Broadband Sharing Gateway

The Prestige is a dual Ethernet Broadband Sharing Gateway with an integrated 4-port switch and robust network management features for Internet access via external Cable/xDSL modem. A combination of switch and router makes your Prestige a cost-effective and viable network solution. A 4-port bandwidth-sensitive 10/100Mbps switch provides greater network efficiency than traditional hubs because the bandwidth is dedicated and not shared. An unlimited number of computers may be connected to your Prestige by adding other hubs if your LAN consists of more than 4 computers.

The Prestige web configurator is a breeze to operate and independent of the operating system you use.

1.2 Features of the Prestige 324

The following are the main hardware and firmware features of the Prestige.

1.2.1 Hardware Features

10/100MB Auto-negotiating Ethernet WAN

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.

Integrated 4-Port 10/100MB Auto-sensing Ethernet Switch

The 10/100M LAN interface enables fast data transfers of 10Mbps or 100Mbps in either half-duplex or full-duplex mode depending on your Ethernet network. Auto-sensing allows you to use either a crossover Ethernet cable or a straight-through Ethernet cable to connect your device to either a computer or external hub. In other words these ports automatically adjust according to the type of cable so that either straight-through Ethernet cable or crossover Ethernet cable may be used.

All-in-one Console and Auxiliary Port

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

1.2.2 Firmware Features

Full Network Management

Your Prestige offers you a variety of options for network management. It supports password protected local and remote network management via the console port or a telnet connection using SMT (System Management Interface). Your Prestige includes an intuitive web configurator that makes setup and configuration easy. Included with the web configurator is embedded help designed to assist you during setup/configuration. It also supports FTP (File Transfer Protocol) server for remote management, TFTP (Trivial FTP), SNMP (Simple Network Management Protocol) and CI (Command Interpreter) mode.

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, NETBIOS packet filtering, reports and logs.

Content Filtering

The Prestige can block web features such as ActiveX controls, Java applets and cookies, as well as disable web proxies. The Prestige can also block specific URLs by using the keyword feature.

Packet Filtering

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

Universal Plug and Play (UPnP)

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

Traffic Redirect

Traffic Redirect is used to sustain the Internet connection. The Prestige detects if the connectivity has been lost and will forward the outgoing traffic to another specified gateway.

NAT (Network Address Translation)

NAT (Network Address Translation - NAT, RFC 1631) allows the translation of an Internet Protocol address used within one network to a different IP address known within another network. The Prestige can now map multiple global IP addresses to local IP addresses of clients or servers.

Port Forwarding

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

DHCP Support

DHCP (Dynamic Host Configuration Protocol) allows the individual clients (workstations) to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The Prestige has built-in DHCP server capability, enabled by default, which means it can assign IP addresses, an IP default gateway and DNS servers to Windows 9x, Windows NT, Windows 2000 and other systems that support the DHCP client.

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.

IP Multicast

Traditionally, IP packets are transmitted in two ways - unicast or broadcast. Multicast is a third way to deliver IP packets to a group of hosts. IGMP (Internet Group Management Protocol) is the protocol used to support multicast groups. The latest version is version 2 (see RFC 2236). The Prestige supports versions 1 and 2.

IP Alias

IP alias allows you to partition a physical network into logical networks over the same Ethernet interface.

Call Scheduling

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

Call Control

The Prestige provides budget management for outgoing calls and chronicles incoming and outgoing calls.

RoadRunner Support

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

PPPoE Support

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

PPTP Support

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

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

Time and Date Setting

This feature (menu 24.10) allows you to get the current time and date from an external server when you power up your Prestige. The real time is then displayed in the Prestige **Menu 24.1- System Status** and error logs. If you do not choose a time service protocol that your timeserver will send when the Prestige powers up you can enter the time manually but each time the system is booted, the time and date will be reset to 1/1/2000 0:0:0.

Logging and Tracing

- Built-in message logging and packet tracing.
- Unix syslog facility support.

Embedded FTP and TFTP Services

The Prestige's embedded FTP and TFTP services enable the fast upgrade of firmware via standard file transfer protocols.

SNMP

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

Brute-Force Password Guessing Protection

The Prestige has a special protection mechanism to discourage brute-force password guessing attacks on the Prestige's management interfaces. Brute-force password guessing is repeatedly trying different combinations of letters, numbers and so on until the password is found. Brute-Force Password Guessing Protection enforces a wait-time after a certain number of incorrect passwords have been entered This wait-time must expire before another password can be entered. Please see the appendices for details about configuring this feature using CI commands.[1]

1.3 Broadband Internet Access via Cable or DSL Modem

A cable modem or DSL modem can be connected to the Prestige WAN Ethernet port and up to four computers can be connected to the four Prestige 10/100M LAN Ethernet ports for super-fast broadband Internet access. The Prestige provides not only the high speed Internet access but also a complete solution to efficiently manage data traffic on your network.

[1] Not available at the time of writing.

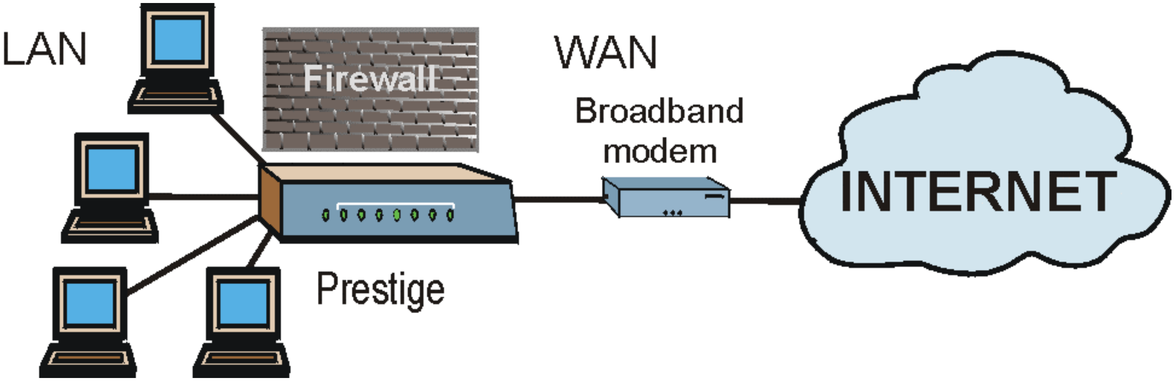


Figure 1-1 Internet Access Application

1.4 Internet Access Configuration Checklist

The following table shows the minimum SMT menu configurations you'll need to make (without changing the default Prestige values) in order to access the Internet. See your Quick Start Guide and the embedded web configurator online help for information on using the web configurator Internet access wizard to access the Internet (preferred method for non-experienced SMT users).

Table 1-1 Internet Access Configuration Checklist

SMT #	FIELD	ACTION
1	System Name	This field is for identification purposes but because some ISPs check this name you should enter your computer's "Computer Name". • In Windows 95/98 click **Start**, **Settings**, **Control Panel**, **Network**. Click the **Identification** tab, note the entry for the **Computer Name** field and enter it as the **System Name**. • In Windows 2000, click **Start**, **Settings**, Control **Panel**, **Network Identification**. Click the **Identification** tab, note the entry for the **Computer Name** field and enter it as the **System Name**. • In Windows XP, click **Start, Control Panel, System**. Click the **Computer Name** tab. Note the entry for the **Computer Description** field and enter it as the **System Name**.
2	MAC Address: Assigned By	The default is **Factory Default**, which is the factory assigned default MAC Address. We recommend you choose **IP Address attached on LAN** and enter the IP address of the workstation on the LAN whose MAC you are cloning.

Table 1-1 Internet Access Configuration Checklist

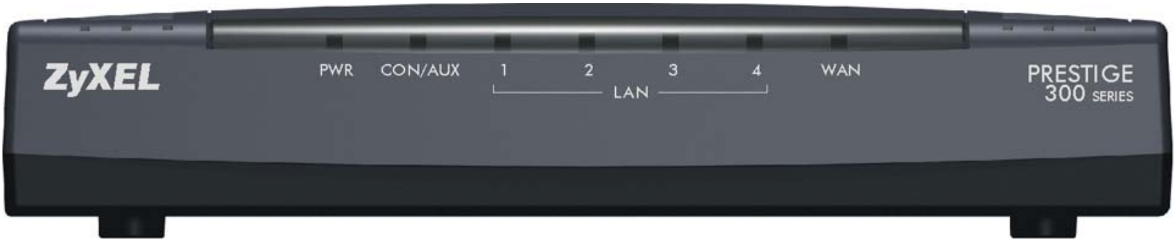
SMT #	FIELD	ACTION
4	Encapsulation	Choose **PPPoE** if you have a dial-up connection to the Internet (or **PPTP** if you reside in France or Austria); otherwise choose **Ethernet**. Choose from **RR-Manager**, **RR-Telstra** or **RR- Toshiba** if your ISP is Time Warner's RoadRunner; otherwise choose **Standard**.
	PPTP	You need to know your login name, password and connection ID/Name. The latter may not be obligatory for some ISPs, but if it is you must follow the “c:id” and “n:name” format.
	PPPoE	You need to know your login name, password and service name. The latter may not be obligatory for some ISPs.
	IP Address Assignment	If your ISP did not assign you a fixed IP address, select **Dynamic**, otherwise select **Static** and enter the IP address & subnet mask in the IP address and IP Subnet Mask fields.
Once these key fields have been configured, you should be able to enjoy super-fast Internet access with your Prestige!		

Chapter 2
Hardware Installation & Initial Setup

This chapter shows you how to connect hardware and perform the initial setup.

2.1 Front Panel

Prestige.



Panel

CON/AUX	Console/ Auxiliary	Green	On	The port is in console mode (CON/AUX switch set to CON) and is connected to a management computer.

2.2 Prestige Rear Panel and Connections

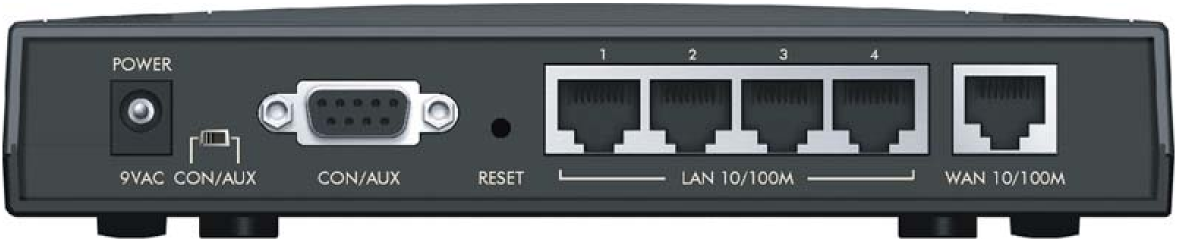


Figure 2-1 Prestige Rear Panel Connections

Table 2-1Prestige Rear Panel Connections

CONNECTION	DESCRIPTION AND FUNCTION
Power 9V AC	Connect the included power adaptor to the power supply and connect the other end of the power adaptor cable to this socket. **Do this step last. Use only the included power adapter!** **See the *Power Adapter Specification Appendix* for regional specifications.**
Power 9V AC	Connect the end of the included power adaptor (use only this adapter) to this power socket. **Use only the included power adapter! See the *Power Adapter Specification Appendix* for regional specifications.**
CON/AUX switch CON/AUX port	Set this switch to the "CON" side to use the CON/AUX port as a regular console port for local device configuration and management. Connect the 9-pin male end of the console cable to the console port of the Prestige and the other end (choice of 9-pin or 25-pin, depending on your computer) end to a serial port (COM1, COM2 or other COM port) of your computer. You can use an extension RS-232 cable if the enclosed one is too short. Your computer should have a terminal emulation communications program (such as HyperTerminal) set to VT100 terminal emulation, no parity, 8 data bits, 1 stop bit, no data flow and 9600 bps port speed. Set this switch to the "AUX" side to use the CON/AUX port as an auxiliary dial-up WAN connection. Connect the 9-pin male end of the RS-232 Y-cable to the CON/AUX port and use the included CON/AUX converter on the other 9-pin end of the cable to connect to a modem or TA.

CON/AUX switch CON/AUX port	Just connect this port if you want to configure the Prestige using the SMT via console port or set up a backup WAN connection. Set this switch to the "CON" side to use the CON/AUX port as a regular console port for local device configuration and management. Connect the 9-pin male end of the console cable to the console port of the Prestige and the other end to a serial port (COM1, COM2 or other COM port) of your computer. You can use an extension RS-232 cable if the enclosed one is too short. Your computer should have a terminal emulation communications program (such as HyperTerminal) set to VT100 terminal emulation, no parity, 8 data bits, 1 stop bit, no data flow and 9600 bps port speed. Set this switch to the "AUX" side to use the CON/AUX port as an auxiliary dial-up WAN connection. Connect the 9-pin male end of the RS-232 Y-cable to the CON/AUX port and use the included CON/AUX converter on the other 9-pin end of the cable to connect to a modem or TA.
Reset	You only need to use this button if you've forgotten the Prestige's password. It returns the Prestige to the factory defaults (password is 1234, LAN IP address 192.168.1.1, terminal emulation settings set to VT100 terminal emulation, no parity, 8 data bits, 1 stop bit, no data flow and 9600 bps port speed).
LAN 10/100M	Connect these auto-negotiating (10/100M) auto-sensing LAN ports to local computers or to an external hub using straight-through Ethernet or crossover Ethernet cables. Auto-sensing means that these ports can automatically adjust to the type of Ethernet cable you use.
WAN 10/100M	Connect your Cable/DSL modem to this port with the cable that came with your modem. If you want to connect a cable modem, you must connect the coaxial cable from your cable service to the threaded coaxial cable connector on the back of the cable modem. Connect an DSL modem to the DSL wall jack. The WAN connection cable should be STP (Shielded Twisted Pair).

2.3 Turning on Your Prestige

After you've made the connections, connect the power cable to a power supply and look at the front panel LEDs. The **PWR** LED blinks while performing system testing and then turns steady on if the testing is successful. The **CON/AUX**, **LAN**, and **WAN** LEDs turn on if they are properly connected.

2.4 Front Panel LEDs

The LEDs on the front panel indicate the operational status of the Prestige.

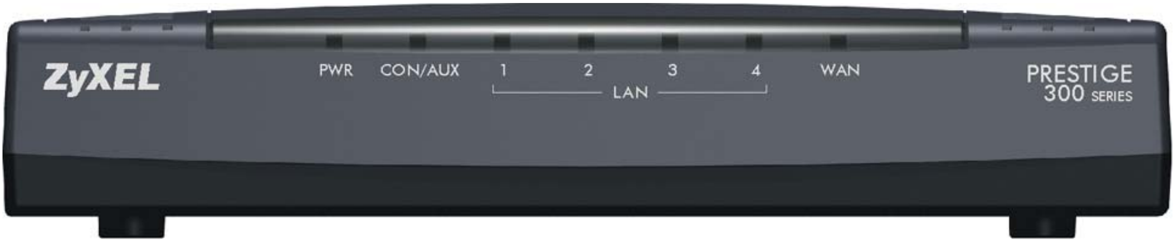


Figure 2-2 Front Panel

The following table describes the LED functions.

Table 2-2 LED Descriptions

LED	FUNCTION	COLOR	STATUS	MEANING
PWR	Power	Green	On	The Prestige is receiving power.
			Off	The system is not ready or failed.
			Flashing	The system is performing system tests.
CON/AUX	Console/ Auxiliary	Green	On	The port is in console mode (CON/AUX switch set to CON) and is connected to a management computer.
		Orange	On	The port is in auxiliary mode (CON/AUX switch set to AUX), is connected to a modem or TA and the link is up.
		Orange	Flashing	Data is being sent/received through the backup modem or TA.
			Off	There is no connection to the CON/AUX port.
10M LAN1,2,3,4	LAN	Green	Off	The 10M LAN port(s) is not connected.
			On	The Prestige is connected to a 10M LAN port(s).
			Flashing	The 10M LAN is sending/receiving packets.
100M LAN1,2,3,4			Off	The 100M LAN port(s) is not connected.

Table 2-2 LED Descriptions

LED	FUNCTION	COLOR	STATUS	MEANING
		Orange	On	The Prestige is connected to a 100Mbps LAN port(s).
			Flashing	The 100M LAN port(s) is sending/receiving packets.
WAN	WAN		Off	The WAN Link is not ready, or has failed.
		Green	On	The 10M WAN Link is ok.
			Flashing	The 10M WAN link is sending/receiving packets.
		Orange	On	The 100M WAN Link is ok.
			Flashing	The 10oM WAN link is sending/receiving packets.

Chapter 3
Introducing the Web Configurator

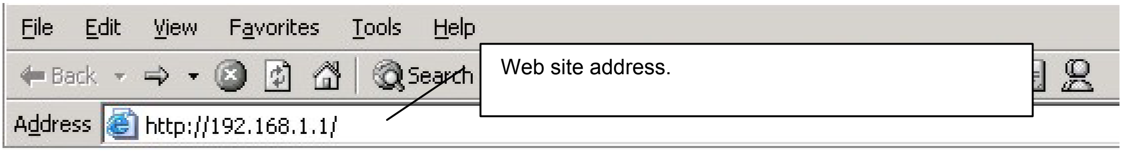
This chapter describes how to access the Prestige web configurator.

3.1 Accessing the Prestige Web Configurator

Step 1. Make sure your Prestige hardware is properly connected (refer to instructions in the hardware installation chapter*)*.

Step 2. Prepare your computer/computer network to connect to the Internet (refer to the *Quick Start Guide* or *the appendices* in this guide).

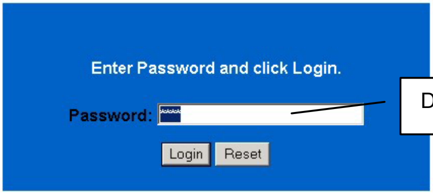
Step 3. Launch your web browser. Enter "192.168.1.1" as the web site address.



Web site address.

Figure 3-1 Web Site Address

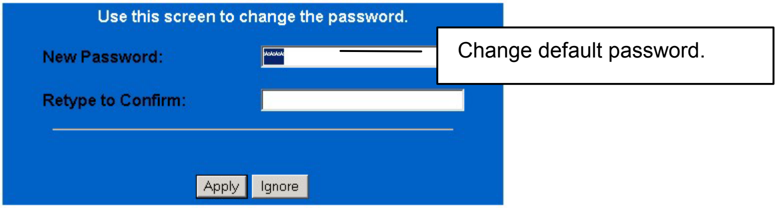
Step 1. The default password ("1234") is already in the password field (in non-readable format). Click **Login** to proceed to a screen asking you to change your password. Click **Reset** to revert to the default password in the password field.



Default password.

Figure 3-2 Default Password

Step 2. It is highly recommended you change the default password! Enter a new password, retype it to confirm and click **Apply**; alternatively click **Ignore** to proceed to the main menu if you do not want to change the password now.



Use this screen to change the password.

New Password:

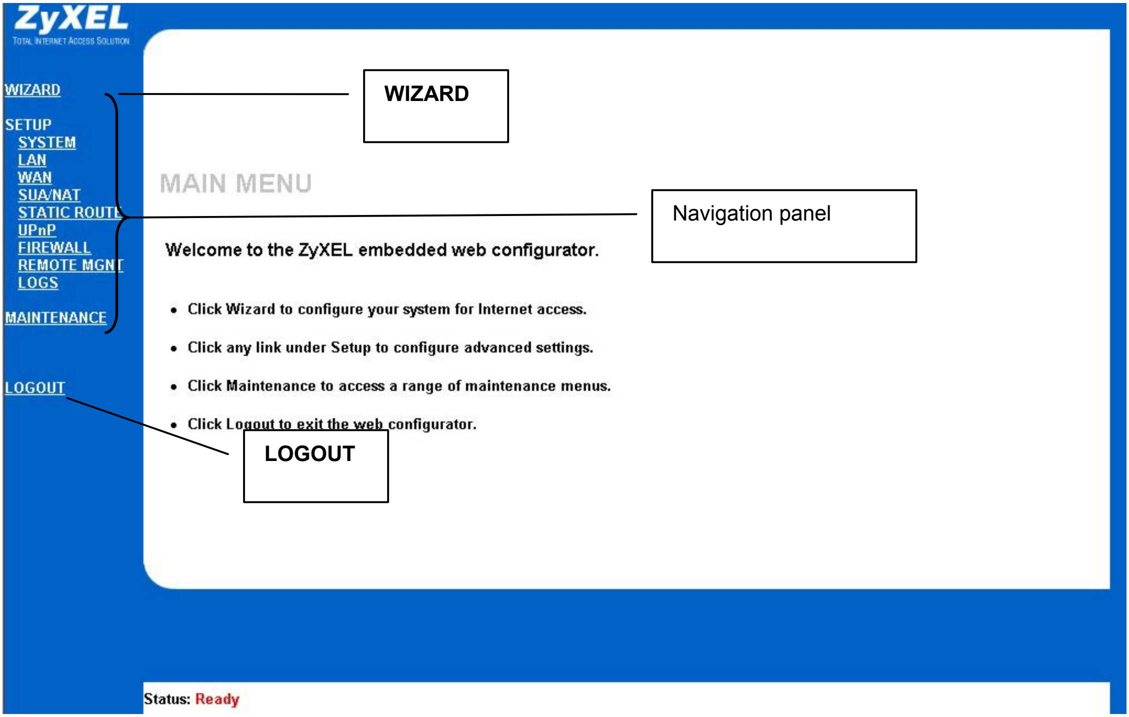
Retype to Confirm:

Change default password.

Figure 3-3 Change Password

Step 3. You should now see the web configurator **MAIN MENU** screen.

- Click **WIZARD** to begin a series of screens to help you configure your Prestige for the first time.
- Click a link under **SETUP** in the navigation panel to configure advanced Prestige features.
- Click **MAINTENANCE** in the navigation panel to see Prestige performance statistics, upload firmware and back up, restore or upload a configuration file.
- Click **LOGOUT** when you have finished a Prestige management session. The Prestige web configurator automatically logs you out if it is left idle for five minutes. This idle timeout timer is one of the many Prestige features that you may edit using the web configurator.



MAIN MENU

Welcome to the ZyXEL embedded web configurator.

- Click Wizard to configure your system for Internet access.
- Click any link under Setup to configure advanced settings.
- Click Maintenance to access a range of maintenance menus.
- Click Logout to exit the web configurator.

Status: Ready

Figure 3-4 The MAIN MENU Screen of the Web Configurator

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

The HELP ? icon does not appear in the MAIN MENU screen.

If you forget your password, refer to *section 5.3.1* to reset the default configuration file.

Chapter 4 Wizard Setup

This chapter shows you how to use the Wizard to access the Internet for the first time.

4.1 Introduction to Wizard Screens

The Wizard consists of screens to help you configure your device to access the Internet. The second screen has three variations depending on what encapsulation type you use. Refer to your ISP checklist in the *Quick Start Guide* to know what to enter in each field. Leave a field blank if you don't have that information.

4.1.1 General Setup and System Name

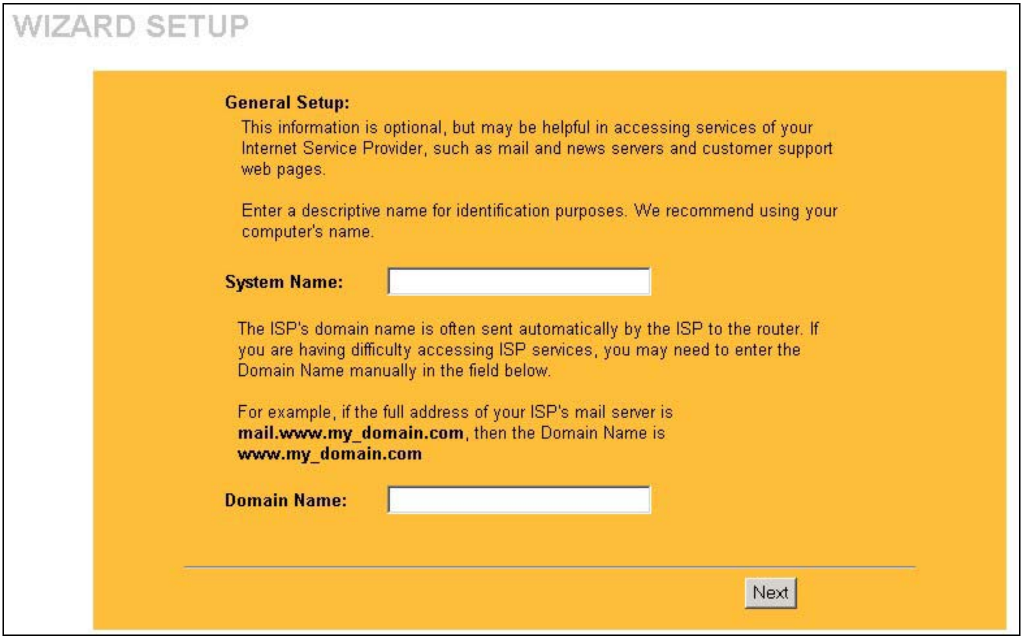
General Setup contains administrative and system-related information. **System Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name".

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

4.1.2 Domain Name

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

Click **Next** to configure the Prestige for internet access.



WIZARD SETUP

General Setup:

This information is optional, but may be helpful in accessing services of your Internet Service Provider, such as mail and news servers and customer support web pages.

Enter a descriptive name for identification purposes. We recommend using your computer's name.

System Name:

The ISP's domain name is often sent automatically by the ISP to the router. If you are having difficulty accessing ISP services, you may need to enter the Domain Name manually in the field below.

For example, if the full address of your ISP's mail server is **mail.www.my_domain.com**, then the Domain Name is **www.my_domain.com**

Domain Name:

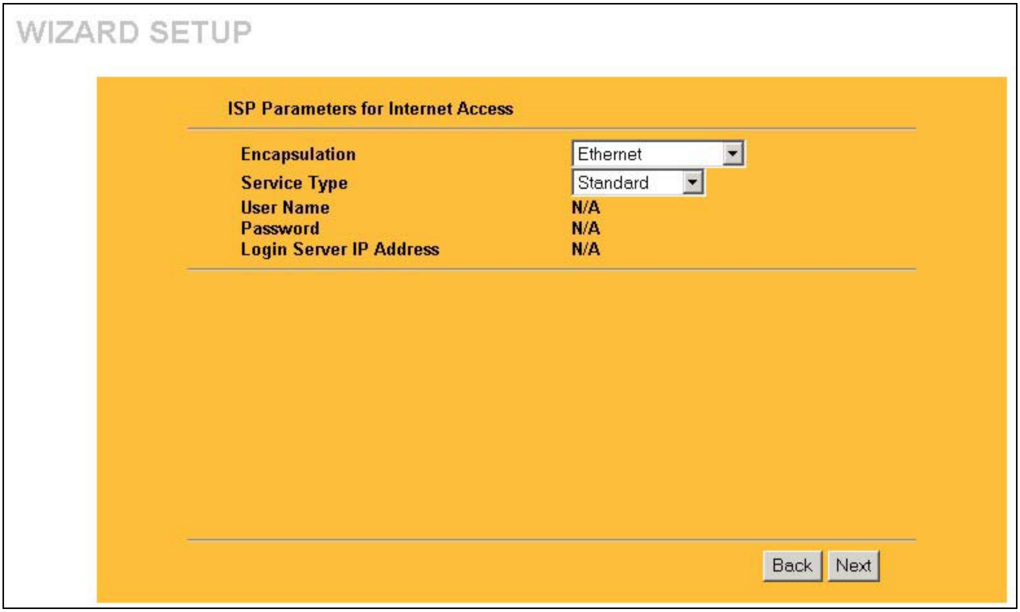
Figure 4-1 Wizard 1

4.2 Wizard Setup: Screen 2

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

4.2.1 Ethernet

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



WIZARD SETUP

ISP Parameters for Internet Access

Encapsulation: Ethernet

Service Type: Standard

User Name: N/A

Password: N/A

Login Server IP Address: N/A

Table 4-1 Wizard 2: Ethernet Encapsulation

Table 4-2 Ethernet Encapsulation

FIELD	**DESCRIPTION**
ISP Parameters for Internet Access	
Encapsulation	You must choose the **Ethernet** option when the WAN port is used as a regular Ethernet. Otherwise, choose **PPPoE** or **PPTP** for a dial-up connection.
Service Type	Choose from **Standard** or a RoadRunner version. The **User Name**, **Password** and **Login Server IP Address** fields are not applicable (N/A) for the latter.
To continue, click **Next**. To return to the previous screen, click **Back**.	

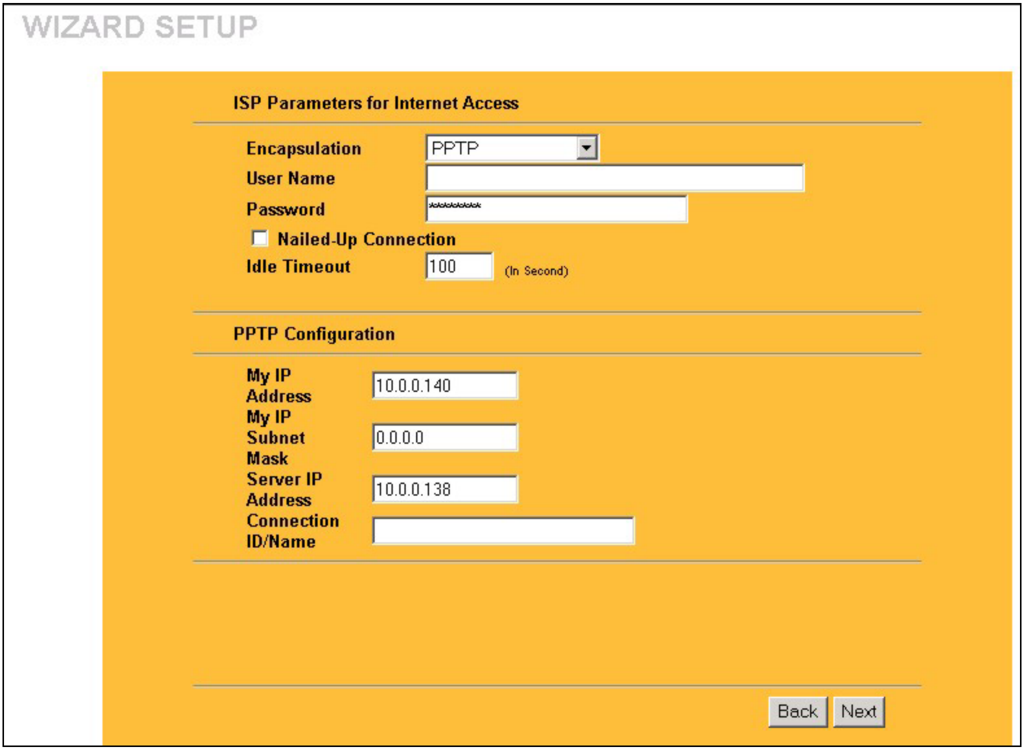
4.2.2 PPTP Encapsulation

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

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

For more information on PPTP, please refer to *the appendices*

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



WIZARD SETUP

ISP Parameters for Internet Access

Encapsulation: PPTP

User Name:

Password: ********

□ Nailed-Up Connection

Idle Timeout: 100 (In Second)

PPTP Configuration

My IP Address: 10.0.0.140

My IP Subnet Mask: 0.0.0.0

Server IP Address: 10.0.0.138

Connection ID/Name:

Figure 4-2 Wizard 2: PPTP Encapsulation

Table 4-3 PPTP Encapsulation

FIELD	DESCRIPTION
ISP Parameters for Internet Access	

Table 4-3 PPTP Encapsulation

FIELD	DESCRIPTION
Encapsulation	Select **PPTP** from the pull-down list box.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the User Name above.
Nailed Up Connection	Select **Nailed Up Connection** if you do not want the connection to time out.
Idle Timeout	Type the time in seconds that elapses before the router automatically disconnects from the PPTP server. The default is 45 seconds.
PPTP Configuration	
My IP Address	Type the (static) IP address assigned to you by your ISP.
My IP Subnet Mask	Type the subnet mask assigned to you by your ISP (if given).
Server IP Address	Type the IP address of the PPTP server.
Connection ID/Name	Enter the connection ID or connection name in this field. It must follow the "c:id" and "n:name" format. For example, C:12 or N:My ISP. This field is optional and depends on the requirements of your xDSL modem.
To continue, click **Next**. To return to the previous screen, click **Back**.	

4.2.3 PPPoE Encapsulation

Point-to-Point Protocol over Ethernet (PPPoE) functions as a dial-up connection. PPPoE is an IETF (Internet Engineering Task Force) draft standard specifying how a host personal computer interacts with a broadband modem (for example xDSL, cable, wireless, etc.) to achieve access to high-speed data networks. It preserves the existing Microsoft Dial-Up Networking experience and requires no new learning or procedures.

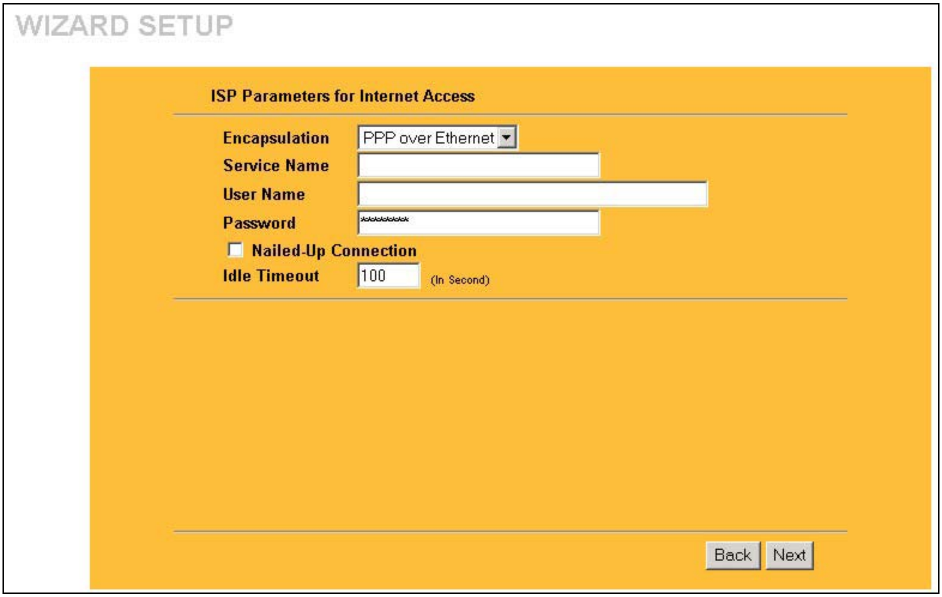
For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for instance, Radius). For the user, PPPoE provides a login and authentication method that the existing Microsoft Dial-Up Networking software can activate, and therefore requires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

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

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

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

For more information on PPPoE, please refer *Appendix A*.



WIZARD SETUP

ISP Parameters for Internet Access

Encapsulation: PPP over Ethernet

Service Name:

User Name:

Password: ********

□ Nailed-Up Connection

Idle Timeout: 100 (In Second)

Figure 4-3 Wizard2: PPPoE Encapsulation

Table 4-4 PPPoE Encapsulation

FIELD	DESCRIPTION
ISP Parameter for Internet Access	
Encapsulation	Choose an encapsulation method from the pull-down list box. PPPoE forms a dial-up connection.
Service Name (Optional)	Type the name of your service provider.
User Name	Type the user name given to you by your ISP.
Password	Type the password associated with the user name above.
Nailed Up Connection	Select **Nailed Up Connection** if you do not want the connection to time out.
Idle Timeout	Type the time in seconds that elapses before the router automatically disconnects from the PPPoE server. The default time is **100** seconds.
To continue, click **Next**. To return to the previous screen, click **Back**.	

4.3 Wizard Setup: Screen 3

4.3.1 WAN IP Address Assignment

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

Table 4-5 Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

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

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

4.3.2 IP Address and Subnet Mask

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

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

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

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.

4.3.3 DNS Server Address Assignment

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

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

1. The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the DNS Server fields in DHCP Setup.
2. Leave the DNS Server fields in DHCP Setup blank (for example 0.0.0.0). The Prestige acts as a DNS proxy when this field is blank.

4.3.4 WAN MAC Address

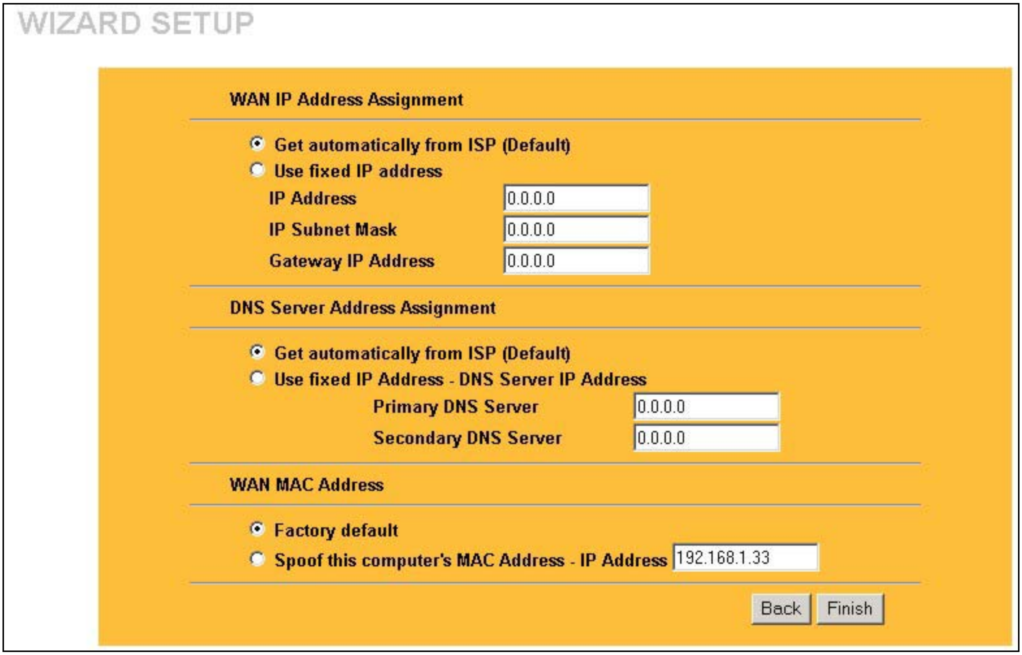
You can configure the WAN port's MAC Address by either using the factory default or cloning the MAC address from a workstation on your LAN. Once it is successfully configured, the address will be copied to the "rom" file (ZyNOS configuration file). It will not change unless you change the setting or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

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

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

Table 4-6 Example of Network Properties for LAN Servers with Fixed IP Addresses

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



WIZARD SETUP

WAN IP Address Assignment

● Get automatically from ISP (Default)
○ Use fixed IP address
IP Address 0.0.0.0
IP Subnet Mask 0.0.0.0
Gateway IP Address 0.0.0.0

DNS Server Address Assignment

● Get automatically from ISP (Default)
○ Use fixed IP Address - DNS Server IP Address
Primary DNS Server 0.0.0.0
Secondary DNS Server 0.0.0.0

WAN MAC Address

● Factory default
○ Spoof this computer's MAC Address - IP Address 192.168.1.33

Figure 4-4 Wizard 3

Table 4-7 WAN Setup

FIELD	DESCRIPTION
WAN IP Address Assignment	
Get automatically from ISP	Select this option If your ISP did not assign you a fixed IP address. This is the default selection.
Use fixed IP address	Select this option If the ISP assigned a fixed IP address.

Table 4-7 WAN Setup

FIELD	DESCRIPTION
IP Address	Enter your WAN IP address in this field when you selected **Use Fixed IP Address.**
IP Subnet Mask	Enter the IP subnet mask in this field if applicable when you selected **Use Fixed IP Address**. This field is not visible when you chose **PPPoE** encapsulation in the previous wizard screen.
Gateway IP Address	Enter the gateway IP address in this field if applicable when you selected **Use Fixed IP Address**. This field is not visible when you chose **PPPoE** encapsulation in the previous wizard screen.
DNS Server Address Assignment	
Get automatically from ISP	Select this option if your ISP does not give you DNS server addresses. This option is selected by default.
Use fixed IP address - DNS Server IP Address	Select this option If your ISP provides you a DNS server address.
Primary/Secondary DNS Server	If you selected the **Use fixed IP address – Primary/Secondary DNS Server** option, enter the provided DNS addresses in these fields.
WAN MAC Address	The MAC address field allows users to configure the WAN port's MAC Address by either using the factory default or cloning the MAC address from a workstation on your LAN.
Factory Default	Select this option to use the factory assigned default MAC Address.
Spoof this Computer's MAC address - IP Address	Select this option and enter the IP address of the workstation on the LAN whose MAC you are cloning. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting or upload a different rom file. It is advisable to clone the MAC address from a workstation on your LAN even if your ISP does not presently require MAC address authentication.
To return to the previous screen, click **Back**. To save and complete the wizard setup, click **Finish**.	

4.4 Basic Setup Complete

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

The rest of this *User's Guide* shows you how to configure the SMT menus except where no SMT menus exist for certain features such as UPnP and the firewall. For web configurator screens that have SMT menu equivalents, read this guide for background information, but refer to the web screen online help for actual screen configuration.

Chapter 5
Introducing the SMT and General Setup

This chapter shows you how to access the SMT menus via the console port, how to navigate the SMT and how to configure SMT menu 1.

5.1 Accessing the Prestige via the Console Port

Make sure you have the physical connection properly set up as described in the hardware installation chapter.

In addition to the contents of your package, there are other hardware and software requirements you need before you can install and use your Prestige. These requirements include:

1. A computer(s) with an installed Ethernet NIC (Network Interface Card).
2. A computer equipped with terminal emulation communications software configured to the following parameters:

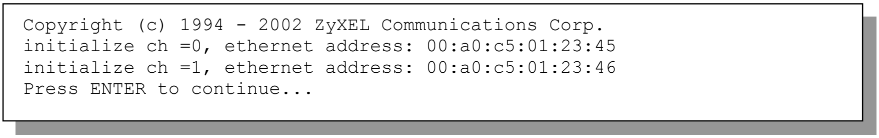
- ♦ VT100 terminal emulation.
- ♦ 9600 baud.
- ♦ No parity, 8 data bits, 1 stop bit, flow control set to none.

3. A cable/DSL modem and an ISP account.

5.1.1 Initial Screen

When you turn on your Prestige, it performs several internal tests as well as line initialization.

After the tests, the Prestige asks you to press [ENTER] to continue, as shown next.



```
Copyright (c) 1994 - 2002 ZyXEL Communications Corp.
initialize ch =0, ethernet address: 00:a0:c5:01:23:45
initialize ch =1, ethernet address: 00:a0:c5:01:23:46
Press ENTER to continue...
```

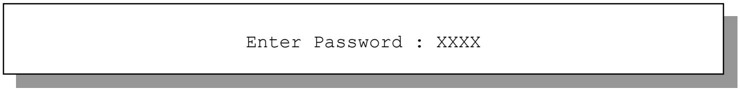
Figure 5-1 Initial Screen

5.1.2 Entering the 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 (X) for each character you type.

Note that if there is no activity for longer than five minutes after you log in, your Prestige will automatically log you out and will display a blank screen. If you see a blank screen, press [ENTER] to bring up the login screen again.



```
Enter Password : XXXX
```

Figure 5-2 Password Screen

5.2 Navigating the SMT Interface

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

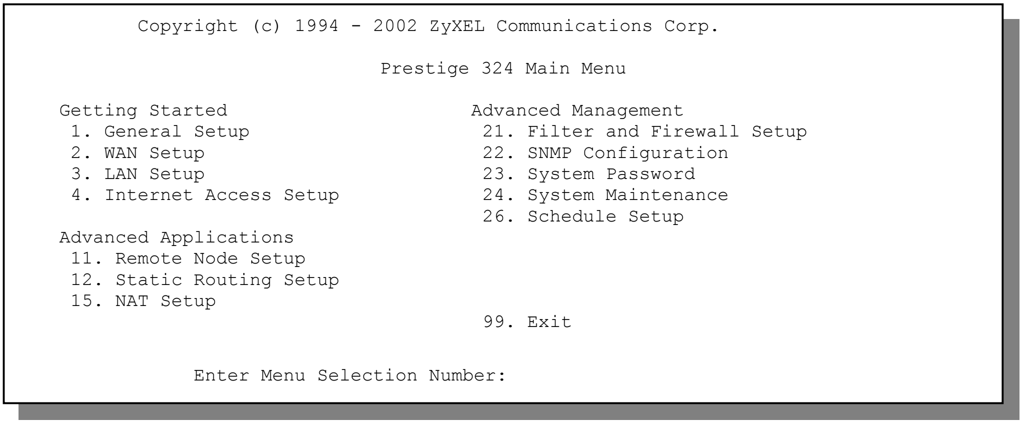
Several operations that you should be familiar with before you attempt to modify the configuration are listed next.

Table 5-1 Main Menu Commands

OPERATION	DESCRIPTION
Move down to another menu	To move forward to a submenu, type in the number of the desired submenu and press [ENTER].
Move up to a previous menu	Press the [ESC] key to move back to the previous menu.
Move to a “hidden” menu	Fields beginning with “Edit” lead to hidden menus and have a default setting of **No**. Press [SPACE BAR] to change **No** to **Yes**, and then press [ENTER] to go to a “hidden” menu.
Move the cursor	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	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] and then [ENTER].
Required fields	All fields with the symbol <?> or ChangeMe must be filled in order be able to save the new configuration.
N/A fields	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	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 at the main menu prompt and press [ENTER] to exit the SMT interface.

5.2.1 Main Menu

After you enter the password, the SMT displays the **Prestige Main Menu**, as shown next.



```
          Copyright (c) 1994 - 2002 ZyXEL Communications Corp.

                              Prestige 324 Main Menu

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


               Enter Menu Selection Number:
```

Figure 5-3 Prestige Main Menu

5.2.2 System Management Terminal Interface Summary

Table 5-2 Main Menu Summary

NO.	Menu Title	FUNCTION
1	General Setup	Use this menu to set up routing/bridging and general information.
2	WAN Setup	Use this menu to clone a MAC address from a computer on your LAN.
3	LAN Setup	Use this menu to configure LAN DHCP and TCP/IP settings as well as apply LAN filters.
4	Internet Access Setup	Configure your Internet Access setup (Internet address, gateway, login, etc.) with this menu.
11	Remote Node Setup	Use this menu to configure detailed remote node settings (your ISP is also a remote node) as well as apply WAN filters.
12	Static Routing Setup	Configure static routes for bridging and IP in this menu.
15	NAT Setup	Use this menu to configure network address translation.
21	Filter and Firewall Setup	Use these menus to activate the firewall and configure packet filters.
22	SNMP Configuration	Use this menu to configure SNMP-related parameters.
23	System Password	Change your password in this menu (recommended).

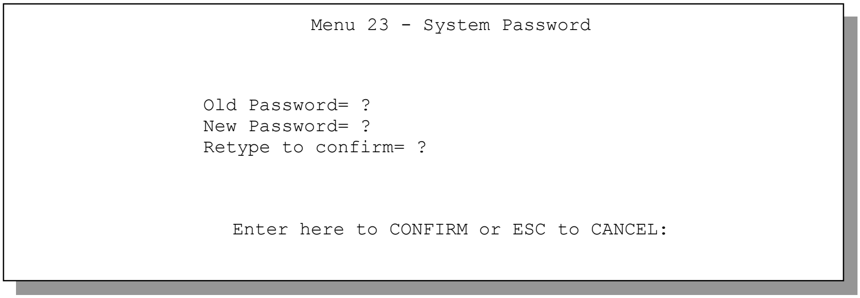
Table 5-2 Main Menu Summary

NO.	Menu Title	FUNCTION
24	System Maintenance	From displaying system status to uploading firmware, this menu provides comprehensive system maintenance.
26	Schedule Setup	Use this menu to schedule outgoing calls.
99	Exit	Use this menu to exit (necessary for remote configuration).

5.3 Changing the System Password

The first thing you should do is change the default system password by following the steps shown next.

