Prestige 314

P314 Broadband Sharing Gateway with 4-Port Switch

User's Guide

Version 3.20

August 2000

ZyXEL

TOTAL INTERNET ACCESS SOLUTION

Prestige 314

P314 Broadband Sharing Gateway With 4-Port Switch

Copyright

Disclaimer

Trademarks

Federal Communications Commission (FCC) Interference Statement

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

This device may not cause harmful interference.

This device must accept any interference received, including interference that may cause undesired operations.

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

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

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and the receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

Notice 1

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

Notice 2

Shielded RS-232 cables are required to be used to ensure compliance with FCC Part 15, and it is the responsibility of the user to provide and use shielded RS-232 cables.

Information for Canadian Users

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

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

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

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

Caution

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

Note

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

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 314

is in conformity with
(reference to the specification under which conformity is declared)

Standard	Standard Item	Version
• EN 55022	Radio disturbance characteristics – Limits and method of measurement.	1994
• 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
• EN 61000-4-11	Voltage dips, short interruptions and voltage variations immunity tests	1994

CE
Declaration of Conformity

The following products is herewith confirmed to comply with the requirements set out in the Council Directive on the Approximation of the laws of the Member States relating to Electromagnetic Compatibility Directive (89/336/EEC). The listed standard as below were applied:

The following Equipment:

Product   :   LAN Hub Router
Model Number   :   PRESTIGE 314

RFI Emission: Limit class B according to EN 55022:1994

Limit class B for harmonic current emission according to EN 61000-3-2:1995

Limitation of voltage fluctuation and flicker a low-voltage supply system according to EN 61000-3-3/1995

Immunity :   Generic immunity standard according to EN 50082-1:1997

Electrostatic Discharge according to EN 61000-4-2:1995

Contact Discharge: 4 kV, Air Discharge : 8 kV

Radio-frequency electromagnetic field according to EN 61000-4-3:1996

80 – 1000MHz with 1kHz AM 80% Modulation: 10V/m

Electromagnetic field from digital telephones according to ENV 50204:1995

900 ±5MHz with 200Hz rep. Frequency ,Duty Cycle 50%

Electrical fast transient/burst according to EN 61000-4-4:1995

AC/DC power supply: 2kV, Data/Signal lines: 1kV

Surge immunity test according to EN 61000-4-5:1995

AC/DC Line to Line: 2kV, AC/DC Line to Earth: 4kV

Immunity to conducted disturbance, Induced by radio-frequency fields: EN 61000-4-6:1996

0.15 –80MHz with 1kHz AM 80% Modulation: 10V/m

Power-frequency magnetic field immunity test according to EN 61000-4-8:1993

30A/m at frequency 50Hz

Voltage dips, short interruptions and voltage variations immunity test according to EN 61000-4-11:1994

30% Reduction @ 10ms, 90% Reduction @100ms, >95%Reduction @5000ms

The following importer/manufacturer is responsible for this declaration:

Company Name   **ZyXEL** Communications Services GmbH.

Company Address : Thaliastrasse 125a/2/2/4
A-1160 Wien • AUSTRIA

Telephone   : Tel.: 01 / 494 86 77-0 Facsimile :
Fax: 01 / 494 86 78

Person is responsible for making this declaration:

Manfred RECLA ---- ZyXEL-European Techn. Support
Name (Full Name)   Position/ Title

Vienna July 31, 2000
Date   Legal Signature:

ZyXEL Communications Services GmbH.
Thaliastrasse 125a/2/2/4
A-1160 Wien • AUSTRIA
Tel.: 01 / 494 86 77-0
Fax: 01 / 494 86 78

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; refer to the separate Warranty Card 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 (USA and territories only). If the customer desires some other return destination beyond the U.S. borders, the customer shall bear the cost of the return shipment. This warranty gives you specific legal rights, and you may also have other rights that vary from state to state.

Please register your Prestige (fast, easy online registration at www.zyxel.com) for free product updates and information.