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



```
                         Menu 23 - System Password



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



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

Figure 5-4 Menu 23 — System Security

Step 2. Enter your existing password and press [ENTER].

Step 3. Enter your new system password and press [ENTER].

Step 4. Re-type your new system password for confirmation and press [ENTER].

Note that as you type a password, the screen displays a (X) for each character you type.

5.3.1 Resetting the Prestige

If you forget your password or cannot access the SMT menu, you will need to reload the factory-default configuration file or use the **RESET** button the back of the Prestige. Uploading this configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all configurations that you had previously and the speed of the console port will be reset to the default of 9600bps with 8 data bit, no parity, one stop bit and flow control set to none. The password will be reset to “1234”, also.

Uploading a Configuration File Via Console Port

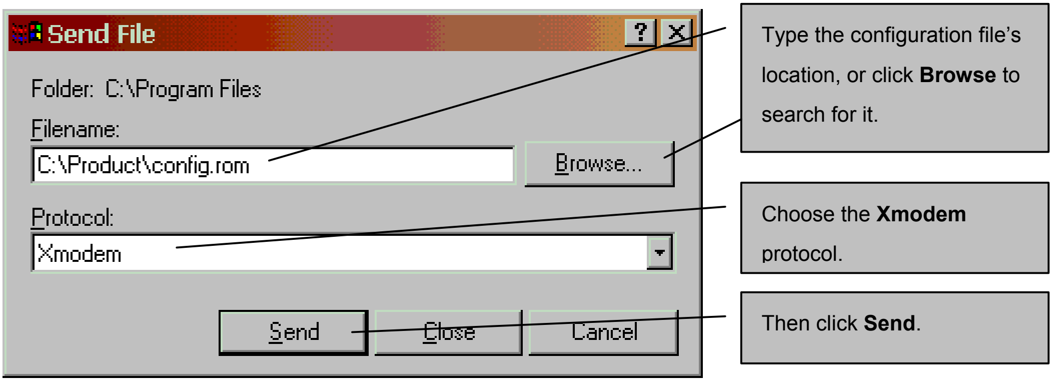
Turn off the Prestige, begin a terminal emulation software session and turn on the Prestige again. When you see the message "Press Any key to enter Debug Mode within 3 seconds", press any key to enter debug mode.

Step 1. Enter "y" at the prompt below to go into debug mode.

Step 2. Enter "atlc" after "Enter Debug Mode" message.

Step 3. Wait for "Starting XMODEM upload" message before activating Xmodem upload on your terminal. This is an example Xmodem configuration upload using HyperTerminal. You should already have downloaded the correct file from your nearest ZyXEL FTP site.

Step 4. Click **Transfer**, then **Send File** to display the following screen.



Folder: C:\Program Files

Filename: C:\Product\config.rom

Protocol: Xmodem

Type the configuration file’s location, or click **Browse** to search for it.

Choose the **Xmodem** protocol.

Then click **Send**.

Figure 5-5 Example Xmodem Upload

Step 5. After successful firmware upload, enter "atgo" to restart the router.

Procedure To Use The RESET Button

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

Step 1. Press the **RESET** button for ten seconds, then release it. If the **PWR** LED begins to blink, the defaults have been restored and the Prestige restarts. Otherwise, go to step 2.

Step 2. Turn the Prestige off.

Step 3. While pressing the **RESET** button, turn the Prestige on.

Step 4. Continue to hold the **RESET** button. The **PWR** LED will begin to blink and flicker very quickly after about 10 or 15 seconds. This indicates that the defaults have been restored and the Prestige is now restarting.

5.4 General Setup

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

- In Windows 95/98 click **Start**, **Settings**, **Control Panel**, **Network**. Click the **Identification** tab, note the entry for the **Computer Name** field and enter it as the **System Name**.
- In Windows 2000, click **Start**, **Settings**, **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**.
- In Windows XP, click **Start, Control Panel, System**. Click the **Computer Name** tab. Note the entry for the **Computer Description** field and enter this entry as the **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.

5.4.1 Dynamic DNS

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

First of all, you need to have registered a dynamic DNS account with www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that would still like to have a DNS name.

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

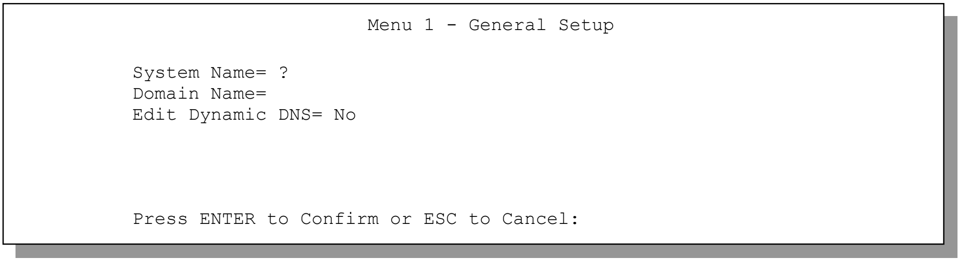
DYNDNS Wildcard

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

5.4.2 Procedure For Configuring Menu 1

Step 1. Enter 1 in the main menu to open **Menu 1 – General Setup** (shown next).

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



```
                                Menu 1 - General Setup

                 System Name= ?
                 Domain Name=
                 Edit Dynamic DNS= No





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

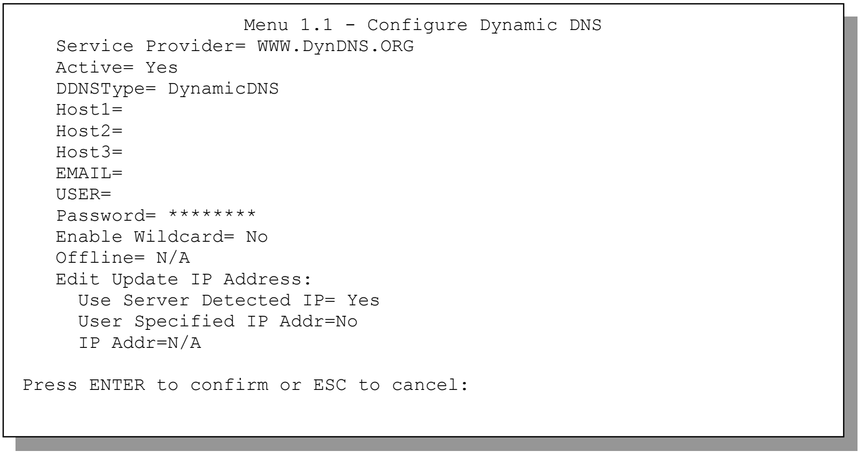
Figure 5-6 Menu 1 — General Setup

Table 5-3 General Setup Menu Field

FIELD	DESCRIPTION	EXAMPLE
System Name	Choose a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.	P324_PLUS
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**
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.		

5.4.3 Configuring Dynamic DNS

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



```
                    Menu 1.1 - Configure Dynamic DNS
     Service Provider= WWW.DynDNS.ORG
     Active= Yes
     DDNSType= DynamicDNS
     Host1=
     Host2=
     Host3=
     EMAIL=
     USER=
     Password= ********
     Enable Wildcard= No
     Offline= N/A
     Edit Update IP Address:
       Use Server Detected IP= Yes
       User Specified IP Addr=No
       IP Addr=N/A

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

Figure 5-7 Configure Dynamic DNS

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

Table 5-4 Configure Dynamic DNS Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Service Provider	This is the name of your Dynamic DNS service provider.	WWW.DynDNS.ORG (default)
Active	Press [SPACE BAR] to select **Yes** and then press [ENTER] to make dynamic DNS active.	**Yes**
DDNS Type	Press [SPACE BAR] and then [ENTER] to select **DynamicDNS** if you have a dynamic IP address(es). Select **StaticDNS** if you have a static IP address(s). Select **CustomDNS** to have dyns.org provide DNS service for a domain name that you already have from a source other than dyndns.org.	**DynamicDNS** (default)
Host1-3	Enter your host name(s) in the fields provided. You can specify up to two host names separated by a comma in each field.	me.dyndns.org
EMAIL	Enter your e-mail address.	mail@mailserver
USER	Enter your user name.	
Password	Enter the password assigned to you.	

Table 5-4 Configure Dynamic DNS Menu Fields

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

The IP address will be updated when you reconfigure menu 1 or perform DHCP client renewal. If you have a private WAN IP address, then you cannot use Dynamic DNS.

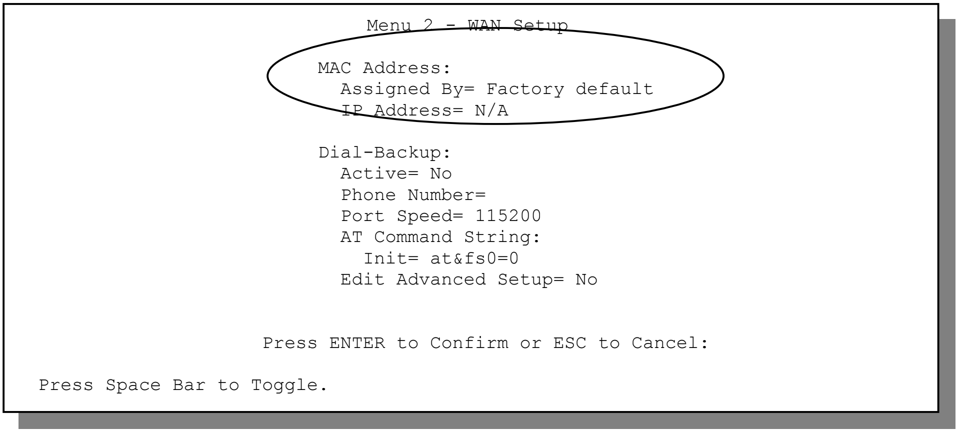
Chapter 6
WAN Setup and Dial Backup

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

6.1 Cloning The MAC Address

The MAC address field allows users to configure the WAN port's MAC address by using either the factory default or cloning the MAC address from a computer on your LAN. Once it is successfully configured, the address will be copied to the rom file (ZyNOS configuration file). It will not change unless you change the setting in menu 2 or upload a different rom file.

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



```
                              Menu 2 - WAN Setup

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

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


                   Press ENTER to Confirm or ESC to Cancel:

  Press Space Bar to Toggle.
```

Figure 6-1 MAC Address Cloning in WAN Setup Menu

Table 6-1 MAC Address Cloning in WAN Setup Menu

FIELD	DESCRIPTION	EXAMPLE
MAC Address:		
Assigned By	Press [SPACE BAR] and then [ENTER] to choose one of two methods to assign a MAC Address. Choose **Factory Default** to select the factory assigned default MAC Address. Choose **IP address attached on LAN** to use the MAC Address of that workstation whose IP you give in the following field.	**IP address attached on LAN**
IP Address	This field is applicable only if you choose the **IP address attached on LAN** method in the **Assigned By** field. Enter the IP address of the computer on the LAN whose MAC you are cloning.	192.168.1.35
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.		

6.2 Dial Backup

The AUX/CON port can be used in reserve, as a traditional dial-up connection should the broadband connection from the WAN port fail. To set up the auxiliary port (Dial Backup) for use in the event that the regular WAN connection is dropped, first make sure you have set up the CON/AUX switch and port connection (see the *Hardware Installation* chapter), then configure:

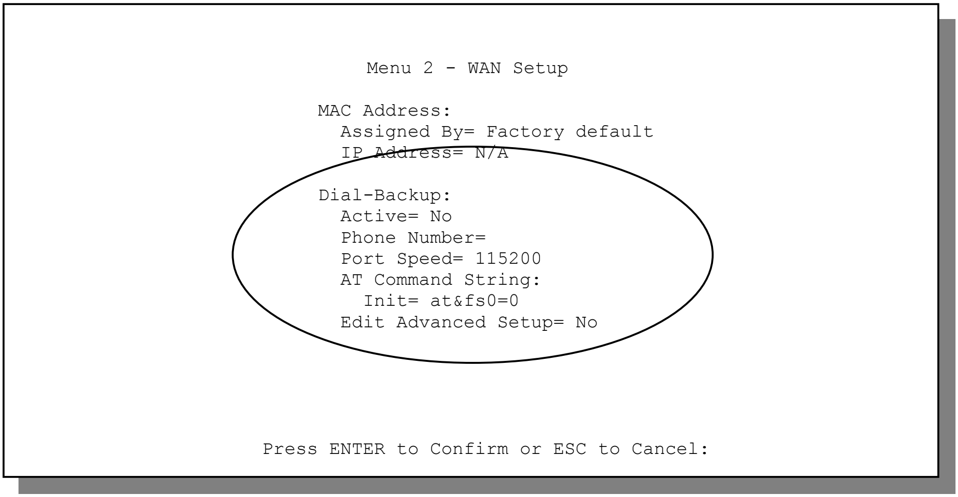
Menu 2 - WAN Setup,

Menu 2.1 - Advanced WAN Setup and

Menu 11.1 - Remote Node Profile (Backup ISP) as shown next.

Refer also to the traffic redirect section in this User's Guide for information on an alternate backup WAN connection.

6.2.1 Configuring Dial Backup in Menu 2



```
                   Menu 2 - WAN Setup

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

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




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

Figure 6-2 Configuring Dial Backup in Menu 2

The following table contains instructions on how to configure your WAN setup.

Table 6-2 Configuring Dial Backup in Menu 2

FIELD	DESCRIPTION	EXAMPLE
Dial-Backup:		
Active	Use this field to turn the dial-backup feature on (**Yes**) or off (**No**).	**No**
Phone Number	Enter the telephone number assigned to your line by your telephone company. This field only accepts digits; do not include dashes and spaces.	1234567
Port Speed	Press [SPACE BAR] and then press [ENTER] to select the speed of the connection between the Dial Backup port and the external device. Available speeds are: **9600**, **19200**, **38400**, **57600**, **115200** or **230400** bps.	**115200**
AT Command String:		
Init	Enter the AT command string to initialize the WAN device. Consult the manual of your WAN device connected to your Dial Backup port for specific AT commands.	at&fs0=0

Table 6-2 Configuring Dial Backup in Menu 2

FIELD	DESCRIPTION	EXAMPLE
Edit Advanced Setup	To edit the advanced setup for the Dial Backup port, move the cursor to this field; press the [SPACE BAR] to select **Yes** and then press [ENTER] to go to **Menu 2.1: Advanced Setup**.	**Yes**
When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel.		

6.2.2 Configuring Dial Backup Using Advanced WAN Setup

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

6.2.3 AT Command Strings

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

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

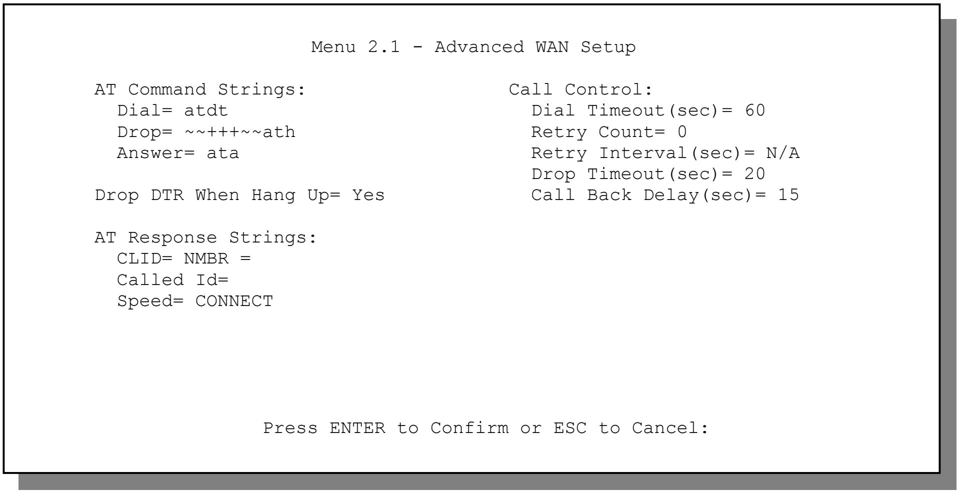
6.2.4 DTR Signal

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

6.2.5 Response Strings

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

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



```
                         Menu 2.1 - Advanced WAN Setup

        AT Command Strings:                   Call Control:
          Dial= atdt                            Dial Timeout(sec)= 60
          Drop= ~~+++~~ath                      Retry Count= 0
          Answer= ata                           Retry Interval(sec)= N/A
                                                Drop Timeout(sec)= 20
        Drop DTR When Hang Up= Yes              Call Back Delay(sec)= 15

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




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

Figure 6-3 Menu 2.1 Advanced WAN Setup

The following table describes fields in this menu.

Table 6-3 Advanced WAN Port Setup: AT Commands Fields

FIELD	DESCRIPTION	DEFAULT
AT Command Strings:		
Dial	Enter the AT Command string to make a call.	atdt
Drop	Enter the AT Command string to drop a call. "~" represents a one second wait, e.g., "~~~+++~~ath" can be used if your modem has a slow response time.	+++ath
Answer	Enter the AT Command string to answer a call.	ata
Drop DTR When Hang Up	Press the [SPACE BAR] to choose either **Yes** or **No**. When **Yes** is selected (the default), the DTR (Data Terminal Ready) signal is dropped after the "AT Command String: Drop" is sent out.	**Yes**

Table 6-3 Advanced WAN Port Setup: AT Commands Fields

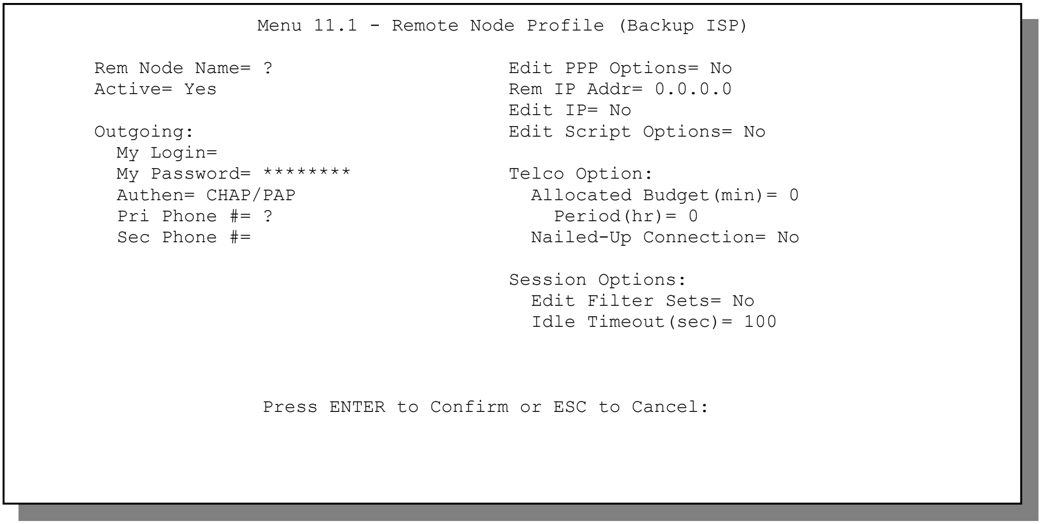
FIELD	DESCRIPTION	DEFAULT
AT Response String:		
CLID (Calling Line Identification)	Enter the keyword that precedes the CLID (Calling Line Identification) in the AT response string. This lets the Prestige capture the CLID in the AT response string that comes from the WAN device. CLID is required for CLID authentication.	NMBR =
Called Id	Enter the keyword preceding the dialed number.	TO
Speed	Enter the keyword preceding the connection speed.	CONNECT

Table 6-4 Advanced WAN Port Setup: Call Control Parameters

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

6.2.6 Configuring Remote Node Profile (Backup ISP)

Enter **2** in **Menu 11 Remote Node Setup** to open **Menu 11.1 Remote Node Profile (Backup ISP)** (shown below) and configure the setup for your Dial Backup port connection. Not available on all models.



```
                    Menu 11.1 - Remote Node Profile (Backup ISP)

       Rem Node Name= ?                    Edit PPP Options= No
       Active= Yes                         Rem IP Addr= 0.0.0.0
                                           Edit IP= No
       Outgoing:                           Edit Script Options= No
         My Login=
         My Password= ********             Telco Option:
         Authen= CHAP/PAP                    Allocated Budget(min)= 0
         Pri Phone #= ?                        Period(hr)= 0
         Sec Phone #=                        Nailed-Up Connection= No

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



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

Figure 6-4 Menu 11.1 Remote Node Profile (Backup ISP)

Table 6-5 Menu 11.1 Remote Node Profile (Backup ISP)

FIELD	DESCRIPTION	EXAMPLE
Rem Node Name	Enter a descriptive name for the remote node. This field can be up to eight characters.	LAoffice
Active	Press [SPACE BAR] and then [ENTER] to select **Yes** to enable the remote node or **No** to disable the remote node.	**Yes**
Outgoing		
My Login	Enter the login name assigned by your ISP for this remote node.	jim
My Password	Enter the password assigned by your ISP for this remote node.	*****

Table 6-5 Menu 11.1 Remote Node Profile (Backup ISP)

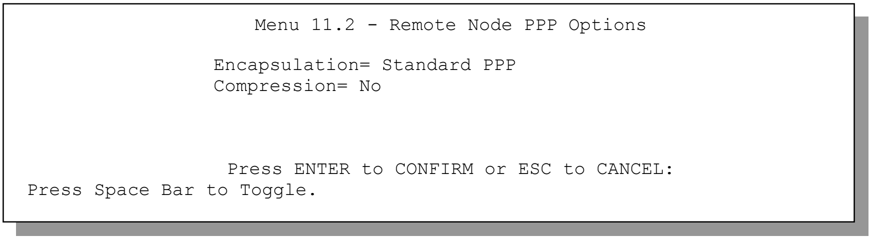
FIELD	DESCRIPTION	EXAMPLE
Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are: **CHAP**/**PAP** - Your Prestige will accept either **CHAP** or **PAP** when requested by this remote node. **CHAP** - accept CHAP only. **PAP** - accept PAP only.	**CHAP/PAP**
Pri Phone # Sec Phone #	Enter the first (primary) phone number from the ISP for this remote node. If the Primary Phone number is busy or does not answer, your Prestige dials the Secondary Phone number if available. Some areas require dialing the pound sign # before the phone number for local calls. Include a # symbol at the beginning of the phone numbers as required.	
Edit PPP Options	Move the cursor to this field and use the space bar to select **Yes** and press [ENTER] to edit the PPP options for this remote node. This brings you to **Menu 11.2 - Remote Node PPP Options** (see *section 6.2.7.*	**No** (default)
Edit PPP Options	Move the cursor to this field and use the space bar to select **Yes** and press [ENTER] to edit the PPP options for this remote node. This brings you to **Menu 11.2 - Remote Node PPP Options** (see *section 6.2.7.*	**No** (default)
Rem IP Addr	Leave the field set to 0.0.0.0 (default) if the remote gateway has a dynamic IP address. Enter the remote gateway's IP address here if it is static.	0.0.0.0 (default)
Edit IP	This field leads to a "hidden" menu. Press [SPACE BAR] to select **Yes** and press [ENTER] to go to M**enu 11.3 - Remote Node Network Layer Options**. See the *Remote Node Setup* chapter for more information on this menu	**No** (default)
Edit Script Options	Press [SPACE BAR] to select **Yes** and press [ENTER] to edit the AT script for the dial backup remote node (**Menu 11.4 - Remote Node Script**). See *section 6.2.8* for more details.	**No** (default)
Edit Script Options	Press [SPACE BAR] to select **Yes** and press [ENTER] to edit the AT script for the dial backup remote node (**Menu 11.4 - Remote Node Script**). See *section 6.2.8* for more details.	**No** (default)
Telco Option		

Table 6-5 Menu 11.1 Remote Node Profile (Backup ISP)

FIELD	DESCRIPTION	EXAMPLE
Allocated Budget	Enter the maximum number of minutes that this remote node may be called within the time period configured in the **Period** field. The default for this field is 0 meaning there is no budget control and no time limit for accessing this remote node.	0 (default)
Period(hr)	Enter the time period (in hours) for how often the budget should be reset. For example, to allow calls to this remote node for a maximum of 10 minutes every hour, set the **Allocated Budget** to 10 (minutes) and the **Period** to 1 (hour).	0 (default)
Nailed-Up Connection	Press [SPACE BAR] to select **Yes** to set this connection to always be on, regardless of whether or not there is any traffic. Select **No** to have this connection act as a dial-up connection.	**No** (default)
Session Options		
Edit Filter sets	This field leads to another "hidden" menu. Use [SPACE BAR] to select **Yes** and press [ENTER] to open menu 11.5 to edit the filter sets.	**No** (default)
Idle Timeout	Enter the number of seconds of idle time (when there is no traffic from the Prestige to the remote node) that can elapse before the Prestige automatically disconnects the PPP connection. This option only applies when the Prestige initiates the call.	100 seconds (default)
Once you have configured this menu, press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		

6.2.7 Editing PPP Options

To edit the remote node PPP Options, move the cursor to the **Edit PPP Options** field in **Menu 11.1 - Remote Node Profile**, and press [SPACE BAR] to select **Yes** and open Menu 11.2, as shown next.



```
                          Menu 11.2 - Remote Node PPP Options

                      Encapsulation= Standard PPP
                      Compression= No



                        Press ENTER to CONFIRM or ESC to CANCEL:
 Press Space Bar to Toggle.
```

Figure 6-5 Menu 11.2 - Remote Node PPP Options

Table 6-6 Menu 11.2 - Remote Node PPP Options

FIELD	DESCRIPTION
Encapsulation	Select the vendor-specific encapsulation for the link. There are two options in this field.
	Standard PPP - Standard PPP encapsulation is used.
	CISCO PPP - Cisco PPP encapsulation is used.
Compression	Turn on/off Stac data compression. The default for this field is Off.
Once you have completed filling in **Menu 11.2 - Remote Node PPP Options**, press [ENTER] at the message “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.	

6.2.8 Edit Script Options

The Prestige provides this script facility if text login is required before PPP negotiation is started. The script consists of programmable sets; each set is composed of an **Expect** string and a **Send** string. After matching a message from the server to the **Expect** field, the Prestige returns the set’s **Send** string to the server.

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

Welcome to Acme, Inc.

Login: myLogin

Password:

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

You can use two variables, $USERNAME and $PASSWORD (all UPPER case), to represent the actual user name and password in the script, so they will not show in clear text. They are replaced with the outgoing login name and password in the advanced dial backup setup screen, when the Prestige sees them in a **Send** string. Please note that both variables must been entered exactly as shown.

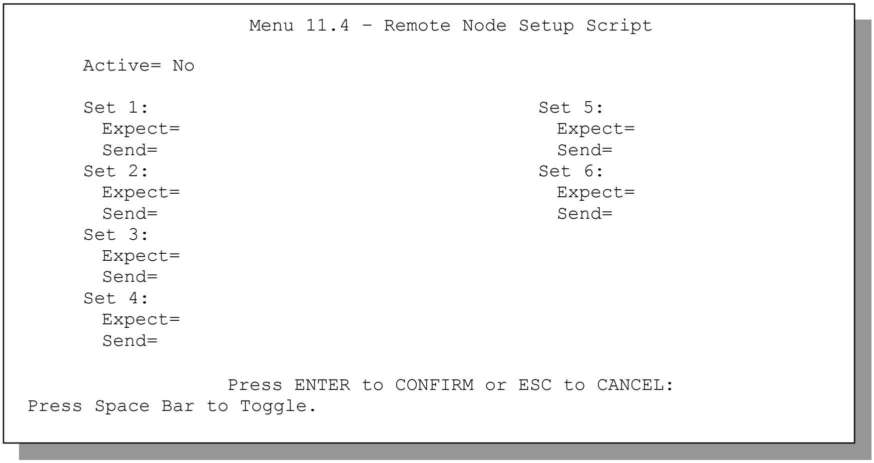
Also note that the ordering of the sets is significant, i.e., starting from set 1, the Prestige will wait until the **Expect** string is matched before it proceeds to set 2, and so on for the rest of the script. When both the **Expect** and the **Send** fields of the current set are empty, the Prestige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

login successful.

Starting PPP...

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

If there are errors in the script and it gets stuck at a set for longer than the **Dial Timeout** in the advanced dial backup setup screen, then Prestige will timeout and drop the line. To debug a script, initiate a manual call and watch the trace display to see if the sequence of messages and prompts from the server differs from what you expect.



```
                     Menu 11.4 - Remote Node Setup Script

     Active= No

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

                   Press ENTER to CONFIRM or ESC to CANCEL:
Press Space Bar to Toggle.
```

Figure 6-6 Remote Node Setup Script

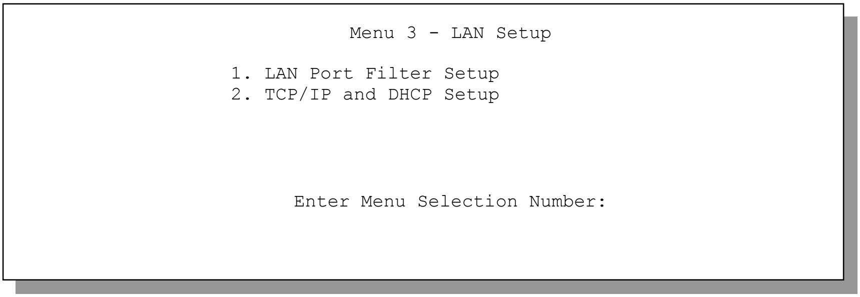
FIELD	DESCRIPTION
Active	Press the space bar to toggle between Yes and No.
Set 1-6: Expect	Enter an **Expect** string to match. After matching the **Expect** string, the Prestige returns the string in the **Send** field.
Set 1-6: Send	Enter a string to send out after the **Expect** string is matched.

Chapter 7
LAN Setup

This chapter describes how to configure the WAN using menu 3.

7.1 Introduction

From the main menu, enter 3 to display menu 3 (shown next).

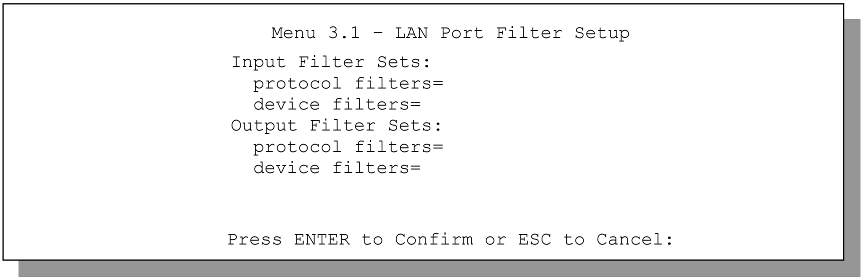


```
                        Menu 3 - LAN Setup

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





                    Enter Menu Selection Number:
```

Figure 7-1 Menu 3 — LAN Setup

7.1.1 LAN Port Filter Setup

This menu allows you to specify the filter sets that you wish to apply to the LAN traffic. You seldom need to filter the LAN 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 7-2 Menu 3.1 — LAN Port Filter Setup

Menu 3.2 is discussed in the next part of the manual. Please read on.

7.2 TCP/IP and DHCP for LAN

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

7.2.1 Factory LAN Defaults

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

1. IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits)
2. 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), skip to the *DNS Server Address section* to see how to enter the DNS server address(es).

7.2.2 DHCP Configuration

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 workstation must be manually configured.

IP Pool Setup

The Prestige is pre-configured with a pool of 32 IP addresses starting from 192.168.1.33 to 192.168.1.64. This configuration leaves 31 IP addresses (excluding the Prestige itself) in the lower range for other server computers, e.g., server for mail, FTP, telnet, web, etc., that you may have.

DNS Server Address

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

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

1. The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the **DNS Server** fields in DHCP Setup**.**
2. Leave the **DNS Server** fields in DHCP Setup blank (for example 0.0.0.0). The Prestige acts as a DNS proxy when this field is blank.

Table 7-1 Example of Network Properties for LAN Servers with Fixed IP Addresses

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

7.2.3 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 workstation on that network.

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

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.

7.2.4 Private IP Addresses

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

Table 7-2 Private IP Address Ranges

10.0.0.0 — 10.255.255.255
172.16.0.0 — 172.31.255.255
192.168.0.0 — 192.168.255.255

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

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address

assignment, please refer to *RFC 1597, Address Allocation for Private Internets* and *RFC 1466, Guidelines for Management of IP Address Space.*

7.2.5 RIP Setup

RIP (Routing Information Protocol, RFC1058 and RFC 1389) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. When set to **Both** or **Out Only**, the Prestige will broadcast its routing table periodically. When set to **Both** or **In Only**, it will incorporate the RIP information that it receives; when set to **None**, it will not send any RIP packets and will ignore any RIP packets received.

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. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.

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

7.2.6 IP Multicast

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

IGMP (Internet Group Multicast Protocol) is a session-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 using menus 3.2 (LAN) and 11.3 (WAN). Select **None** to disable IP Multicasting on these interfaces.

7.2.7 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.

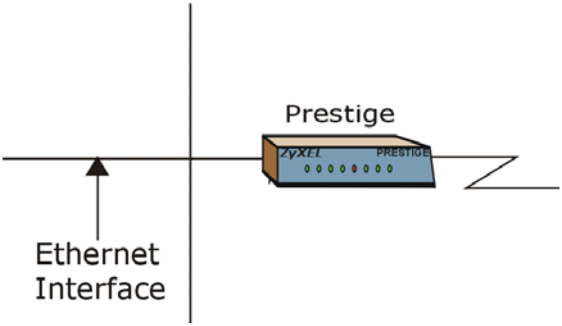


Figure 7-3 Physical Network

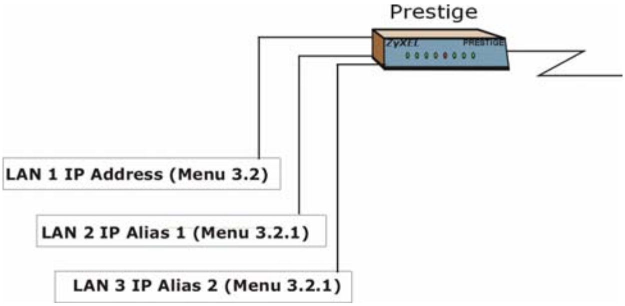
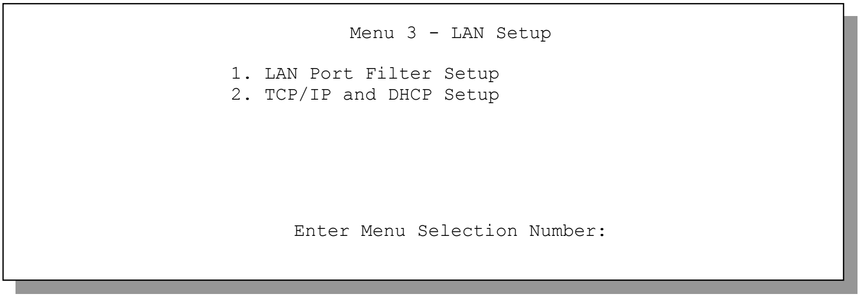

Prestige
ZyXEL
PRESTIGE
LAN 1 IP Address (Menu 3.2)
LAN 2 IP Alias 1 (Menu 3.2.1)
LAN 3 IP Alias 2 (Menu 3.2.1)

Figure 7-4 Partitioned Logical Networks

Use menu 3.2.1 to configure IP Alias on your Prestige.

7.3 TCP/IP and DHCP Ethernet Setup

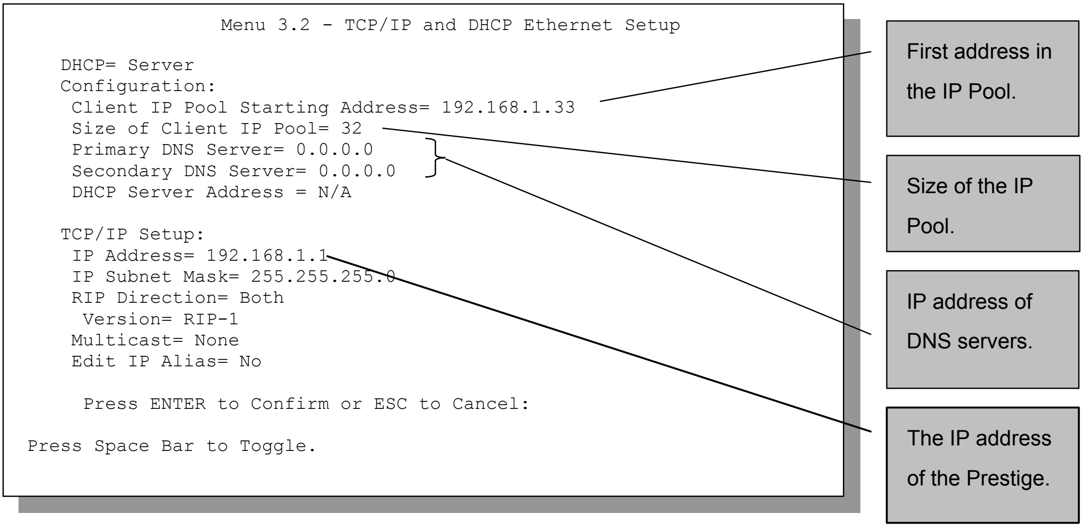
From the main menu, enter 3 to open **Menu 3 - LAN Setup** (10/100 Mbps Ethernet) to configure TCP/IP (RFC 1155) and DHCP Ethernet setup.



```
                          Menu 3 - LAN Setup

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






                     Enter Menu Selection Number:
```

Figure 7-5 Menu 3 — LAN Setup (10/100 Mbps Ethernet)

To edit the TCP/IP and DHCP configuration, enter 2 to display **Menu 3.2 - TCP/IP and DHCP Ethernet Setup** as shown next.



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

     DHCP= Server
     Configuration:
      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
      DHCP Server Address = 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
      Edit IP Alias= No

       Press ENTER to Confirm or ESC to Cancel:

  Press Space Bar to Toggle.
```

First address in the IP Pool.

Size of the IP Pool.

IP address of DNS servers.

The IP address of the Prestige.

Figure 7-6 Menu 3.2 — TCP/IP and DHCP Ethernet Setup

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

Table 7-3 LAN DHCP Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
DHCP	This field enables/disables the DHCP server. If it is set to **Server**, your Prestige will act as a DHCP server. If set to **None**, DHCP service will be disabled and you must have another DHCP sever on your LAN, or else the workstation must be manually configured. When DHCP is set to **Server**, the following four items need to be set.	**Server** (default)
Configuration: Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.	192.168.1.33
Size of Client IP Pool	This field specifies the size, or count, of the IP address pool.	32
Primary DNS Server Secondary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask. Leave these entries at 0.0.0.0 if a WAN DHCP server provides them.	

Follow the instructions in the table shown next to configure TCP/IP parameters for the LAN port.

Table 7-4 LAN TCP/IP Setup Menu Fields

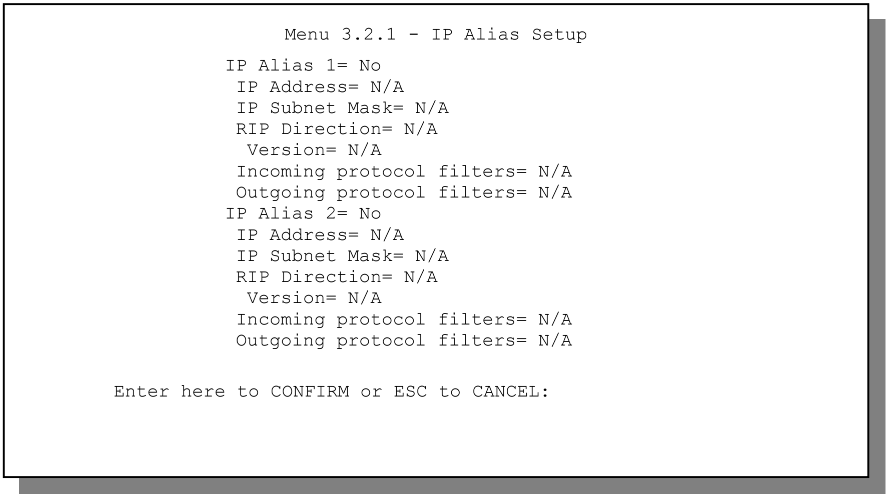
FIELD	DESCRIPTION	EXAMPLE
TCP/IP Setup: IP Address	Enter the IP address of your Prestige in dotted decimal notation	192.168.1.1 (default)
IP Subnet Mask	Your Prestige will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Prestige	255.255.255.0
RIP Direction	Press the [SPACE BAR] to select the RIP direction. Options are **Both**, **In Only**, **Out Only** or **None**.	**Both** (default)
Version	Press the [SPACE BAR] to select the RIP version. Options are **RIP-1**, **RIP-2B** or **RIP-2M**.	**RIP-1** (default)
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The Prestige supports both IGMP version 1 (**IGMP-v1**) and **IGMP-v2**. Press the [SPACE BAR] to enable IP Multicasting or select **None** (default) to disable it.	**None**

FIELD	DESCRIPTION	EXAMPLE
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 the [SPACE BAR] to select **Yes**, then press [ENTER] to display menu 3.2.1	**Yes**
When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm…] to save your configuration, or press [ESC] at any time to cancel.		

7.3.1 IP Alias Setup

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

Pressing [ENTER] opens **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 7-7 Menu 3.2.1 — IP Alias Setup

Follow the instructions in the table shown next to configure IP Alias parameters.

Table 7-5 IP Alias Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
IP Alias	Choose **Yes** to configure the LAN network for the Prestige.	**Yes**

Table 7-5 IP Alias Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
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 the [SPACE BAR] to select the RIP direction. Options are **None**, **Both**, **In Only** or **Out Only**.	**None**
Version	Press the [SPACE BAR] to select the RIP version. Options are **RIP-1**, **RIP-2B** or **RIP-2M**.	**RIP-1**
Incoming Protocol Filters	Enter the filter set(s) you wish to apply to the incoming traffic between this node and the Prestige.	
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.		

Chapter 8
Internet Access

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

8.1 Internet Access Setup

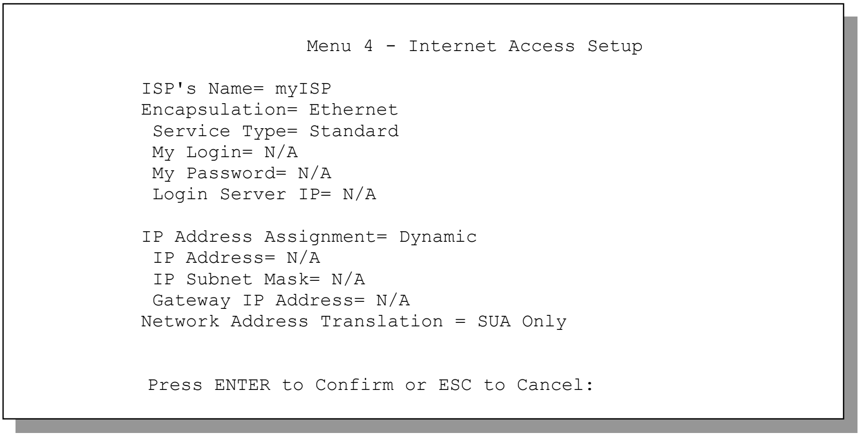
You will see three different menu 4 screens depending on whether you chose **Ethernet, PPTP** or **PPPoE** encapsulation.

In the **Encapsulation** field in menu 4, choose:

- Ethernet when the WAN port is used as a regular Ethernet.
- PPTP or PPPoE if you have a dial-up connection to the Internet.

8.1.1 Ethernet Encapsulation

You must choose the **Ethernet** option when the WAN port is used as a regular Ethernet. If you choose **Ethernet** in menu 4 you will see the next screen.



```
                    Menu 4 - Internet Access Setup

            ISP's Name= myISP
            Encapsulation= Ethernet
             Service Type= Standard
             My Login= N/A
             My Password= N/A
             Login Server IP= N/A

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


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

Figure 8-1 Internet Access Setup (Ethernet)

The following table describes this screen.

Table 8-1 Internet Access Setup Menu Fields

FIELD	DESCRIPTION
ISP's Name	Enter the name of your Internet Service Provider, e.g., myISP. This information is for identification purposes only.
Encapsulation	Press the [SPACE BAR] and then press [ENTER] to choose **Ethernet**. The encapsulation method influences your choices for IP Address.
Service Type	This is applicable only when you choose Ethernet as your encapsulation method. Press the [SPACE BAR] to select **Standard**, **RR-Toshiba** (RoadRunner Toshiba authentication method), **RR-Manager** (RoadRunner Manager authentication method) or **RR-Telstra** (RoadRunner Telstra authentication method). Choose a RoadRunner service type if your ISP is Time Warner's RoadRunner; otherwise choose **Standard**.
Note: xDSL users must choose the **Standard** option only. The **Server IP**, **My Login IP** and **My Password** fields are not applicable in this case.	
My Login	Enter the login name given to you by your ISP.
My Password	Enter the password associated with the login name above.
Login Server IP	The Prestige will find the RoadRunner Server IP if this field is left blank. If it does not, then you must enter the authentication server IP address.

Table 8-1 Internet Access Setup Menu Fields

FIELD	DESCRIPTION
IP Address Assignment	If your ISP did not assign you a fixed IP address, select **Dynamic**, otherwise select **Static** and enter the IP address & subnet mask in the following fields.
IP Address	Enter the (fixed) IP address assigned to you by your ISP (Static IP Address Assignment is selected in the previous field).
IP Subnet Mask	Enter the subnet mask associated with your static IP.
Gateway IP Address	Enter the gateway IP address associated with your static IP.
Network Address Translation	Refer to the following chapter for a more detailed discussion on the Single User Account and NAT. Options are **SUA only, Full Feature** or **None**.
Once you have finished configuring a rule in this menu, press [ENTER] at the message “Press ENTER to Confirm…” to save your configuration, or press [ESC] to cancel.	

8.1.2 PPTP Encapsulation

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

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

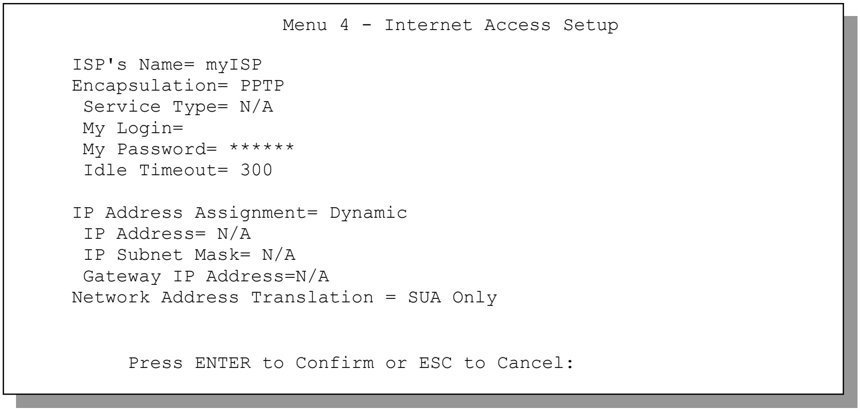
The P324 supports one PPTP server connection at any given time.

8.1.3 Configure PPTP Client

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

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

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



```
                        Menu 4 - Internet Access Setup

      ISP's Name= myISP
      Encapsulation= PPTP
       Service Type= N/A
       My Login=
       My Password= ******
       Idle Timeout= 300

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


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

Figure 8-2 Internet Access Setup (PPTP)

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

Table 8-2 New Fields in Menu 4 (PPTP) screen

FIELD	DESCRIPTION	EXAMPLE
Encapsulation	Press the [SPACE BAR] and then press [ENTER] to choose PPTP. The encapsulation method influences your choices for IP Address.	**PPTP**
Idle Timeout	This value specifies the time in seconds that elapses before the Prestige automatically disconnects from the PPTP server.	300 (default)

8.1.4 PPPoE Encapsulation

The Prestige supports PPPoE (Point-to-Point Protocol over Ethernet). You can use PPPoE encapsulation only when you're using the Prestige with an xDSL modem as the WAN device.

PPPoE is an IETF Draft standard specifying how a host personal computer interacts with a broadband modem (i.e. xDSL, cable, wireless, etc.) to achieve access to high-speed data networks. It preserves the existing Microsoft Dial-Up Networking experience and requires no new learning or procedures.

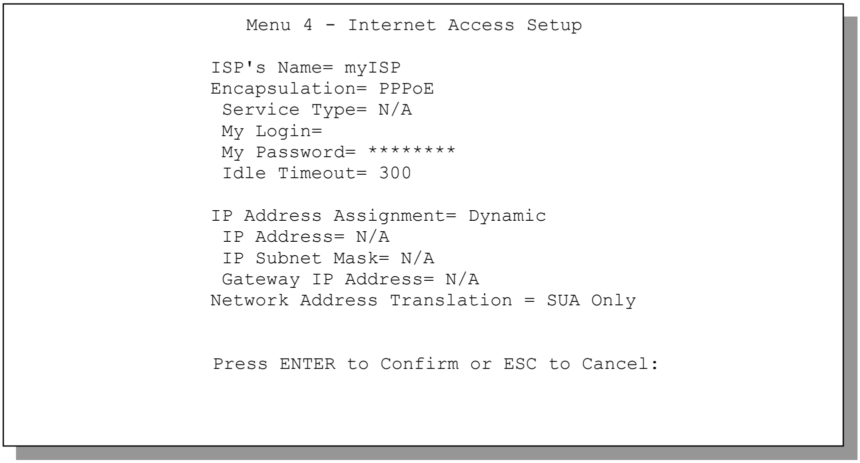
For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (e.g., Radius). For the user, PPPoE provides a login and authentication method that the existing Microsoft Dial-Up Networking software can activate, and therefore requires no new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

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

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

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

If you enable PPPoE in menu 4, you will see the next screen. For more information on PPPoE, please refer to the *PPPoE Appendix*.