Customer Support

If you have questions about your ZyXEL product or desire assistance, contact ZyXEL Communications Corporation offices worldwide, in one of the following ways:

Method / Region	EMAIL – Support / EMAIL – Sales	Telephone / Fax	Web Site / FTP Site	Regular Mail
Worldwide	support@zyxel.com.tw support@europe.zyxel.com	+886-3-578-3942	www.zyxel.com www.europe.zyxel.com	ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, HsinChu, Taiwan.
	sales@zyxel.com.tw	+886-3-578-2439	ftp.europe.zyxel.com	
North America	support@zyxel.com	+1-714-632-0882 800-255-4101	www.zyxel.com	ZyXEL Communications Inc., 1650 Miraloma Avenue, Placentia, CA 92870, U.S.A.
	sales@zyxel.com	+1-714-632-0858	ftp.zyxel.com	
Scandinavia	support@zyxel.dk	+45-3955-0700	www.zyxel.dk	ZyXEL Communications A/S, Columbusvej 5, 2860 Soeborg, Denmark.
	sales@zyxel.dk	+45-3955-0707	ftp.zyxel.dk	
Austria	support@zyxel.at	+43-1-4948677-0 0810-1-ZyXEL 0810-1-99935	www.zyxel.at	ZyXEL Communications Services GmbH., Thaliastrasse 125a/2/2/4, A-1160 Vienna, Austria
	sales@zyxel.at	+43-1-4948678	ftp.zyxel.at Note: for Austrian users with *.at domain only!	
Germany	support@zyxel.de	+49-2405-6909-0 0180-5213247 Tech Support hotline 0180-5099935 RMA/Repair hotline	www.zyxel.de	ZyXEL Deutschland GmbH., Adenauerstr. 20/A4, D-52146 Wuerselen, Germany.
	sales@zyxel.de	+49-2405-6909-99	ftp.europe.zyxel.com	

Table of Contents

List of Figures

List Of Tables

Preface

About Your Router

Congratulations on your purchase of the Prestige 314 Broadband Sharing Gateway with 4-Port Switch

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

The Prestige 314 is a dual Ethernet Broadband Access Gateway 4-Port Switch integrated with network management features that allows access to the Internet via Cable/ADSL modem or broadband router. It is designed for:

❑ Home offices and small businesses with Cable or DSL modem via Ethernet port as Internet access media.
❑ Multiple office/department connections via access devices.

Your Prestige 314 is easy to install and to configure.

The Embedded Web Configurator is a web-based utility that allows you to access the Prestige's management settings and configure the Prestige. All functions of the Prestige 314 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 over a telnet connection.

About This User's Manual

This manual is designed to guide you through the SMT configuration of your Prestige 314 for its various applications.

Structure of this Manual

This manual is structured as follows:

Part I. *Getting Started* (Chapters 1 – 3) is structured as a step-by-step guide to help you connect, install and setup your Prestige to operate on your network and access the Internet.

Part II. *Advanced Applications* (Chapters 4 – 6) describe the advanced applications of your Prestige, such as Remote Node Setup, IP Static routes and SUA.

Part III. *Advanced Management* (Chapter 7 – 11) provides information on Prestige Filtering, System Information and Diagnosis, Transferring Files and Telnet.

Part IV. *Troubleshooting* (Chapter 12) provides information about solving common problems as well as some Appendices, a Glossary and an Index.

Regardless of your particular application, it is important that you follow the steps outlined in *Chapters 1-2* to connect your Prestige to your LAN. You can then refer to the appropriate chapters of the manual, depending on your applications.

Related Documentation

➢ Support Disk

More detailed information about the Prestige and examples of its use can be found on the included CD or on www.zyxel.com. This CD contains information on configuring your Prestige for Internet Access, a General

---

FAQ, an Advanced FAQ, Applications Notes, Troubleshooting, Reference CI Commands as well as bundled software.

➢　　　Read Me First

Our Read Me First is designed to help you get your Prestige up and running right away. It contains a detailed easy to follow connection diagram, Prestige default settings, handy checklists, information on setting up your PC, information on installing and using the Embedded Web Configurator, our web-based Internet Access configuration wizard.

➢　　　Packing List Card

Finally, you should have a Packing List Card, which lists all items that should have come with your Prestige.

➢　　　ZyXEL Web and FTP Server Sites

You can access release notes for firmware upgrades and other information at ZyXEL web and FTP server sites. Refer to the Customer Support page in this User's Guide for more information.

Syntax Conventions

- "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** 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.
- For brevity's sake, we will use "e.g." as a shorthand for "for instance" and "i.e." for "that is" or "in other words" throughout this manual.

Part I:

Getting Started

Chapters 1-3 are structured as a step-by-step guide to help 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 features and applications of the Prestige.