```
   Menu 4 - Internet Access Setup

ISP's Name= myISP
Encapsulation= PPPoE
 Service Type= N/A
 My Login=
 My Password= ********
 Idle Timeout= 300

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


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

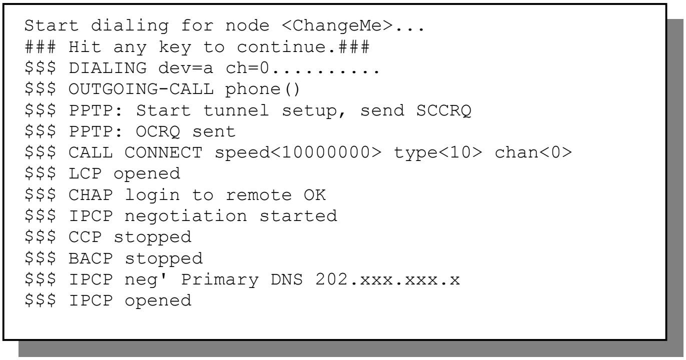
Figure 8-3 Internet Access (PPPoE)

Table 8-3 New Fields in Menu 4 (PPPoE) screen

FIELD	DESCRIPTION	EXAMPLE
Encapsulation	Press the [SPACE BAR] and then press [ENTER] to choose **PPPoE**. The encapsulation method influences your choices for IP Address.	**PPPoE**
Idle Timeout	This value specifies the time in seconds that elapses before the Prestige automatically disconnects from the PPPoE server.	300 (default)

8.2 Internet Test Setup

After configuring the menu 4 fields when you press [ENTER] to confirm you will see the message, " Do you wish to perform the Internet Setup Test[y/n]:" if you have chosen PPTP or PPPoE as your encapsulation method. Say 'Y' to test your setup. An example of Internet Setup Test is shown next.



```
Start dialing for node <ChangeMe>...
### Hit any key to continue.###
$$$ DIALING dev=a ch=0..........
$$$ OUTGOING-CALL phone()
$$$ PPTP: Start tunnel setup, send SCCRQ
$$$ PPTP: OCRQ sent
$$$ CALL CONNECT speed<10000000> type<10> chan<0>
$$$ LCP opened
$$$ CHAP login to remote OK
$$$ IPCP negotiation started
$$$ CCP stopped
$$$ BACP stopped
$$$ IPCP neg' Primary DNS 202.xxx.xxx.x
$$$ IPCP opened
```

Figure 8-4 Internet Setup Test Example

Part II:

Advanced Applications

This section describes the advanced applications of your Prestige, such as NAT, Remote Node Setup and IP Static Route Setup.

Chapter 9
Remote Node Setup

This chapter shows you how to configure menu 11 and all its sub-menus including traffic redirect.

9.1 Introduction

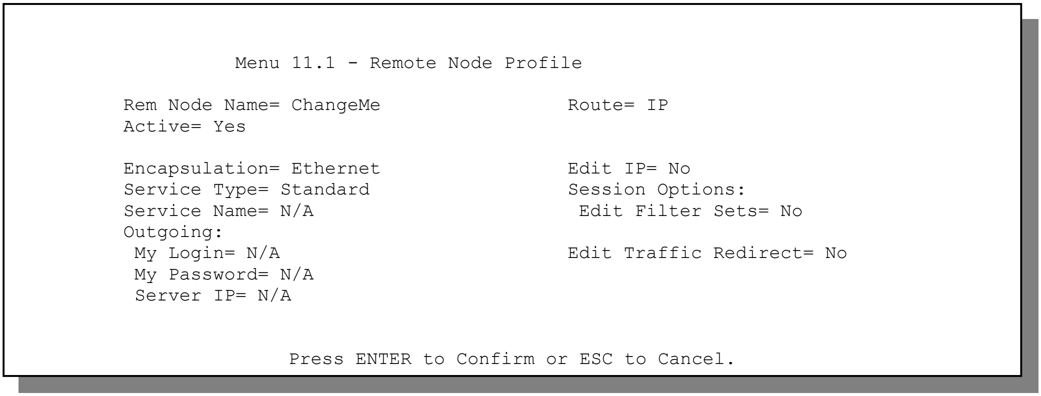
A remote node is required for placing calls to a remote gateway. A remote node represents both the remote gateway and the network behind it across a WAN connection. Note that when you use menu 4 to set up Internet access, you are actually configuring a remote node. We will show you how to configure **Menu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

9.2 Remote Node Profile

From the main menu, select option 11 to display **Menu 11.1 - Remote Node Profile**. There are three variations of this menu depending on whether you choose **Ethernet Encapsulation, PPTP** or **PPPoE Encapsulation.**

9.2.1 Ethernet Encapsulation

Choose the **Ethernet** option when the WAN port is used as a regular Ethernet. The first menu 11.1 screen you see is for **Ethernet Encapsulation** shown next.



```
              Menu 11.1 - Remote Node Profile

    Rem Node Name= ChangeMe                Route= IP
    Active= Yes

    Encapsulation= Ethernet                Edit IP= No
    Service Type= Standard                 Session Options:
    Service Name= N/A                       Edit Filter Sets= No
    Outgoing:
     My Login= N/A                         Edit Traffic Redirect= No
     My Password= N/A
     Server IP= N/A


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

Figure 9-1 Menu 11.1 Remote Node Profile for Ethernet Encapsulation

Table 9-1 Fields in Menu 11.1 (Ethernet Encapsulation)

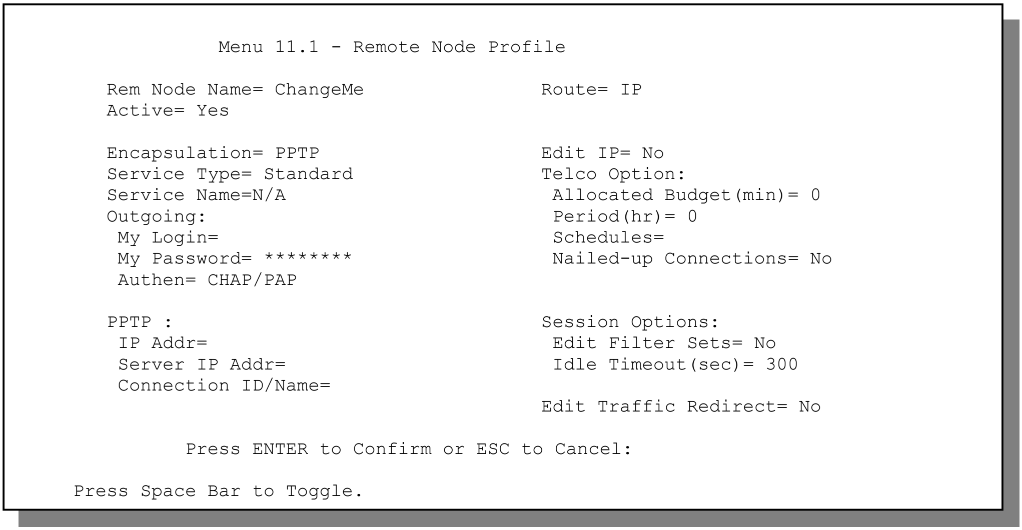
FIELD	DESCRIPTION	EXAMPLE
Rem Node Name	Enter a descriptive name for the remote node. This field can be up to eight characters.	LAoffice
Active	Press [SPACE BAR] to select **Yes** (activate remote node) or **No** (deactivate remote node).	**Yes**
Encapsulation	**Ethernet** is the default encapsulation. Press [SPACE BAR] if you wish to change to **PPPoE** or **PPTP** encapsulation.	**Ethernet**
Service Type	Press [SPACE BAR] to select from **Standard**, **RR-Toshiba** (RoadRunner Toshiba authentication method), **RR-Manager** (RoadRunner Manager authentication method) or, **RR-Telstra** (RoadRunner Telstra authentication method). Choose one of the RoadRunner methods if your ISP is Time Warner's RoadRunner; otherwise choose **Standard**.	**Standard**
Service Type	Press [SPACE BAR] to select from **Standard**, **RR-Toshiba** (RoadRunner Toshiba authentication method), **RR-Manager** (RoadRunner Manager authentication method) or, **RR-Telstra** (RoadRunner Telstra authentication method). Choose one of the RoadRunner methods if your ISP is Time Warner's RoadRunner; otherwise choose **Standard**.	**Standard**
Note: xDSL users must choose the **Standard** option only. The **Server IP**, **My Login IP** and **My Password** fields are not applicable in this case.		

Table 9-1 Fields in Menu 11.1 (Ethernet Encapsulation)

FIELD	DESCRIPTION	EXAMPLE
Service Name	This is valid only when you have chosen **PPPoE** encapsulation. If you are using **PPPoE** encapsulation, then type the name of your PPPoE service here.	poellc
Outgoing		
My Login	This field is applicable for **PPPoE** encapsulation only. Enter the login name assigned by your ISP when the Prestige calls this remote node. Some ISPs append this field to the **Service Name** field above (e.g., jim@poellc) to access the PPPoE server.	**jim**
My Password	Enter the password assigned by your ISP when the Prestige calls this remote node. Valid for **PPPoE** encapsulation only.	*****
Server IP	This field is valid for RoadRunner service type only. The Prestige will find the RoadRunner Server IP automatically if this field is left blank. If it does not, then you must enter the authentication server IP address here.	
Route	This field refers to the protocol that will be routed by your Prestige – IP is the only option for the Prestige 10.	**IP**
Edit IP	This field leads to a "hidden" menu. Press [SPACE BAR] to select **Yes** and press [ENTER] to go to M**enu 11.3 - Remote Node Network Layer Options**.	**Yes**
Session Options Edit Filter sets	This field leads to another "hidden" menu. Use the [SPACE BAR] to select **Yes** and press [ENTER] to open menu 11.5 to edit the filter sets. See the *Remote Node Filter* section for more details.	**Yes**
Once you have configured the Remote Node Profile Menu, press [ENTER] to return to menu 11. Press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		

9.2.2 PPTP Encapsulation

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



```
             Menu 11.1 - Remote Node Profile

   Rem Node Name= ChangeMe                Route= IP
   Active= Yes

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

   PPTP :                                 Session Options:
    IP Addr=                               Edit Filter Sets= No
    Server IP Addr=                        Idle Timeout(sec)= 300
    Connection ID/Name=
                                          Edit Traffic Redirect= No

          Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 9-2 Remote Node Profile for PPTP Encapsulation

Table 9-2 Fields in Menu 11.1 (PPTP Encapsulation)

FIELD	DESCRIPTION	EXAMPLE
Encapsulation	Press the [SPACE BAR] to choose **PPTP**. You must also go to menu 11.3 to check the IP Address setting once you have selected the encapsulation method.	**PPTP**
My IP Addr	Enter the IP address of the WAN Ethernet port.	10.0.0.140
Server IP Addr	Enter the IP address of the ANT modem.	10.0.0.138
Connection ID/Name	Enter the connection ID or connection name in the ANT. It must follow the “c:id” and “n:name” format. This field is optional and depends on the requirements of your xDSL Modem.	N:My ISP
Schedules	You can apply up to four schedule sets here. For more details please refer to the *Call Schedule Scheduling* chapter.	
Nailed-Up Connections	Use the [SPACE BAR] to select **Yes** if you want to make the connection to this remote node a nailed-up connection.	**No**

Nailed-Up Connection

A nailed-up connection is a dial-up line where the connection is always up regardless of traffic demand. The Prestige does two things when you specify a nailed-up connection. The first is that idle timeout is disabled. The second is that the Prestige will try to bring up the connection at power-on and whenever the connection is down. 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.

9.2.3 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 (i.e. xDSL, cable, wireless, etc.) connection.

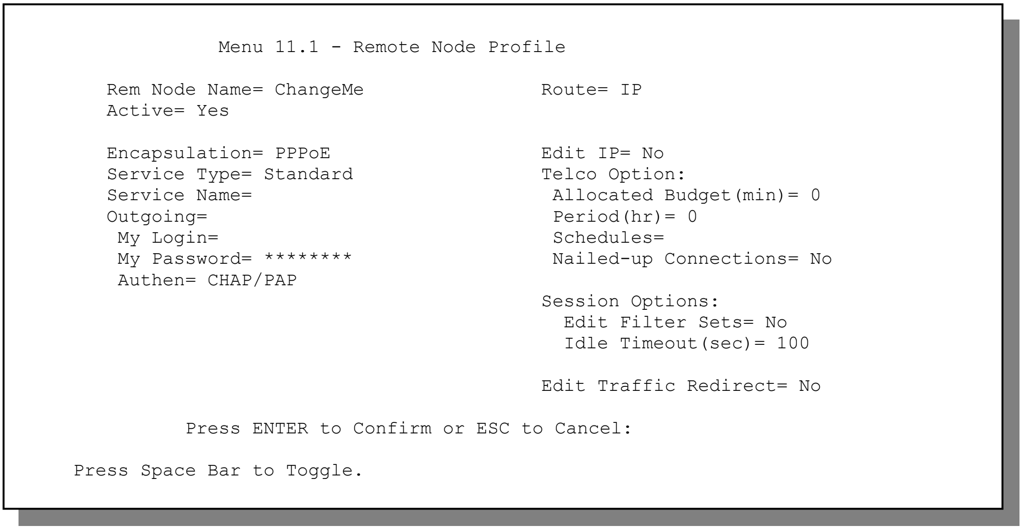
For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (e.g., Radius). For the user, PPPoE provides a login and authentication method that the existing Microsoft Dial-Up Networking software can activate, and therefore requires no new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

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

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

By implementing PPPoE directly on the 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.

Enable PPPoE in menu 11.1 by pressing the [SPACE BAR] to select **PPPoE** in the **Encapsulation** field.



```
                   Menu 11.1 - Remote Node Profile

         Rem Node Name= ChangeMe                Route= IP
         Active= Yes

         Encapsulation= PPPoE                   Edit IP= No
         Service Type= Standard                 Telco Option:
         Service Name=                           Allocated Budget(min)= 0
         Outgoing=                               Period(hr)= 0
          My Login=                              Schedules=
          My Password= ********                  Nailed-up Connections= No
          Authen= CHAP/PAP
                                                Session Options:
                                                  Edit Filter Sets= No
                                                  Idle Timeout(sec)= 100

                                                Edit Traffic Redirect= No

                Press ENTER to Confirm or ESC to Cancel:

      Press Space Bar to Toggle.
```

Figure 9-3 Menu 11.1 Remote Node Profile for PPPoE Encapsulation

The next table describes the fields NOT already described in *Table 9-1* already.

Table 9-3 Fields in Menu 11.1 (PPPoE Encapsulation Specific Only)

FIELD	DESCRIPTION	EXAMPLE
Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are: **CHAP/PAP** - Your Prestige will accept either **CHAP** or **PAP** when requested by this remote node. **CHAP** - accept CHAP only. **PAP** - accept PAP only.	**CHAP/PAP**
Telco Option		
Allocated Budget (min)	The field sets a ceiling for outgoing call time for this remote node. The default for this field is 0 meaning no budget control.	10
Period(hr)	This field is the time period that the budget should be reset. For example, if we are allowed to call this remote node for a maximum of 10 minutes every hour, then the **Allocated Budget(min)** is (10 minutes) and the **Period(hr)** is 1 (hour).	1

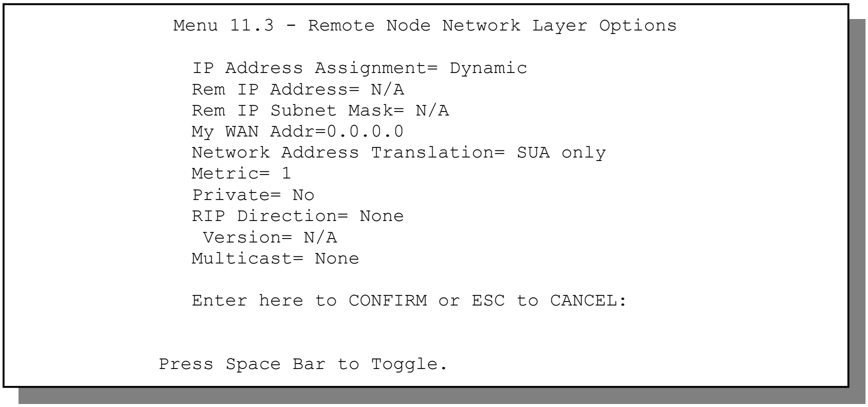
Table 9-3 Fields in Menu 11.1 (PPPoE Encapsulation Specific Only)

FIELD	DESCRIPTION	EXAMPLE
Schedules	You can apply up to four schedule sets here. For more details please refer to the *Call Scheduling* chapter.	
Nailed-Up Connection	This field specifies if you want to make the connection to this remote node a nailed-up connection. More details are given earlier in this section.	
Session Options Idle Timeout	This value specifies the idle time (i.e., the length of time there is no traffic from the Prestige to the remote node) in seconds that can elapse before the Prestige automatically disconnects the PPPoE connection. *This option only applies when the Prestige initiates the call*.	300 seconds (default)

9.3 Edit IP Remote Node Network Layer Options

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

This menu displays the **My WAN Addr** field for **PPPoE** and **PPTP** encapsulations and **Gateway IP Addr** field for **Ethernet** encapsulation.



```
               Menu 11.3 - Remote Node Network Layer Options

                 IP Address Assignment= Dynamic
                 Rem IP Address= N/A
                 Rem IP Subnet Mask= N/A
                 My WAN Addr=0.0.0.0
                 Network Address Translation= SUA only
                 Metric= 1
                 Private= No
                 RIP Direction= None
                  Version= N/A
                 Multicast= None

                 Enter here to CONFIRM or ESC to CANCEL:


              Press Space Bar to Toggle.
```

Figure 9-4 Remote Node Network Layer Options

The next table gives you instructions about configuring remote node network layer options.

Table 9-4 Remote Node Network Layer Options Menu Fields

FIELD	DESCRIPTION	EXAMPLE
IP Address Assignment	If your ISP did not assign you an explicit IP address, select **Dynamic**; otherwise select **Static** and enter the IP address & subnet mask in the following fields.	**Dynamic**
Rem IP Address	If you have a Static IP Assignment, enter the IP address assigned to you by your ISP.	
Rem IP Subnet Mask	If you have a Static IP Assignment, enter the subnet mask assigned to you.	
Gateway IP Addr	This field is applicable to **Ethernet** encapsulation only. Enter the gateway IP address assigned to you if you are using a static IP address.	
My WAN Addr	If you have a Static IP Assignment, enter the gateway IP address assigned to you.	
My WAN Addr	This field is applicable to **PPPoE** and **PPTP** encapsulations only. Some implementations, especially the UNIX derivatives, require the WAN link to have a separate IP network number from the LAN and each end must have a unique address within the WAN network number. If this is the case, enter the IP address assigned to the WAN port of your Prestige. Note that this is the address assigned to your local Prestige, not the remote router.	
Network Address Translation	Use the [SPACE BAR] to select either **Full Feature**, **None** or **SUA Only**. See the *NAT* chapter for a full discussion of this feature.	**SUA Only**
Metric	This field is valid only for PPTP/PPPoE encapsulation. The metric represents the “cost” of transmission for routing purposes. RIP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.	3
Private	This field is valid only for PPTP/PPPoE encapsulation. This parameter determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and not included in RIP broadcast. If **No**, the route to this remote node will be propagated to other hosts through RIP	**Yes**

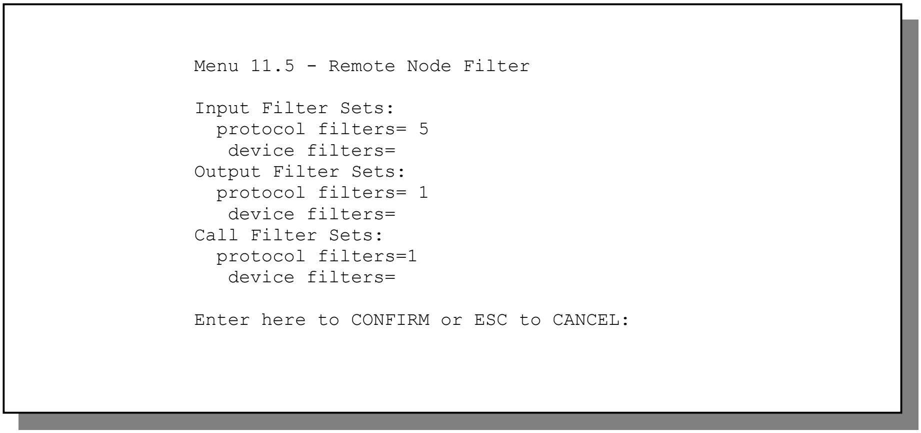
Table 9-4 Remote Node Network Layer Options Menu Fields

FIELD	DESCRIPTION	EXAMPLE
	broadcasts.	
RIP	Press the [SPACE BAR] to select the **RIP direction.** Options are: **Both**, **None**, **In Only**, **Out Only** or **None**. Please see the *RIP Setup section* for more information on RIP. The default for RIP on the WAN side is **None**. It is recommended that you do not change this setting.	**None** (default)
Version	Press the [SPACE BAR] to select the RIP version. Options are **RIP-1**, **RIP-2B** or **RIP-2M**.	**None**
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The Prestige supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2)**. Press [SPACE BAR] to enable IP Multicasting or select **None** to disable it. See the previous *Part* for more information on this feature.	**IGMP-v2**
Once you have completed filling in the Network Layer Options Menu, press [ENTER] to return to menu 11. Press [ENTER] at the message “Press ENTER to Confirm...” to save your configuration, or press [ESC] at any time to cancel.		

9.4 Remote Node Filter

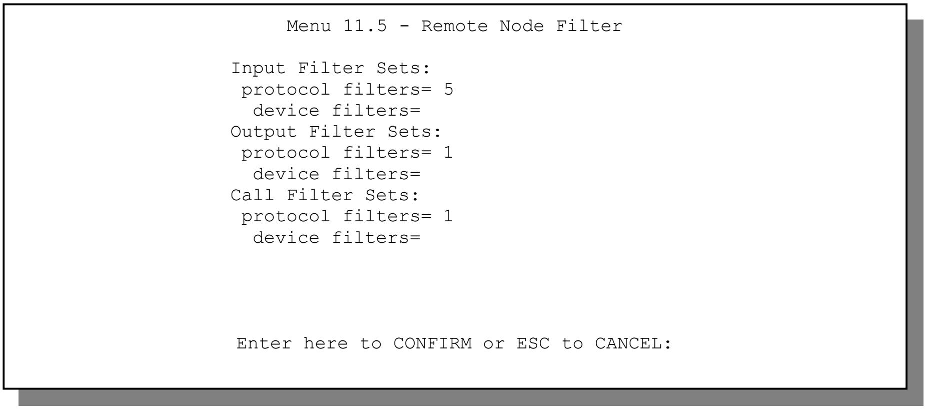
Move the cursor to the field **Edit Filter Sets** in menu 11.1, then press the [SPACE BAR] to set the value to **Yes**. Press [ENTER] to open **Menu 11.5 - Remote Node Filter**.

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



```
Menu 11.5 - Remote Node Filter

Input Filter Sets:
  protocol filters= 5
   device filters=
Output Filter Sets:
  protocol filters= 1
   device filters=
Call Filter Sets:
  protocol filters=1
   device filters=

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

Figure 9-5 Remote Node Filter (Ethernet Encapsulation)



```
     Menu 11.5 - Remote Node Filter

Input Filter Sets:
 protocol filters= 5
  device filters=
Output Filter Sets:
 protocol filters= 1
  device filters=
Call Filter Sets:
 protocol filters= 1
  device filters=




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

Figure 9-6 Remote Node Filter (PPTP/PPPoE Encapsulation)

9.5 Traffic Redirect

Traffic redirect forwards WAN traffic to a backup gateway when the Prestige cannot connect to the Internet through its normal gateway.

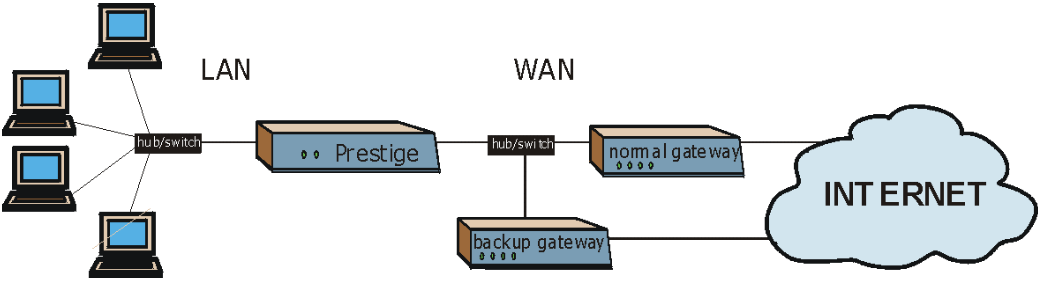


Figure 9-7 Traffic Redirect WAN Setup

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

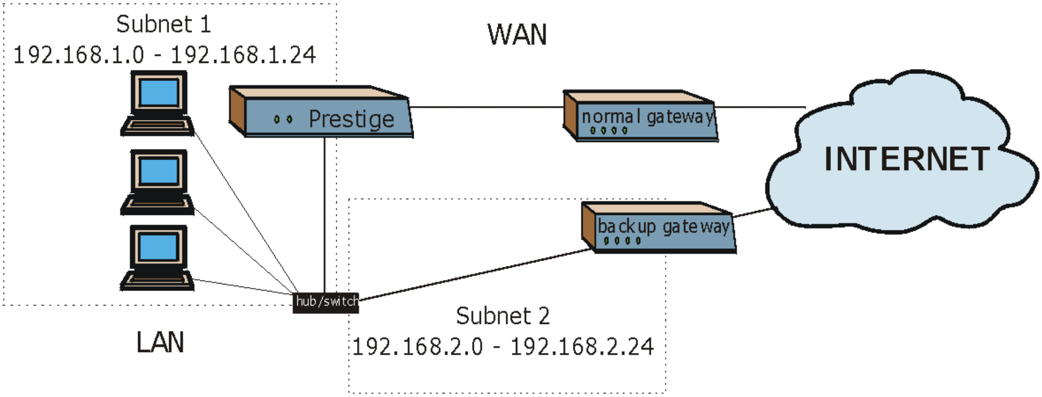


Figure 9-8 Traffic Redirect LAN Setup

9.5.1 Route Priority and Metric

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

1. Normal route: designated by the ISP or a static route.

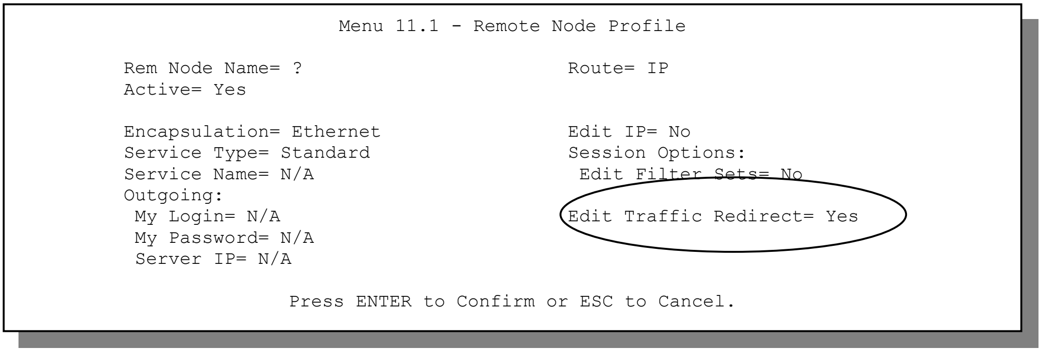
2. Traffic-redirect route.

3. Dial-backup route.

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).

To configure the parameters for traffic redirect, enter 11 from the main menu to display **Menu 11.1— Remote Node Profile** as shown next.



```
                              Menu 11.1 - Remote Node Profile

          Rem Node Name= ?                       Route= IP
          Active= Yes

          Encapsulation= Ethernet                Edit IP= No
          Service Type= Standard                 Session Options:
          Service Name= N/A                       Edit Filter Sets= No
          Outgoing:
           My Login= N/A                         Edit Traffic Redirect= Yes
           My Password= N/A
           Server IP= N/A

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

Figure 9-9 Menu 11.1 — Remote Node Profile

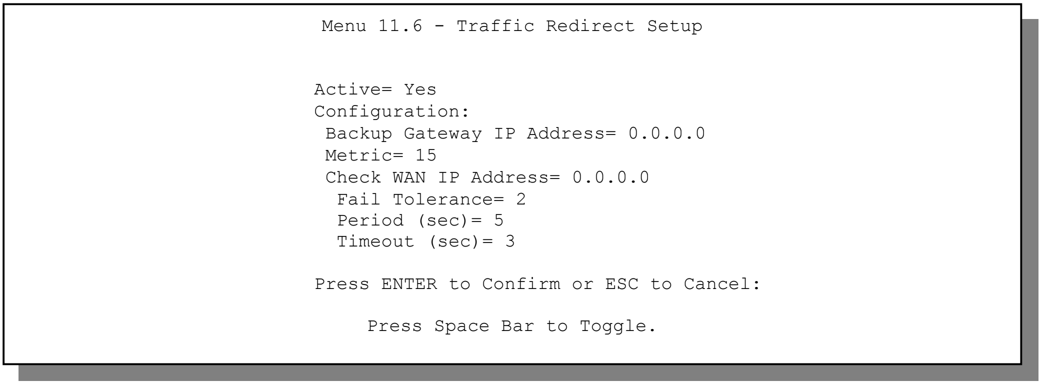
To configure traffic redirect properties, press [SPACE BAR] to select **Yes** in the **Edit Traffic Redirect** field and then press [ENTER].

Table 9-5 Menu 11.1 — Remote Node Profile (Traffic Redirect Field)

FIELD	DESCRIPTION	EXAMPLE
Edit Traffic Redirect	Press [SPACE BAR] to select **Yes** or **No**. Select **No** (default) if you do not want to configure this feature. Select **Yes** and press [ENTER] to configure **Menu 11.6 — Traffic Redirect Setup**.	**Yes**
Press [ENTER] at the message "Press ENTER to Confirm..." to save your configuration, or press [ESC] at any time to cancel.		

9.5.2 Traffic Redirect Setup

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



```
                              Menu 11.6 - Traffic Redirect Setup


                             Active= Yes
                             Configuration:
                              Backup Gateway IP Address= 0.0.0.0
                              Metric= 15
                              Check WAN IP Address= 0.0.0.0
                               Fail Tolerance= 2
                               Period (sec)= 5
                               Timeout (sec)= 3

                             Press ENTER to Confirm or ESC to Cancel:

                                  Press Space Bar to Toggle.
```

Figure 9-10 Menu 11.6 — Traffic Redirect Setup

Table 9-6 Traffic Redirect Setup

FIELD	DESCRIPTION	EXAMPLE
Active	Press [SPACE BAR] and select Yes (to enable) or No (to disable) traffic redirect setup. The default is No. When the Active field is Yes, you must configure every field in this screen unless you are using PPPoE or PPTP encapsulation (except Check WAN IP Address and Timeout). If you don’t configure these fields and are using PPTP or PPPoE encapsulation, then the Prestige checks the PPPoE channel or PPTP tunnel to determine if the WAN connection is down.	Yes
Configuration: Backup Gateway IP Address	Enter the IP address of your backup gateway in dotted decimal notation. The Prestige automatically forwards traffic to this IP address if the Prestige’s Internet connection terminates.	0.0.0.0
Metric	Enter a number from 1 to 15 to set this route’s priority among the Prestige’s routes (see *Route* Priority and Metric on page *9-11*) The smaller the number, the higher priority the route has.	15 (default)

Table 9-6 Traffic Redirect Setup

FIELD	DESCRIPTION	EXAMPLE
Metric	Enter a number from 1 to 15 to set this route's priority among the Prestige's routes (see *Route* Priority and Metric on page *9-11*) The smaller the number, the higher priority the route has.	15 (default)
Check WAN IP Address	Enter the IP address of a reliable nearby computer (for example, your ISP's DNS server address) to test your Prestige's WAN accessibility. The Prestige uses the default gateway IP address if you do not enter an IP address here. If you are using PPTP or PPPoE Encapsulation, enter "0.0.0.0" to configure the Prestige to check the PVC (Permanent Virtual Circuit) or PPTP tunnel.	0.0.0.0
Fail Tolerance	Enter the number of times your Prestige may attempt and fail to connect to the Internet before traffic is forwarded to the backup gateway. Two to five is usually a good number.	2
Period (sec)	Enter the time interval (in seconds) between WAN connection checks. Five to 60 is usually a good number.	5
Timeout (sec)	Enter the number of seconds the Prestige waits for a ping response from the IP Address in the Check WAN IP Address field before it times out. The number in this field should be less than the number in the Period field. Three to 50 is usually a good number. The WAN connection is considered "down" after the Prestige times out the number of times specified in the Fail Tolerance field.	3
When you have completed this menu, press [ENTER] at the prompt "Press [ENTER] to confirm or [ESC] to cancel" to save your configuration or press [ESC] to cancel and go back to the previous screen.		

Chapter 10
IP Static Route Setup

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

Static routes tell the Prestige routing information what it cannot learn automatically through other means. This can arise in cases where RIP is disabled on the LAN.

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 diagram through remote node Router 1. However, the Prestige is unable to route a packet to network N3 because it doesn't know that there is a route through the same remote node Router 1 (via gateway Router 2). The static routes are for you to tell the Prestige about the networks beyond the remote nodes.

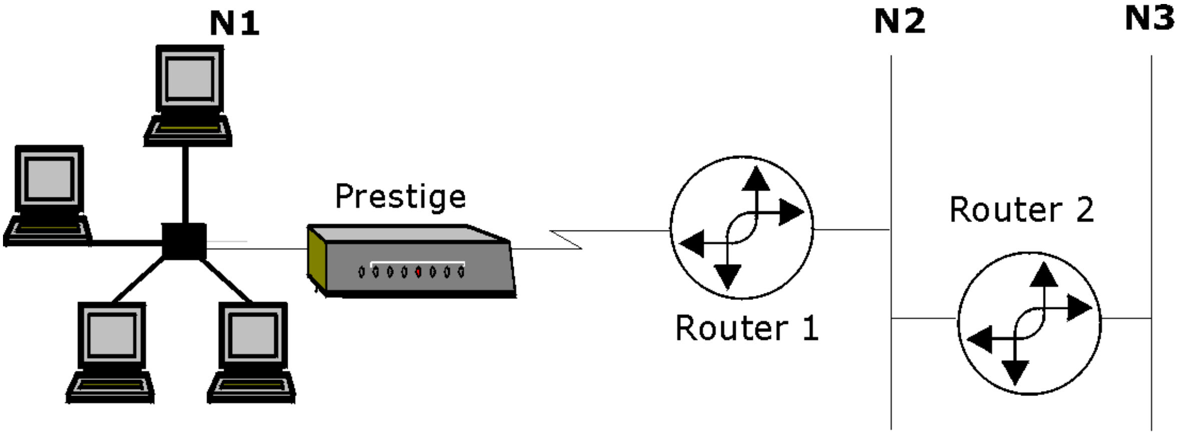
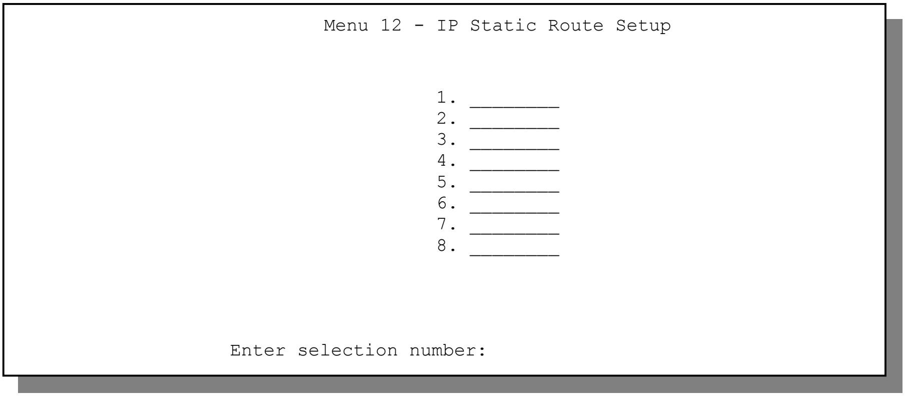


Figure 10-1 Example of Static Routing Topology

10.1 IP Static Route Setup

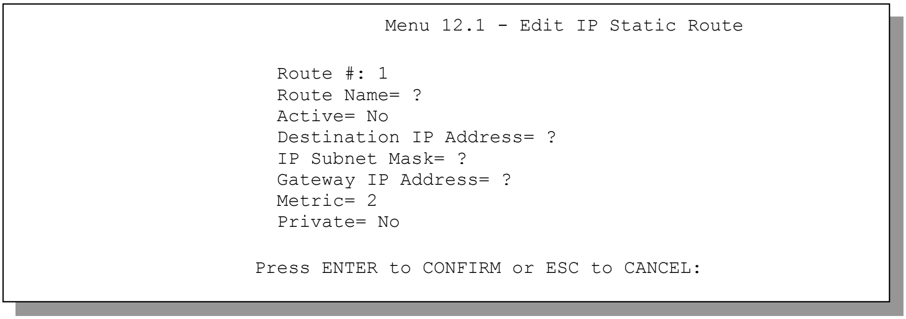
You configure IP static routes in menu 12. 1, by selecting one of the IP static routes as shown below. Enter 12 from the main menu.



```
                         Menu 12 - IP Static Route Setup


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



                 Enter selection number:
```

Figure 10-2 Menu 12 — IP Static Route Setup

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



```
                              Menu 12.1 - Edit IP Static Route

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

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

Figure 10-3 Menu 12. 1 — Edit IP Static Route

`The following table describes the IP Static Route Menu fields.

Table 10-1 IP Static Route Menu Fields

FIELD	DESCRIPTION
Route #	This is the index number of the static route that you chose in menu 12.
Route Name	Enter a descriptive name for this route. This is for identification purposes 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	Enter the IP subnet mask for this destination.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your Prestige that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your Prestige; over the WAN, the gateway must be the IP address of one of the Remote Nodes.
Metric	Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Private	This parameter determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and not included in RIP broadcast. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.
Once you have completed filling in this menu, press [ENTER] at the message “Press ENTER to Confirm…” to save your configuration, or press [ESC] to cancel.	

Chapter 11
Network Address Translation (NAT)

This chapter discusses how to configure NAT on the Prestige.

11.1 Introduction

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

11.1.1 NAT Definitions

Inside/outside denotes where a host is located relative to the Prestige, e.g., the workstations 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, e.g., the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

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

Table 11-1 NAT Definitions

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

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

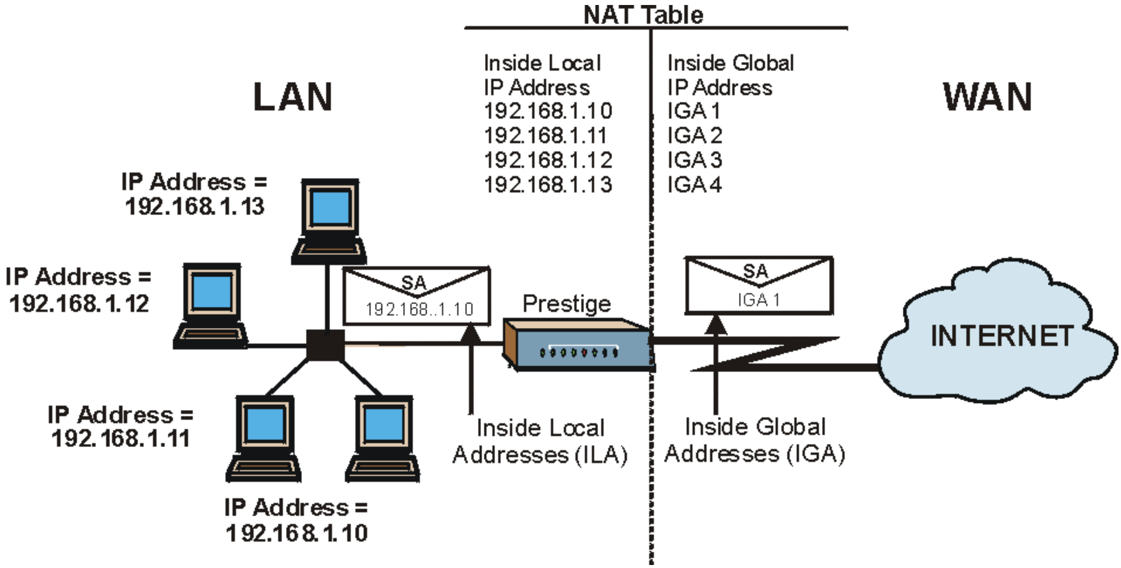
11.1.2 What NAT Does

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back 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, e.g., 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 11-2*), NAT offers the additional benefit of firewall protection. If no server is defined in these cases, all incoming inquiries will be filtered out by your Prestige, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631*, *The IP Network Address Translator (NAT).*

11.1.3 How NAT Works

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



NAT Table

Inside Local IP Address	Inside Global IP Address
192.168.1.10	IGA 1
192.168.1.11	IGA 2
192.168.1.12	IGA 3
192.168.1.13	IGA 4

LAN
WAN
IP Address = 192.168.1.13
IP Address = 192.168.1.12
IP Address = 192.168.1.11
IP Address = 192.168.1.10
SA
192.168..1.10
Prestige
SA
IGA 1
INTERNET
Inside Local Addresses (ILA)
Inside Global Addresses (IGA)

Figure 11-1 How NAT Works

11.1.4 NAT Application

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

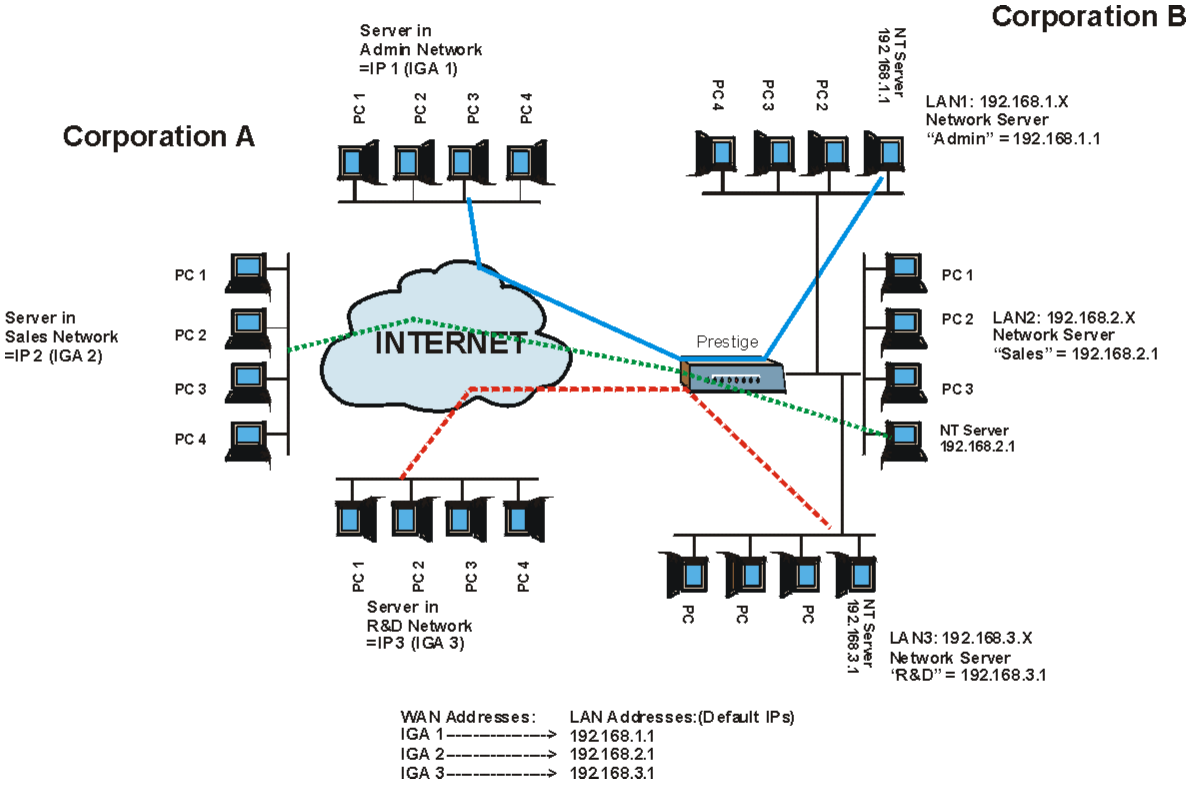


Figure 11-2 NAT Application With IP Alias

11.1.5 NAT Mapping Types

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

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

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

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

4. **Many One-to-One**: In **Many One-to-One** mode, the Prestige maps the each local IP addresses 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.

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

When you select One-to-One **or** Many- One-to-One **NAT mapping, the firewall automatically allows traffic through to the LAN computers you specify in the** One-to-One **or** Many- One-to-One **mapping rules. This means that these LAN computers do not have firewall protection.**

The following table summarizes these types.

Table 11-2 NAT Mapping Types

TYPE	IP MAPPING	SMT ABBREVIATION
One-to-One	ILA1←→ IGA1	1:1

Many-to-One (SUA/PAT)	ILA1←→ IGA1
	ILA2←→ IGA1
	…
		M:1

Many-to-Many Overload	ILA1←→ IGA1
	ILA2←→ IGA2
	ILA3←→ IGA1
	ILA4←→ IGA2
	…
		M:M Ov

Table 11-2 NAT Mapping Types

TYPE	IP MAPPING	SMT ABBREVIATION

Many-One-to-One	ILA1←→ IGA1
	ILA2←→ IGA2
	ILA3←→ IGA3
	…
		M-1-1

Server	Server 1 IP←→ IGA1 Server 2 IP←→ IGA1 Server 3 IP←→ IGA1	Server

11.2 SUA (Single User Account) Versus NAT

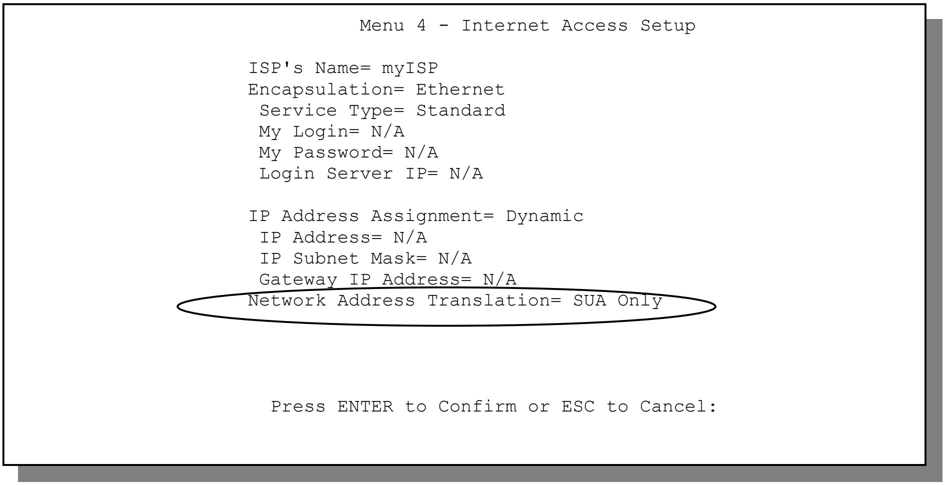
SUA (Single User Account) is a ZyXEL implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. See section *11.3.1* for a detailed description of the NAT set for SUA. The Prestige supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types as outlined in *Table 11-2*.