1.1 The Prestige 314 Broadband Sharing Gateway With 4-Port Switch

The Prestige 314 is a dual Ethernet Broadband Sharing Gateway with an integrated 4-port switch and advanced network management features. It is designed for home offices and small businesses to easily and quickly access the Internet via Cable/ADSL modem or broadband router. ZyXEL's Prestige 314 provides not only ease of installation and Internet access, but also a complete solution to efficiently manage data traffic on your network. The embedded web configurator is a breeze to operate and totally independent of the operating system platform you use.

1.2 Features of the Prestige 314

The following are the essential features of the Prestige 314.

Broadband WAN Connection with Integrated Four-Port Switch

The P314 sports a 10 Mbps Ethernet port for a cable or DSL modem connection as well as an integrated 4-Port Switch allowing up to 4 computers on your network to enjoy super-fast Internet access without the need for an additional hub.

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 with a Dynamic DNS client to use this service.

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). Both versions 1 and 2 are supported by the Prestige.

Packet Filtering

The Packet Filtering mechanism blocks unwanted traffic from entering/leaving your network.

PPPoE

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.

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) or the Embedded Web Configurator. It also supports FTP (File Transfer Protocol) server for remote management, TFTP (Trivial FTP), SNMP (Simple Network Management Protocol) and CI (Command Interpreter) mode.

Auto-negotiating 10/100 Mbps Ethernet

The 4 LAN ports automatically detect if it's on a 10 or a 100 Mbps Ethernet.

Single User Account (SUA)

SUA is ZyXEL's version of NAT (Network Address Translation) which enables multiple users to share a single ISP account, thereby accessing the Internet for the cost of a single IP address.

DHCP (Dynamic Host Configuration Protocol)

The Prestige supports DHCP Server and Client (RFC 2131 and RFC 2132). The Prestige's DHCP server capability allows you to automatically assign TCP/IP settings to a workstation on your LAN. The Prestige's DHCP client capability allows it to get automatically its IP address from the ISP on the WAN.

RoadRunner Support

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

Logging and Tracing

The Prestige has the following features:
♦ Built-in message logging and packet tracing.
♦ UNIX syslog facility support.

Upgrade Prestige Firmware via LAN

The firmware of the Prestige 314 can be upgraded via the LAN.

Embedded FTP and TFTP Servers

The Prestige's embedded FTP and TFTP servers enable fast firmware upgrade as well as configuration file backup and restoration.

1.3   Broadband Internet Access via Cable or DSL Modem

A cable modem or DSL modem can be connected to the Prestige 10M 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.
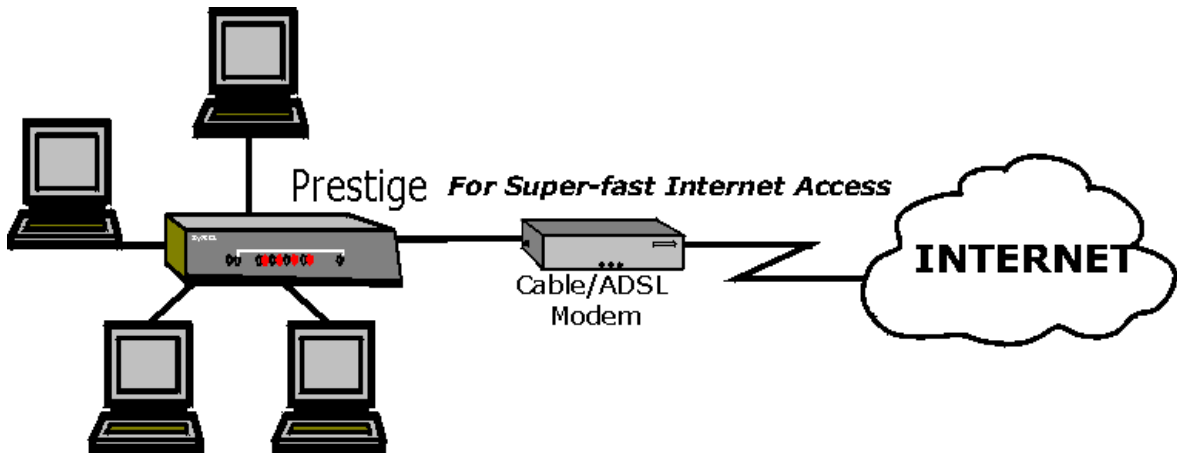
Figure 1-1   Internet Access