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

2. **Choose** Full Feature **if you have multiple public WAN IP addresses for your Prestige.**

11.2.1 Applying NAT

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



```
                       Menu 4 - Internet Access Setup

             ISP's Name= myISP
             Encapsulation= Ethernet
              Service Type= Standard
              My Login= N/A
              My Password= N/A
              Login Server IP= N/A

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



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

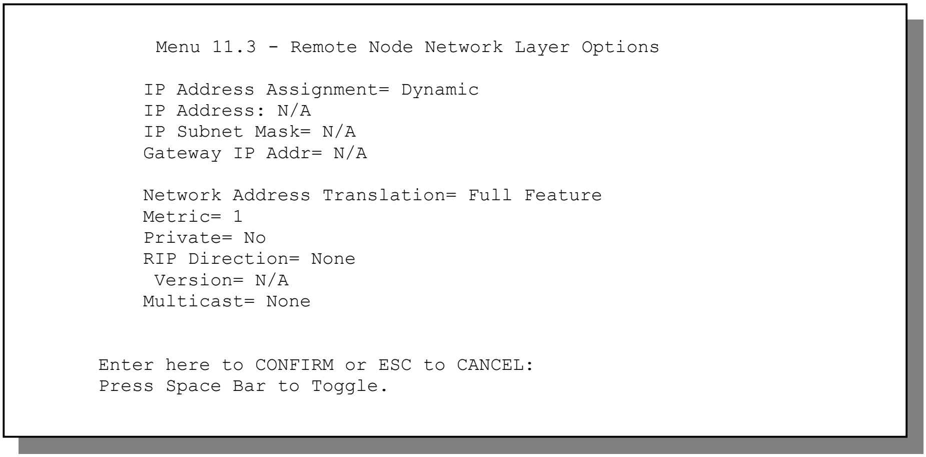
Figure 11-3 Menu 4 — Applying NAT for Internet Access

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

Step 1. Enter 11 from the main menu.

Step 2. Move the cursor to the **Edit IP** field, press the [SPACE BAR] to select **Yes** and then press

Step 3. [ENTER] to bring up **Menu 11.3 - Remote Node Network Layer Options.**



```
             Menu 11.3 - Remote Node Network Layer Options

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

            Network Address Translation= Full Feature
            Metric= 1
            Private= No
            RIP Direction= None
             Version= N/A
            Multicast= None


        Enter here to CONFIRM or ESC to CANCEL:
        Press Space Bar to Toggle.
```

Figure 11-4 Menu 11.3 — Applying NAT to the Remote Node

The following table describes the options for Network Address Translation.

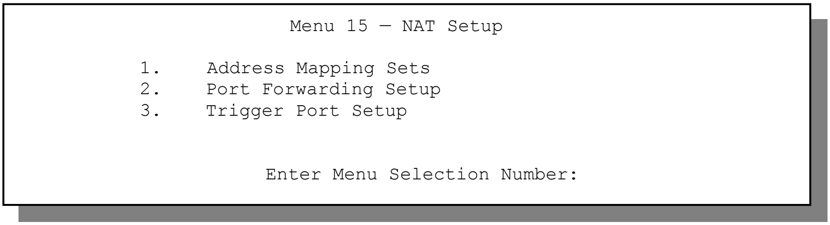
Table 11-3 Applying NAT in Menus 4 & 11.3

FIELD	OPTIONS	DESCRIPTION
Network Address Translation	**Full Feature**	When you select this option the SMT will use Address Mapping Set 1 (menu 15.1 - see section *11.3.1* for further discussion). You can configure any of the mapping types described in *Table 11-2*. Choose **Full Feature** if you have multiple public WAN IP addresses for your Prestige.
	None	NAT is disabled when you select this option.
	SUA Only	When you select this option the SMT will use Address Mapping Set 255 (menu 15.1 - see section *11.3.1*). Choose **SUA Only** if you have just one public WAN IP address for your Prestige.

11.3 NAT Setup

Use the Address Mapping Sets menus and submenus to create the mapping table used to assign global addresses to computers on the LAN. You can see two NAT Address Mapping sets in menu 15.1. You can only configure **Set 1**. **Set 255** is used for SUA. When you select **Full Feature** in menu 4 or 11.3, the SMT will use **Set 1**, which supports all mapping types as outlined in *Table 11-2.* When you select **SUA Only**, the SMT will use the pre-configured **Set 255** (read only).

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

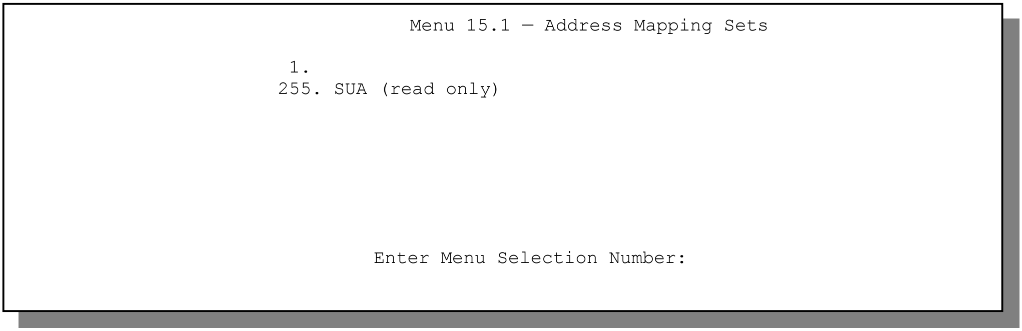


```
                         Menu 15 — NAT Setup

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


                       Enter Menu Selection Number:
```

Figure 11-5 Menu 15 — NAT Setup

11.3.1 Address Mapping Sets

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

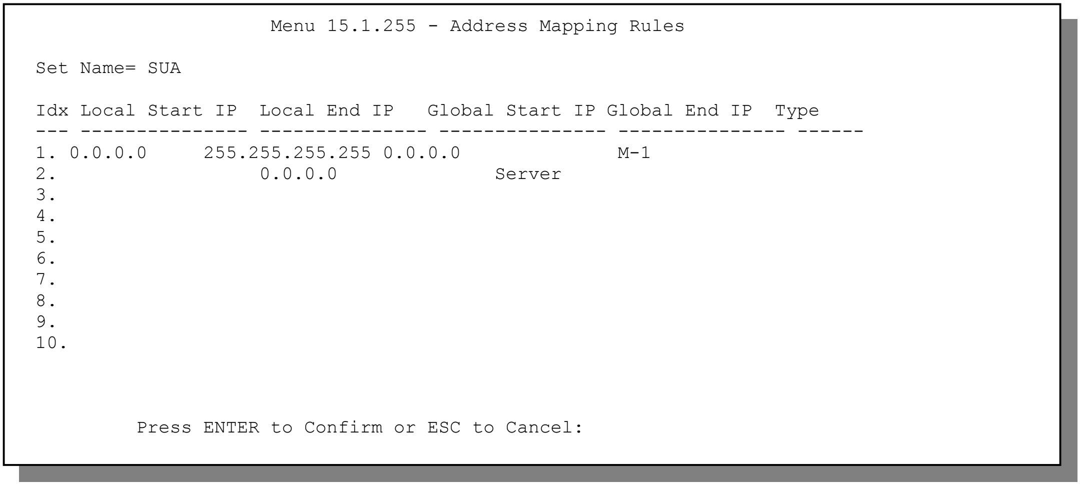


```
                                    Menu 15.1 — Address Mapping Sets

                        1.
                       255. SUA (read only)







                                 Enter Menu Selection Number:
```

Figure 11-6 Menu 15.1 — Address Mapping Sets

SUA Address Mapping Set

Enter 255 to display the next screen (see also *section 11.2)*. 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              Server
3.
4.
5.
6.
7.
8.
9.
10.



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

Figure 11-7 Menu 15.1.255 — SUA Address Mapping Rules

The following table explains the fields in this screen.

The fields in menu 15.1.255 are read-only.

Table 11-4 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 End IP	**Local Start IP** is the starting local IP address (ILA) (see *Figure 11-1)*. **Local End IP** is the ending local IP address (ILA). If the rule is for all local IPs, then the Start IP is 0.0.0.0 and the End IP is 255.255.255.255.	0.0.0.0 255.255.255.255
Local Start IP Local End IP	**Local Start IP** is the starting local IP address (ILA) (see *Figure 11-1)*. **Local End IP** is the ending local IP address (ILA). If the rule is for all local IPs, then the Start IP is 0.0.0.0 and the End IP is 255.255.255.255.	0.0.0.0 255.255.255.255

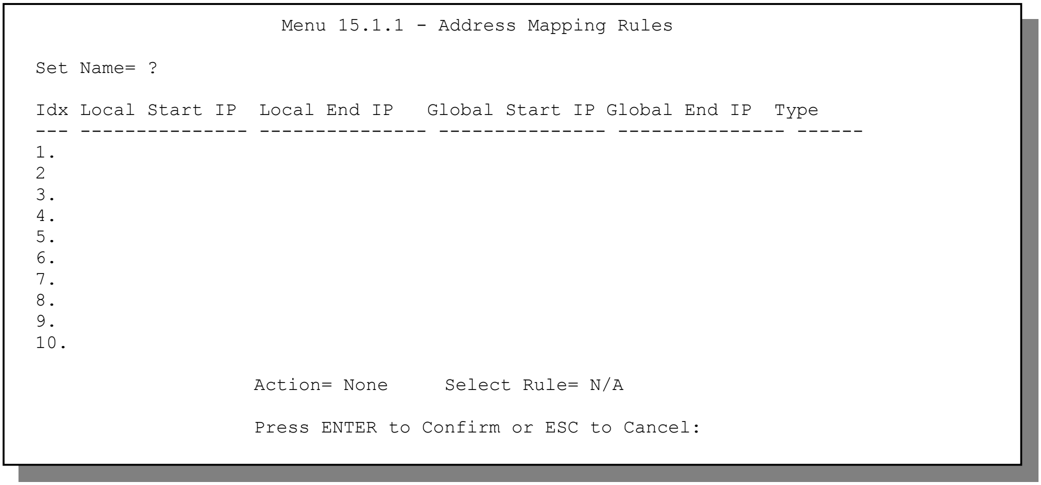
Table 11-4 SUA Address Mapping Rules

FIELD	DESCRIPTION	EXAMPLE
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).	**N/A**
Type	These are the mapping types discussed above (see *Table 11-2*). **Server** allows you to specify multiple servers of different types behind NAT to this machine. See later for some examples.	**Server**
Type	These are the mapping types discussed above (see *Table 11-2*). **Server** allows you to specify multiple servers of different types behind NAT to this machine. See later for some examples.	**Server**
Once you have finished configuring a rule in this menu, press [ENTER] at the message “Press ENTER to Confirm…” to save your configuration, or press [ESC] to cancel.		

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.

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



```
                        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 11-8 Menu 15.1.1 — First Set

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

Ordering Your Rules

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

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

Table 11-5 Fields in Menu 15.1.1

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

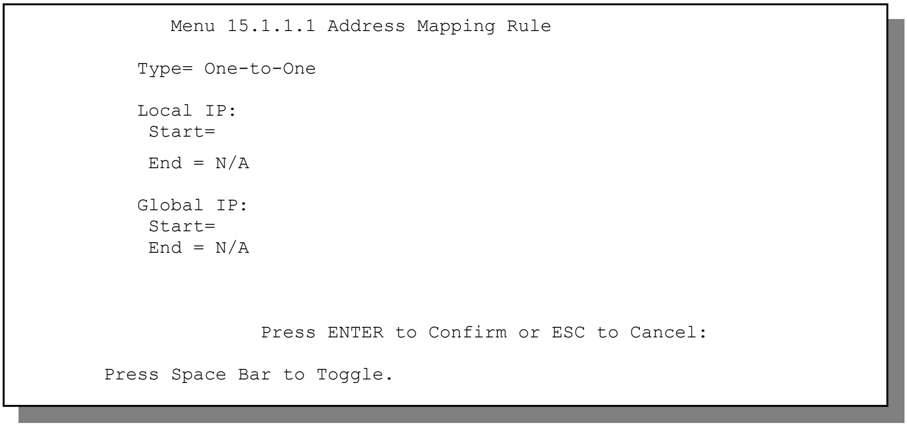
Table 11-5 Fields in Menu 15.1.1

FIELD	DESCRIPTION	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



                      Press ENTER to Confirm or ESC to Cancel:

        Press Space Bar to Toggle.
```

Figure 11-9 Menu 15.1.1.1 — Editing/Configuring an Individual Rule in a Set

Table 11-6 Menu 15.1.1.1 — Editing/Configuring an Individual Rule in a Set

FIELD	DESCRIPTION	EXAMPLE
Type	Press the [SPACE BAR] to select one of five types. These are the mapping types discussed in *Table 11-2*. **Server** allows you to specify multiple servers of different types behind NAT to this computer. See *section 11.4.3 below* for an example.	**One-to-One**
Type	Press the [SPACE BAR] to select one of five types. These are the mapping types discussed in *Table 11-2*. **Server** allows you to specify multiple servers of different types behind NAT to this computer. See *section 11.4.3 below* for an example.	**One-to-One**
Local IP	Only local IP fields are **N/A** for server; Global IP fields MUST be set for **Server**.	
Start	This is the starting local IP address (ILA).	0.0.0.0
End	This is the ending local IP address (ILA). If the rule is for all local IPs, then put the Start IP as 0.0.0.0 and the End IP as 255.255.255.255. This field is **N/A** for One-to-One and Server types.	N/A
Global IP		
Start	This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global IP Start**. Note that **Global IP Start** can be set to 0.0.0.0 only if the types are **Many-to-One** or **Server**.	0.0.0.0
End	This is the ending global IP address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server types**.	N/A

Table 11-6 Menu 15.1.1.1 — Editing/Configuring an Individual Rule in a Set

FIELD	DESCRIPTION	EXAMPLE
Once you have finished configuring a rule in this menu, press [ENTER] at the message "Press ENTER to Confirm…" to save your configuration, or press [ESC] to cancel.		

When you configure One-to-One **and** Many-One-to-One **mapping rules, the firewall automatically allows traffic originating from the WAN to be forwarded to the LAN IP address(es) of the computers specified in those rules. These computers do *not* have firewall protection in this case.**

11.3.2 Port Forwarding Setup

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

Use **Menu 15 - NAT Setup** to forward incoming service requests to the server(s) on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. Entry 12 (port 1026) is non-editable (see *Figure 11-10*).

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

When you configure NAT port forwarding rules, the firewall automatically allows traffic originating from the WAN to be forwarded to the LAN IP address(es) of the computers specified. These computers do *not* have firewall protection in this case.

The most often used port numbers are shown in the following table. Please refer to *RFC 1700* for further information about port numbers and refer to the included disk for more examples and details on NAT.

Table 11-7 Services & Port Numbers

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

Configuring a Server behind NAT

Follow these steps to configure a server behind NAT:

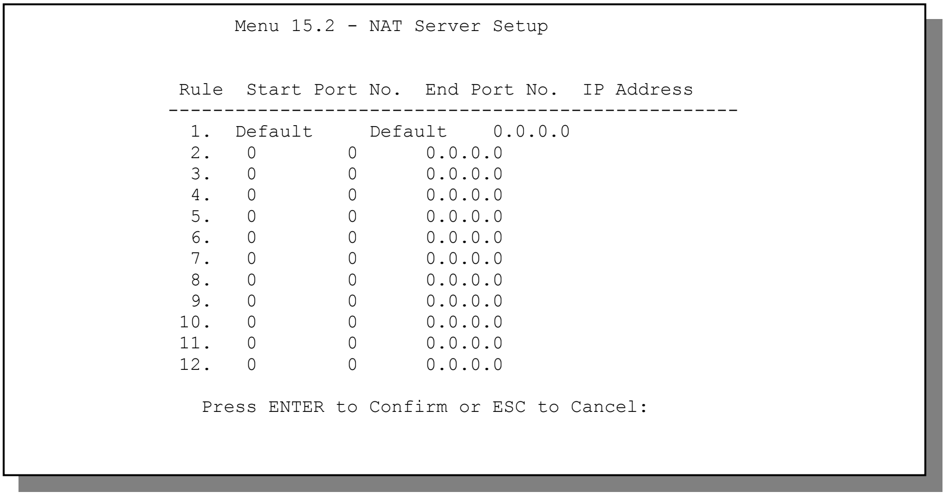
Step 1. Enter 15 in the main menu to go to **Menu 15 - NAT Setup.**

Step 2. Enter 2 to go to **Menu 15.2 - NAT Server Setup**.

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

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

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



```
                    Menu 15.2 - NAT Server Setup


               Rule  Start Port No.  End Port No.  IP Address
              ---------------------------------------------------
                1.  Default      Default    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

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

Figure 11-10 Menu 15.2 — NAT Server Setup

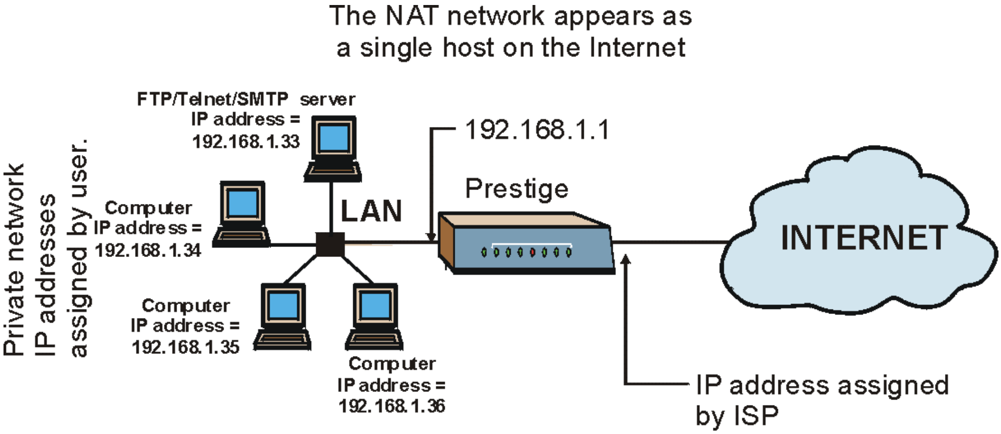


Figure 11-11 Multiple Servers Behind NAT Example

11.3.3 Trigger Port Setup

The Prestige records the IP address of a LAN computer that requests a service that you have defined as a “trigger port”. The response from the Internet can then be forwarded directly to the LAN computer. Trigger ports are transient; they only exist while in use or are timed out. The following is a trigger port example

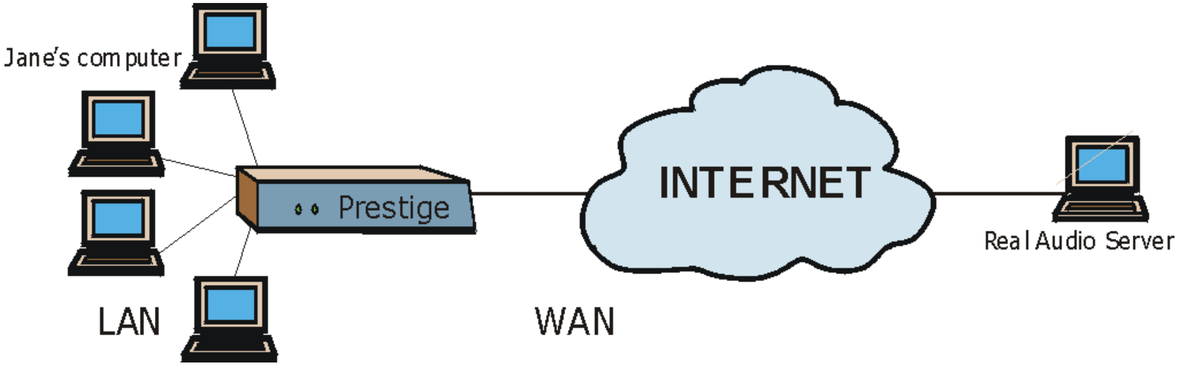


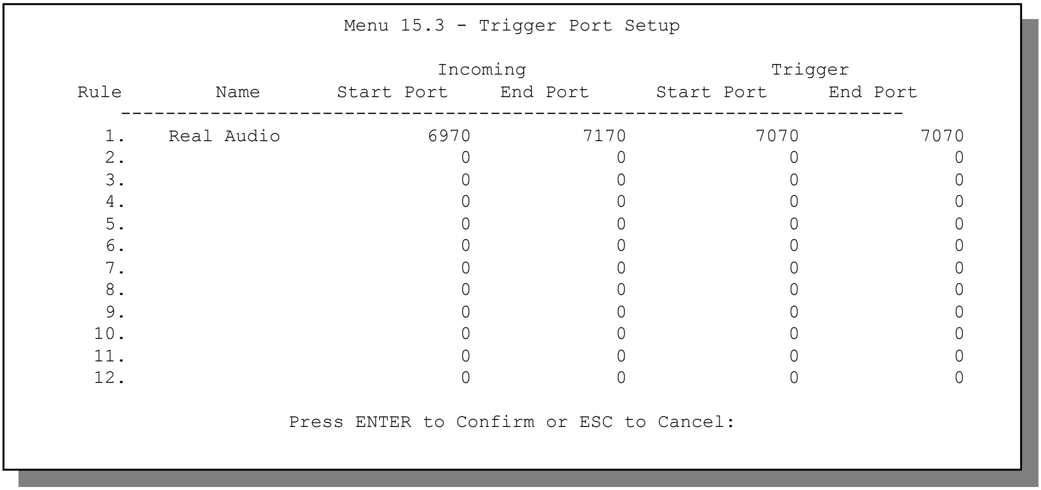
Figure 11-12 Trigger Port Forwarding Process: Example

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

Two Points To Remember About Trigger Ports

1. Trigger events only happen on outgoing data (from the Prestige to the WAN).
2. Only one LAN computer can use a trigger port (range) at a time.

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



```
                          Menu 15.3 - Trigger Port Setup

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

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

Figure 11-13 Menu 15.3: Trigger Port Setup

Table 11-8 Menu 15.3—Trigger Port Setup Description

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

11.4 General NAT Examples

11.4.1 Internet Access Only

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

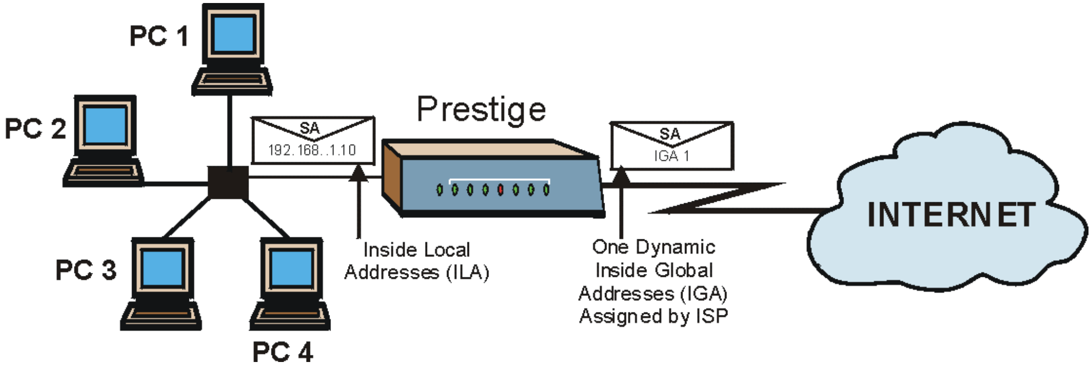
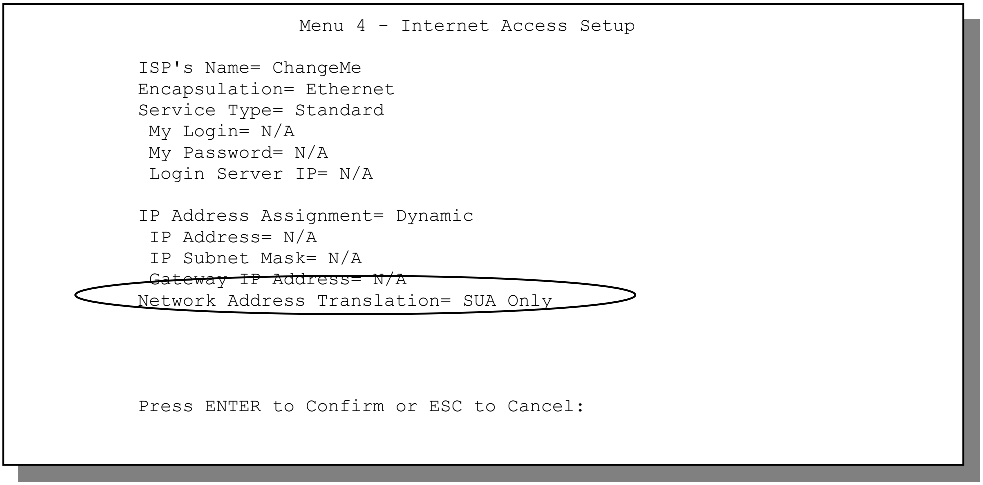


Figure 11-14 NAT Example 1



```
                    Menu 4 - Internet Access Setup

            ISP's Name= ChangeMe
            Encapsulation= Ethernet
            Service Type= Standard
             My Login= N/A
             My Password= N/A
             Login Server IP= N/A

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



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

Figure 11-15 Menu 4 — Internet Access & NAT Example

From menu 4 shown above, simply choose the **SUA Only** option from the **Network Address Translation** field. This is the Many-to-One mapping discussed in *section 11.1.5.* The **SUA Only** read-only option from the **Network Address Translation** field in menus 4 and 11.3 is specifically pre-configured to handle this case.

11.4.2 Example 2: Internet Access with an Inside Server

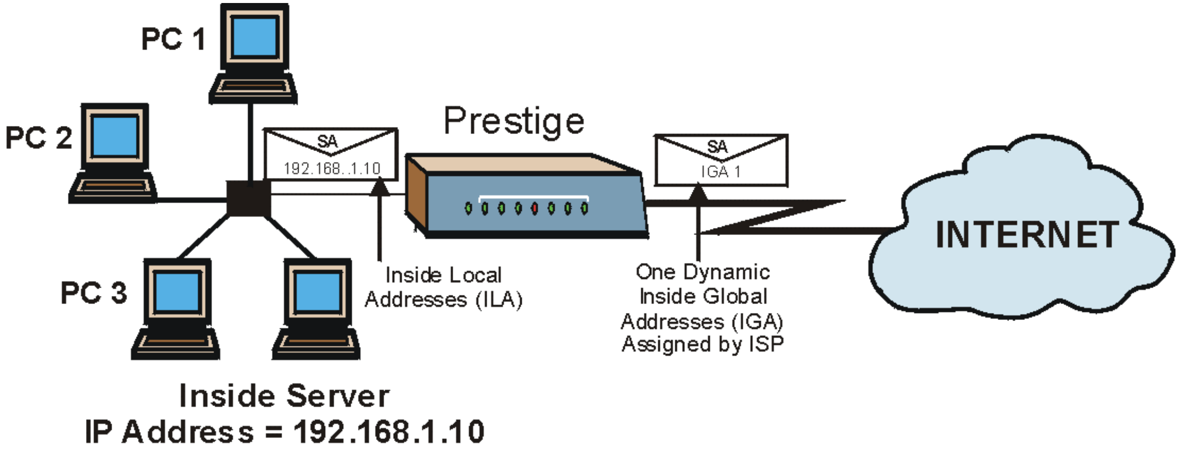


Figure 11-16 NAT Example 2

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 later.

11.4.3 Example 3: Multiple Public IP Addresses With Inside Servers

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

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

Rule 2. Map the second IGA to our second inside FTP server for FTP traffic in both directions (**1 : 1** mapping, giving both local and global IP addresses).

Rule 3. Map the other outgoing LAN traffic to IGA3 (**Many : 1** mapping).

Rule 4. You also map your third IGA to the web server and mail server on the LAN. Type **Server** allows you to specify multiple servers, of different types, to other computers behind NAT on the LAN.

The example situation looks somewhat like this:

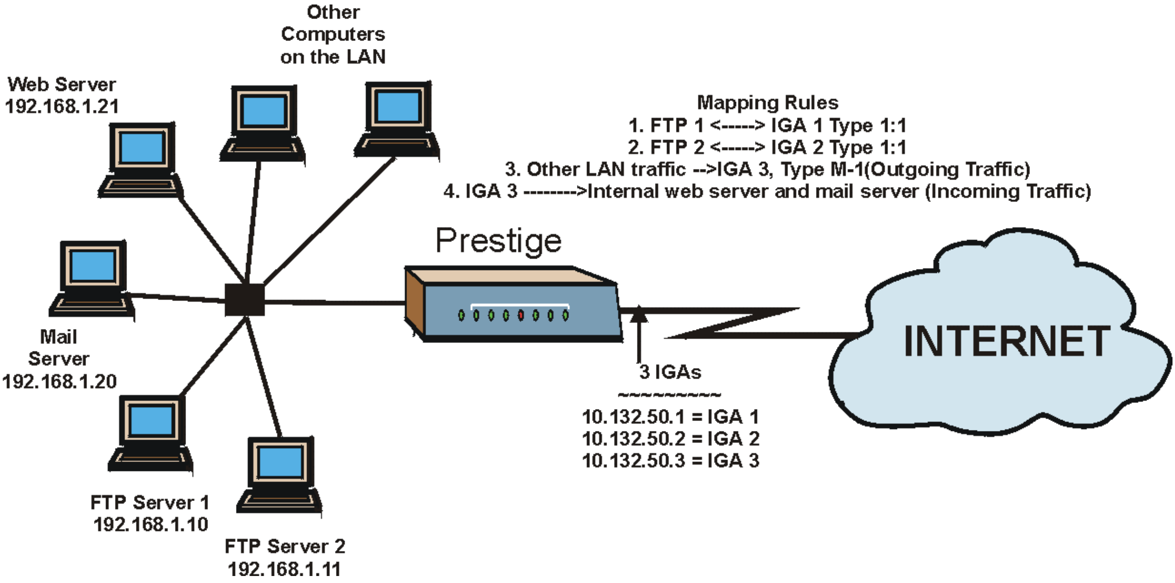

Other Computers on the LAN
Web Server 192.168.1.21
Mapping Rules
1. FTP 1 <-----> IGA 1 Type 1:1
2. FTP 2 <-----> IGA 2 Type 1:1
3. Other LAN traffic -->IGA 3, Type M-1(Outgoing Traffic)
4. IGA 3 -------->Internal web server and mail server (Incoming Traffic)
Prestige
Mail Server 192.168.1.20
INTERNET
3 IGAs
~~~~~~~~~~
10.132.50.1 = IGA 1
10.132.50.2 = IGA 2
10.132.50.3 = IGA 3
FTP Server 1 192.168.1.10
FTP Server 2 192.168.1.11

Figure 11-17 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 11-18*.

Step 1. Then enter 15 from the main menu.

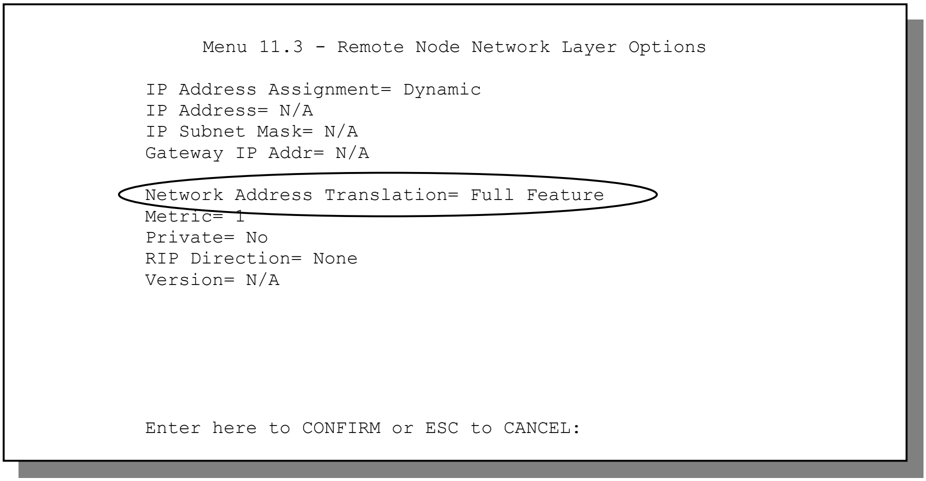
Step 2. Enter 1 to configure the Address Mapping Sets.

Step 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.
~~~~~~~~~~

Step 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 11-19).*

Step 5. Repeat the previous step for rules 2 to 4 as outlined above.

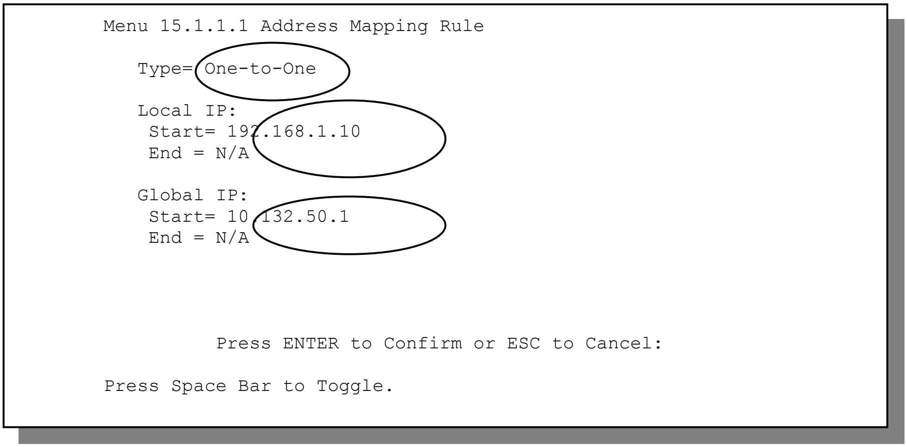
Step 6. When finished, menu 15.1.1 should look like as shown in *Figure 11-20.*



```
          Menu 11.3 - Remote Node Network Layer Options

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

     Network Address Translation= Full Feature
     Metric= 1
     Private= No
     RIP Direction= None
     Version= N/A







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

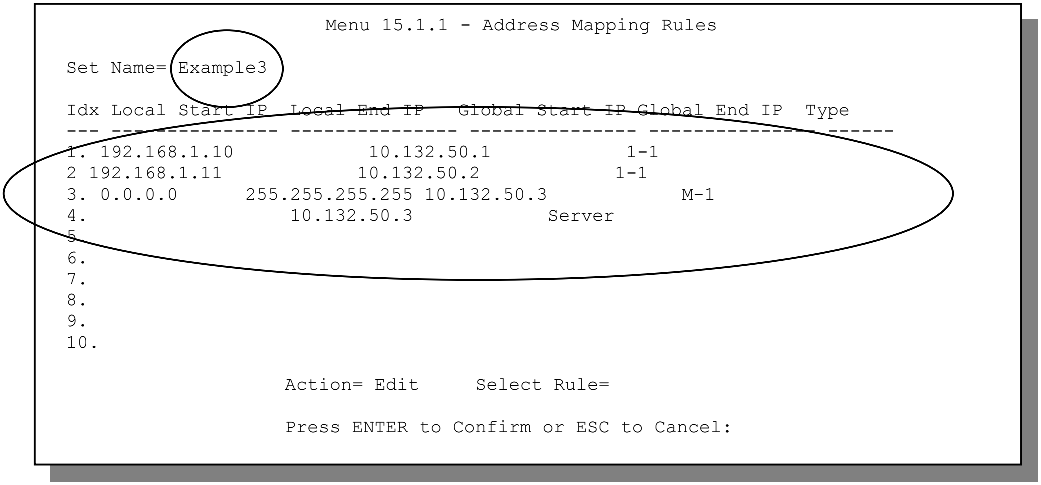
Figure 11-18 Example 3: Menu 11.3

The following figure shows how to configure the first rule.



```
        Menu 15.1.1.1 Address Mapping Rule

           Type= One-to-One

           Local IP:
            Start= 192.168.1.10
            End = N/A

           Global IP:
            Start= 10.132.50.1
            End = N/A



                  Press ENTER to Confirm or ESC to Cancel:

        Press Space Bar to Toggle.
```

Figure 11-19 Example 3: Menu 15.1.1.1



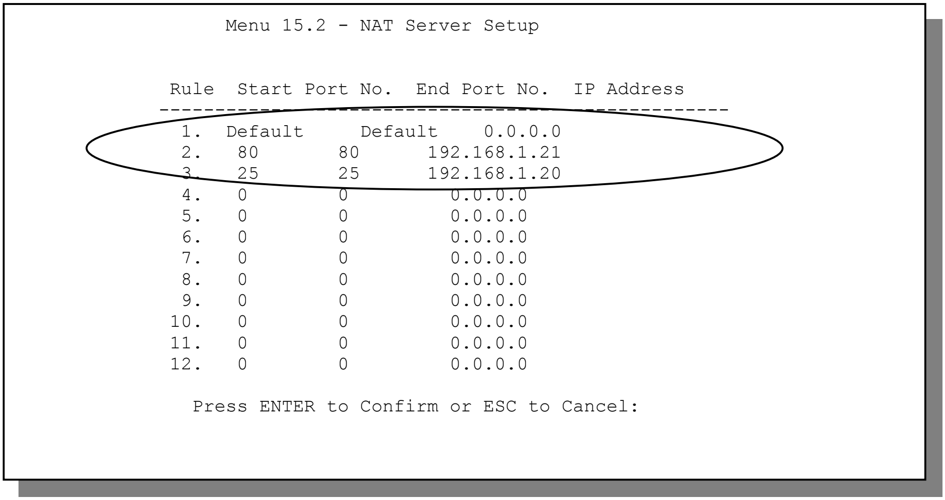
```
                         Menu 15.1.1 - Address Mapping Rules

  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 11-20 Example 3: Final Menu 15.1.1

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

Step 7. Enter 15 from the main menu.

Step 8. Now enter 2 from this menu and configure it as shown in *Figure 11-21*.



```
                    Menu 15.2 - NAT Server Setup


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

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

Figure 11-21 Example 3: Menu 15.2

11.4.4 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-One-to-One** mapping as port numbers do *not* change for this mapping type. The following figure illustrates this.

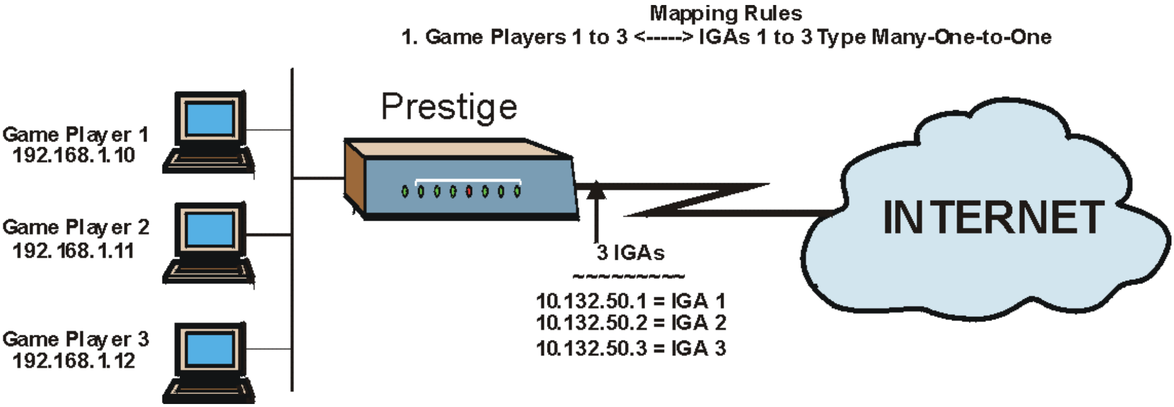
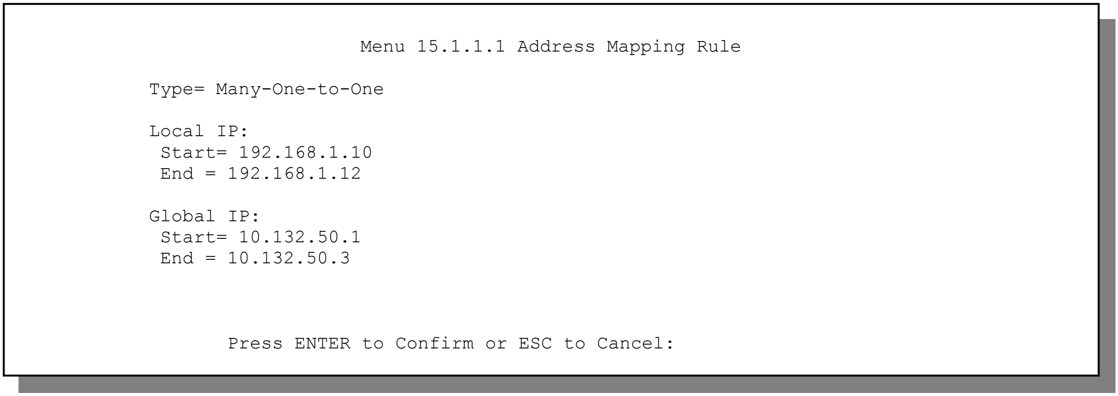


Figure 11-22 NAT Example 4

Other applications, for example, gaming programs are NAT unfriendly because they embed addressing information in the data stream. These applications still won't work through NAT even when using One-to-One **and** Many One-to-One **mapping types.**

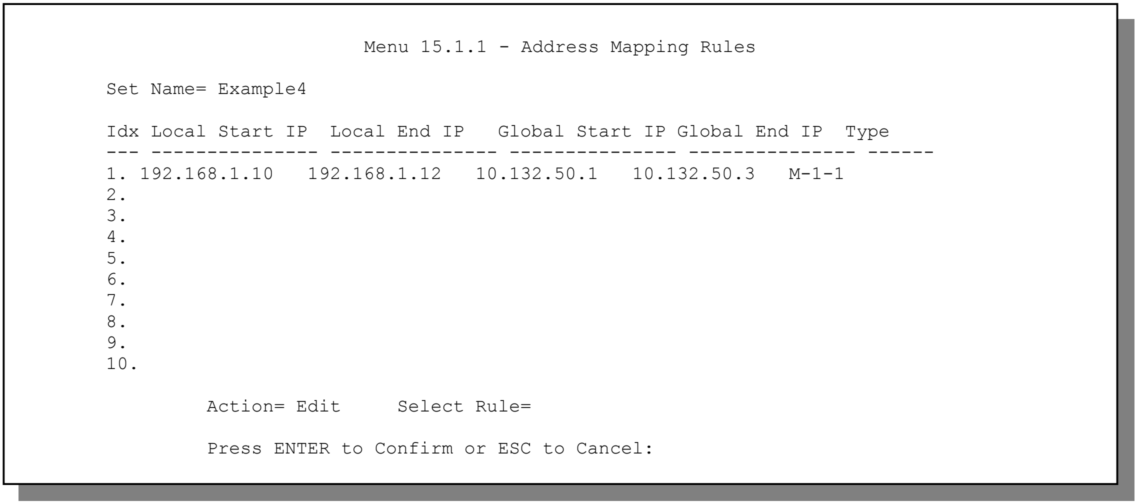
Follow the steps outlined in example 3 above to configure these two menus as follows.



```
                    Menu 15.1.1.1 Address Mapping Rule

  Type= Many-One-to-One

  Local IP:
   Start= 192.168.1.10
   End = 192.168.1.12

  Global IP:
   Start= 10.132.50.1
   End = 10.132.50.3



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

Figure 11-23 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-1-1
2.
3.
4.
5.
6.
7.
8.
9.
10.

         Action= Edit     Select Rule=

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

Figure 11-24 Example 4: Menu 15.1.1 — Address Mapping Rules

Part III:

Advanced Management

This section provides information on Firewall, Filter Configuration, SNMP Configuration, System Information and Diagnosis, Firmware and Configuration File Maintenance, System Maintenance and Call Scheduling.

Chapter 12
Firewall

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

12.1 Introduction

What is a Firewall?

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

Stateful Inspection Firewall.

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

About the Prestige Firewall

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

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

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

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

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

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

12.1.1 Guidelines For Enhancing Security With Your Firewall

1. Change the default password via web configurator.

Think about access control before you connect to the network in any way, including attaching a modem to the port.

Limit who can access 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.

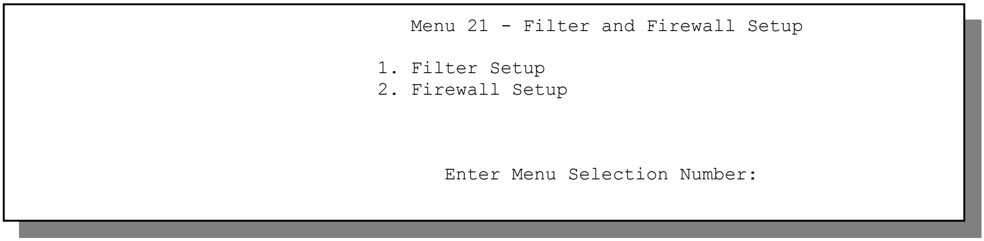
For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.

Protect against IP spoofing by making sure the firewall is active.

Keep the firewall in a secured (locked) room.

12.2 SMT Firewall Menu

Enter “21” from the main menu to display the following screen.



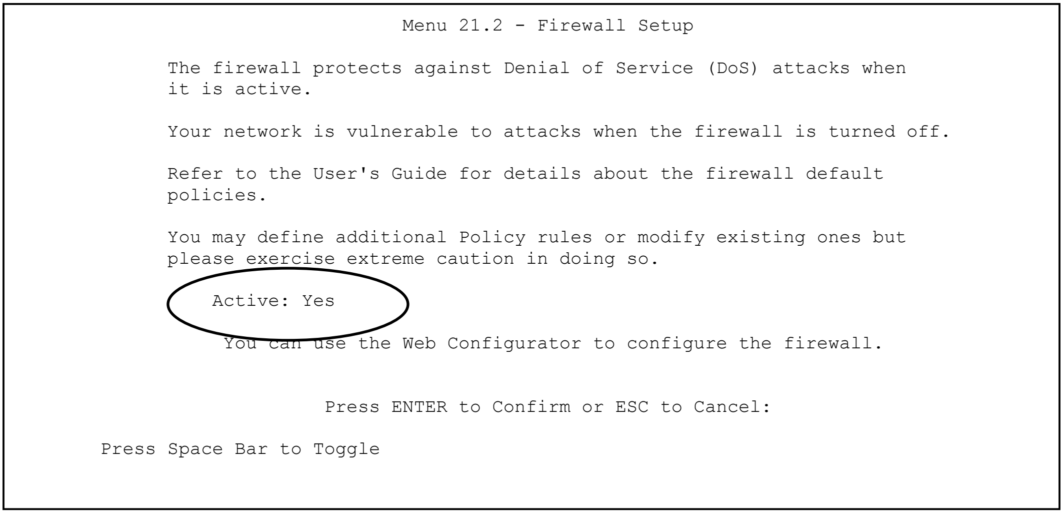
```
                                    Menu 21 - Filter and Firewall Setup

                                 1. Filter Setup
                                 2. Firewall Setup



                                       Enter Menu Selection Number:
```

Figure 12-1 Menu 21 - Filter and Firewall Setup

Enter “2” to display the firewall setup menu. You may only enable or disable the firewall in this screen. Use the web configurator to configure the firewall.

In the **Active** field press [SPACE BAR] and select **Yes** (to enable) or **No** (to disable) the Prestige firewall.

The firewall protects against Denial of Service (DoS) attacks when it is active. Your network is vulnerable to attacks when the firewall is turned off.

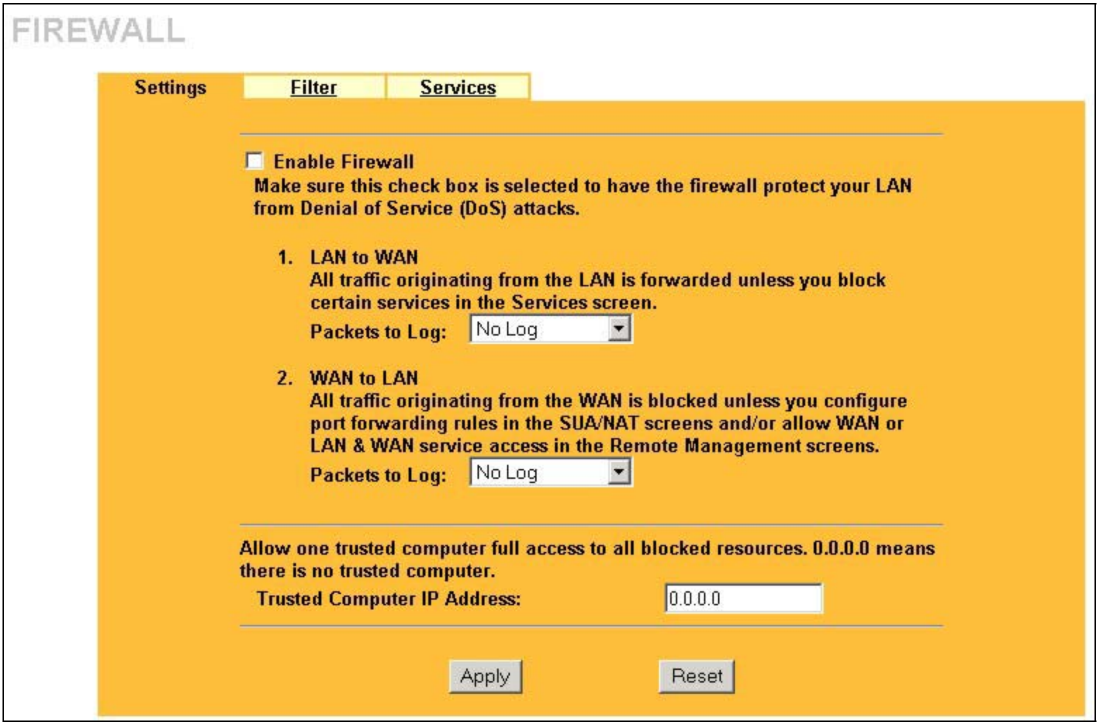


```
                          Menu 21.2 - Firewall Setup

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

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

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

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

              Active: Yes

               You can use the Web Configurator to configure the firewall.


                         Press ENTER to Confirm or ESC to Cancel:

    Press Space Bar to Toggle
```

Figure 12-2 Menu 21.2 - Firewall Setup

12.3 Web Configurator Firewall Settings Screen

From the **MAIN MENU**, then **FIREWALL**. The screen as shown next is the **Firewall Settings** tab.



FIREWALL

□ Enable Firewall

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

1. LAN to WAN
   All traffic originating from the LAN is forwarded unless you block certain services in the Services screen.
   Packets to Log: No Log
2. WAN to LAN
   All traffic originating from the WAN is blocked unless you configure port forwarding rules in the SUA/NAT screens and/or allow WAN or LAN & WAN service access in the Remote Management screens.
   Packets to Log: No Log

Allow one trusted computer full access to all blocked resources. 0.0.0.0 means there is no trusted computer.

Trusted Computer IP Address: 0.0.0.0

Figure 12-3 Firewall Settings

Table 12-1 Firewall Settings

FIELD	DESCRIPTION
Enable Firewall	Select this check box to activate the firewall. The Prestige performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
LAN to WAN	To log packets related to firewall rules, make sure that **Access Control** under **Log** is selected in the **Logs**, **Log Settings** screen.

Table 12-1 Firewall Settings

FIELD	DESCRIPTION
Packets to Log	Choose what **LAN to WAN** packets to log. Choose from: ➢ **No Log** ➢ **Log Blocked** (blocked LAN to WAN services appear in the **Blocked Services** textbox in the **Services** screen (with **Enable Services Blocking** selected)) ➢ **Log All** (log all **LAN to WAN** packets)
WAN to LAN	To log packets related to firewall rules, make sure that **Access Control** under **Log** is selected in the **Logs**, **Log Settings** screen.
Packets to Log	Choose what **WAN to LAN** and WAN to WAN/Prestige packets to log. Choose from: ➢ **No Log** ➢ **Log Forwarded** (see how to forward WAN to LAN traffic in the next section) ➢ **Log All** (log all **WAN to LAN** packets).
Allow one specific computer full access to all blocked resources.	
Trusted Computer	You can allow a specific computer to access all Internet resources without restriction. Enter the IP address of the trusted computer in this field.
To save your changes to the Prestige, click **Apply**. To reconfigure all the fields in this screen, click **Reset**.	

12.4 The Firewall, NAT and Remote Management

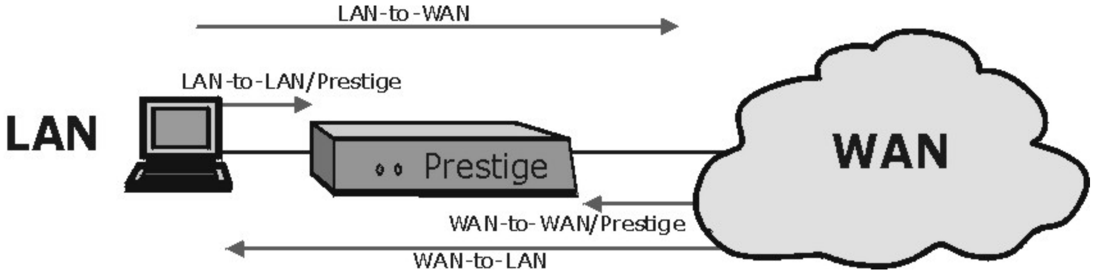


Figure 12-4 Firewall Rule Directions

12.4.1 LAN-to-WAN rules

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

How can you block certain LAN to WAN traffic?

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

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

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

12.4.2 WAN-to-LAN rules

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

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

- Configuring NAT port forwarding rules in the web configurator **SUA Server** screen or SMT NAT menus.

- Configuring **One-to-One** and **Many-One-to-One** NAT mapping rules in the web configurator **Address Mapping** screen or SMT NAT menus.

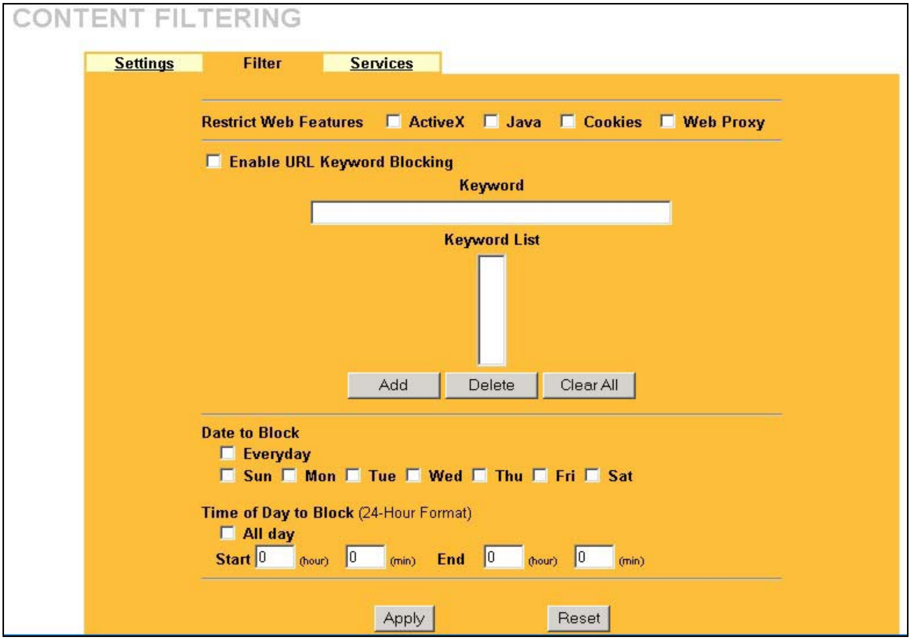
- Configuring **WAN** or **LAN & WAN** access for services in the **Remote Management** screens or SMT menus. When you allow remote management from the WAN, you are actually configuring WAN-to-WAN/Prestige firewall rules. WAN-to-WAN/Prestige firewall rules are Internet to the Prestige WAN interface firewall rules. The default is to block all such traffic. When you decide what WAN-to-LAN packets to log, you are in fact deciding what **WAN-to-LAN** and WAN-to-WAN/Prestige packets to log.

- Allow NetBIOS traffic from the WAN to the LAN using the **WAN IP** web screen or SMT menu 24.8 commands.

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

12.5 Filter

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



CONTENT FILTERING

Settings | Filter | Services

Restrict Web Features □ ActiveX □ Java □ Cookies □ Web Proxy

□ Enable URL Keyword Blocking

Keyword

Keyword List

Add | Delete | Clear All

Date to Block

□ Everyday

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

Time of Day to Block (24-Hour Format)

□ All day

Start 0 (hour) 0 (min) End 0 (hour) 0 (min)

Apply | Reset

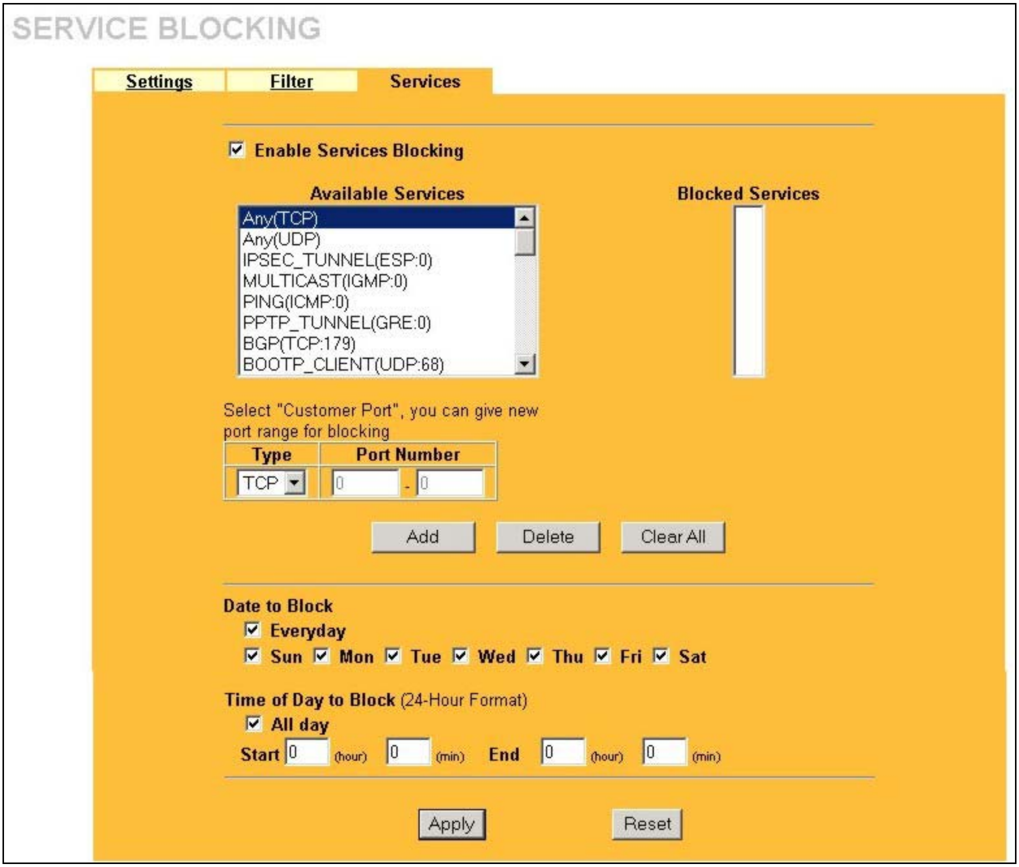
Figure 12-5 Firewall Filter

Table 12-2 Firewall Filter

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

12.6 Services

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



SERVICE BLOCKING

Settings | Filter | Services

☑ Enable Services Blocking

Available Services:
- Any(TCP)
- Any(UDP)
- IPSEC_TUNNEL(ESP:0)
- MULTICAST(IGMP:0)
- PING(ICMP:0)
- PPTP_TUNNEL(GRE:0)
- BGP(TCP:179)
- BOOTP_CLIENT(UDP:68)

Blocked Services

Select "Customer Port", you can give new port range for blocking

Type	Port Number
TCP	0 - 0

Add | Delete | Clear All

Date to Block

☑ Everyday

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time of Day to Block (24-Hour Format)

☑ All day

Start 0 (hour) 0 (min) End 0 (hour) 0 (min)

Apply | Reset

Figure 12-6 Firewall Service

Table 12-3 Firewall Service

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

Chapter 13
Filter Configuration

This chapter shows you how to create and apply filter(s).

13.1 About Filtering

Your Prestige uses filters to decide whether to allow passage of a data packet and/or to make a call. There are two types of filter applications: data filtering and call filtering. Filters are subdivided into device and protocol filters, which are discussed later.

Data filtering screens the data to determine if the packet should be allowed to pass. Data filters are divided into incoming and outgoing filters, depending on the direction of the packet relative to a port. Data filtering can be applied on either the WAN side or the Ethernet side. Call filtering is used to determine if a packet should be allowed to trigger a call. Remote node call filtering is only applicable when using **PPTP or PPPoE** encapsulation (*see **Error! Reference source not found.***). Outgoing packets must undergo data filtering before they encounter call filtering as shown in the following figure.

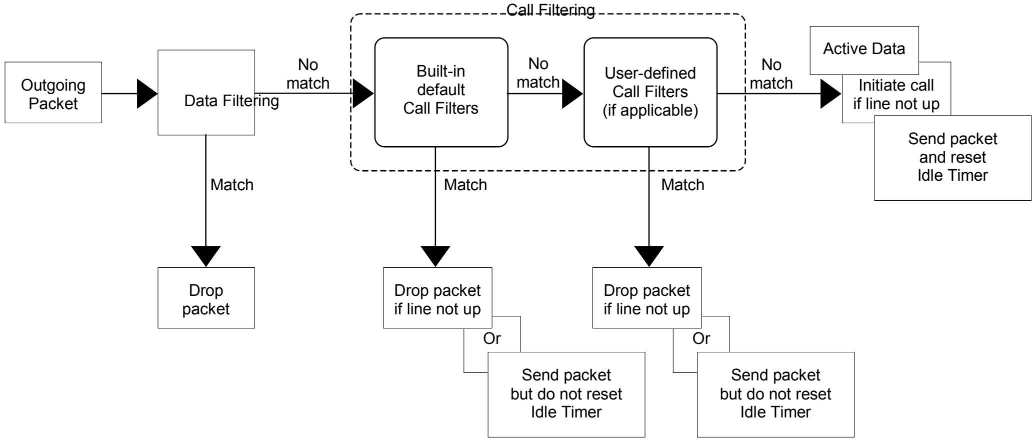

Call Filtering
Outgoing Packet
Data Filtering
No match
Built-in default Call Filters
No match
User-defined Call Filters (if applicable)
No match
Active Data
Initiate call if line not up
Send packet and reset Idle Timer
Match
Match
Match
Drop packet
Drop packet if line not up
Or
Send packet but do not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

Figure 13-1 Outgoing Packet Filtering Process

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

13.1.1 The Filter Structure of the Prestige

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

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

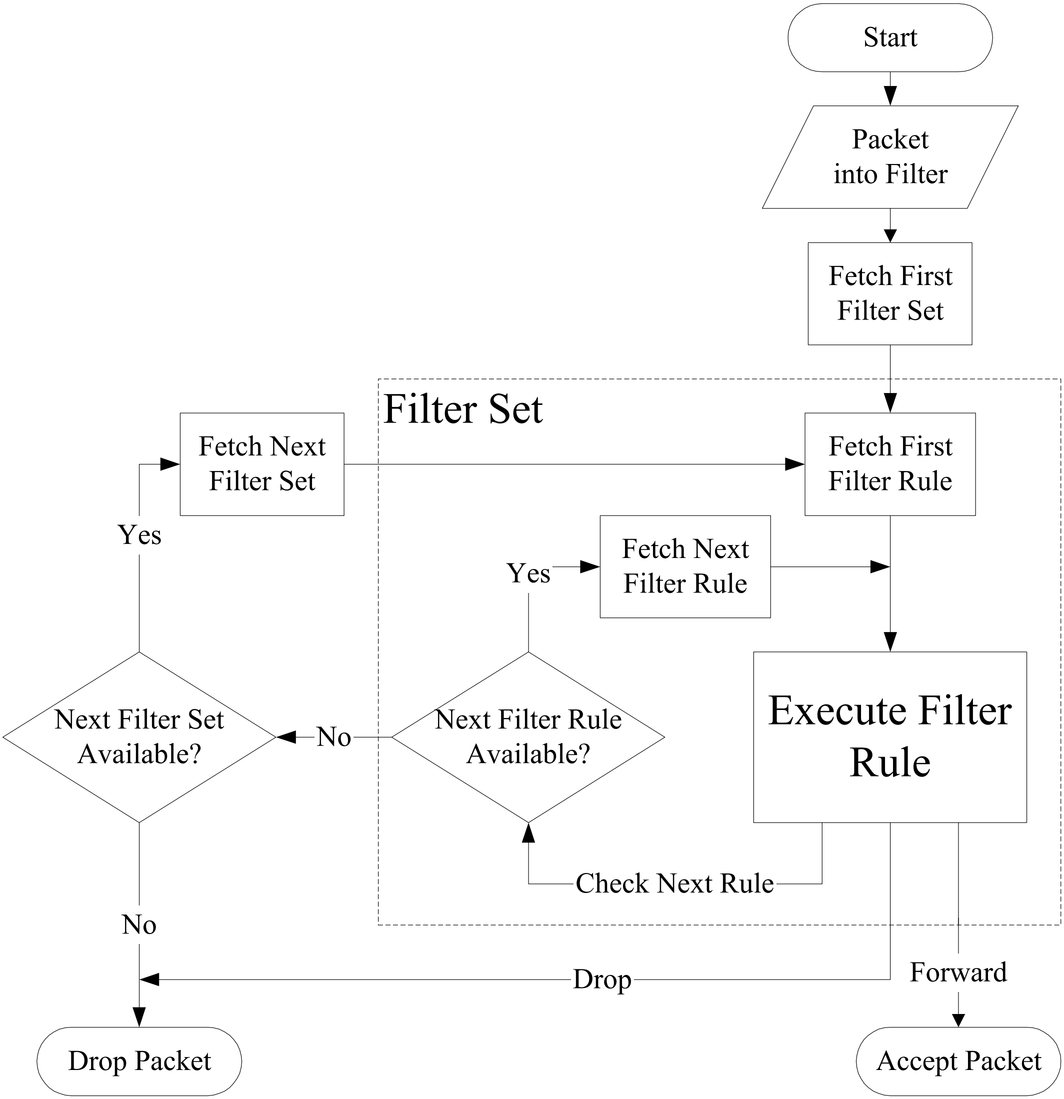


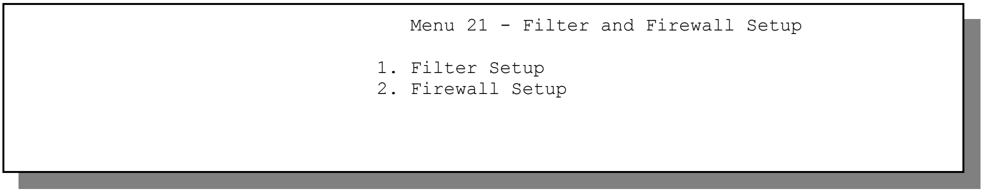
Figure 13-2 Filter Rule Process

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

13.2 Configuring a Filter Set

To configure a filter set, follow the procedure below. Select option 21 from the main menu to display menu 21.

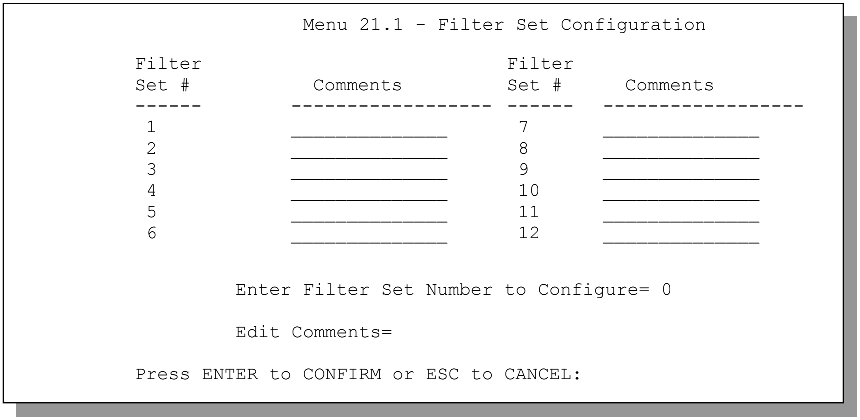
Enter "21" from the main menu.



```
                              Menu 21 - Filter and Firewall Setup

                           1. Filter Setup
                           2. Firewall Setup
```

Figure 13-3 Menu 21 - Filter and Firewall Setup

Enter "1" to display the following menu.



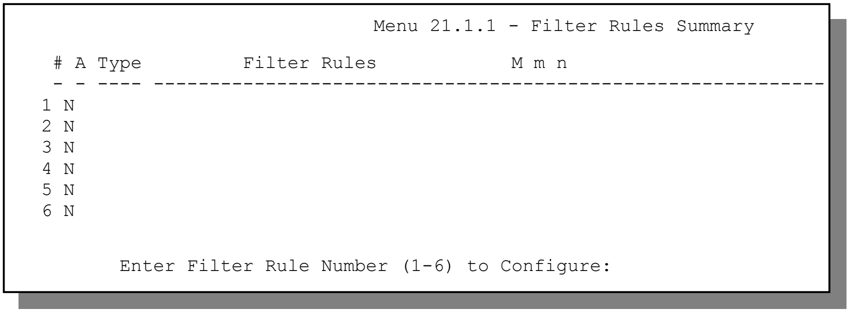
```
                         Menu 21.1 - Filter Set Configuration

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

                   Enter Filter Set Number to Configure= 0

                   Edit Comments=

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

Figure 13-4 Menu 21.1 - Filter Set Configuration

Select the filter set you wish to configure (no. 1-12) and press [ENTER].

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

Press [ENTER] at the message: [Press ENTER to confirm] to open **Menu 21.1.1** — **Filter Rules Summary**.



```
                               Menu 21.1.1 - Filter Rules Summary

   # A Type         Filter Rules           M m n
   - - ---- ------------------------------------------------------------
  1 N
  2 N
  3 N
  4 N
  5 N
  6 N


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

Figure 13-5 Menu 21.1.1 – Filter Rules Summary

13.2.1 Filter Rules Summary Menu

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

Table 13-1 Abbreviations Used in the Filter Rules Summary Menu

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

Table 13-1 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 13-2 Rule Abbreviations Used

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

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

13.2.2 Configuring a Filter Rule

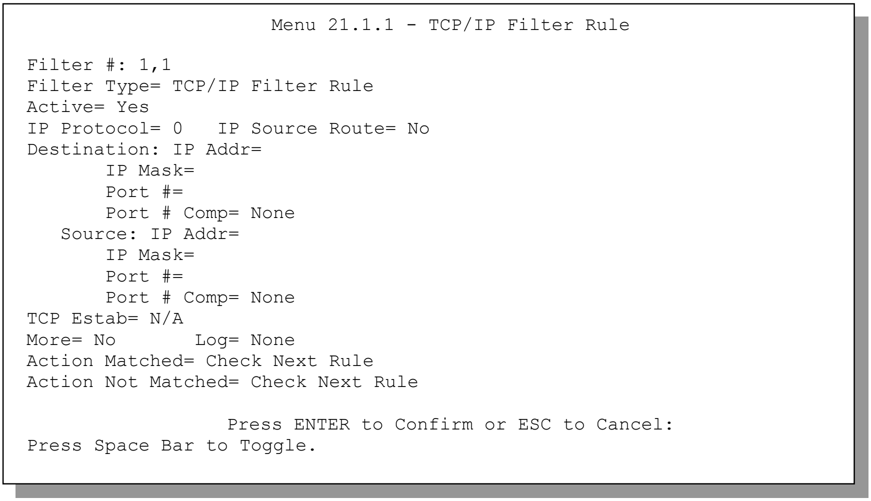
To configure a filter rule, type its number in **Menu 21.1 - Filter Rules Summary** and press [ENTER] to open menu 21.1.1 for the rule.

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

13.2.3 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, e.g., UDP and TCP headers.

To configure TCP/IP rules, select press [ENTER] to open **Menu 21.1.1 - TCP/IP Filter Rule**, as shown next.



```
                        Menu 21.1.1 - TCP/IP Filter Rule

Filter #: 1,1
Filter Type= TCP/IP Filter Rule
Active= Yes
IP Protocol= 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:
Press Space Bar to Toggle.
```

Figure 13-6 Menu 21.1.1 — TCP/IP Filter Rule

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

Table 13-3 TCP/IP Filter Rule Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Active	**Yes** activates and **No** deactivates the filter rule.	**Yes**

Table 13-3 TCP/IP Filter Rule Menu Fields

FIELD	DESCRIPTION	EXAMPLE
IP Protocol	Protocol refers to the upper layer protocol, e.g., TCP is 6, UDP is 17 and ICMP is 1. This value must be between 0 and 255	0-255
IP Source Route	If **Yes**, the rule applies to packet with IP source route option; else the packet must not have source route option. The majority of IP packets do not have source route.	**No**
Destination IP Address	Enter the destination IP Address of the packet you wish to filter. This field reads **don't-care** if it is 0.0.0.0.	IP address
IP Mask	Enter the IP mask that will be used to mask the bits of the IP address given in the **Destination IP Address** field.	IP mask
Port #	Enter the destination port of the packets that you wish to filter. The range of this field is 0 to 65535. This field reads **don't-care** if it is 0.	0-65535
Port # Comp	Select the comparison to apply to the destination port in the packet against the value given in **Destination Port #** field. Options are: **None**, **Less**, **Greater**, **Equal** or **Not Equal**.	**Equal**
Source IP Address	Enter the source IP Address of the packet you wish to filter. This field reads **don't-care** if it is 0.0.0.0.	IP Address
IP Mask	Enter the IP mask that will be used to mask the bits of the IP address given in the **Source IP Address** field.	IP Mask
Port #	Enter the source port of the packets that you wish to filter. The range of this field is 0 to 65535. This field **reads don't-care** if it is 0.	0-65535
Port # Comp	Select the comparison to apply to the source port in the packet against the value given in **Source Port #** field. Options are: **None**, **Less**, Greater, **Equal** or **Not Equal**.	**None**
TCP Estab	This field is applicable only when **IP Protocol** field is 6, TCP. If **Yes**, the rule matches only established TCP connections; else the rule matches all TCP packets.	**Yes** **No**

Table 13-3 TCP/IP Filter Rule Menu Fields

FIELD	DESCRIPTION	EXAMPLE
More	If **Yes**, a matching packet is passed to the next filter rule before an action is taken; else the packet is disposed of according to the action fields. If the **More** field is **Yes**, then **Action Matched** and **Action Not Matched** will be **No**.	**No**
Log	Select the logging option from the following: **None** – No packets will be logged. **Action Matched** - Only packets that match the rule parameters will be logged. **Action Not Matched** - Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.	**None**
Action Matched	Select the action for a matching packet. Options are **Check Next Rule**, **Forward** or **Drop**.	**Drop**
Action Not Matched	Select the action for a packet not matching the rule. Options are **Check Next Rule**, **Forward** or **Drop**.	**Check Next Rule**
Once you have completed filling in **Menu 21.1.1.1 - TCP/IP Filter Rule**, press [ENTER] at the message “Press Enter to Confirm to save your configuration, or press [ESC] to cancel”. This data will now be displayed on **Menu 21.1.1 - Filter Rules Summary**.		

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

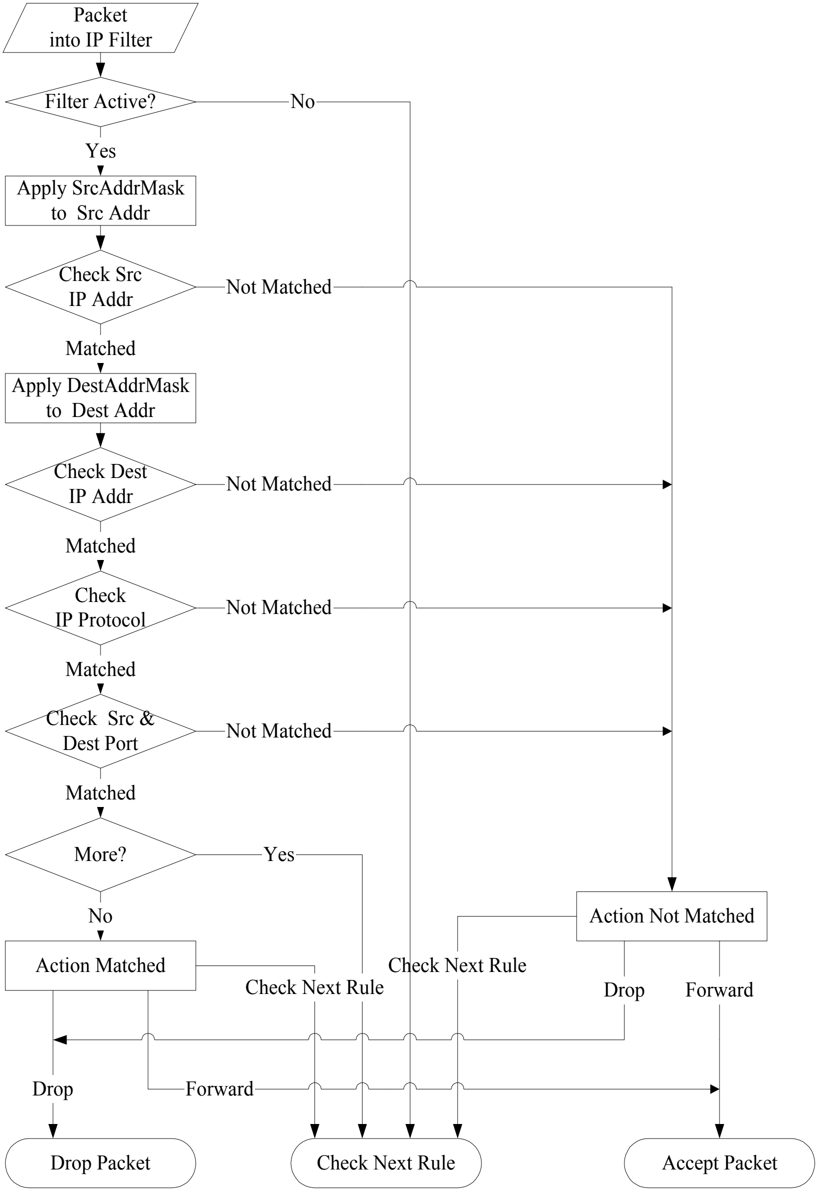


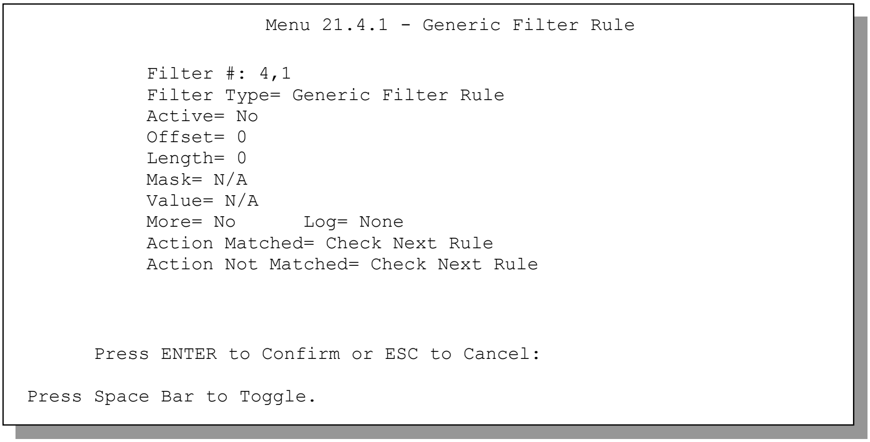
Figure 13-7 Executing an IP Filter

13.2.4 Generic Filter Rule

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

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

To configure a generic rule, select **Generic Filter Rule** in the **Filter Type** field in the menu 21.4.1 and press [ENTER] to open **Menu 21.4.1 - Generic Filter Rule**, as shown below.



```
                         Menu 21.4.1 - Generic Filter Rule

            Filter #: 4,1
            Filter Type= Generic Filter Rule
            Active= No
            Offset= 0
            Length= 0
            Mask= N/A
            Value= N/A
            More= No       Log= None
            Action Matched= Check Next Rule
            Action Not Matched= Check Next Rule



       Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 13-8 Menu 21.4.1 — Generic Filter Rule

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

Table 13-4 Generic Filter Rule Menu Fields

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

Table 13-4 Generic Filter Rule Menu Fields

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

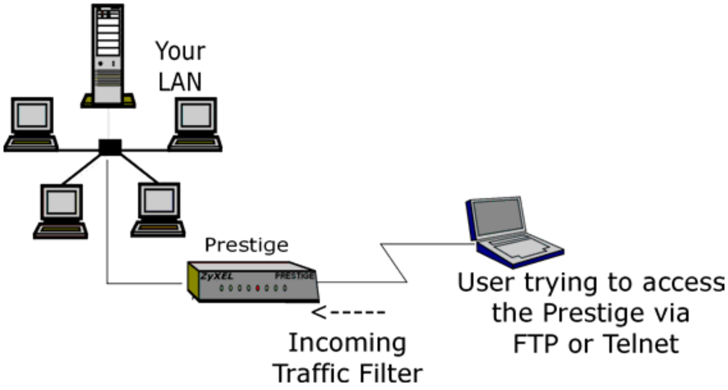
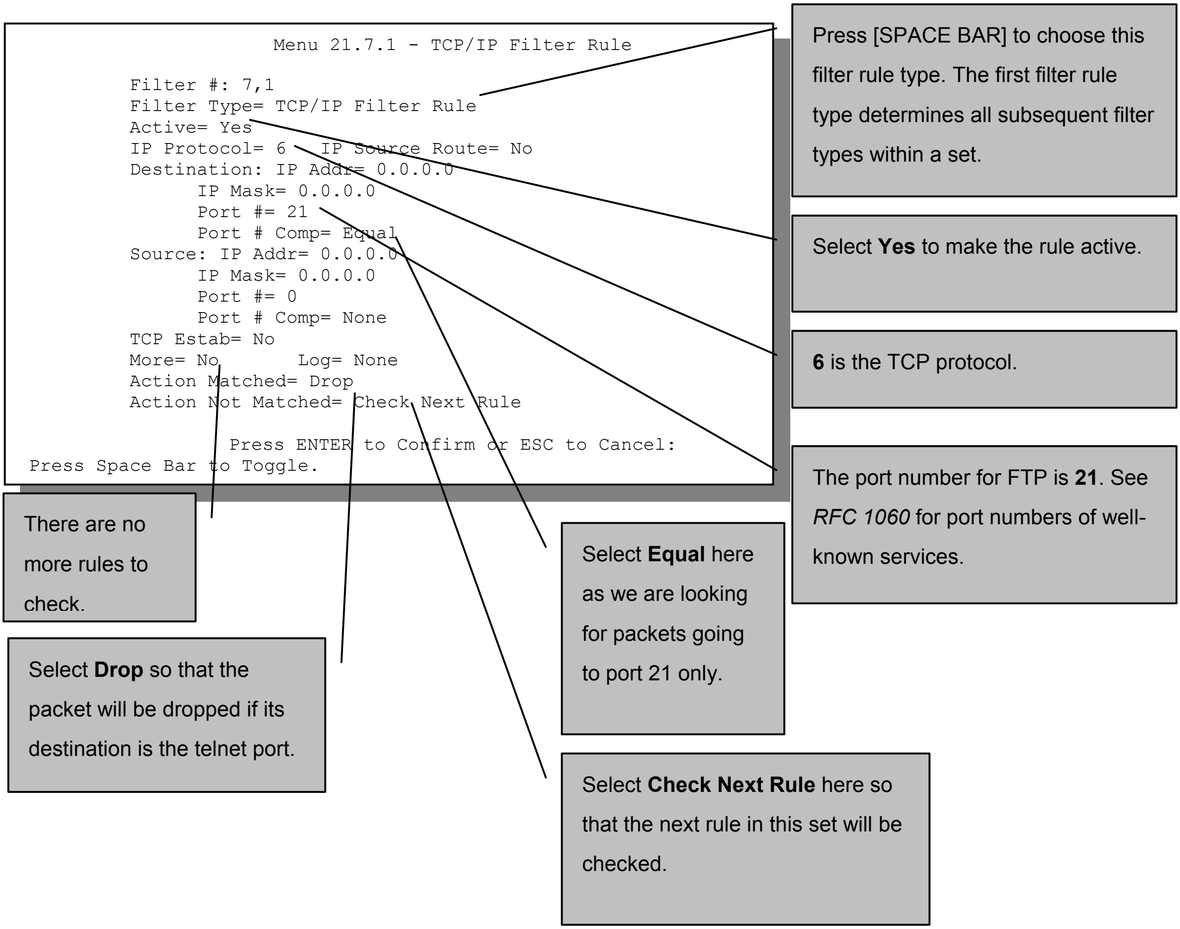


Figure 13-9 Filter Example

13.3 Example Filter

Let's look at an example to block outside users from accessing the Prestige via telnet. See the included support CD for more example filters.

1. Enter 21 from the main menu to open **Menu 21 - Filter Set Configuration**.
2. Enter the index of the filter set you wish to configure (e.g., 7) and press [ENTER].
3. Enter a descriptive name or comment in the **Edit Comments** field (e.g., TELNET_WAN) and press [ENTER].
4. Press [ENTER] at the message "[Press ENTER to confirm] to open **Menu 21.7 - Filter Rules Summary.**
5. Enter 1 to configure the first filter rule. Make the entries in this menu as shown in the following figure.



```
                      Menu 21.7.1 - TCP/IP Filter Rule

         Filter #: 7,1
         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 #= 21
              Port # Comp= Equal
         Source: IP Addr= 0.0.0.0
              IP Mask= 0.0.0.0
              Port #= 0
              Port # Comp= None
         TCP Estab= No
         More= No       Log= None
         Action Matched= Drop
         Action Not Matched= Check Next Rule

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

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 FTP is **21**. See *RFC 1060* for port numbers of well-known services.

Select **Equal** here as we are looking for packets going to port 21 only.

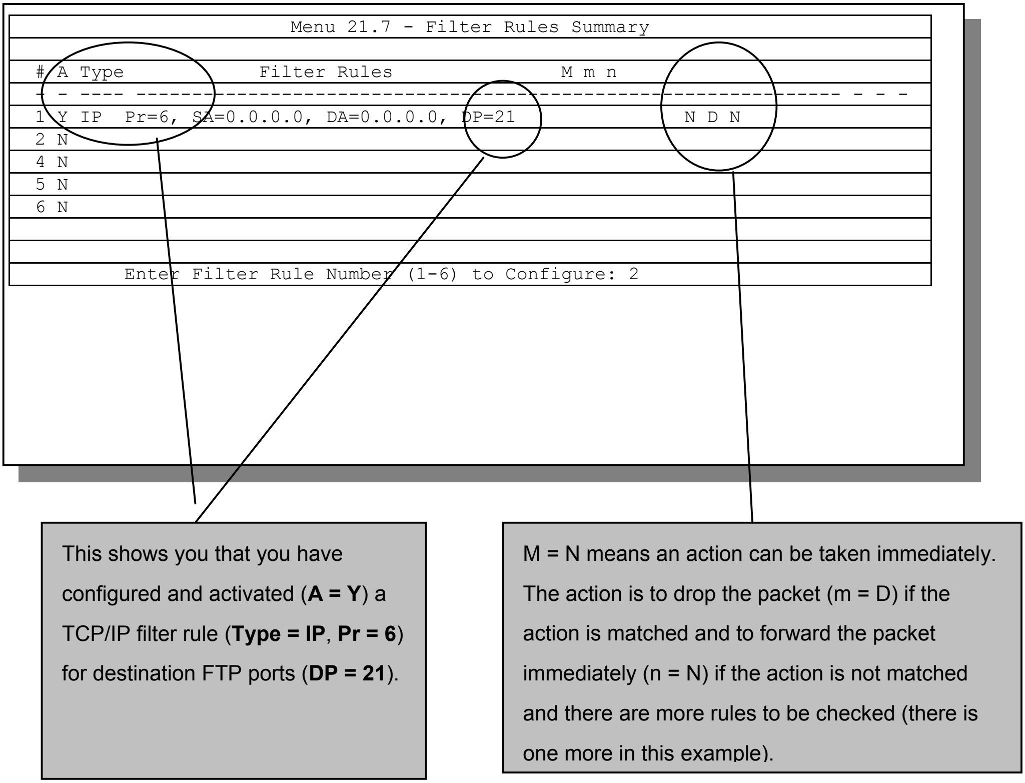
Select **Check Next Rule** here so that the next rule in this set will be checked.

There are no more rules to check.

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

Figure 13-10 Example Filter — Menu 21.3.1

Press [ENTER] to confirm and display the next screen. Note that there is only one filter rule in this set.



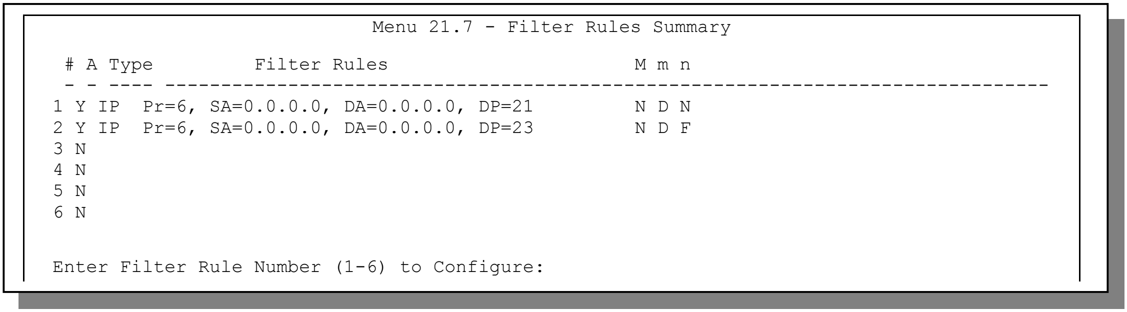
```
                        Menu 21.7 - Filter Rules Summary

 # A Type              Filter Rules                 M m n
 - - ---- ------------------------------------------------------------ - - -
 1 Y IP  Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=21              N D N
 2 N
 4 N
 5 N
 6 N


           Enter Filter Rule Number (1-6) to Configure: 2
```

This shows you that you have configured and activated (**A = Y**) a TCP/IP filter rule (**Type = IP**, **Pr = 6**) for destination FTP ports (**DP = 21**).

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 = N) if the action is not matched and there are more rules to be checked (there is one more in this example).

Figure 13-11 Example Filter Rules Summary — Menu 21.3

Enter 2 in the above menu to configure the second rule**.** Configure this filter rule with port number as 23 (Telnet) as shown in the next screen (after you press [ENTER] to confirm.



```
                              Menu 21.7 - Filter Rules Summary

  # A Type         Filter Rules                      M m n
  - - ---- ------------------------------------------------------------------------------
 1 Y IP  Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=21         N D N
 2 Y IP  Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23         N D F
 3 N
 4 N
 5 N
 6 N


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

Figure 13-12 Example Filter Rules Summary

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

6. Enter 11 from the main menu to display menu 11.

7. Go to the Edit Filter Sets field, press the [SPACE BAR] to select Yes and press [ENTER].

8. This brings you to menu 11.5. Apply the TELNET_FTP_WAN filter set (filter set 7) as shown in *Figure 13-15*.

13.4 Filter Types and NAT

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

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

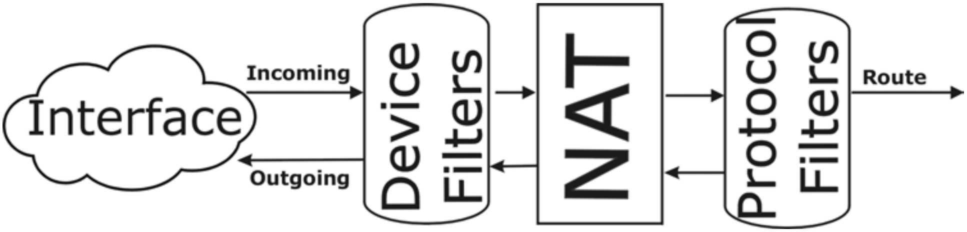


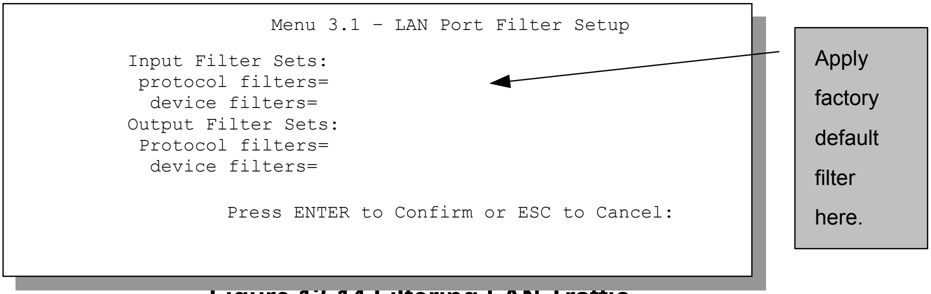
Figure 13-13 Protocol and Device Filter Sets

13.5 Applying a Filter and Factory Defaults

This section shows you where to apply the filter(s) after you design it (them).

13.5.1 LAN traffic

You seldom need to filter LAN traffic; however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 3.1 (shown below) and enter the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by entering their numbers separated by commas, e.g., 3, 4, 6, 11. Input filter sets filter incoming traffic to the Prestige and Output filter sets filter outgoing traffic from the Prestige.



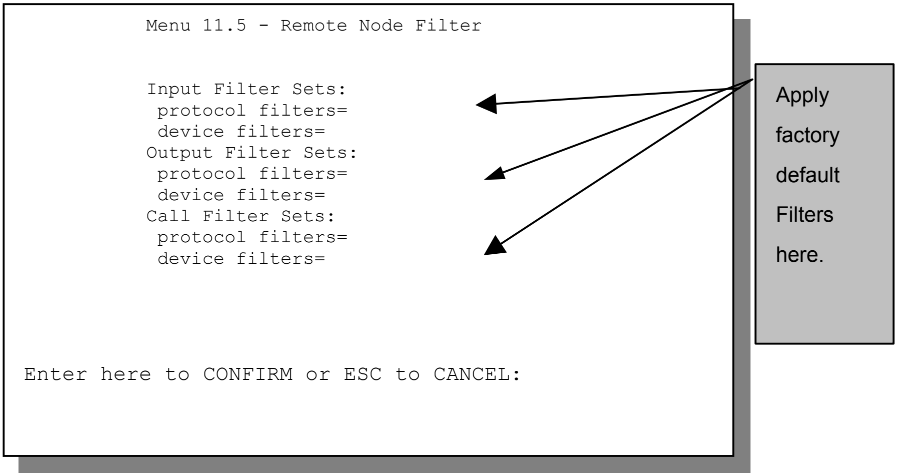
```
                    Menu 3.1 - LAN Port Filter Setup

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

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

Apply factory default filter here.

Figure 13-14 Filtering LAN Traffic

13.5.2 Remote Node Filters

Go to menu 11.5 (shown next – note that call filter sets are only present for PPPoE encapsulation) and enter the number(s) of the filter set(s) as appropriate. You can cascade up to four filter sets by entering their numbers separated by commas. Enter 1 in **protocol filters** under **Output Filter Sets** when using Ethernet encapsulation, and in the **protocol filters** field under **Call Filter Sets** when using PPPoE or PPTP encapsulation. Apply them as shown in the following figure.



```
            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:
```

Apply factory default Filters here.

Figure 13-15 Filtering Remote Node Traffic

Chapter 14
UPnP

This chapter introduces the UPnP feature.

14.1 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.

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

UPnP hardware is identified as an icon in the Network Connections or My Network Places 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.

14.1.2 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 Transversal and UPnP.

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

14.1.3 Cautions with UPnP

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

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

14.2 UPnP and ZyXEL

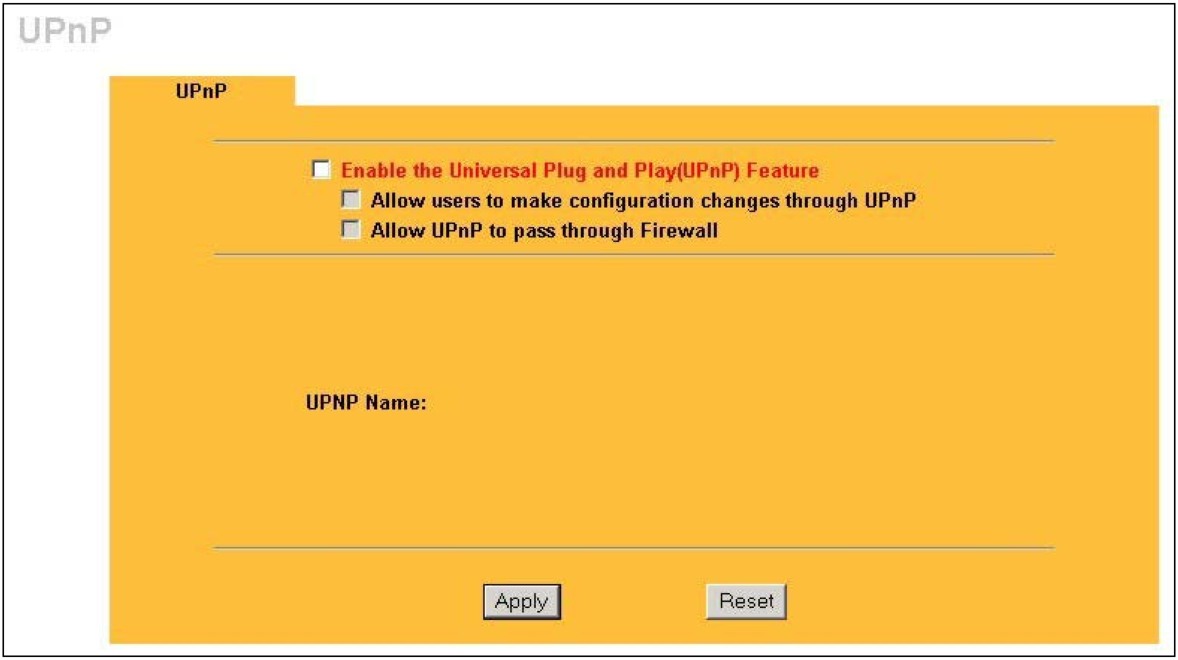
ZyXEL has achieved UPnP certification from the Universal Plug and Play Forum Creates UPnP™ Implementers Corp. (UIC). ZyXEL's UPnP implementation supports IGD 1.0 (Internet Gateway Device). At the time of writing ZyXEL's UPnP implementation supports Windows Messenger 4.6 and 4.7 while Windows Messenger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

UPnP broadcasts are only allowed on the LAN.

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

14.2.1 Configuring UPnP

From the **MAIN MENU** click **UPnP** to display the screen shown next.



UPnP

UPnP

☐ Enable the Universal Plug and Play(UPnP) Feature

☐ Allow users to make configuration changes through UPnP

☐ Allow UPnP to pass through Firewall

UPNP Name:

Figure 14-1 Configuring UPnP

Table 14-1 Configuring UPnP

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

Table 14-1 Configuring UPnP

FIELD	DESCRIPTION
Allow UPnP to pass through firewall	Select this check box to create a static LAN to LAN/Prestige rule that allows forwarding of ports 1900 and 80. Selecting this check box also creates a dynamic firewall rule every time a NAT forwarding port is reserved for UPnP. This setting remains active until you disable UPnP or clear this check box. Clear this check box to have the firewall block all UPnP application packets (for example, MSN packets) instead of creating a firewall rule for them.
UPNP Name	This identifies the ZyXEL device in UPnP applications.
Apply	Click Apply to save the setting to the Prestige.
Reset	Click Reset to begin configuring this screen afresh.