Chapter 2
Hardware Installation & Initial Setup

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

2.1 Front Panel LEDs and Back Panel Ports

2.1.1 Front Panel LEDs

The LEDs on the front panel indicate the operational status of the Prestige.
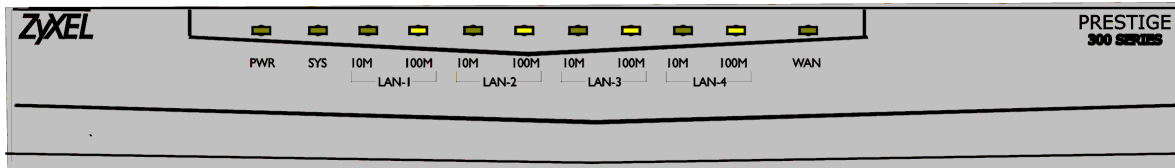
Figure 2-1 Front Panel

The following table describes the LED functions:

Table 2-1 LED Functions

LEDs	Function	Indicator Status	Active	Description
PWR	Power	Green	On	The power adapter is connected to the Prestige.
SYS	System		Off	The system is not ready or failed.
			On	The system is ready and running.
			Flashing	The system is rebooting.
10M LAN	LAN	Green	Off	The 10M LAN is not connected.
			On	The Prestige is connected to a 10M LAN.
			Flashing	The 10M LAN is sending/receiving packets.
100M LAN		Orange	Off	The 100M LAN is not connected.
			On	The Prestige is connected to a 100 Mbps LAN.
			Flashing	The 100M LAN is sending/receiving packets.
WAN	WAN	Green	Off	The WAN Link is not ready, or has failed.

LEDs	Function	Indicator Status	Active	Description
			On	The WAN Link is ok.
			Flashing	The 10M WAN link is sending/receiving packets.

2.2 Prestige 314 Rear Panel and Connections

The following figure shows the rear panel of your Prestige 314 and the connection diagram.
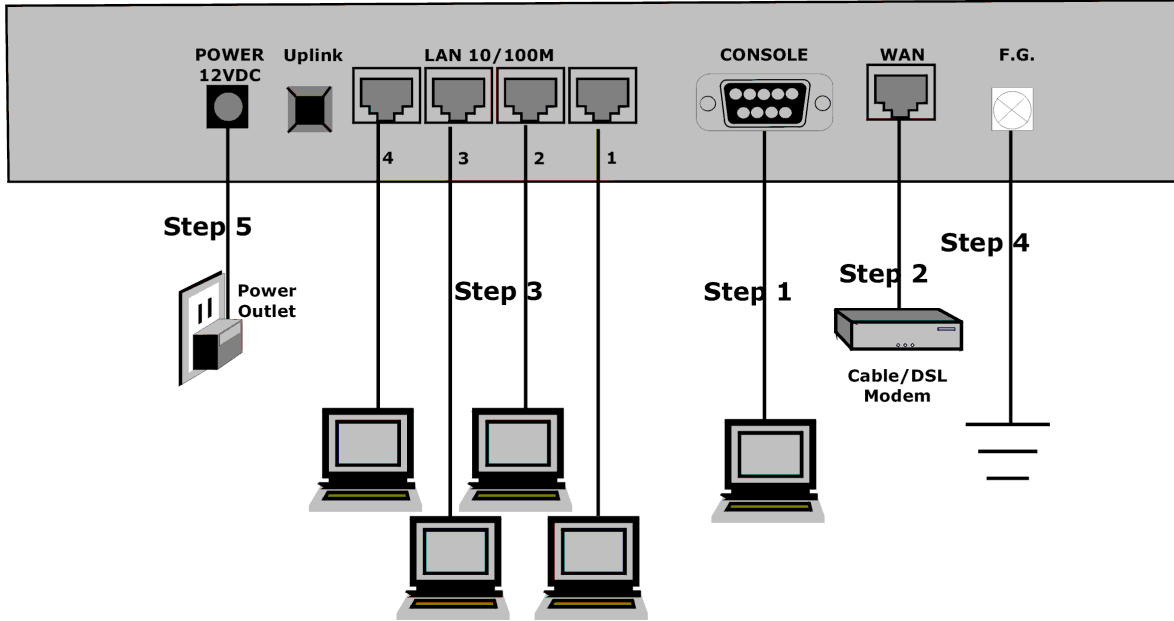
Figure 2-2 Prestige Rear Panel and Connections

This section outlines how to connect your Prestige 314 to the LAN and the WAN. In the case of connecting 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 a DSL Modem to the DSL Wall Jack. Please also *see the Appendices* for important safety instructions on making connections to the Prestige.