14.3 Installing UPnP in Windows Example

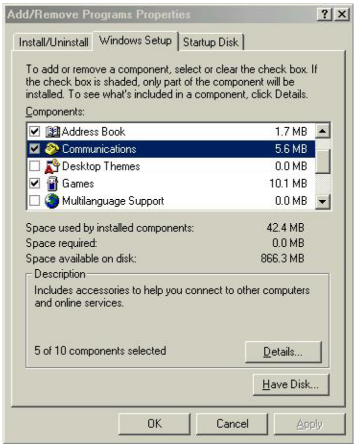
This section shows how to install UPnP in Windows Me and Windows XP.

Installing UPnP in Windows Me

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

9. Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.

10. 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

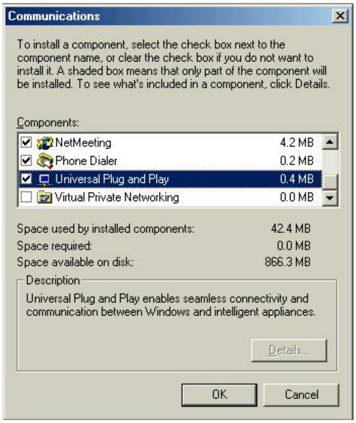
Includes accessories to help you connect to other computers and online services.

5 of 10 components selected

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

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

Restart the computer when prompted.



Communications

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.

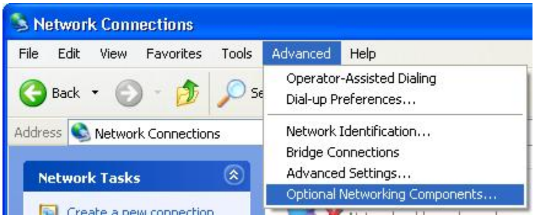
Installing UPnP in Windows XP

Follow the steps below to install the UPnP in Windows XP

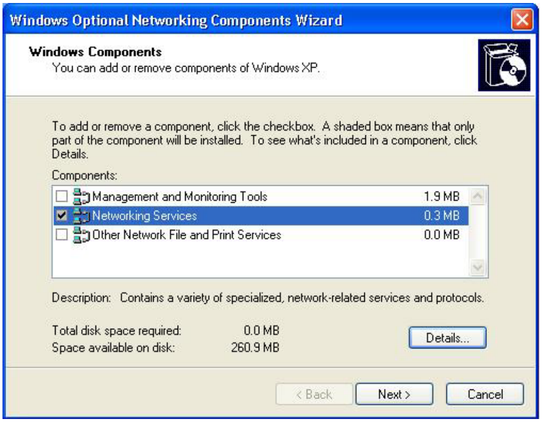
11. Click **start** and **Control Panel**.

12. Double-click **Network Connections**.

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



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



Windows Optional Networking Components Wizard

Windows Components
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:

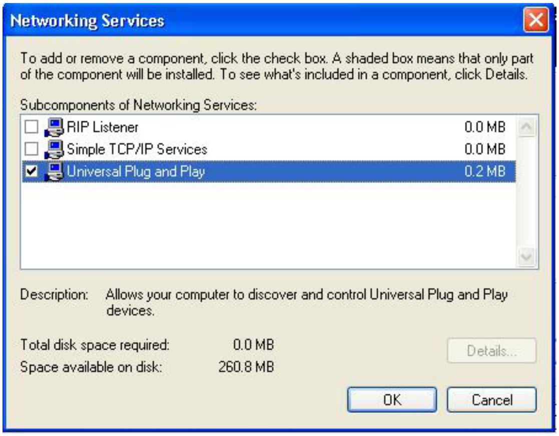
☐	Management and Monitoring Tools	1.9 MB
☑	Networking Services	0.3 MB
☐	Other Network File and Print Services	0.0 MB

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

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

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

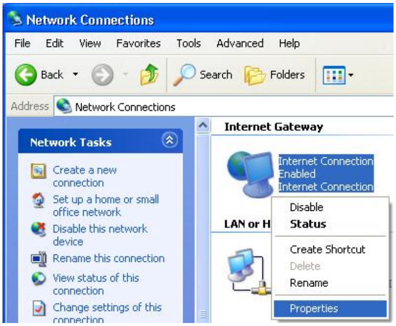
14.4 Using UPnP in Windows XP Example

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 ZyXEL device.

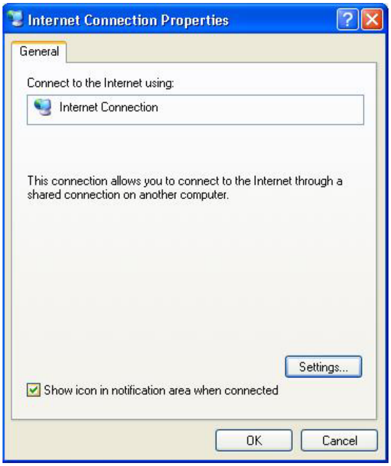
Make sure the computer is connected to a LAN port of the ZyXEL device. Turn on your computer and the ZyXEL device.

Auto-discover Your UPnP-enabled Network Device

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



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



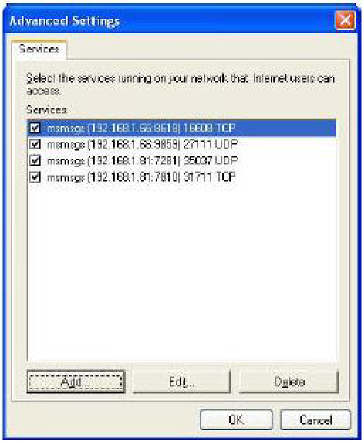
Connect to the Internet using:

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

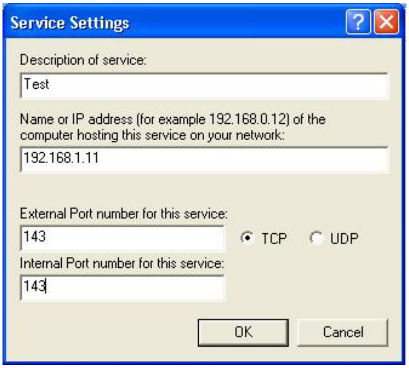
You may edit or delete the port mappings or click **Add** to manually add port mappings.



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



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:

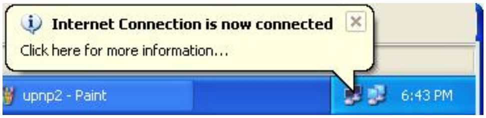
143 ● TCP ○ UDP

Internal Port number for this service:

143

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

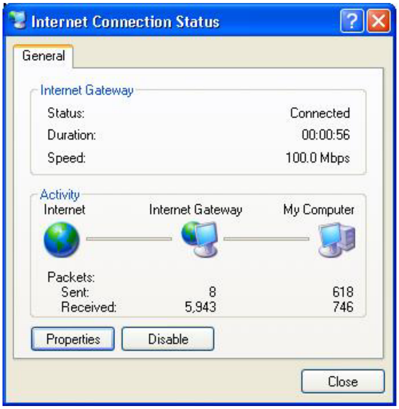
Select **Show icon in notification area when connected** option and click **OK**. An icon displays in the system tray



Internet Connection is now connected

Click here for more information...

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



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

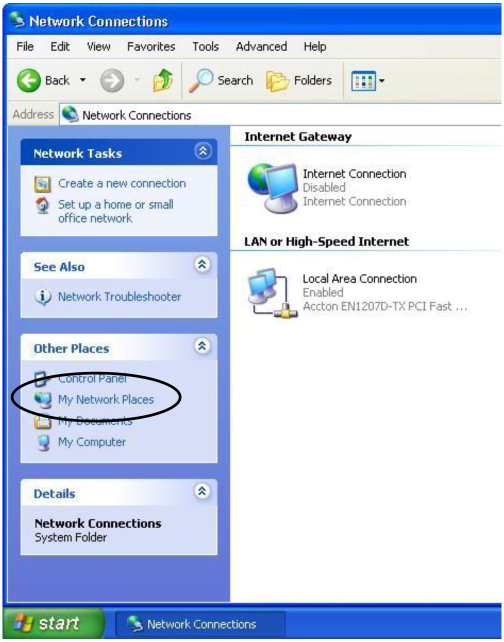
Packets:	Internet Gateway	My Computer
Sent:	8	618
Received:	5,943	746

Web Configurator Easy Access

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

Follow the steps below to access the web configurator.

16. Click **start** and then **Control Panel**.
17. Double-click **Network Connections**.
18. Select **My Network Places** under **Other Places**.

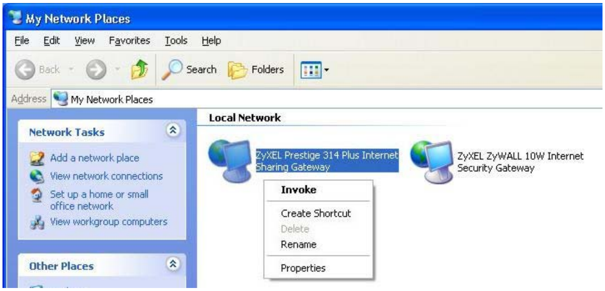


Internet Connection
Disabled
Internet Connection

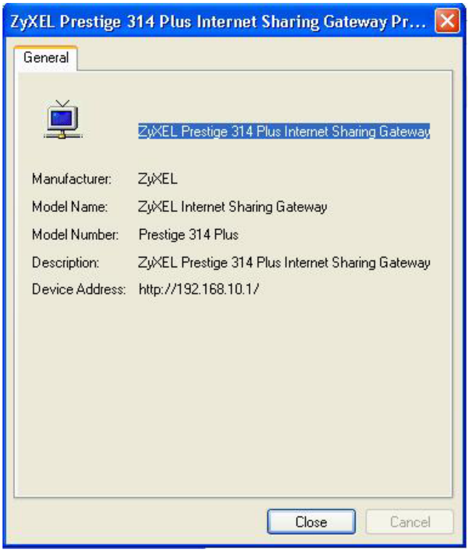
Local Area Connection
Enabled
Accton EN1207D-TX PCI Fast ...

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

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



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



ZyXEL Prestige 314 Plus Internet Sharing Gateway

Manufacturer: ZyXEL

Model Name: ZyXEL Internet Sharing Gateway

Model Number: Prestige 314 Plus

Description: ZyXEL Prestige 314 Plus Internet Sharing Gateway

Device Address: http://192.168.10.1/

Chapter 15
SNMP Configuration

This chapter explains SNMP configuration menu 22.

SNMP is only available if TCP/IP is configured.

15.1 About SNMP

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

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

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

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

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

Table 15-1 SNMP Commands

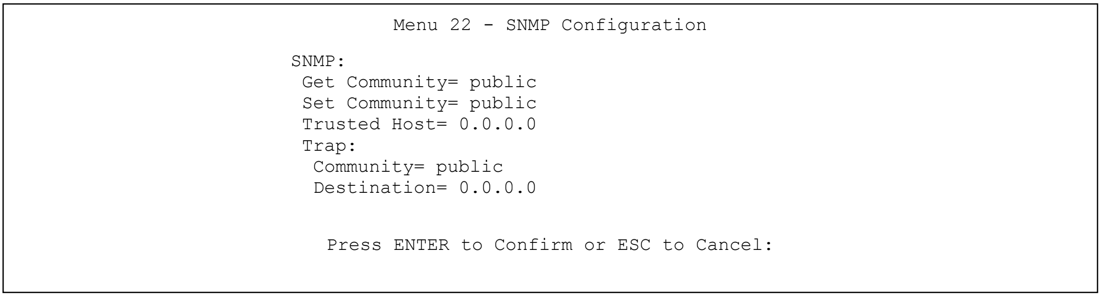
COMMAND	DESCRIPTION
Get	Allows the manager to retrieve an object variable from the agent.
GetNext	Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, 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.

15.2 Supported MIBs

The P324 supports MIB II that is defined in RFC-1213 and RFC-1215. The focus of the MIBs is to let administrators collect statistic data and monitor status and performance.

15.3 SNMP Configuration

To configure SNMP, enter 22 from the main menu to display **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 15-1 Menu 22 — SNMP Configuration

The following table describes the SNMP configuration parameters.

Table 15-2 SNMP Configuration Menu Fields

FIELD	DESCRIPTION	EXAMPLE
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.	**Blank**
Trap: Community	Type the trap community, which is the password sent with each trap to the SNMP manager.	**Public**
Trap: Destination	Type the IP address of the station to send your SNMP traps to.	**Blank**
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.		

15.4 SNMP Traps

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

Table 15-3 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
0	coldStart (defined in *RFC-1215*)	A trap is sent after booting (power on).
1	warmStart (defined in *RFC-1215*)	A trap is sent after booting (software reboot).
2	LinkUp	A trap is sent when the link is established.
3	LinkDown	A trap is sent when the link is down.
4	authenticationFailure (defined in *RFC-1215*)	A trap is sent to the manager when receiving any SNMP get or set 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 (warmstart).

Table 15-3 SNMP Traps

TRAP #	TRAP NAME	DESCRIPTION
6a	For intentional reboot:	A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (e.g. download new files, CI command "sys reboot", etc.).
6b	For fatal error:	A trap is sent with the message of the fatal code if the system reboots because of fatal errors.

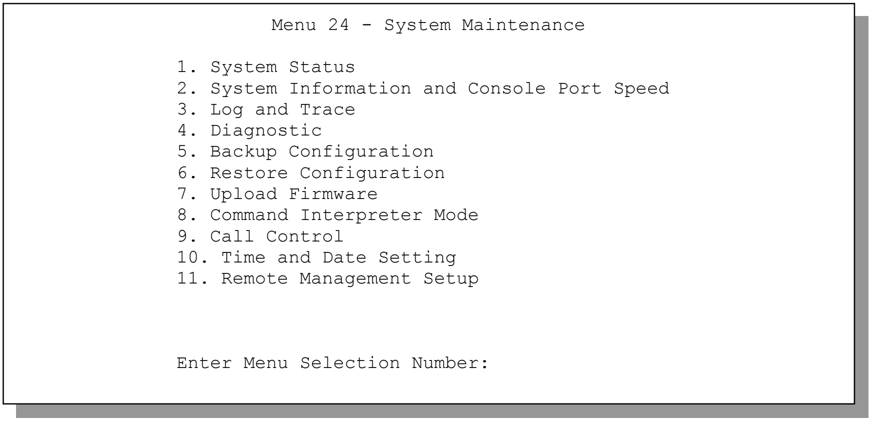
A

Chapter 16
System Information & Diagnosis

This chapter covers SMT menus 24.1 to 24 .4.

This chapter covers the diagnostic tools that help you to maintain your Prestige. These tools include updates on system status, port status, log and trace capabilities and upgrades for the system software.

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



```
                   Menu 24 - System Maintenance

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



          Enter Menu Selection Number:
```

Figure 16-1 Menu 24 — System Maintenance

16.1 System Status

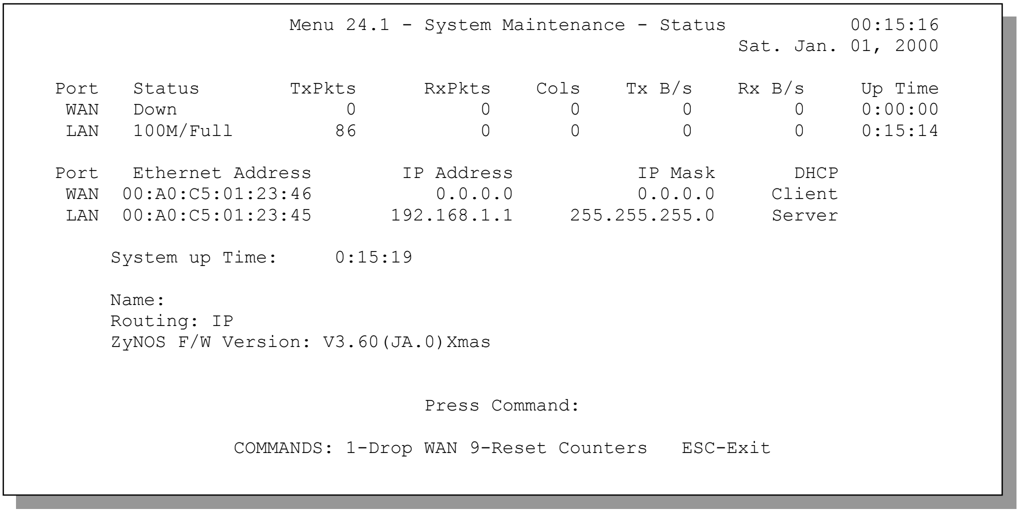
The first selection, System Status, gives you information on the version of your system firmware and the status and statistics of the ports, as shown in the next figure. System Status is a tool that can be used to monitor your Prestige. Specifically, it gives you information on your system firmware version,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

P

16.1.1 To get to the System Status:

- Enter 24 to display Menu 24 - System Maintenance.
- In this menu, enter number 1 to open **System Maintenance - Status**.
- There are three commands in **Menu 24.1 - System Maintenance - Status**. Entering 1 drops the WAN (PPTP/PPPoE) connection, 9 resets the counters and [ESC] takes you back to the previous screen.

The table below describes the fields present in **Menu 24.1 - System Maintenance - Status**. It should be noted that these fields are READ-ONLY and are meant to be used for diagnostic purposes.



```
                         Menu 24.1 - System Maintenance - Status          00:15:16
                                                                  Sat. Jan. 01, 2000

    Port   Status         TxPkts      RxPkts    Cols    Tx B/s    Rx B/s     Up Time
     WAN   Down                0           0       0         0         0     0:00:00
     LAN   100M/Full          86           0       0         0         0     0:15:14

    Port   Ethernet Address        IP Address           IP Mask       DHCP
     WAN  00:A0:C5:01:23:46           0.0.0.0           0.0.0.0     Client
     LAN  00:A0:C5:01:23:45       192.168.1.1     255.255.255.0     Server

         System up Time:     0:15:19

         Name:
         Routing: IP
         ZyNOS F/W Version: V3.60(JA.0)Xmas


                                     Press Command:

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

Figure 16-2 Menu 24.1 — System Maintenance — Status

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

Table 16-1 System Maintenance — Status Menu Fields

FIELD	DESCRIPTION
Port	The WAN or LAN port.
Status	Shows the port speed and duplex setting if you're using **Ethernet Encapsulation** and **Down** (line is down), **idle** (line (ppp) idle), **dial** (starting to trigger a call) and **drop** (dropping a call) if you're using **PPPoE Encapsulation**.
TxPkts	The number of transmitted packets on this port.

A

Table 16-1 System Maintenance — Status Menu Fields

FIELD	DESCRIPTION
RxPkts	The number of received packets on this port.
Cols	The number of collisions on this port.
Tx B/s	Shows the transmission speed in Bytes per second on this port.
Rx B/s	Shows the reception speed in Bytes per second on this port.
Up Time	Total amount of time the line has been up.
LAN	
Ethernet Address	The LAN port Ethernet address.
IP Address	The LAN port IP address.
IP Mask	The LAN port IP mask.
DHCP	The LAN port DHCP role.
WAN	
Ethernet Address	The WAN port Ethernet address.
IP Address	The WAN port IP address.
IP Mask	The WAN port IP mask.
DHCP	The WAN port DHCP role.
System up Time	The total time the Prestige has been on.
Name	This is the Prestige's system name + domain name assigned in menu 1. e.g., System Name= xxx; Domain Name= baboo.mickey.com. Name= xxx.baboo.mickey.com
ZyNOS F/W Version	The ZyNOS Firmware version and the date created.
You may enter 1 to drop the PPPoE/PPTP connection, 9 to reset the counters or [ESC] to return to menu 24.	

16.2 System Information and Console Port Speed

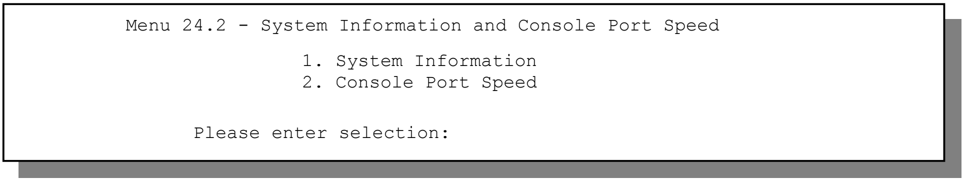
This section describes your system and allows you to choose different console port speeds. To get to the system information and console port speed:

P

Enter 24 to go to **Menu 24 - System Maintenance**.

Enter 2 to open **Menu 24.2 - System Information and Console Port Speed**.

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

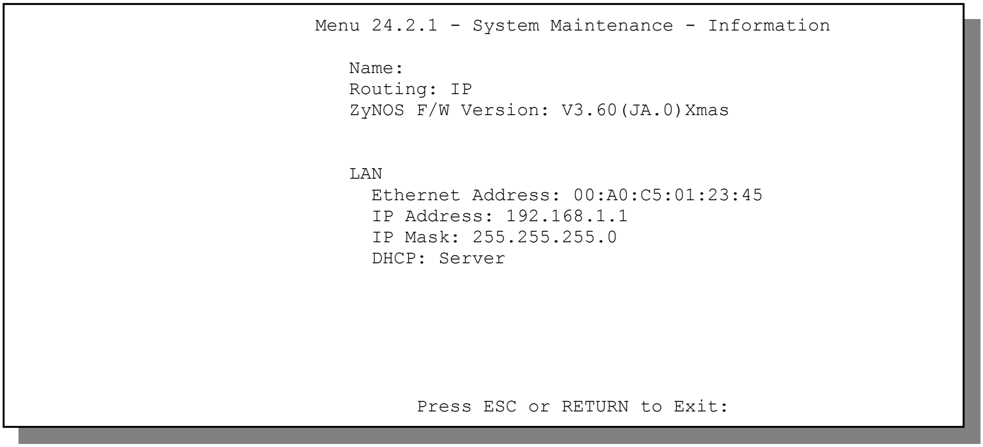


```
          Menu 24.2 - System Information and Console Port Speed

                         1. System Information
                         2. Console Port Speed


                Please enter selection:
```

Figure 16-3 Menu 24.2 — System Information and Console Port Speed

16.2.1 System Information

Menu 24.2.1 - System Maintenance - Information gives you information about your system as shown below. More specifically, it gives you information on your routing protocol, country code, Ethernet address, IP address, etc.



```
                    Menu 24.2.1 - System Maintenance - Information

                       Name:
                       Routing: IP
                       ZyNOS F/W Version: V3.60(JA.0)Xmas


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







                             Press ESC or RETURN to Exit:
```

Figure 16-4 Menu 24.2.1 System Maintenance — Information

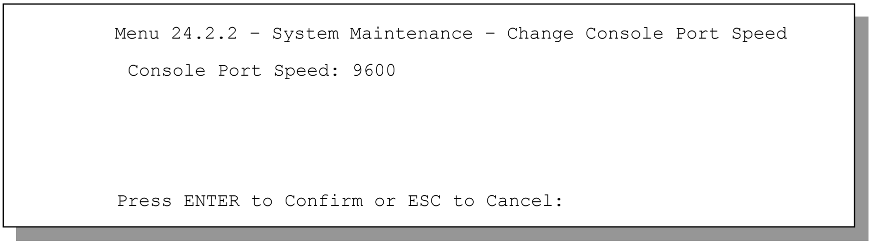
A

Table 16-2 Fields in System Maintenance

FIELD	DESCRIPTION
Name	This is the Prestige's system name + domain name assigned in menu 1. E.G., System Name= Prestige; Domain Name= zyxel.com Name= P324.zyxel.com
Routing	Refers to the routing protocol used.
ZyNOS F/W Version	Refers to the version of ZyXEL's Network Operating System software.
Ethernet Address	Refers to the Ethernet MAC (Media Access Control) address 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 of the Prestige.

16.2.2 Console Port Speed

You can change the speed of the console port through **Menu 24.2.2** — **Console Port Speed**. Your Prestige supports 9600 (default), 19200, 38400, 57600, and 115200 bps for the console port. The recommended maximum port speed fort he Prestige is 57600. Use the [SPACE BAR] to select the desired speed in menu 24.2.2, as shown next.



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

         Console Port Speed: 9600




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

Figure 16-5 Menu 24.2.2 — System Maintenance — Change Console Port Speed

16.3 Log and Trace

There are three 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. UNIX syslog is an external UNIX server used for storing log messages.

16.3.1 Viewing Error Log

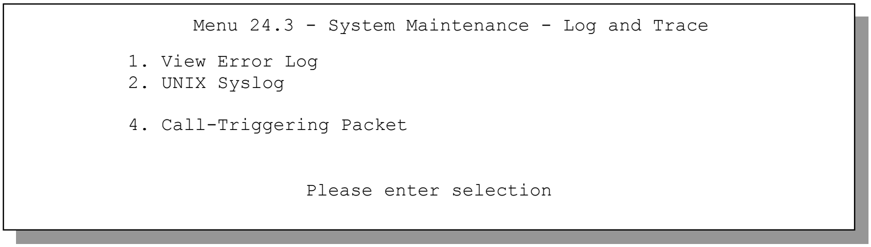
The first place you should look for clues when something goes wrong is the error/trace log. Follow the procedure below to view the local error/trace log:

Step 1. Select option 24 from the main menu to open **Menu 24 - System Maintenance**.

Step 2. From menu 24, select option 3 to display Menu 24.3 - System Maintenance - Log and Trace.

Step 3. Select the first option from **Menu 24.3 - System Maintenance - Log and Trace** to display the error log in the system.

After the Prestige finishes displaying, you will have the option to clear the error log.

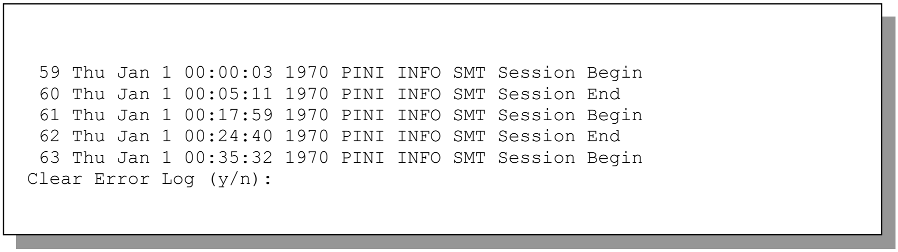


```
                 Menu 24.3 - System Maintenance - Log and Trace

           1. View Error Log
           2. UNIX Syslog

           4. Call-Triggering Packet


                           Please enter selection
```

Figure 16-6 Menu 23.3 System Maintenance — Log and Trace

Examples of typical error and information messages are presented in the figure below.

A

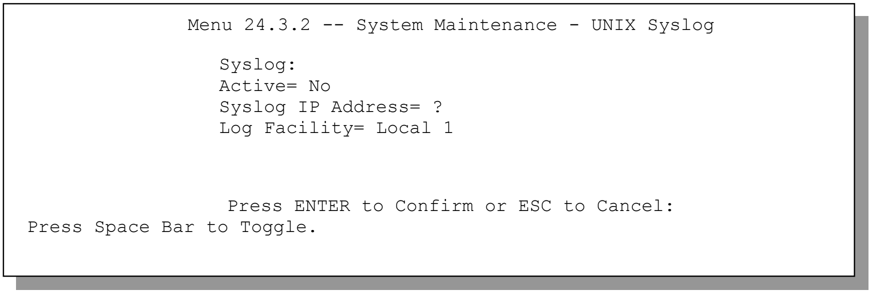


```
 59 Thu Jan 1 00:00:03 1970 PINI INFO SMT Session Begin
 60 Thu Jan 1 00:05:11 1970 PINI INFO SMT Session End
 61 Thu Jan 1 00:17:59 1970 PINI INFO SMT Session Begin
 62 Thu Jan 1 00:24:40 1970 PINI INFO SMT Session End
 63 Thu Jan 1 00:35:32 1970 PINI INFO SMT Session Begin
Clear Error Log (y/n):
```

Figure 16-7 Examples of Error and Information Messages

16.3.2 UNIX Syslog

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 - Syslog and Accounting**, as shown next.



```
                Menu 24.3.2 -- System Maintenance - UNIX Syslog

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



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

Figure 16-8 Menu 24.3.2 — System Maintenance — UNIX Syslog

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

Table 16-3 System Maintenance Menu Syslog Parameters

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

P

Table 16-3 System Maintenance Menu Syslog Parameters

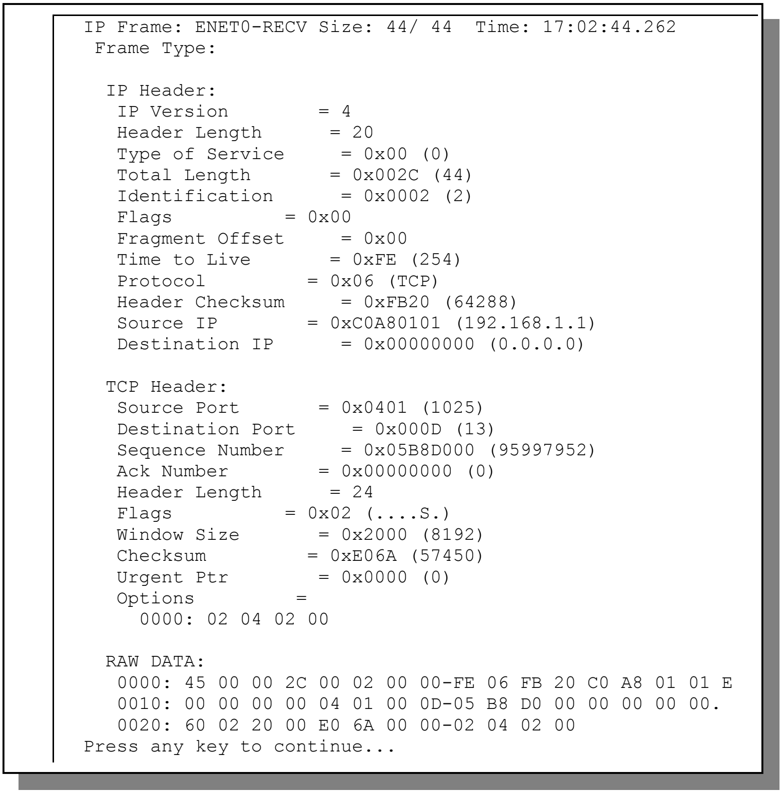
PARAMETER	DESCRIPTION
Syslog IP Address	Enter the IP Address of the server that will log the CDR (Call Detail Record) and system messages i.e., the syslog server.
Log Facility	Press the [SPACE BAR] to toggle between the 7 different Local options. The log facility allows you to log the message to different files in the server. Please refer to your UNIX manual for more detail.
When finished viewing, press [ESC] or [ENTER] to exit.	

16.3.3 Call-Triggering Packet

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

Note: This feature is available for PPTP/PPPoE Encapsulation only

A

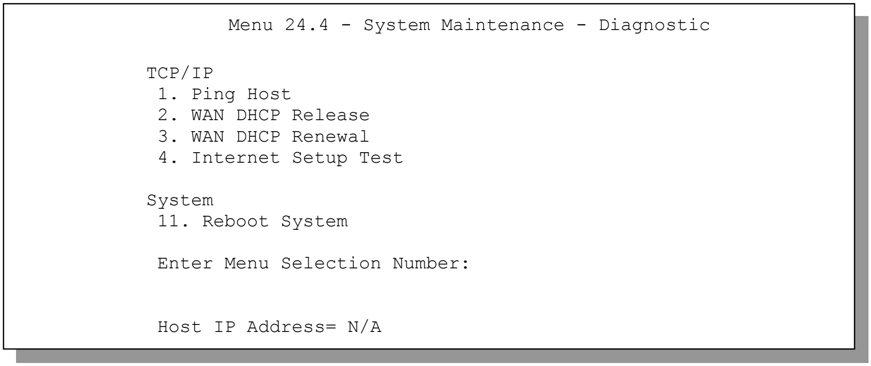


```
IP Frame: ENET0-RECV Size: 44/ 44  Time: 17:02:44.262
 Frame Type:

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

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

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

Figure 16-9 Call-Triggering Packet Example

16.4 Diagnostic

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



```
                    Menu 24.4 - System Maintenance - Diagnostic

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

             System
              11. Reboot System

              Enter Menu Selection Number:


              Host IP Address= N/A
```

Figure 16-10 Menu 24.4 — System Maintenance — Diagnostic

Follow the procedure below to get to **Menu 24.4 - System Maintenance – Diagnostic.**

Step 4. From the main menu, select option 24 to open **Menu 24 - System Maintenance**.

Step 5. From this menu, select option 4 (Diagnostic). This will open **Menu 24.4 - System Maintenance - Diagnostic**.

16.4.1 WAN DHCP

DHCP functionality can be enabled on the LAN or WAN as shown in *Figure 16-11*. The Prestige can act either as a WAN DHCP client (**IP Address Assignment** field in menu 4 or menu 11.3 is **Dynamic** and the **Encapsulation** field in menu 4 or menu 11 is **Ethernet**) or "none", i.e., you have a static IP. The WAN Release and Renewal fields in menu 24.4 conveniently allow you to release and/or renew the assigned WAN IP address, subnet mask and default gateway.

A

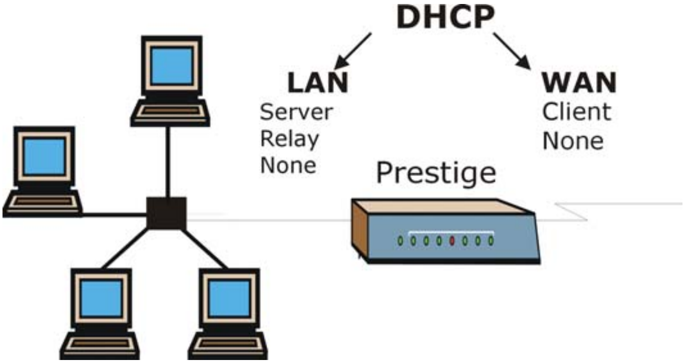


Figure 16-11 WAN & LAN DHCP

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

Table 16-4 System Maintenance Menu Diagnostic

NUMBER	FIELD	DESCRIPTION
1	Ping Host	Enter 1 to ping any machine (with an IP address) on your LAN or WAN. Enter its IP address in the **Host IP Address** field mentioned in the last row of this table.
2	WAN DHCP Release	Enter 2 to release your WAN DHCP settings.
3	WAN DHCP Renewal	Enter 3 to renew your WAN DHCP settings. The renewal timeout is 32 seconds.
4	Internet Setup Test	Enter 4 to test the Internet Setup. You can also test the Internet Setup in menu 4 - Internet Access. Please refer to the chapter- *Internet Access* for more details.
11	Reboot System	Enter 11 to reboot the Prestige.
	Host IP Address	If you entered 1 above, then enter the IP address of the machine you want to ping in this field.

Chapter 17
Firmware and Configuration File Maintenance

This chapter tells you how to back up and restore your configuration file as well as upload new firmware and a new configuration file.

17.1 Filename Conventions

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

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

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

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

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

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

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

The following table is a summary. Please note that the internal filename refers to the filename on the Prestige and the external filename refers to the filename not on the Prestige, that is, on your computer, local network or ftp site and so the name (but not the extension) will 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 17-1 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	Rom-0	*.rom	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.
Firmware	Ras	*.bin	This is the generic name for the ZyNOS firmware on the Prestige.

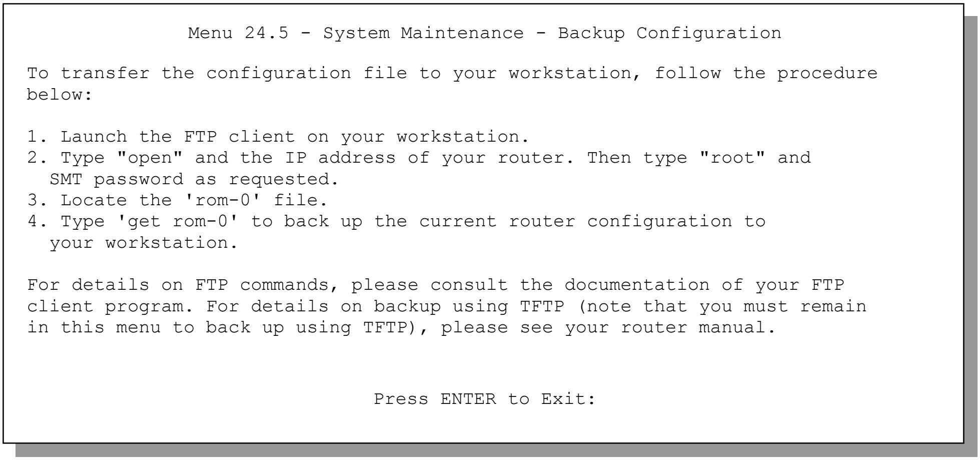
17.2 Backup Configuration

The Prestige displays different messages explaining different ways to backup, restore and upload files in menus 24.5, 24.6, 24. 7.1 and 24.7.2 when you use the serial/console port and when you telnet in.

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 and TFTP are the preferred methods for backing up your current configuration to your computer since FTP and TFTP are faster. You can also perform backup and restore using menu 24 through the console port. Any serial communications program should work fine; however, you must use Xmodem protocol to perform the download/upload and you don't have to rename the files (see *section 17.1*).

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.

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 router. Then type "root" and
  SMT password as requested.
3. Locate the 'rom-0' file.
4. Type 'get rom-0' to back up the current router 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 router manual.



                                 Press ENTER to Exit:
```

Figure 17-1 Telnet in Menu 24.5

17.2.1 Using the FTP Command from the DOS Prompt

Step 6. Launch the FTP client on your computer.

Step 7. Enter “open”, followed by a space and the IP address of your Prestige.

Step 8. Press [ENTER] when prompted for a username.

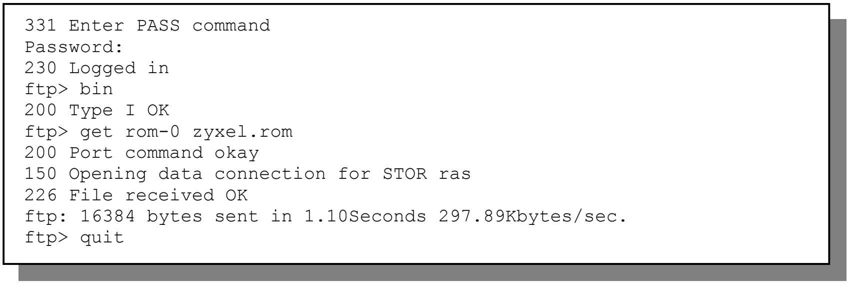
Step 9. Enter your password as requested (the default is “1234”).

Step 10. Enter “bin” to set transfer mode to binary.

Step 11. Use “get” to transfer files from the Prestige to the computer, for example, “get rom-0 config.rom” transfers the configuration file on the Prestige to your computer and renames it “config.rom”. See earlier in this chapter for more information on filename conventions.

Step 12. Enter “quit” to exit the ftp prompt.

Example of FTP Commands from the DOS Prompt



```
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 17-2 FTP Session Example

FTP GUI Clients

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

Table 17-2 General Commands for GUI 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).

TFTP and FTP over WAN Will Not Work When

- Telnet service is disabled in menu 24.11.
- A filter in menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block Telnet service.
- 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 Telnet session immediately.

- There is a SMT console session running.

17.2.2 Backup Configuration Using TFTP

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

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

Step 1. Use telnet from your computer to connect to the Prestige and log in. Because TFTP does not have any security checks, the Prestige records the IP address of the telnet client and accepts TFTP requests only from this address.

Step 2. Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.

Step 3. Enter command “sys stdio 0” to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter command “sys stdio 5” to restore the five-minute SMT timeout (default) when the file transfer is complete.

Step 4. Launch the TFTP client on your computer and connect to the Prestige. Set the transfer mode to binary before starting data transfer.

Step 5. Use the TFTP client (see the example below) to transfer files between the Prestige and the computer. The file name for the configuration file is “rom-0” (rom-zero, not capital o).

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

17.2.3 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.

TFTP GUI Clients

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

Table 17-3 General Commands for TFTP GUI Clients

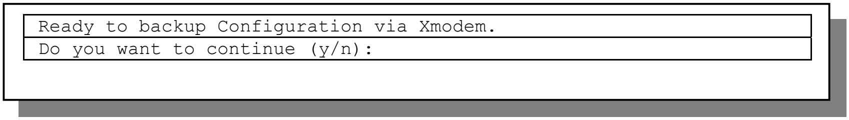
COMMAND	DESCRIPTION
Host	Enter the IP address of the Prestige. 192.168.1.1 is the Prestige’s default IP address when shipped.
Send/Fetch	Use “Send” to upload the file to the Prestige and “Fetch” to back up the file on your computer.
Local File	Enter the path and name of the firmware file (*.bin extension)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

Refer to the *TFTP and FTP over WAN Will Not Work When* section to read about configurations that disallow TFTP and FTP to work over WAN.

17.2.4 Backup Via Console Port

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

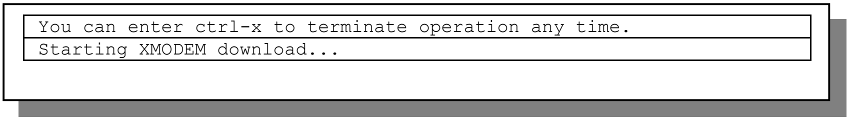
Step 13. Display menu 24.5 and enter “y” at the following screen.



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

Figure 17-3 System Maintenance — Backup Configuration

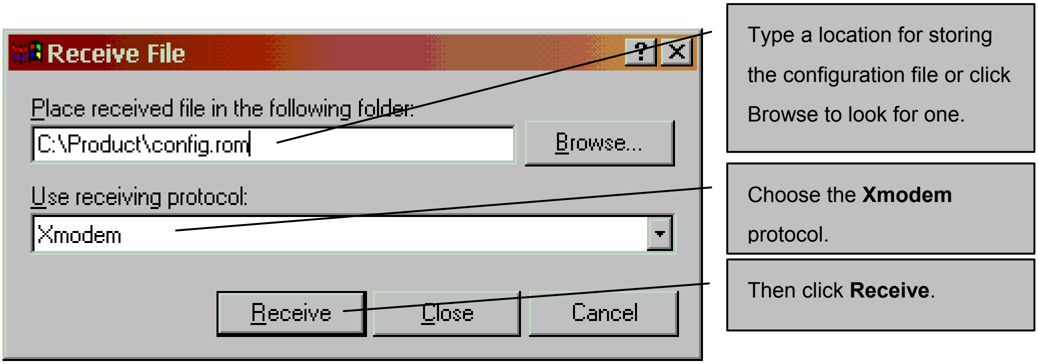
Step 1. The following screen indicates that the Xmodem download has started.



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

Figure 17-4 System Maintenance — Starting Xmodem Download Screen

Step 2. Run the HyperTerminal program by clicking **Transfer**, then **Receive File** as shown in the following screen.



Receive File

Place received file in the following folder: C:\Product\config.rom

Use receiving protocol: Xmodem

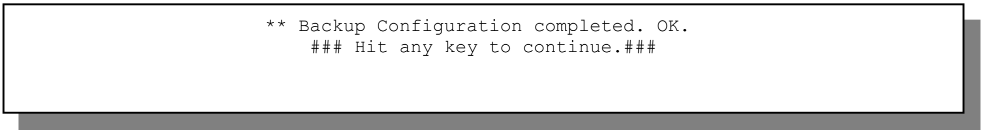
Type a location for storing the configuration file or click Browse to look for one.

Choose the **Xmodem** protocol.

Then click **Receive**.

Figure 17-5 Backup Configuration Example

Step 3. After a successful backup you will see the following screen. Press any key to return to the SMT menu.



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

Figure 17-6 Successful Backup Confirmation Screen

17.3 Restore Configuration

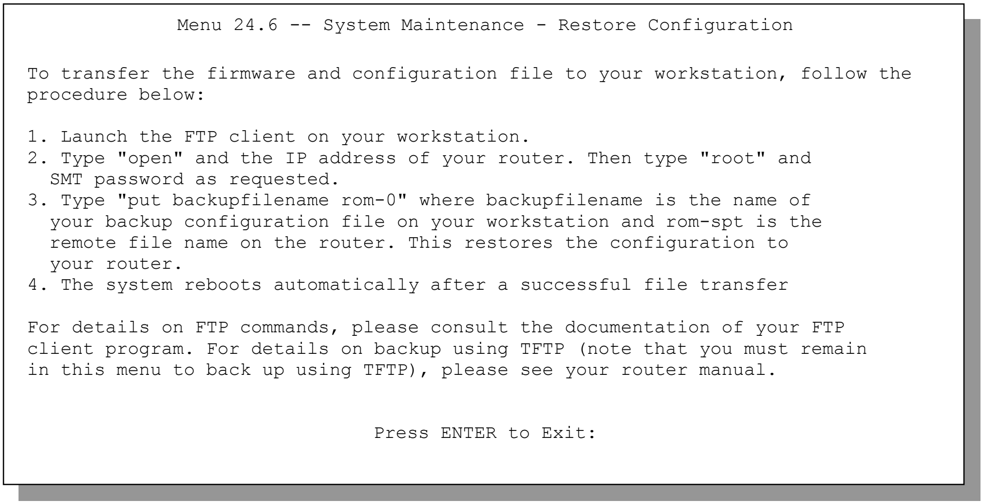
This section shows you how to restore a previously saved configuration. Note that this function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

FTP and TFTP are the preferred methods for restoring your current computer configuration to your Prestige since FTP and TFTP are faster. Please note that you must restart the system after the file transfer is complete.

WARNING!
DO NOT INTERUPT THE FILE TRANSFER PROCESS AS THIS MAY PERMANENTLY DAMAGE YOUR PRESTIGE. WHEN THE RESTORE CONFIGURATION PROCESS IS COMPLETE, THE PRESTIGE WILL AUTOMATICALLY RESTART.

17.3.1 Restore Using FTP or TFTP

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 router. 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-spt is the
     remote file name on the router. This restores the configuration to
     your router.
  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 router manual.


                               Press ENTER to Exit:
```

Figure 17-7 Telnet into Menu 24.6

Step 14. Launch the FTP client on your computer.

Step 15. Enter “open”, followed by a space and the IP address of your Prestige.

Step 16. Press [ENTER] when prompted for a username.

Step 17. Enter your password as requested (the default is “1234”).

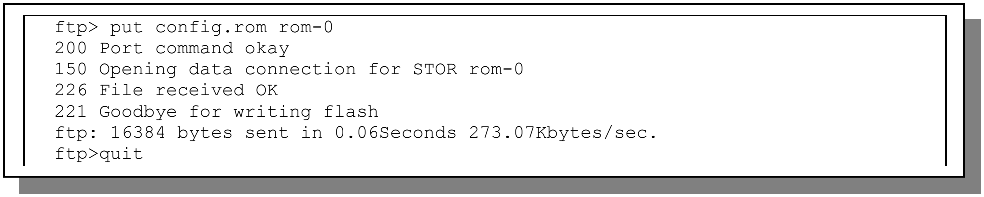
Step 18. Enter “bin” to set transfer mode to binary.

Step 19. Find the “rom” file (on your computer) that you want to restore to your Prestige.

Step 20. Use “put” to transfer files from the Prestige to the computer, for example, “put config.rom rom-0” transfers the configuration file on the Prestige to your computer and renames it “config.rom”. See earlier in this chapter for more information on filename conventions.

Step 21. Enter “quit” to exit the ftp prompt. The Prestige will automatically restart after a successful restore process.

Restore Using FTP or TFTP 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
```

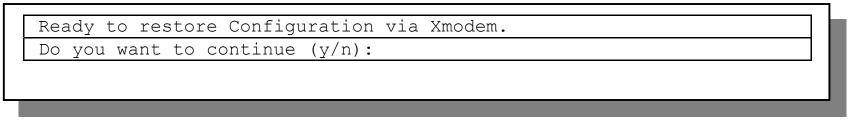
Figure 17-8 Restore Using FTP or TFTP Session Example

Refer to the *TFTP and FTP over WAN Will Not Work When* section to read about configurations that disallow TFTP and FTP to work over WAN.

17.3.2 Restore Via Console Port

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

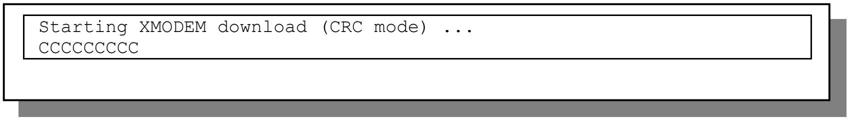
Step 22. Display menu 24.6 and enter "y" at the following screen.



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

Figure 17-9 System Maintenance — Restore Configuration

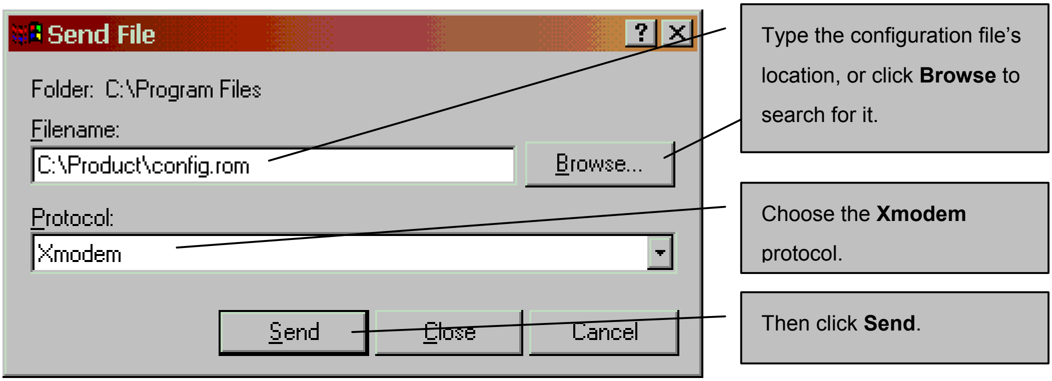
Step 4. The following screen indicates that the Xmodem download has started.



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

Figure 17-10 System Maintenance — Starting Xmodem Download Screen

Step 5. Run the HyperTerminal program by clicking **Transfer**, then **Receive File** as shown in the following screen.



Folder: C:\Program Files

Filename: C:\Product\config.rom

Protocol: Xmodem

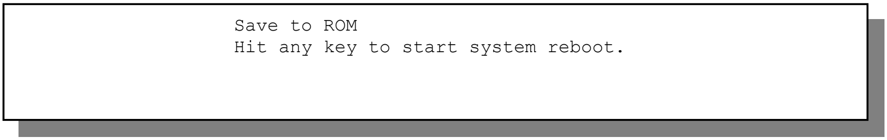
Type the configuration file's location, or click **Browse** to search for it.

Choose the **Xmodem** protocol.

Then click **Send**.

Figure 17-11 Restore Configuration Example

Step 6. After a successful restoration you will see the following screen. Press any key to restart the Prestige and return to the SMT menu.



```
Save to ROM
Hit any key to start system reboot.
```

Figure 17-12 Successful Restoration Confirmation Screen

17.4 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 Router Configuration File** (for console port).

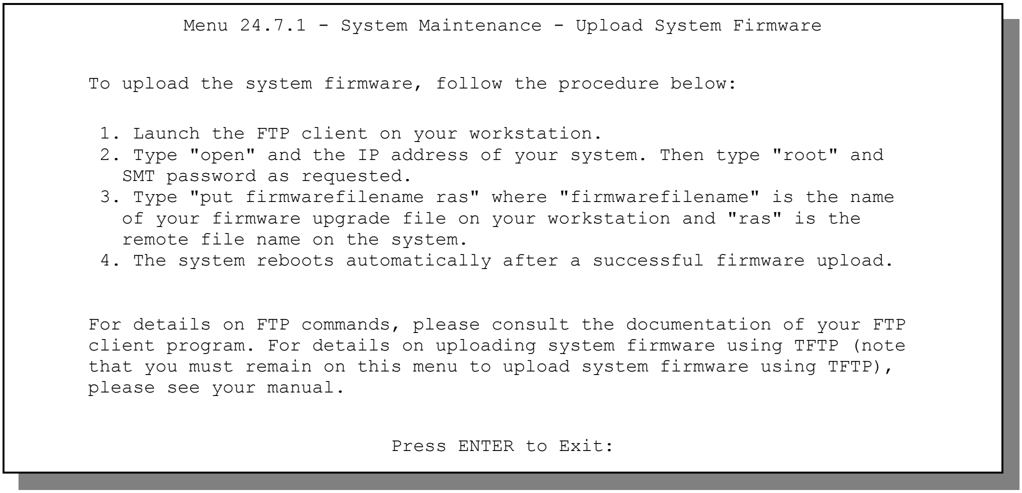
WARNING!

DO NOT INTERUPT THE FILE TRANSFER PROCESS AS THIS MAY PERMANENTLY DAMAGE YOUR PRESTIGE.

17.4.1 Firmware File Upload

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

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

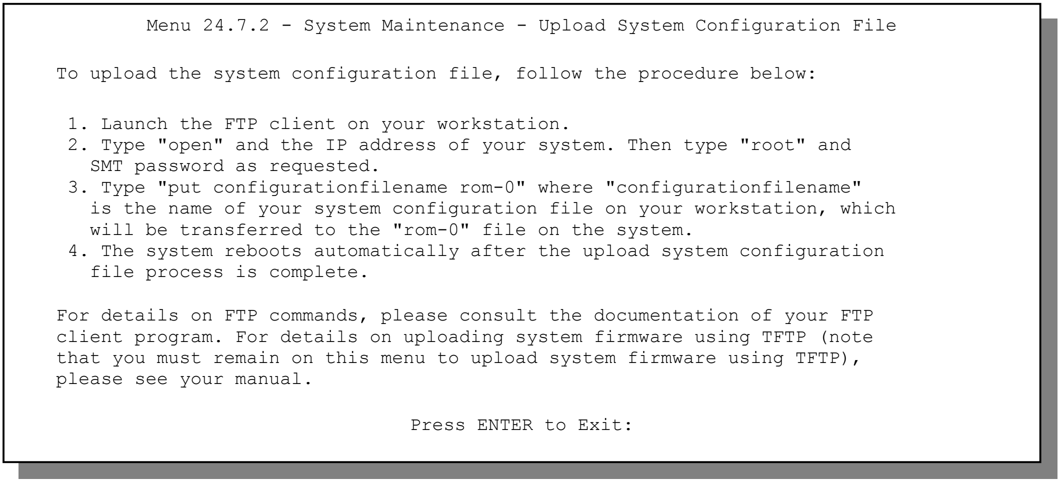


```
                Menu 24.7.1 - System Maintenance - Upload System Firmware


        To upload the system firmware, follow the procedure below:

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


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


                                  Press ENTER to Exit:
```

Figure 17-13 Telnet Into Menu 24.7.1 — Upload System Firmware

17.4.2 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 configurationfilename rom-0" where "configurationfilename"
     is the name of your system configuration file on your workstation, which
     will be transferred to the "rom-0" file on the system.
   4. The system reboots automatically after the upload system configuration
     file process is complete.

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

                              Press ENTER to Exit:
```

Figure 17-14 Telnet Into Menu 24.7.2 — System Maintenance

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

FTP File Upload Command from the DOS Prompt Example

Step 23. Launch the FTP client on your computer.

Step 24. Enter “open”, followed by a space and the IP address of your Prestige.

Step 25. Press [ENTER] when prompted for a username.

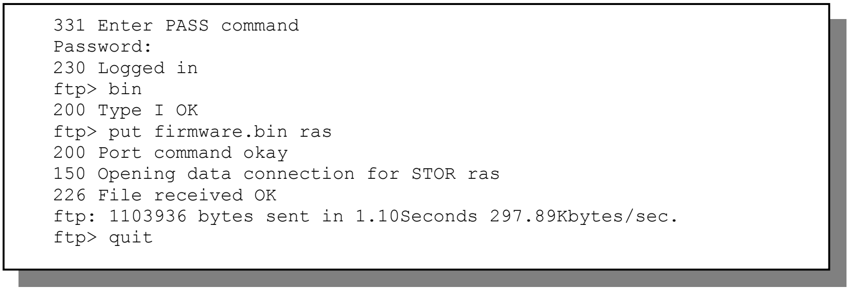
Step 26. Enter your password as requested (the default is “1234”).

Step 27. Enter “bin” to set transfer mode to binary.

Step 28. Use “put” to transfer files from the computer to the Prestige, for example, put firmware.bin ras transfers the firmware on your computer (firmware.bin) to the Prestige and renames it “ras”. Similarly put config.rom rom-0 transfers the configuration file on your computer (config.rom) to the Prestige and renames it “rom-0”. Likewise get rom-0 config.rom transfers the configuration file on the Prestige to your computer and renames it “config.rom.” See earlier in this chapter for more information on filename conventions.

Step 29. Enter “quit” to exit the ftp prompt.

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 17-15 FTP Session Example of Firmware File Upload

More commands (found in third party FTP clients), are listed earlier in this chapter.

Refer to the *TFTP and FTP over WAN Will Not Work When* section to read about configurations that disallow TFTP and FTP to work over WAN.

17.4.3 TFTP File Upload

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

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

Step 30. Use telnet from your computer to connect to the Prestige and log in. Because TFTP does not have any security checks, the Prestige records the IP address of the telnet client and accepts TFTP requests only from this address.

Step 31. Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.

Step 32. Enter the command “sys stdio 0” to disable the console timeout, so the TFTP transfer will not be interrupted. Enter “command sys stdio 5” to restore the five-minute console timeout (default) when the file transfer is complete.

Step 33. Launch the TFTP client on your computer and connect to the Prestige. Set the transfer mode to binary before starting data transfer.

Step 34. 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.

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, “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).

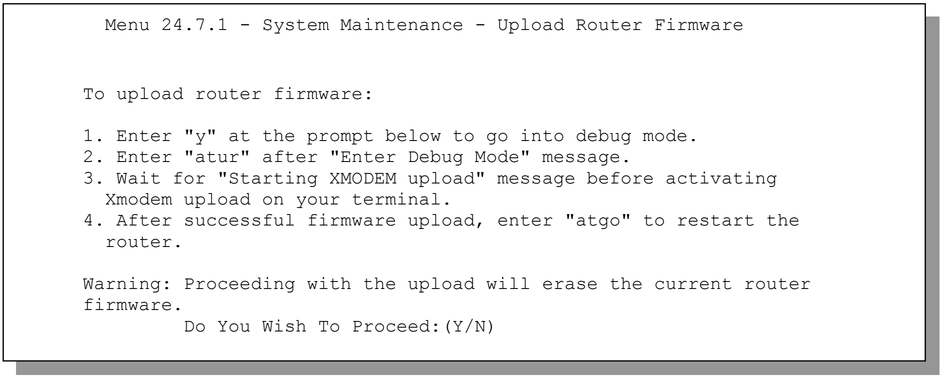
Commands that you may see in third party TFTP clients are listed earlier in this chapter.

17.4.4 Uploading Via Console Port

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

Uploading a Firmware File Via Console Port

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



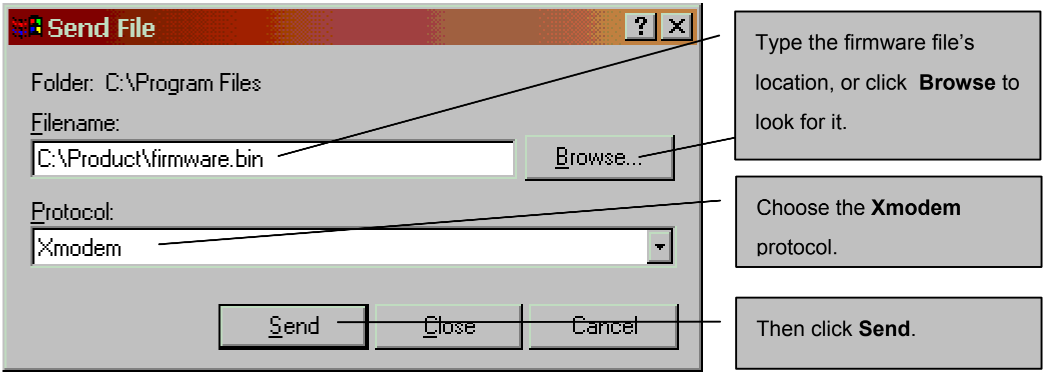
```
          Menu 24.7.1 - System Maintenance - Upload Router Firmware


        To upload router firmware:

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

        Warning: Proceeding with the upload will erase the current router
        firmware.
                 Do You Wish To Proceed:(Y/N)
```

Figure 17-16 Menu 24.7.1 as seen using the Console Port

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

Example Xmodem Firmware Upload Using HyperTerminal

Step 1. Click **Transfer**, then **Send File** to display the following screen.



Send File

Folder: C:\Program Files

Filename: C:\Product\firmware.bin

Protocol: Xmodem

Type the firmware file's location, or click **Browse** to look for it.

Choose the **Xmodem** protocol.

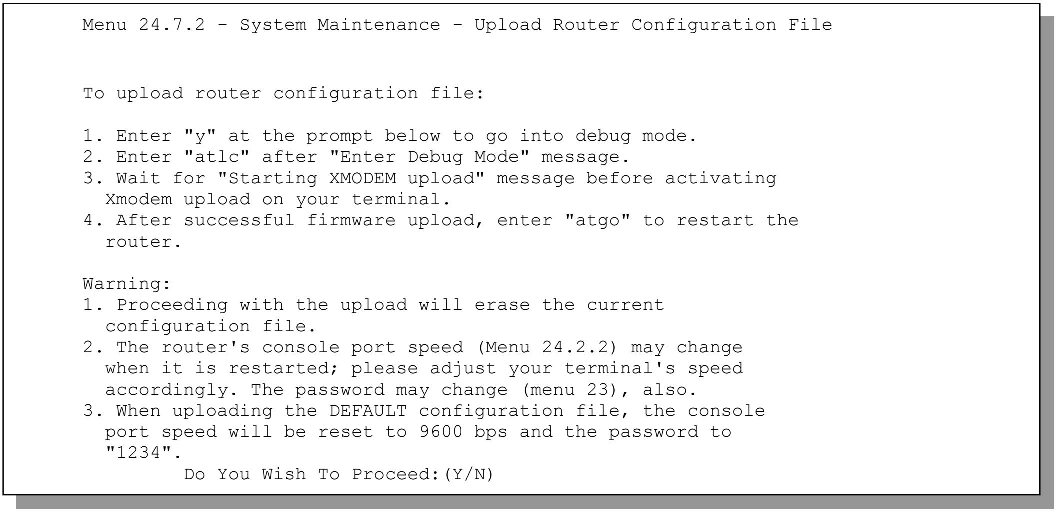
Then click **Send**.

Figure 17-17 Example Xmodem Upload

Step 2. After the firmware upload process has completed, the Prestige will automatically restart.

Uploading a Configuration File Via Console Port

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



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


To upload router configuration file:

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

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

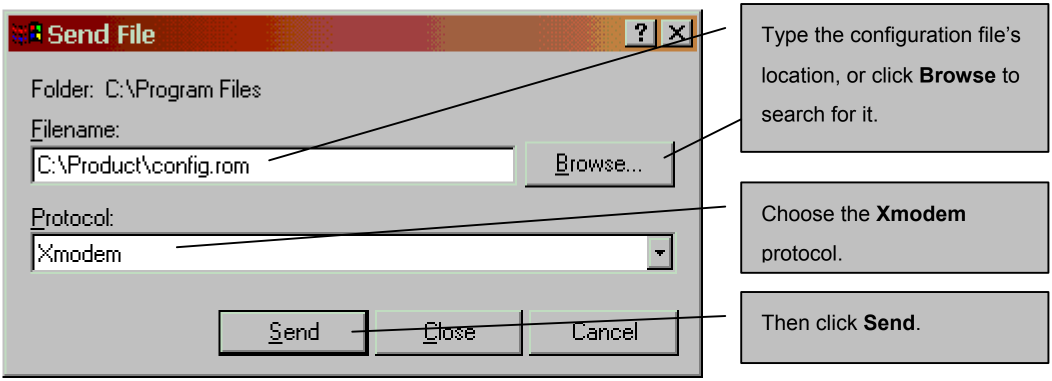
Figure 17-18 Menu 24.7.2 as seen using the Console Port

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

Step 3. Enter “atgo” to restart the Prestige.

Example Xmodem Configuration Upload Using HyperTerminal

Step 1. Click **Transfer**, then **Send File** to display the following screen.



Folder: C:\Program Files

Filename: C:\Product\config.rom

Protocol: Xmodem

Type the configuration file's location, or click **Browse** to search for it.

Choose the **Xmodem** protocol.

Then click **Send**.

Figure 17-19 Example Xmodem Upload

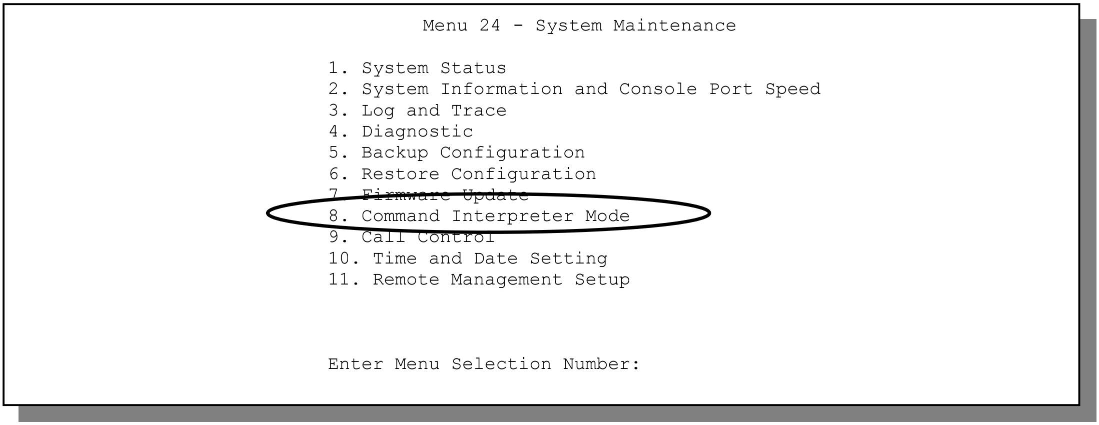
Step 2. After the configuration upload process has completed, restart the Prestige by entering "atgo".

Chapter 18
System Maintenance & Information

This chapter leads you through SMT menus 24.8 to 24.11.

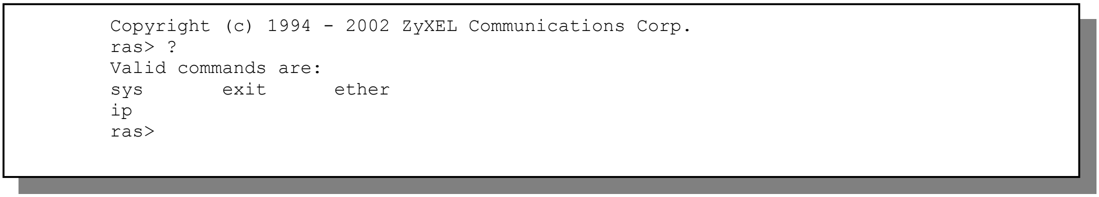
18.1 Command Interpreter Mode

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



```
                    Menu 24 - System Maintenance

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



           Enter Menu Selection Number:
```

Figure 18-1 Command Mode in Menu 24



```
Copyright (c) 1994 - 2002 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys       exit      ether
ip
ras>
```

Figure 18-2 Valid Commands

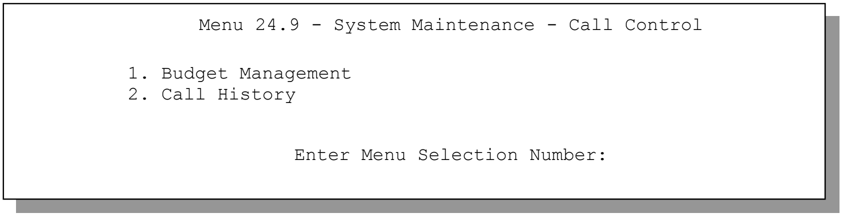
18.2 Call Control Support

The Prestige provides two call control functions: budget management and call history. Please note that this menu is only applicable when **Encapsulation** is set to **PPPoE** or **PPTP** 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.

Call history chronicles preceding incoming and outgoing calls.

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

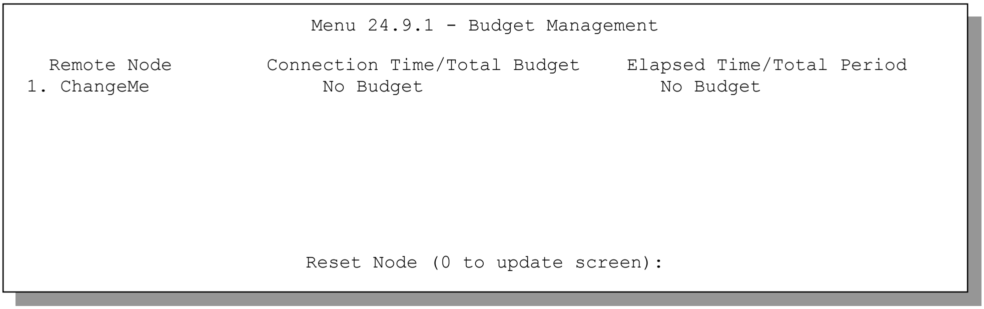


```
                  Menu 24.9 - System Maintenance - Call Control

           1. Budget Management
           2. Call History


                           Enter Menu Selection Number:
```

Figure 18-3 Call Control

18.2.1 Budget Management

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



```
                     Menu 24.9.1 - Budget Management

  Remote Node        Connection Time/Total Budget    Elapsed Time/Total Period
1. ChangeMe               No Budget                        No Budget









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

Figure 18-4 Budget Management

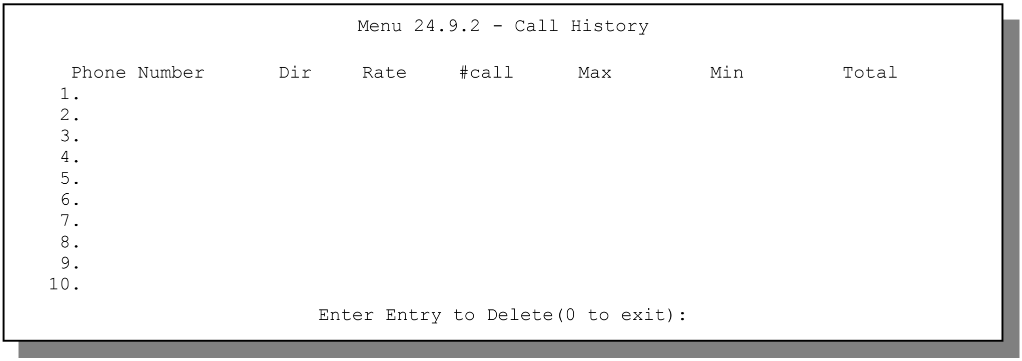
The total budget is the time limit on the accumulated time for outgoing calls to a remote node. When this limit is reached, the call will be dropped and further outgoing calls to that remote node will be blocked. After each period, the total budget is reset. The default for the total budget is 0 minutes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

Table 18-1 Budget Management

FIELD	DESCRIPTION	EXAMPLE
Remote Node	Enter the index number of the remote node you want to reset (just one in this case)	1
Connection Time/Total Budget	This is the total connection time that has gone by (within the allocated budget that you set in menu 11.1.	5/10 means that 5 minutes out of a total allocation of 10 minutes have lapsed.
Elapsed Time/Total Period	The period is the time cycle in hours that the allocation budget is reset (see menu 11.1.) The elapsed time is the time used up within this period.	0.5/1 means that 30 minutes out of the 1 hour time period has lapsed.
Enter “0” to update the screen or press [ESC] to return to the previous screen.		

18.2.2 Call History

This is the second option in **Menu 24.9 - System Maintenance - Call Control**. It displays information about past incoming and outgoing calls. Enter 2 from **Menu 24.9 - System Maintenance - Call Control** to bring up the following menu.



```
                              Menu 24.9.2 - Call History

    Phone Number       Dir     Rate     #call      Max         Min         Total
   1.
   2.
   3.
   4.
   5.
   6.
   7.
   8.
   9.
  10.
                            Enter Entry to Delete(0 to exit):
```

Figure 18-5 Call History

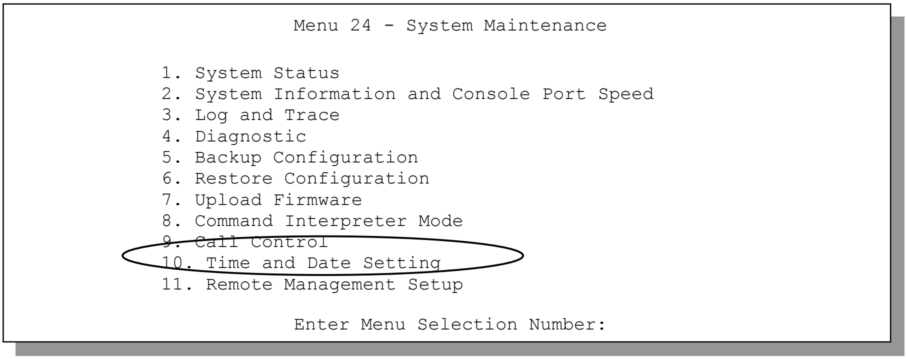
Table 18-2 Call History Fields

FIELD	DESCRIPTION
Phone Number	The PPPoE service names are shown here.
Dir	This shows whether the call was incoming or outgoing.
Rate	This is the transfer rate of the call.
#call	This is the number of calls made to or received from that telephone number.
Max	This is the length of time of the longest telephone call.
Min	This is the length of time of the shortest telephone call.
Total	This is the total length of time of all the telephone calls to/from that telephone number.
Enter “0” to update the screen or press [ESC] to return to the previous screen.	

18.3 Time and Date Setting

Time and Date Setting is 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. If you do not choose a time service protocol that your timeserver will send when you turn on the Prestige, then you can enter the time manually but each time the system is booted, the time and date will be reset to 2000/01/01 00:00:00.

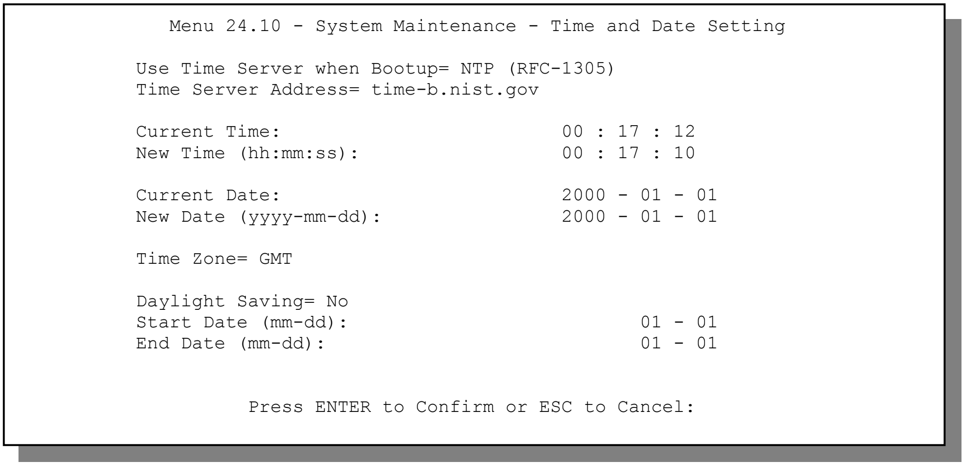
Select menu 24 in the main menu to open **Menu 24 - System Maintenance**, as shown next.



```
                    Menu 24 - System Maintenance

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

                    Enter Menu Selection Number:
```

Figure 18-6 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= NTP (RFC-1305)
             Time Server Address= time-b.nist.gov

             Current Time:                         00 : 17 : 12
             New Time (hh:mm:ss):                  00 : 17 : 10

             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 18-7 Menu 24.10 System Maintenance — Time and Date Setting

Table 18-3 Time and Date Setting Fields

FIELD	DESCRIPTION
Use Time Server when Bootup	Enter the time service protocol that your time server sends when you turn on the Prestige. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. The main differences between them are the format. **Daytime (RFC 867)** format is day/month/year/time zone of the server. **Time (RFC-868)** format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. **NTP (RFC-1305)** is similar to **Time (RFC-868)**. **None** is the default value. Enter the time manually. Each time you turn on the Prestige, the time and date will be reset to 2000-1-1 0:0:0.
Time Server IP Address	Enter the IP address of your time server or its domain name (if your time server is using DNS). 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 reenter this menu. Enter the new date in year, month and day format.

Table 18-3 Time and Date Setting Fields

FIELD	DESCRIPTION
Time Zone	Press [SPACE BAR] to set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Saving	Daylight Saving Time is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daylight time in the evenings. If you use daylight savings time, then choose **Yes**.
Start Date	Enter the month and day that your daylight-savings time starts on if you selected **Yes** in the **Daylight Saving** field.
End Date	Enter the month and day that your daylight-savings time ends on if you selected **Yes** in the **Daylight Saving** field.
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.	

Time Update Frequency

The Prestige resets the time in three instances:

19. On leaving menu 24.10 after making changes.

20. When the Prestige starts up and if there is a time server configured in menu 24.10.

21. 24-hour intervals after booting.

Chapter 19
Remote Management

This chapter covers remote management (SMT menu 24.11).

19.1 Introduction

You may restrict a service that can be used to remotely manage the Prestige using SMT menu 11 and submenus.

19.1.1 Telnet

First configure your Prestige for remote management through an SMT session using the console port. Once your Prestige is configured, you can configure it remotely using Telnet as shown next.

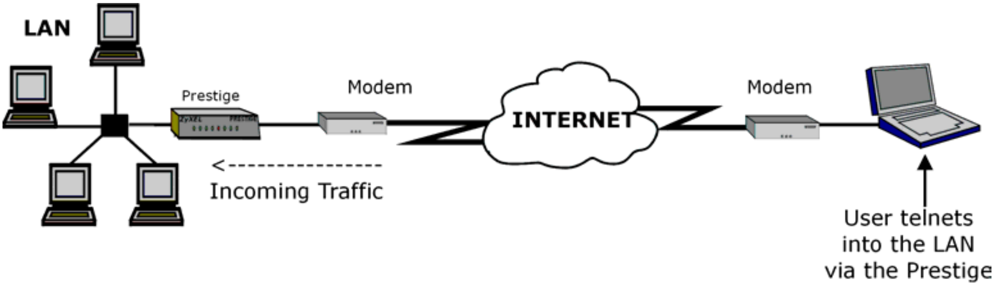


Figure 19-1 Telnet Configuration on a TCP/IP Network

19.1.2 FTP

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

19.1.3 Web

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

19.1.4 SNMP (Simple Network Management Protocol)

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

19.1.5 DNS (Domain Name System)

DNS links names to IP addresses. When you access Web sites on the Internet, you can type the IP address of the site or the DNS name.

DNS servers on the Internet convert domain names to IP addresses. Your own Internet service provider may do this conversion or connect to a specific DNS server that does. When you type a domain name in a Web browser, a query is sent to the primary DNS server defined in your Web browser's configuration dialog box. The DNS server converts the name you specified to an IP address and returns this address to your system. From then on, the IP address is used in all subsequent communications.

DNS service port number (53) is not configurable on the Prestige.

19.2 Remote Management Setup

Remote management setup allows you to choose who can use what services on which interface to manage the Prestige. You can customize the service port, access interface, and the secured client IP address to enhance security and flexibility.

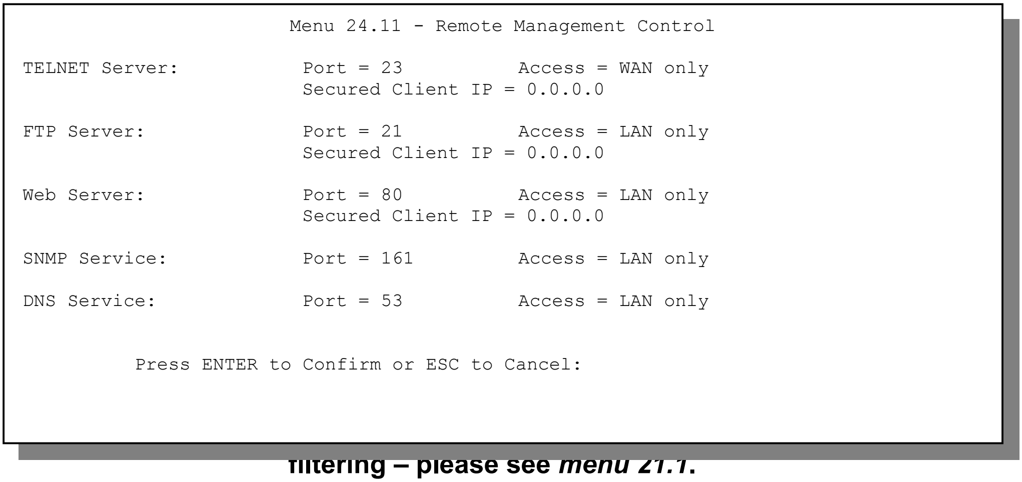
You may manage your Prestige from a remote location, via the Internet (**WAN only**), via the **LAN only**, **Both** (LAN & WAN) or neither (**Disable**).

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.

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

Enter 11 from menu 24 to bring up **Menu 24.11 – Remote Management Control**.

If you just wish to block certain users from using these services, then use



```
                         Menu 24.11 - Remote Management Control

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

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

Web Server:               Port = 80          Access = LAN only
                          Secured Client IP = 0.0.0.0

SNMP Service:             Port = 161         Access = LAN only

DNS Service:              Port = 53          Access = LAN only


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

filtering – please see *menu 21.1*.

Figure 19-2 Menu 24.11 – Remote Management Control

Table 19-1 Menu 24.11 – Remote Management Control

IELD	DESCRIPTION	EXAMPLE
TELNET Server FTP Server Web Server SNMP Server DNS Server	Each of these read-only labels denotes a service that you may use to remotely manage the Prestige.	
Server Port	This field shows the port number for the remote management service. You may change the port number for a service if needed, but you must use the same port number to use that service for remote management.	53

Table 19-1 Menu 24.11 – Remote Management Control

ǀ IELD	DESCRIPTION	EXAMPLE
Server Access	Select the access interface (if any) by pressing [SPACE BAR], then [ENTER] to choose from: **LAN only**, **WAN only**, **ALL** or **Disable**.	**LAN only**
Secured Client IP	The default 0.0.0.0 allows any client to use this service to remotely manage the Prestige. Enter an IP address to restrict access to a client with a matching IP address.	0.0.0.0
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.		

19.2.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

22. A filter in menu 3.1 (LAN) or in menu 11.5 (WAN) is applied to block a service.

23. You have disabled that service in menu 24.11.

24. 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.

25. There is an SMT console session running.

26. There is already another remote management session of the same type running. You may only have one remote management session of the same type running at one time.

19.3 Remote Management and the Firewall

Configuring **WAN** or **LAN & WAN** access for services in the **Remote Management** screens or SMT menus automatically creates a WAN-to-WAN/Prestige firewall rule allowing WAN traffic into the Prestige for that service.

19.4 Remote Management and NAT

When NAT is enabled:

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

19.5 System Timeout

A management session (either via the web configurator or SMT) can be left idle for 5 minutes (default) before the session times out. After it times out you have to log in with your password again. You may adjust the timeout by configuring **Administrator Inactivity Timer** in the web configurator or `sys stdio` in the command line interface (SMT 24.8). Very long idle timeouts may have security risks.

Chapter 20
Call Scheduling

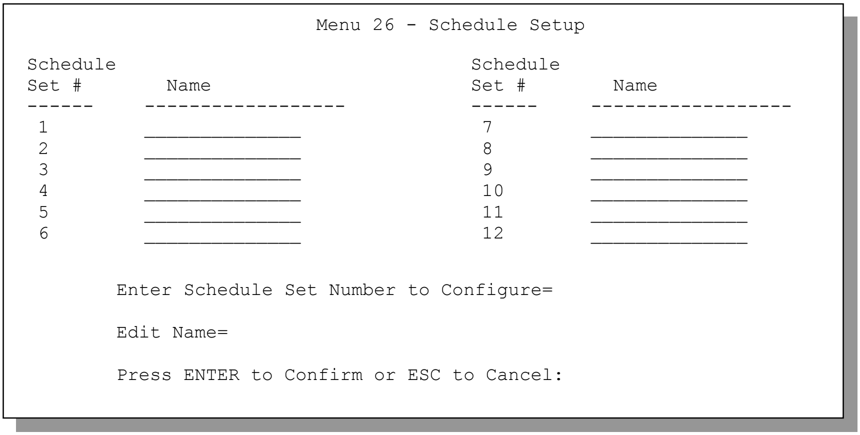
This chapter shows you how to setup call time periods for remote nodes.

20.1 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 video-cassette recorder (you can record programs at times that you specify). You can apply up to four schedule sets in **Menu 11.1 - Remote Node Profile**.

20.2 Schedule Setup

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=

        Edit Name=

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

Figure 20-1 Schedule Setup

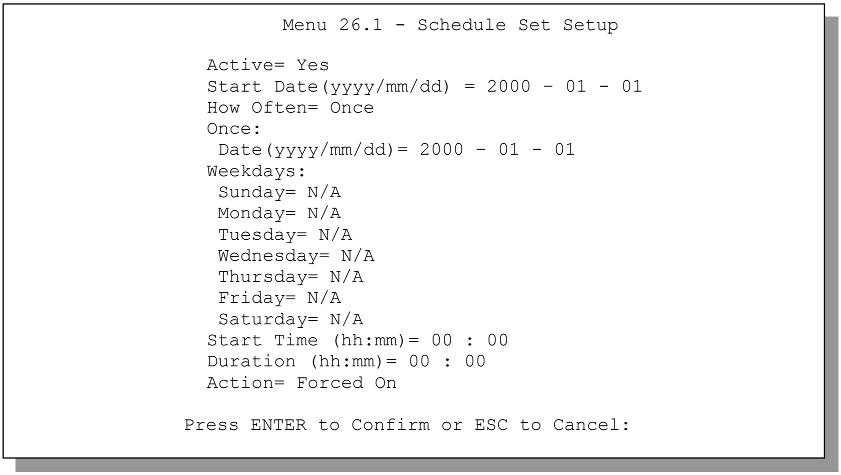
Lower numbered sets take precedence over higher numbered sets thereby avoiding scheduling conflicts. For example, if sets 1, 2, 3 and 4 in are applied in the remote node then set 1 will take precedence over set 2, 3 and 4 as the Prestige, by default, applies the lowest numbered set first. Set 2 will take precedence over set 3 and 4, and so on.

You can design up to 12 schedule sets but you can only apply up to four schedule sets for a remote node.

To delete a schedule set, enter the set number and press the [SPACE BAR] in the Edit Name **field.**

20.3 Schedule Set Setup

To setup a schedule set, select the schedule set you want to setup from menu 26 (1-12), press [ENTER] and then type in a name for the set. Press [ENTER] to display **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 20-2 Schedule Set Setup

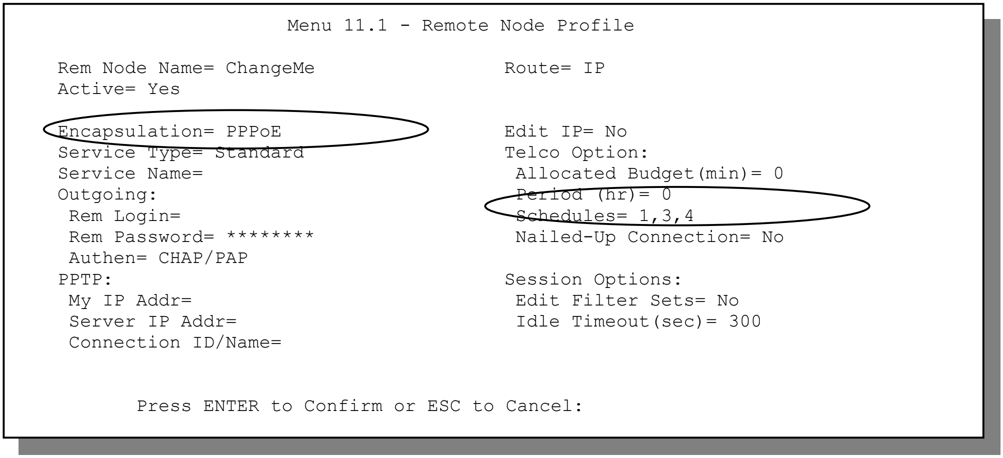
If a connection has been already established, your Prestige will not drop it. Once the connection is dropped manually or it times out, then that remote node can't be triggered again until the time period configured in the **Duration** field expires.

Table 20-1 Schedule Set Setup Fields

FIELD	DESCRIPTION	EXAMPLE
Active	Choose **Yes** to activate and **No** to deactivate the schedule set.	**Yes** (default)
Start Date	Enter the start date that you wish the set to take effect in year -month-day format. Valid dates are from the present to February 5, 2036.	2000 – 07 – 01
How Often	Should this schedule set recur weekly or be used just once? Choose **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** (default)
Once: Date	If you select **Once** in the **How Often** field above, enter the date the set should activate in year-month-day format. If you select **Weekly** in the **How Often** field above, this field is **N/A**.	2001 – 01 – 01
Weekday: Day	If you select **Weekly** in the **How Often** field above, then choose the day(s) the set should activate (and recur). Individual **Day** parameters are active when their fields read **Yes** and inactive when their fields read **No** or **N/A**.	**N/A** (default)
Start Time	Enter the start time that you wish the schedule set to take effect in hour : minute format.	12 : 00
Duration	Enter the maximum duration allowed in hour : minute format for this scheduled connection.	10 : 00
Action	Choose an action. Choices are: **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**

20.4 Applying Schedule Sets to Remote Nodes

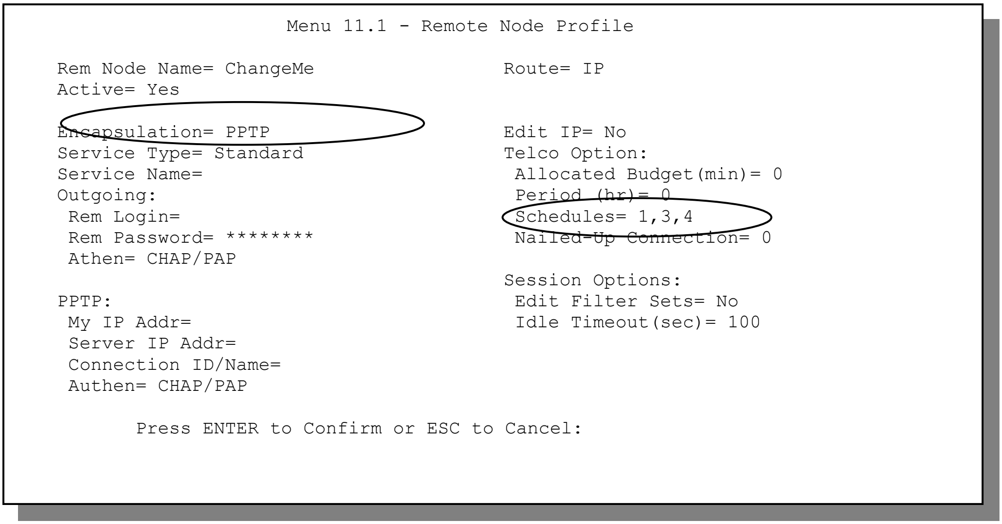
Once your schedule sets are configured, you must apply them to the desired remote node(s). Enter 11 from the main menu and, using the [SPACE BAR], select **PPPoE** or **PPTP** in the **Encapsulation** field. Enter your target remote node index number(s) in the **Schedules** field, as shown next.



```
                     Menu 11.1 - Remote Node Profile

Rem Node Name= ChangeMe                 Route= IP
Active= Yes

Encapsulation= PPPoE                    Edit IP= No
Service Type= Standard                  Telco Option:
Service Name=                            Allocated Budget(min)= 0
Outgoing:                                Period (hr)= 0
 Rem Login=                              Schedules= 1,3,4
 Rem Password= ********                  Nailed-Up Connection= No
 Authen= CHAP/PAP
PPTP:                                   Session Options:
 My IP Addr=                             Edit Filter Sets= No
 Server IP Addr=                         Idle Timeout(sec)= 300
 Connection ID/Name=


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

Figure 20-3 Applying Schedule Sets to a Remote Node Example (PPPoE Encapsulation)

You can apply up to four schedule sets, separated by commas, for one remote node. Enter the schedule set numbers for specific remote nodes in the **Schedules** field. In the examples, shown previously and next, schedule sets 1, 3 and 4 are applied.



```
                    Menu 11.1 - Remote Node Profile

   Rem Node Name= ChangeMe                Route= IP
   Active= Yes

   Encapsulation= PPTP                    Edit IP= No
   Service Type= Standard                 Telco Option:
   Service Name=                           Allocated Budget(min)= 0
   Outgoing:                               Period (hr)= 0
    Rem Login=                             Schedules= 1,3,4
    Rem Password= ********                 Nailed-Up Connection= 0
    Athen= CHAP/PAP
                                          Session Options:
   PPTP:                                   Edit Filter Sets= No
    My IP Addr=                            Idle Timeout(sec)= 100
    Server IP Addr=
    Connection ID/Name=
    Authen= CHAP/PAP

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

Figure 20-4 Applying Schedule Sets to a Remote Node Example (PPTP Encapsulation)

Chapter 21
Troubleshooting

This chapter covers the potential problems and possible remedies. After each problem description, some instructions are provided to help you to diagnose and to solve the problem. See the included CD for further information.

21.1 Problems Starting Up the Prestige

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

PROBLEM	CORRECTIVE ACTION	
None of the LEDs are on when you power on the Prestige	Check the connection between the AC adapter and the Prestige. If the error persists, you may have a hardware problem. In this case, you should contact your vendor.	
Cannot access the Prestige via the console port.	1. Check to see if the Prestige is connected to your computer's console port.	
	2. Check to see if the communications program is configured correctly. The communications software should be configured as follows:	VT100 terminal emulation
		9600 bps
		No parity, 8 data bits, 1 stop bit, data flow set to none.

21.2 Problems with the LAN Interface

Table 21-2 Troubleshooting the LAN Interface

PROBLEM	CORRECTIVE ACTION
Cannot access the Prestige from the LAN.	Check your Ethernet cable type and connections. Refer to the *Rear Panel and Connections* section for LAN connection instructions.

PROBLEM	CORRECTIVE ACTION
Cannot ping any computer on the LAN.	Check the 10M/100M LEDs on the front panel. One of these LEDs should be on. If they are both off, check the cables between your Prestige and hub or the station.
	Verify that the IP addresses and subnet masks of the Prestige and the computers on the LAN are on the same subnet.

21.3 Problems with the WAN Interface

Table 21-3 Troubleshooting the WAN interface

PROBLEM	CORRECTIVE ACTION
Cannot get a WAN IP address from the ISP.	The WAN IP address is provided when the ISP recognizes the user as an authorized user after verifying the MAC address or Host Name or User ID. Find out the verification method used by your ISP.
	If the ISP checks the LAN MAC address, tell the ISP the WAN MAC address of the Prestige. The WAN MAC can be obtained from menu 24.1. In case the ISP does not allow you to use a new MAC, you can clone the MAC from the LAN as the WAN MAC and send it to the ISP using **Menu 2 - WAN Setup**.
	If the ISP checks the Host Name, enter host name in the system field in **Menu 1 - General Setup** when you connect the Prestige to a cable/xDSL modem.
	If the ISP checks the User ID, make sure that you have entered the correct Service Type, User Name and Password in **Menu 4 - Internet Access Setup**.
Cannot connect to a remote node or ISP.	Check menu 24.1 to verify the line status. Contact your service provider if your line remains down.

Part IV:

Appendices and Index

This section provides some Appendices and an Index.

Appendix A
PPPoE

PPPoE in Action

An ADSL modem bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your PC to an ATM PVC (Permanent Virtual Circuit) which connects to a xDSL Access Concentrator where the PPP session terminates (see the next figure). One PVC can support any number of PPP sessions from your LAN. PPPoE provides access control and billing functionality in a manner similar to dial-up services using PPP.

Benefits of PPPoE

PPPoE offers the following benefits:

1. It provides you with a familiar dial-up networking (DUN) user interface.
2. It lessens the burden on the carriers of provisioning virtual circuits all the way to the ISP on multiple switches for thousands of users. For GSTN (PSTN & ISDN), the switching fabric is already in place.
3. It allows the ISP to use the existing dial-up model to authenticate and (optionally) to provide differentiated services.

Traditional Dial-up Scenario

The following diagram depicts a typical hardware configuration where the PCs use traditional dial-up networking.

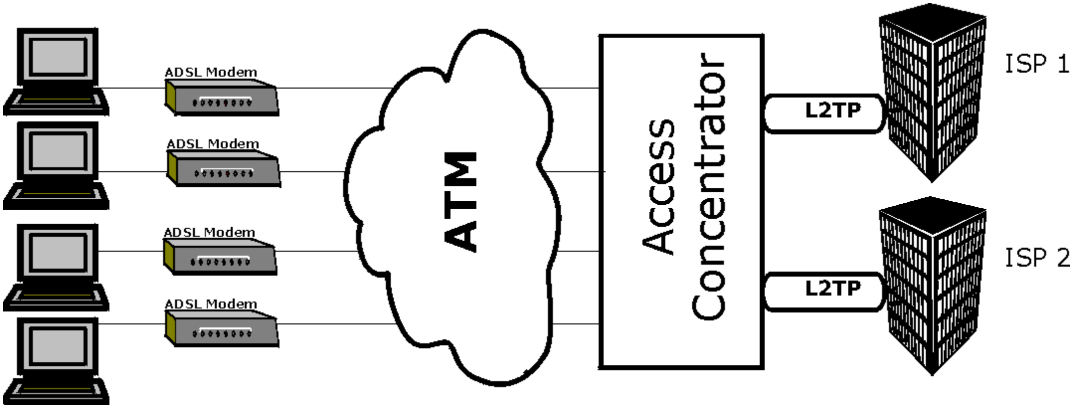


Diagram 1 Single-PC per Modem Hardware Configuration

How PPPoE Works

The PPPoE driver makes the Ethernet appear as a serial link to the PC and the PC runs PPP over it, while the modem bridges the Ethernet frames to the Access Concentrator (AC). Between the AC and an ISP, the AC is acting as a L2TP (Layer 2 Tunneling Protocol) LAC (L2TP Access Concentrator) and tunnels the PPP frames to the ISP. The L2TP tunnel is capable of carrying multiple PPP sessions.