Step 1: Connecting the Console Port

For the initial configuration of your Prestige, you need to use terminal emulator software on a workstation and connect it to the Prestige through the console port. Connect the 9-pin 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 workstation. You can use an extension RS-232

cable if the enclosed one is too short. After the initial setup, you can modify the configuration remotely through telnet connections.

Step 2:   Connecting the Prestige to the <u>Broadband Modem</u>

    Step 2a.   Connecting the Prestige to the <u>Cable Modem</u>

        Connect the WAN port on the Prestige to the Ethernet port on the cable modem using the cable that came with your cable modem. The Ethernet port on the cable modem is sometimes labeled "PC" or "Workstation".

<div align="center">OR</div>

    Step 2b.   Connecting the Prestige to the <u>DSL Modem</u>
        Connect the WAN port on the Prestige to the Ethernet port on the DSL modem using the cable that came with your DSL modem.

Step 3:   Connecting the Prestige to your LAN

You can connect up to four computers directly to the Prestige. For each computer, connect the 10/100M LAN port on the Prestige to the Network Adapter on the PC using a straight through Ethernet cable (white tag). If you have more than four computers, you must use an external hub. Connect LAN port 4 (next to the **Uplink** button) on the Prestige to a port on the external hub using a straight through Ethernet cable (white tag) and press the **Uplink** button. If you do not press the **Uplink** button (LAN port 4) or use LAN ports 1 to 3 to daisy chain the Prestige to an external hub, then you must use a crossover cable (red tag).

Step 4:   Grounding the Prestige

If you want to ground the Prestige then connect a grounded wire to the **F.G.** (Frame Ground) of the Prestige.

Step 5:   Connecting the Power Adapter to your Prestige

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

Caution: To prevent damage to the Prestige, first make sure you have the correct AC power adapter. Please see the Appendices for AC power adapter specifications for your region.

2.3   Additional Installation Requirements

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 with an Ethernet NIC (Network Interface Card) installed.
2.   A computer equipped with 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.
After the Prestige is properly set up, you can make future changes to the configuration through telnet connections.

2.4   Power Up Your Prestige

At this point, you should have connected the console port, the LAN port, the WAN port and the power port to the appropriate devices or lines. Plug the power adapter into a wall outlet. The Power LED should be on. The SYS LED will come on after the system tests are complete. The WAN LED and one of the LAN LEDs come on immediately after the SYS LED comes on, if connections have been made to the LAN and WAN ports.

Initial Screen

When you power 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.

```
Copyright (c) 1994 - 2000 ZyXEL Communications Corp.
initialize ch =0, ethernet address: 00:a0:c5:41:51:61
initialize ch =1, ethernet address: 00:a0:c5:41:51:62
Press ENTER to continue...
```

Figure 2-3   Initial Screen

Entering Password

The login screen appears after you press [Enter], prompting you to enter the password, as shown below. For your first login, enter the default password **1234**. As you type the password, the screen displays an (X) for each character you type.

Please note that if there is no activity for longer than 5 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 2-4   Password Screen

2.5   Navigating the SMT Interface

The SMT (System Management Terminal) is the interface that you use to configure your Prestige. Several operations that you should be familiar with before you attempt to modify the configuration are listed in the table below.

Table 2-2   Main Menu Commands

Operation	Keystrokes	Description
Move down to another menu	[ENTER]	To move forward to a submenu, type in the number of the desired submenu and press [ENTER].
Move up to a previous menu	[Esc]	Press the [Esc] key to move back to the previous menu.
Move to a "hidden" menu	Press the [SPACE BAR] to change **No** to **Yes** then press [ENTER]**.**	Fields beginning with "Edit" lead to hidden menus and have a default setting of **No**. Press the [SPACE BAR] to change **No** to **Yes**, then press [ENTER] to go to a "hidden" menu.
Move the cursor	[ENTER] or [Up]/[Down] arrow keys	Within a menu, press [ENTER] to move to the next field. You can also use the [Up]/[Down] arrow keys to move to the previous and the next field, respectively.
Enter information	Fill in, or Press the [SPACE BAR] to toggle	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 the [SPACE BAR].
Required fields	<? >	All fields with the symbol <?> must be filled in order be able to save the new configuration.
N/A fields	<N/A>	Some of the fields in the SMT will show a <N/A>. This symbol refers to an option that is Not Applicable.
Save your configuration	[ENTER]	Save your configuration by pressing [ENTER] at the message [Press ENTER to confirm or ESC to cancel]. Saving the data on the screen will take you, in most cases to the previous menu.
Exit the SMT	Type 99, then press [ENTER].	Type 99 at the Main Menu prompt and press [ENTER] to exit the SMT interface.