With PPPoE, the VC (Virtual Circuit) is equivalent to the dial-up connection and is between the modem and the AC, as opposed to all the way to the ISP. However, the PPP negotiation is between the PC and the ISP.

The Prestige as a PPPoE Client

When using the Prestige as a PPPoE client, the PCs on the LAN see only Ethernet and are not aware of PPPoE. This alleviates the administrator from having to manage the PPPoE clients on the individual PCs.

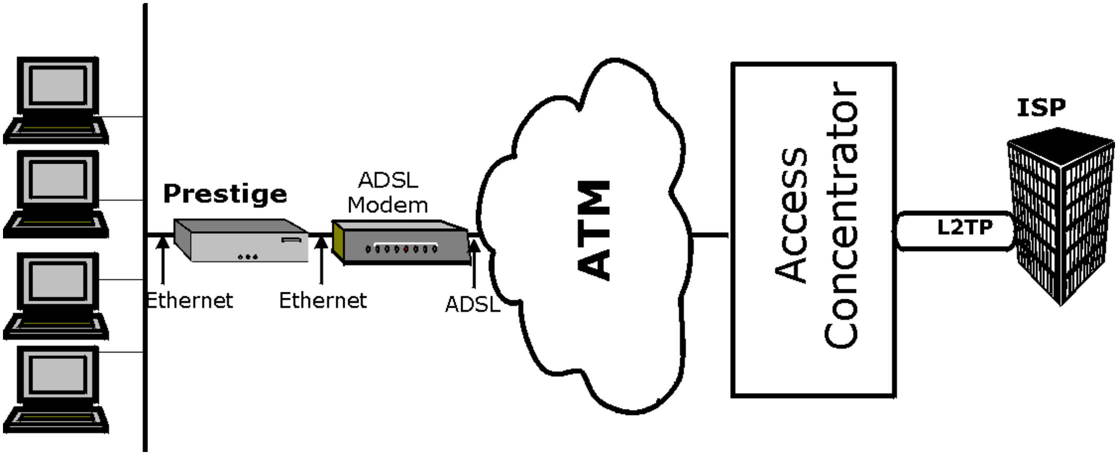


Diagram 2 Prestige as a PPPoE Client

Appendix B
PPTP

What is PPTP?

PPTP (Point-to-Point Tunneling Protocol) is a Microsoft proprietary protocol (RFC 2637 for PPTP is informational only) to tunnel PPP frames.

How can we transport PPP frames from a PC to a broadband modem over Ethernet?

A solution is to build PPTP into the ANT (ADSL Network Termination) where PPTP is used only over the short haul between the PC and the modem over Ethernet. For the rest of the connection, the PPP frames are transported with PPP over AAL5 (RFC 2364). The PPP connection, however, is still between the PC and the ISP. The various connections in this setup are depicted in the following diagram. The drawback of this solution is that it requires one separate ATM VC per destination.

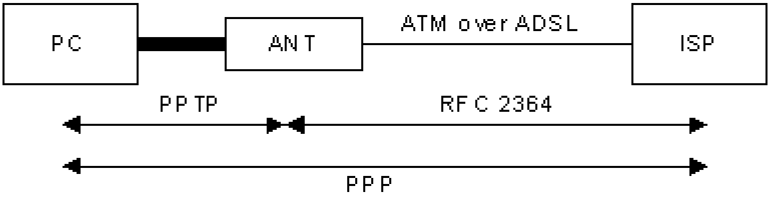


Diagram 3 Transport PPP frames over Ethernet

PPTP and the Prestige

When the Prestige is deployed in such a setup, it appears as a PC to the ANT (ADSL Network Termination).

In Windows VPN or PPTP Pass-Through feature, the PPTP tunneling is created from Windows 95, 98 and NT clients to an NT server in a remote location. The pass-through feature allows users on the network to access a different remote server using the Prestige's Internet connection. In NAT mode, the Prestige is able to pass the PPTP packets to the internal PPTP server (i.e. NT server) behind the NAT. Users need to forward PPTP packets to port 1723 by configuring the server in **Menu 15.2 - Server Set Setup**. In the case above as the PPTP connection is initialized by the remote PPTP Client, the user must configure the PPTP clients. The Prestige initializes the PPTP connection hence, there is no need to configure the remote PPTP clients.

PPTP Protocol Overview

PPTP is very similar to L2TP, since L2TP is based on both PPTP and L2F (Cisco’s Layer 2 Forwarding). Conceptually, there are three parties in PPTP, namely the PNS (PPTP Network Server), the PAC (PPTP Access Concentrator) and the PPTP user. The PNS is the box that hosts both the PPP and the PPTP stacks and forms one end of the PPTP tunnel. The PAC is the box that dials/answers the phone calls and relays the PPP frames to the PNS. The PPTP user is not necessarily a PPP client (can be a PPP server too). Both the PNS and the PAC must have IP connectivity; however, the PAC must in addition have dial-up capability. The phone call is between the user and the PAC and the PAC tunnels the PPP frames to the PNS. The PPTP user is unaware of the tunnel between the PAC and the PNS.

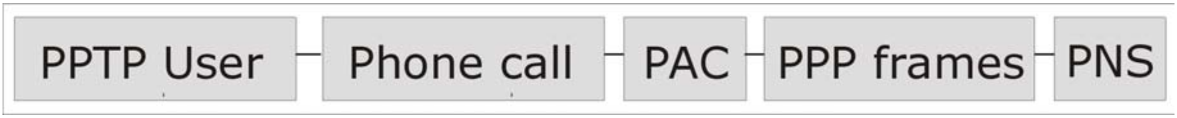


Diagram 4 PPTP Protocol Overview

Microsoft includes PPTP as a part of the Windows OS. In Microsoft’s implementation, the PC, and hence the Prestige, is the PNS that requests the PAC (the ANT) to place an outgoing call over AAL5 to an RFC 2364 server.

Control & PPP connections

Each PPTP session has distinct control connection and PPP data connection.

Call Connection

The control connection runs over TCP. Similar to L2TP, a tunnel control connection is first established before call control messages can be exchanged. Please note that a tunnel control connection supports multiple call sessions.

The following diagram depicts the message exchange of a successful call setup between a PC and an ANT.

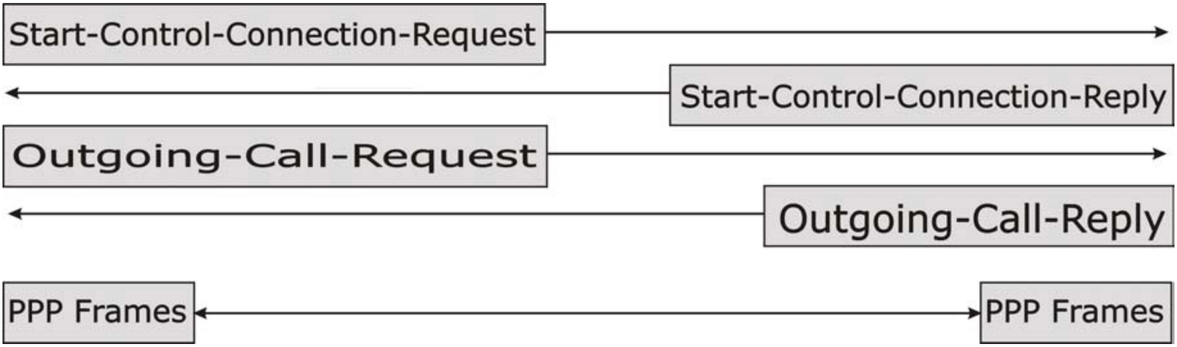

Start-Control-Connection-Request
Start-Control-Connection-Reply
Outgoing-Call-Request
Outgoing-Call-Reply
PPP Frames
PPP Frames

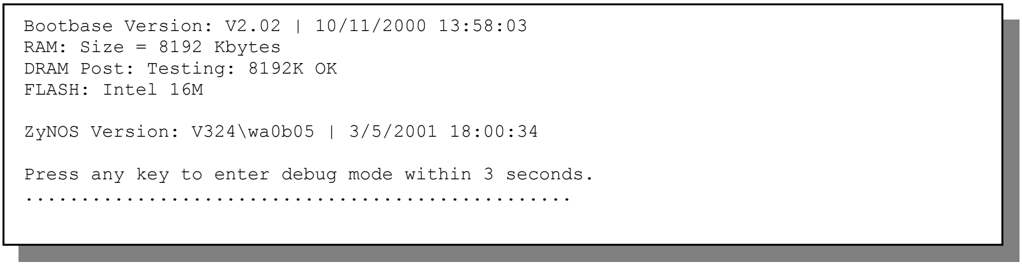
Diagram 5 Example Message Exchange between PC and an ANT

PPP Data Connection

The PPP frames are tunneled between the PNS and PAC over GRE (General Routing Encapsulation, RFC 1701, 1702). The individual calls within a tunnel are distinguished using the Call ID field in the GRE header.

Appendix C
Boot Commands

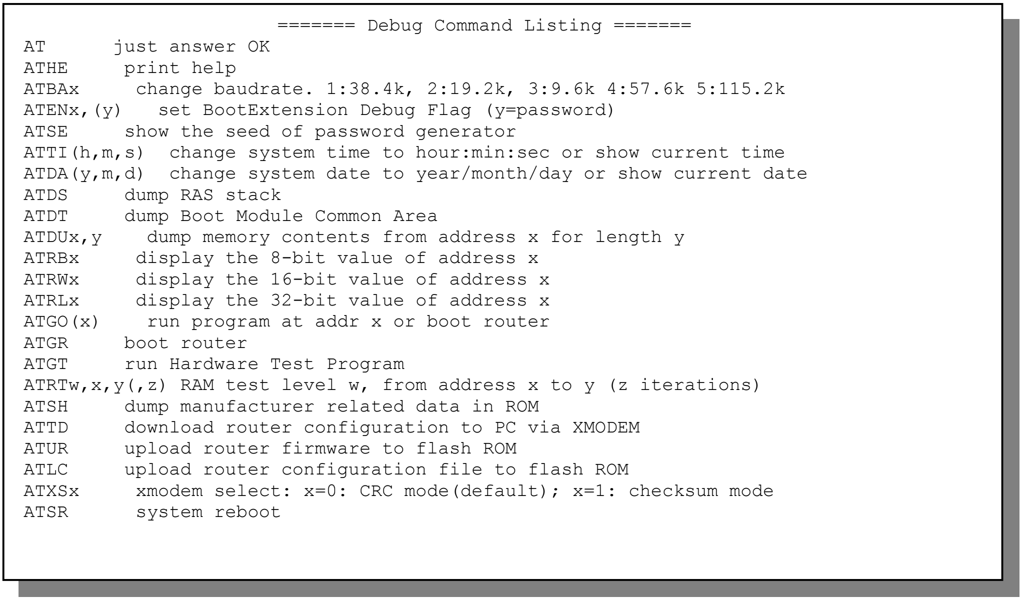
The BootModule AT commands execute from within the router's bootup software, when debug mode is selected before the main router firmware (ZyNOS) is started. When you start up your Prestige, you are given a choice to go into debug mode by pressing a key at the prompt shown in the following screen. In debug mode you have access to a series of boot module commands, for example `ATUR` (for uploading firmware) and `ATLC` (for uploading the configuration file). These are already discussed in the *Transferring Files* chapter.



```
Bootbase Version: V2.02 | 10/11/2000 13:58:03
RAM: Size = 8192 Kbytes
DRAM Post: Testing: 8192K OK
FLASH: Intel 16M

ZyNOS Version: V324\wa0b05 | 3/5/2001 18:00:34

Press any key to enter debug mode within 3 seconds.
.................................................
```

Diagram 6 Option to Enter Debug Mode

Enter `ATHE` to view all available Prestige boot module commands as shown in the next screen. `ATBAx` allows you to change the console port speed. The x denotes the number preceding the colon to give the console port speed following the colon in the list of numbers that follows; e.g., `ATBA3` will give a console port speed of 9.6 Kbps. `ATSE` displays the seed that is used to generate a password to turn on the debug flag in the firmware. The `ATSH` command shows product related information such as boot module version, vendor name, product model, RAS code revision, etc. `ATGO` allows you to continue booting the system. Most other commands aid in advanced troubleshooting and should only be used by qualified engineers.



```
                       ======= Debug Command Listing =======
AT      just answer OK
ATHE     print help
ATBAx     change baudrate. 1:38.4k, 2:19.2k, 3:9.6k 4:57.6k 5:115.2k
ATENx,(y)   set BootExtension Debug Flag (y=password)
ATSE     show the seed of password generator
ATTI(h,m,s)  change system time to hour:min:sec or show current time
ATDA(y,m,d)  change system date to year/month/day or show current date
ATDS     dump RAS stack
ATDT     dump Boot Module Common Area
ATDUx,y    dump memory contents from address x for length y
ATRBx     display the 8-bit value of address x
ATRWx     display the 16-bit value of address x
ATRLx     display the 32-bit value of address x
ATGO(x)    run program at addr x or boot router
ATGR     boot router
ATGT     run Hardware Test Program
ATRTw,x,y(,z) RAM test level w, from address x to y (z iterations)
ATSH     dump manufacturer related data in ROM
ATTD     download router configuration to PC via XMODEM
ATUR     upload router firmware to flash ROM
ATLC     upload router configuration file to flash ROM
ATXSx     xmodem select: x=0: CRC mode(default); x=1: checksum mode
ATSR      system reboot
```

Diagram 7 Boot Module Commands

Appendix D
NetBIOS Filter Commands

The following describes the NetBIOS packet filter commands.

Introduction

NetBIOS (Network Basic Input/Output System) are TCP or UDP broadcast packets that enable a computer to connect to and communicate with a LAN.

For some dial-up services such as PPPoE or PPTP, NetBIOS packets cause unwanted calls.

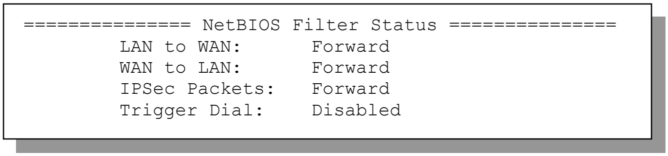
You can configure NetBIOS filters to:

- Block or forward NetBIOS packets from being sent from the LAN to the WAN.
- Block or forward NetBIOS packets from being sent from the WAN to the LAN.
- Allow or deny NetBIOS packets to be sent through VPN connections.
- Block or forward NetBIOS packets from initiating calls.

Display NetBIOS Filter Settings

Syntax: `sys filter netbios disp`

This command displays the current NetBIOS filter settings.



```
=============== NetBIOS Filter Status ===============
        LAN to WAN:       Forward
        WAN to LAN:       Forward
        IPSec Packets:    Forward
        Trigger Dial:     Disabled
```

Diagram 8 NetBIOS Display Filter Settings Command

The filter types and their default settings are as follows.

NAME	DESCRIPTION	EXAMPLE
LAN to WAN	This field displays whether NetBIOS packets are blocked or forwarded from the LAN to the WAN.	Block
WAN to the LAN	This field displays whether NetBIOS packets are blocked or forwarded from the WAN to the LAN.	Block
IPSec Packets	This field displays whether NetBIOS packets sent through a VPN connection are blocked or forwarded.	Forward
Trigger dial	This field displays whether NetBIOS packets are allowed to initiate calls. Disabled means that NetBIOS packets are blocked from initiating calls.	Disabled

NetBIOS Filter Configuration

Syntax: `sys filter netbios config <type> <on|off>`

where

`<type> =` Identify which NetBIOS filter (numbered 0-3) to configure.

`0` = LAN to WAN

`1` = WAN to the LAN

`2` = IPSec Packets

`3` = Trigger dial

`<on|off> =` For types `0` and `1`, use `on` to enable the filter and block NetBIOS packets. Use `off` to disable the filter and forward NetBIOS packets.

For type `2`, use `on` to block NetBIOS packets from being sent through a VPN connection. Use `off` to allow NetBIOS packets to be sent through a VPN connection.

For type `3`, use `on` to allow NetBIOS packets to initiate calls. Use `off` to block NetBIOS packets from initiating calls.

Example commands

Command: `sys filter netbios config 0 on`

This command blocks LAN to WAN NetBIOS packets

Command: `sys filter netbios config 1 off`

This command forwards WAN to the LAN NetBIOS packets

Command: `sys filter netbios config 2 on`

This command blocks IPSec NetBIOS packets

Command: `sys filter netbios config 3 off`

This command stops NetBIOS commands from initiating calls.

Appendix E Log Descriptions

Configure centralized logs using the embedded web configurator; see the online help for details. This appendix describes some of the log messages.

Chart 1 System Error Logs

LOG MESSAGE	DESCRIPTION
`%s exceeds the max. number of session per host!`	This attempt to create a NAT session exceeds the maximum number of NAT session table entries allowed to be created per host.

Chart 2 System Maintenance Logs

LOG MESSAGE	DESCRIPTION
`Time calibration is successful`	The router has adjusted its time based on information from the time server.
`Time calibration failed`	The router failed to get information from the time server.
`DHCP client gets %s`	A DHCP client got a new IP address from the DHCP server.
`DHCP client IP expired`	A DHCP client's IP address has expired.
`DHCP server assigns %s`	The DHCP server assigned an IP address to a client.
`SMT Login Successfully`	Someone has logged on to the router's SMT interface.
`SMT Login Fail`	Someone has failed to log on to the router's SMT interface.
`WEB Login Successfully`	Someone has logged on to the router's web configurator interface.
`WEB Login Fail`	Someone has failed to log on to the router's web configurator interface.

Chart 2 System Maintenance Logs

`TELNET Login Successfully`	Someone has logged on to the router via telnet.
`TELNET Login Fail`	Someone has failed to log on to the router via telnet.
`FTP Login Successfully`	Someone has logged on to the router via ftp.
`FTP Login Fail`	Someone has failed to log on to the router via ftp.
`NAT Session Table is Full!`	The maximum number of NAT session table entries has been exceeded and the table is full.
`!! Phase 1 ID type mismatch`	The ID type of an incoming packet does not match the local's peer ID type.
`!! Phase 1 ID content mismatch`	The ID content of an incoming packet does not match the local's peer ID content.
`!! No known phase 1 ID type found`	The ID type of an incoming packet does not match any known ID type.

Chart 3 UPnP Logs

LOG MESSAGE	DESCRIPTION
`UPnP pass through Firewall`	UPnP packets can pass through the firewall.

Chart 4 Content Filtering Logs

CATEGORY	LOG MESSAGE	DESCRIPTION
URLFOR	`IP/Domain Name`	The Prestige allows access to this IP address or domain name and forwarded traffic addressed to the IP address or domain name.
URLBLK	`IP/Domain Name`	The Prestige blocked access to this IP address or domain name due to a forbidden keyword. All web traffic is disabled except for trusted domains, untrusted domains, or the cybernot list.

Chart 4 Content Filtering Logs

JAVBLK	IP/Domain Name	The Prestige blocked access to this IP address or domain name because of a forbidden service such as: ActiveX, a Java applet, a cookie, or a proxy.

Chart 5 ICMP Type and Code Explanations

TYPE	CODE	DESCRIPTION
0		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

Chart 5 ICMP Type and Code Explanations

TYPE	CODE	DESCRIPTION
11		Time Exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter Problem
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp Reply
	0	Timestamp reply message
15		Information Request
	0	Information request message
16		Information Reply
	0	Information reply message

Appendix F
Power Adapter Specifications

North American Plug Standards	
AC Power Adapter Model: MW41-0901000A	AC Power Adapter Model: DV-9750-4
Input Power: AC120Volts/60Hz/13W	Input Power: AC120Volts/60Hz/15W
Output Power: AC 9Volts/1.0A	Output Power: AC 9Volts/1.0A
Power Consumption: 10 W	Power Consumption: 10 W
Safety Standards: UL, CUL (UL 1310, CSA C22.2 No.223)	Safety Standards: UL, CUL (UL 1310, CSA C22.2 No.223)
European Plug Standards	
AC Power Adapter Model: JAA-091000E	AC Power Adapter Model: DV-91AACUP
Input Power: AC230Volts/50Hz/65mA	Input Power: AC230Volts/50Hz/85mA
Output Power: AC 9Volts/1.0A	Output Power: AC 9Volts/1.0A
Power Consumption: 10 W	Power Consumption: 10 W
Safety Standards: TUV, CE (EN 60950)	Safety Standards: TUV, CE (EN 60950)
United Kingdom Plug Standards	**Australia and New Zealand Plug Standards**
AC Power Adapter Model: AD-0901000AK	AC Power Adapter Model: JAA-0901000AS
Input Power: AC230Volts/50Hz/0.2A	Input Power: AC240Volts/50Hz/130mA
Output Power: AC 9Volts/1.0A	Output Power: AC 9Volts/1.0A
Power Consumption: 10 W	Power Consumption: 10 W
Safety Standards: TUV, CE (EN 60950, BS 7002)	Safety Standards: NATA (AS 3260)

Appendix G
Hardware Specifications

SPECIFICATIONS	
Power Specification	I/P AC 120V / 60Hz ; O/P DC 12V 1200 mA
MTBF	(Mean Time Between Failure) 100000 hrs
Operation Temperature	0º C ~ 40 degrees Celsius
Ethernet Specification for WAN	10Mbit Half / Full Manual Setting
Ethernet Specification for LAN	10/100 Mbit Half / Full Auto-negotiation

Cable Pin Assignments

In a serial communications connection, generally a computer is DTE (Data Terminal Equipment) and a modem is DCE (Data Circuit-terminating Equipment). The Prestige is DCE when you connect a computer to the console port.

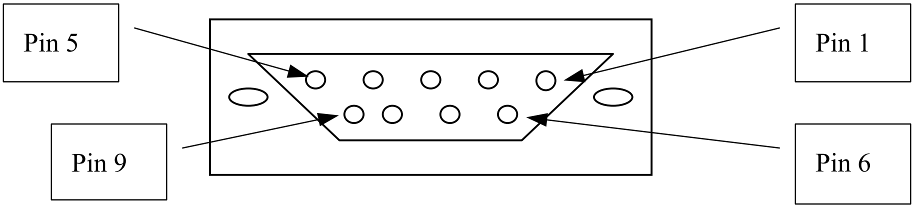


Diagram 9 Console Port Pin Layouts [1]

Chart 6 CONSOLE Port RS-232 (Female) DB-9F Pin Assignments

Pin 1 = NON	Pin 4 = DCE –DSR	Pin 7 = DCE –CTS
Pin 2 = DCE-TXD	Pin 5 = GND	Pin 8 = DCE –RTS
Pin 3 = DCE –RXD	Pin 6 = DCE –DTR	PIN 9 = NON

[1] Products without flow control only use pins 2,3 and 5.

Appendix H
Setting up Your Computer's IP Address

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

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

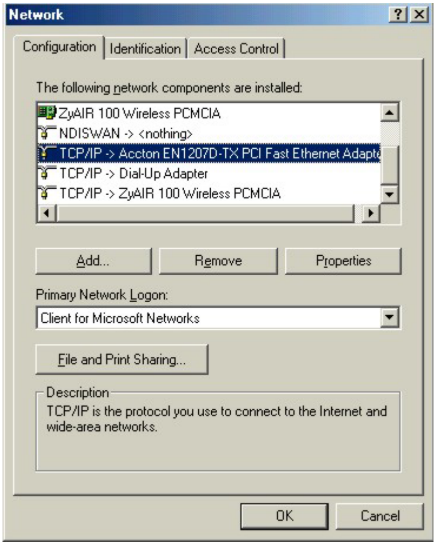
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

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

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet (192.168.1.2 to 192.168.1.254 range with a subnet mask of 255.255.255.0.) as the default Prestige's LAN port IP address (192.168.1.1).

Windows 95/98/Me

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



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.

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

If you need the adapter:

a. In the **Network** window, click **Add**.

b. Select **Adapter** and then click **Add**.

c. Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

a. In the **Network** window, click **Add**.

b. Select **Protocol** and then click **Add**.

c. Select **Microsoft** from the list of **manufacturers**.

d. Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

a. Click **Add**.

b. Select **Client** and then click **Add**.

c. Select **Microsoft** from the list of manufacturers.

d. Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.

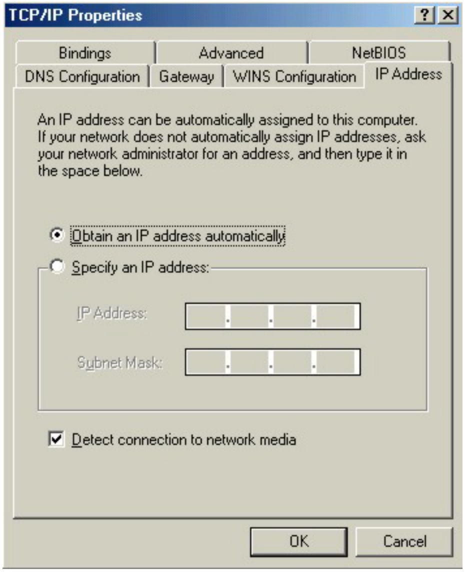
e. Restart your computer so the changes you made take effect.

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

1. Click the **IP Address** tab.

   -To have your computer assigned a dynamic IP address, select **Obtain an IP address automatically**.

   -To give your computer a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.



TCP/IP Properties

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: . . .

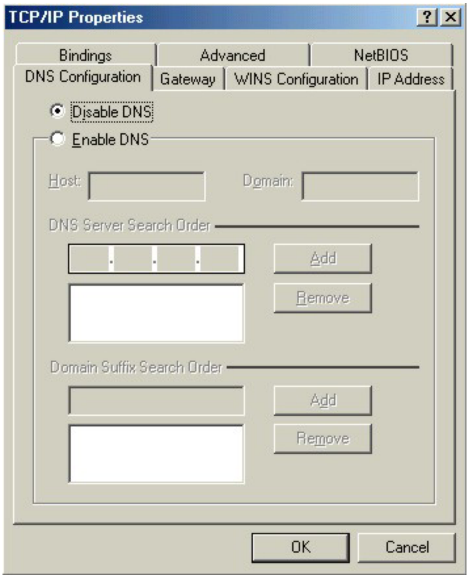
Subnet Mask: . . .

☑ Detect connection to network media

2. Click the **DNS** Configuration tab.

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

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



TCP/IP Properties

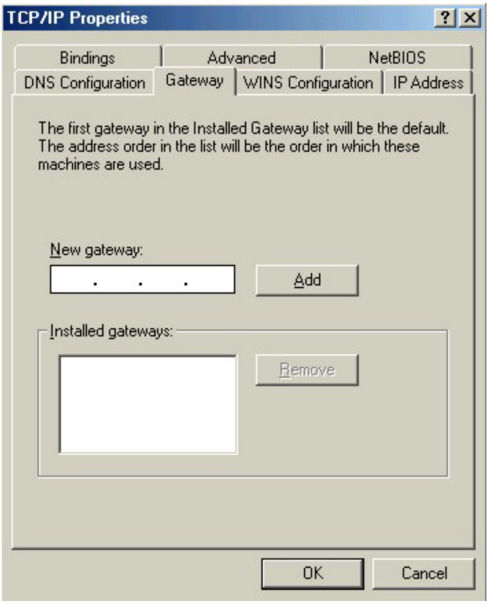
● Disable DNS

○ Enable DNS

3. Click the **Gateway** tab.

   -If you do not know your gateway's IP address, remove previously installed gateways.

   -If you have a gateway IP address, type it in the **New gateway field** and click **Add**.



TCP/IP Properties

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.

4. Click **OK** to save and close the **TCP/IP Properties** window.

5. Click **OK** to close the **Network** window. Insert the Windows CD if prompted.

6. Turn on your Prestige and restart your computer when prompted.

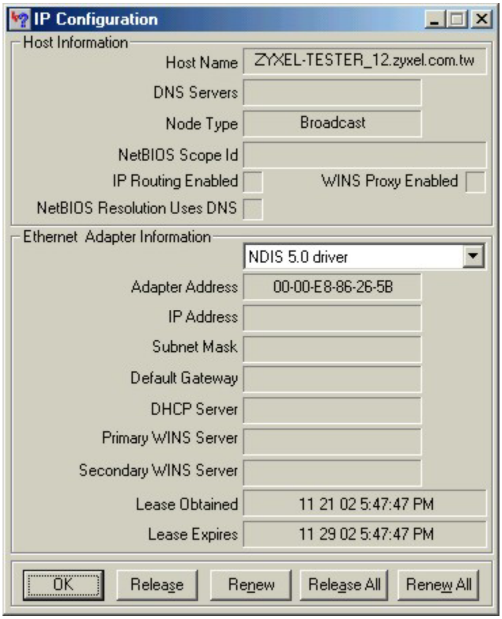
Checking/Modifying Your Computer's IP Address

1. Click **Start** and then **Run**.

2. In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.

3. Select your network adapter. You should see your computer's (static) IP address, subnet mask and default gateway in this screen. Verify that your computer's static IP address is in the correct subnet (192.168.1.2 to 192.168.1.254 if using the default Prestige LAN IP address). Alternatively, to have the Prestige assign your computer a new IP address (from the IP pool), make sure your Prestige is turned on and click **Renew** in this screen.

   Your computer can now communicate with the Prestige using the LAN port.



IP Configuration

Host Information

Host Name: ZYXEL-TESTER_12.zyxel.com.tw
DNS Servers:
Node Type: Broadcast
NetBIOS Scope Id:
IP Routing Enabled □ WINS Proxy Enabled □
NetBIOS Resolution Uses DNS □

Ethernet Adapter Information

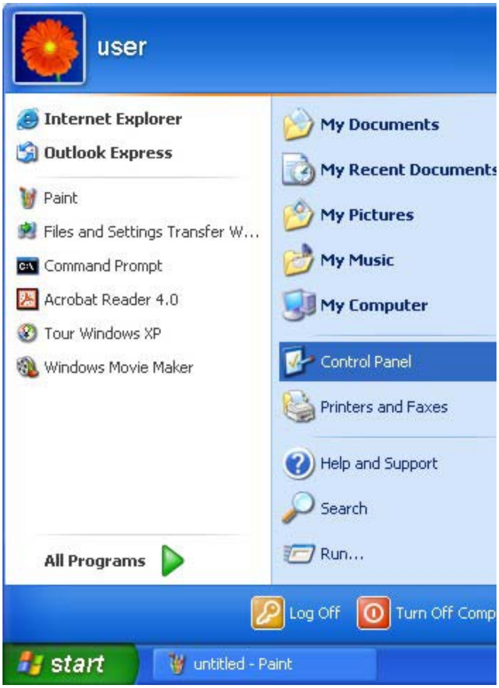
NDIS 5.0 driver

Adapter Address: 00-00-E8-86-26-5B
IP Address:
Subnet Mask:
Default Gateway:
DHCP Server:
Primary WINS Server:
Secondary WINS Server:
Lease Obtained: 11 21 02 5:47:47 PM
Lease Expires: 11 29 02 5:47:47 PM

Windows 2000/NT/XP

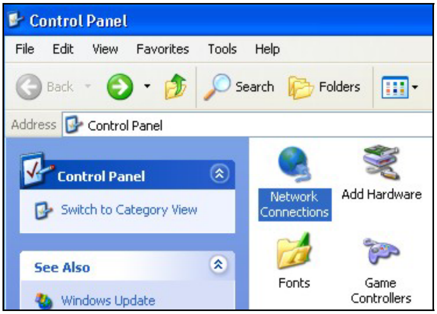
1. In Windows XP, click **start**, **Control Panel**.

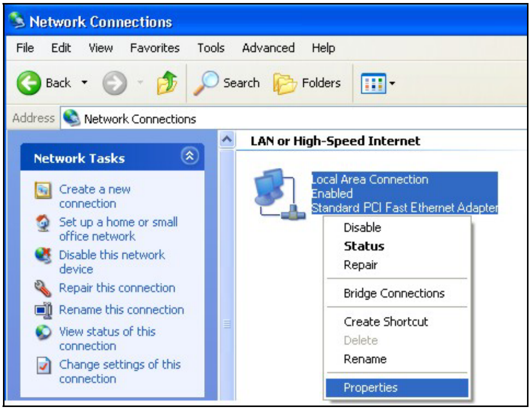
   In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.



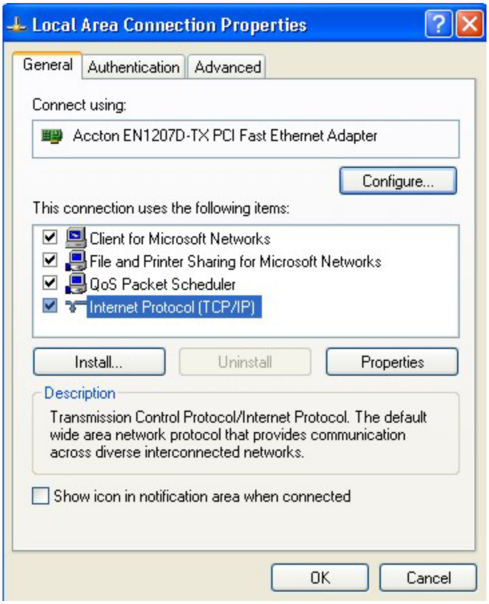
2. In Windows XP, click **Network Connections**. In Windows 2000/NT, click **Network and Dial-up Connections**.

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




Network Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network Connections
Network Tasks
Create a new connection
Set up a home or small office network
Disable this network device
Repair this connection
Rename this connection
View status of this connection
Change settings of this connection
LAN or High-Speed Internet
Local Area Connection
Enabled
Standard PCI Fast Ethernet Adapter
Disable
Status
Repair
Bridge Connections
Create Shortcut
Delete
Rename
Properties

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



Connect using:

Accton EN1207D-TX 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.

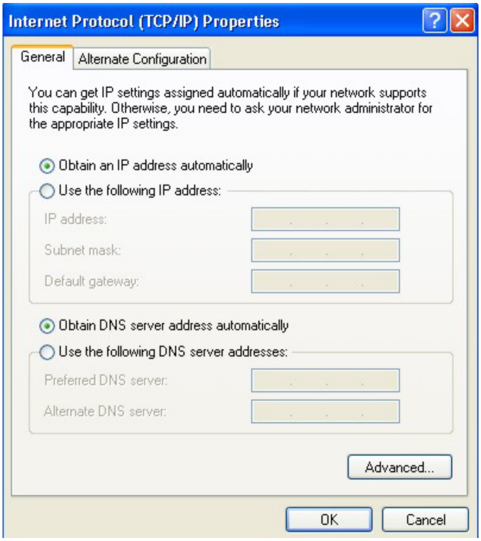
□ Show icon in notification area when connected

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

   - To have your computer assigned a dynamic IP address, click **Obtain an IP address automatically**.

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

   Click **Advanced** to go to the **Advanced TCP/IP Settings** screen shown next.



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:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

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

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

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

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

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

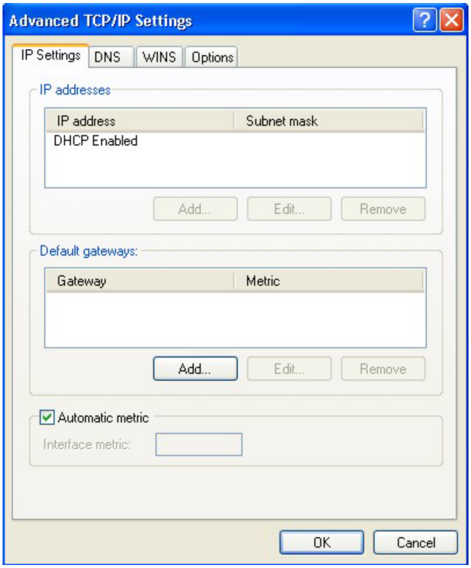
   -Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.

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

   -Click **Add**.

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

   -Click **OK** when finished.



IP address	Subnet mask
DHCP Enabled	

Gateway	Metric

☑ Automatic metric

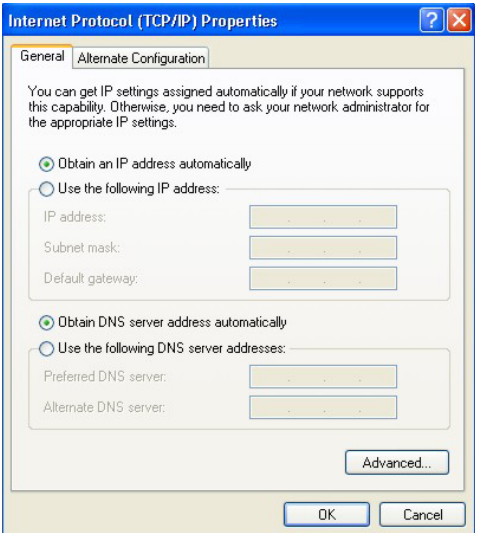
Interface metric:

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

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

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

   If you wish to have more than two DNS servers, click **Advanced**, the **DNS** tab and then configure them using **Add**.



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).

Checking/Modifying Your Computer's IP Address

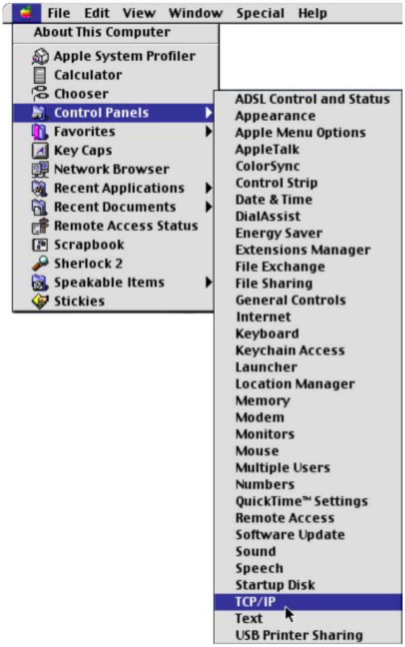
1. Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

2. In the **Command Prompt** window, type "ipconfig" and then press **ENTER** to verify that your computer's static IP address is in the correct subnet (192.168.1.2 to 192.168.1.254 if using the default Prestige LAN IP address). Alternatively, to have the Prestige assign your computer a new IP address (from the IP pool), make sure your Prestige is turned on, type "ipconfig/renew" and then press **ENTER**.

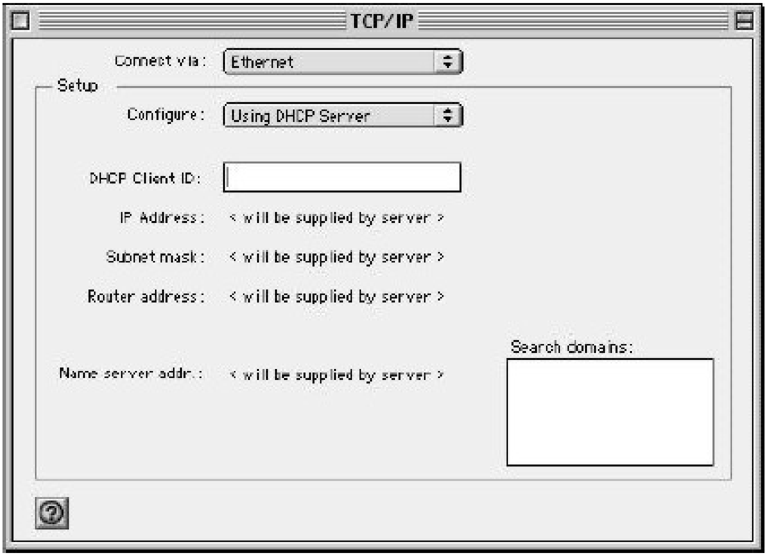
   Your computer can now communicate with the Prestige using the LAN port.

Macintosh OS 8/9

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



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



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.

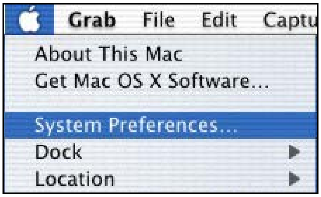
   -Type the IP address of your Prestige in the **Router address** box.
5. Close the **TCP/IP Control Panel**.
6. Click **Save** if prompted, to save changes to your configuration.
7. Turn on your Prestige and restart your computer (if prompted).

Verifying Your Computer's IP Address

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

Macintosh OS X

1. Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

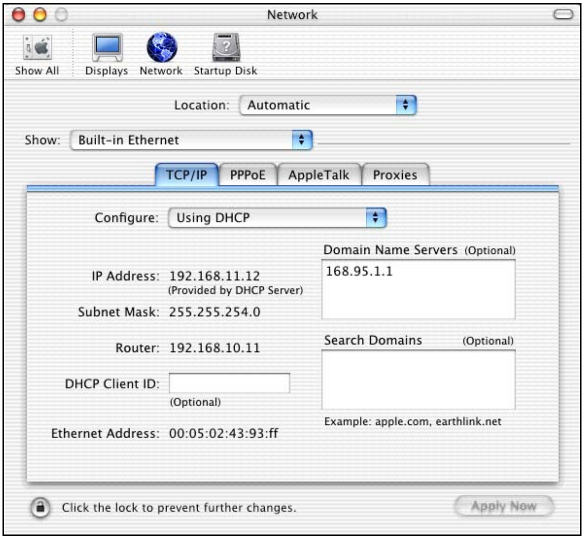


2. Click **Network** in the icon bar.

   - Select **Automatic** from the **Location** list.

   - Select **Built-in Ethernet** from the **Show** list.

   - Click the **TCP/IP** tab.



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 Your Computer's IP Address

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

Appendix I
Brute-Force Password Guessing Protection

The following describes the commands for enabling, disabling and configuring the brute-force password guessing protection mechanism for the password. See other *appendices* for information on the command structure.

Chart 7 Brute-Force Password Guessing Protection Commands

COMMAND	DESCRIPTION
`sys pwderrtm`	This command displays the brute-force guessing password protection settings.
`sys pwderrtm 0`	This command turns off the password's protection from brute-force guessing. The brute-force password guessing protection is turned off by default.
`sys pwderrtm N`	This command sets the password protection to block all access attempts for N (a number from 1 to 60) minutes after the third time an incorrect password is entered.

Example

`sys pwderrtm 5`	This command sets the password protection to block all access attempts for five minutes after the third time an incorrect password is entered.

Appendix J
Triangle Route

The Ideal Setup

When the firewall is on, your Prestige acts as a secure gateway between your LAN and the Internet. In an ideal network topology, all incoming and outgoing network traffic passes through the Prestige to protect your LAN against attacks.

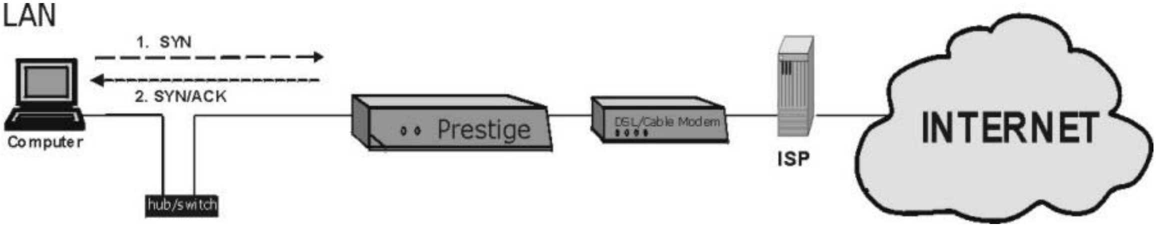


Diagram 10 Ideal Setup

The “Triangle Route” Problem

A traffic route is a path for sending or receiving data packets between two Ethernet devices. Some companies have more than one alternate route to one or more ISPs. If the LAN and ISP(s) are in the same subnet, the “triangle route” problem may occur. The steps below describe the “triangle route” problem.

Step 1. A computer on the LAN initiates a connection by sending out a SYN packet to a receiving server on the WAN.

Step 2. The Prestige reroutes the SYN packet through Gateway **B** on the LAN to the WAN.

Step 3. The reply from the WAN goes directly to the computer on the LAN without going through the Prestige.

As a result, the Prestige resets the connection, as the connection has not been acknowledged.

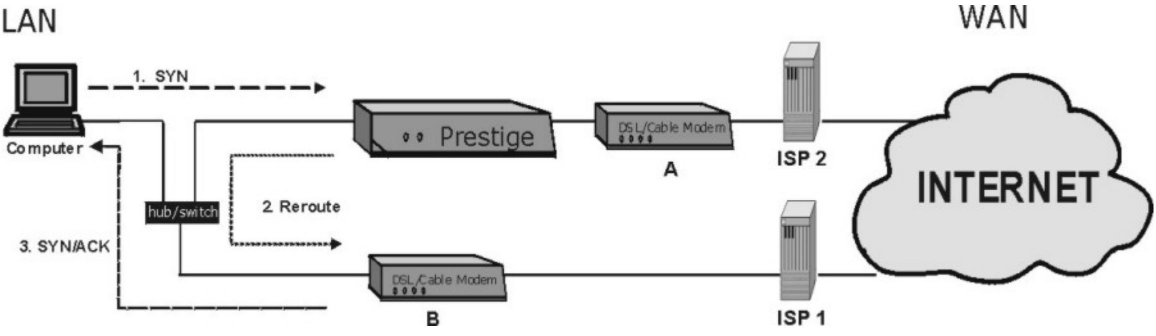


Diagram 11 "Triangle Route" Problem

The "Triangle Route" Solutions

This section presents you two solutions to the "triangle route" problem.

IP Aliasing

IP alias allows you to partition your network into logical sections over the same Ethernet interface. Your Prestige supports up to three logical LAN interfaces with the Prestige being the gateway for each logical network. By putting your LAN and Gateway **B** in different subnets, all returning network traffic must pass through the Prestige to your LAN. The following steps describe such a scenario.

Step 1. A computer on the LAN initiates a connection by sending a SYN packet to a receiving server on the WAN.

Step 2. The Prestige reroutes the packet to Gateway **B** which is in Subnet 2.

Step 3. The reply from WAN goes through the Prestige to the computer on the LAN in Subnet 1.

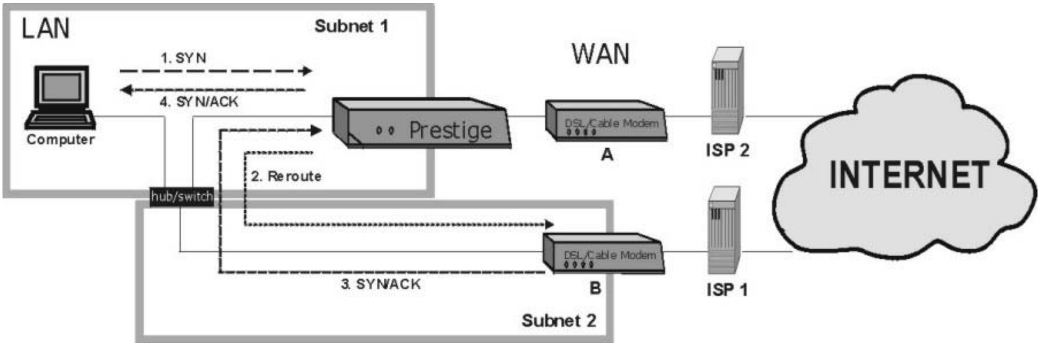


Diagram 12 IP Alias

Gateways on the WAN Side

A second solution to the "triangle route" problem is to put all of your network gateways on the WAN side as the following figure shows. This ensures that all incoming network traffic passes through your Prestige to your LAN. Therefore your LAN is protected.

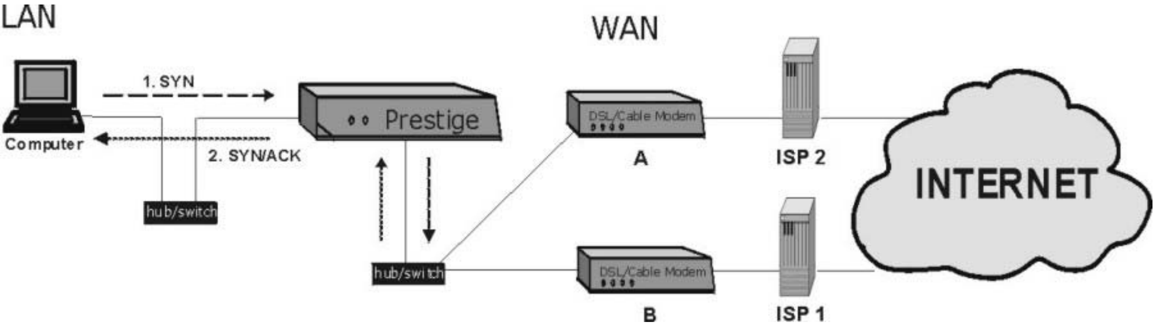


Diagram 13 Gateways on the WAN Side

How To Configure Triangle Route:

Step 1. From the SMT main menu, enter 24.

Step 2. Enter “8” in menu 24 to enter CI command mode.

Step 3. Use the following commands to allow/disallow triangle route.

`sys firewall ignore triangle all off`	This command allows triangle route.
`sys firewall ignore triangle all on`	This command disallows triangle route.

Index