2.5.1 Main Menu

After you enter the password, the SMT displays the **Prestige 314 Main Menu**, as shown below.

```
                    Copyright (c) 1994 - 2000 ZyXEL Communications Corp.

                          Prestige 314 Main Menu
        Getting Started              Advanced Management
          1. General Setup             21. Filter Set Configuration
          2. WAN Setup
          3. LAN Setup                 23. System Password
          4. Internet Access Setup     24. System Maintenance

        Advanced Applications
          11. Remote Node Setup
          12. Static Routing Setup
          15. SUA Server Setup
                                       99. Exit


                          Enter Menu Selection Number:
```

Figure 2-5   Prestige 314 Main Menu

2.5.2 System Management Terminal Interface Summary

Table 2-3   Main Menu Summary
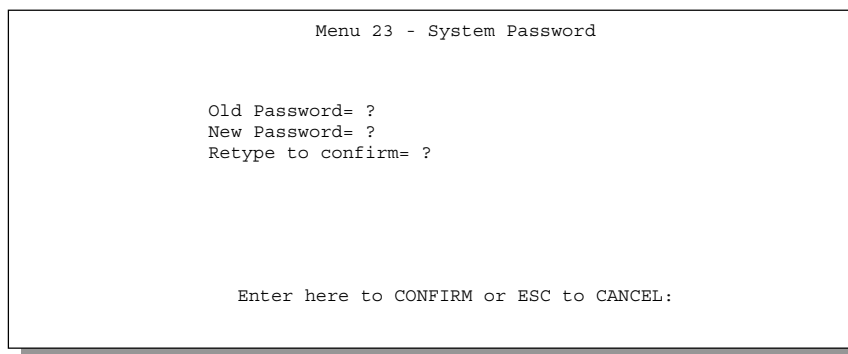
#	Menu Title	Description
1	General Setup	Use this menu to set up general information.
2	WAN Setup	Use this menu to set up the WAN.
3	LAN Setup	Use this menu to set up the LAN.
4	Internet Access Setup	A quick and easy way to set up Internet connection.
11	Remote Node Setup	Use this menu to set up the remote node.
12	Static Routing Setup	Use this menu to set up static route.
15	SUA Server Setup	Use this menu to specify inside servers when SUA is enabled.
21	Filter Set Configuration	Use this menu to set up filters to provide security.
23	System Password	Use this menu to set up a new password.
24	System Maintenance	This menu provides system status, diagnostics, firmware upload, etc.
99	Exit	To exit from SMT and return to the blank screen.

2.6   Changing the System Password

The first thing your should do before anything else is to change the default system password by following the steps below.

Step 1.   Enter 23 in the Main Menu to open **Menu 23 – System Password** as shown below.

```
                        Menu 23 - System Password



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






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

Figure 2-6   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.

2.6.1 Resetting the Prestige

If you have forgotten your password or for some reason cannot access the SMT menu you will need to reinstall the configuration file. Uploading the configuration file replaces the current configuration file with the default configuration file, you will lose all configurations that you had before and the speed of the console port will be reset to the default of 9600bps with 8 data bit, no parity and 1 stop bit (8n1). The password will be reset to the default of 1234, also.

Turn off the Prestige and begin a Terminal session with the current console port settings. 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. You should already have downloaded the correct file from your nearest ZyXEL FTP site. *See Chapter 9* for more information on how to transfer the configuration file to your Prestige.

2.7   General Setup

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

To enter Menu 1 and fill in the required information, follow these steps:

Step 1.   Enter 1 in the Main Menu to open **Menu 1 – General Setup**.
Step 2.   The **Menu 1 – General Setup** screen appears, as shown below. Fill in the required fields.

```
                  Menu 1 - General Setup

        System Name= xxx
        Domain Name= zyxel.com.tw
        Configure Dynamic DNS= No




             Press ENTER to Confirm or ESC to Cancel:
```
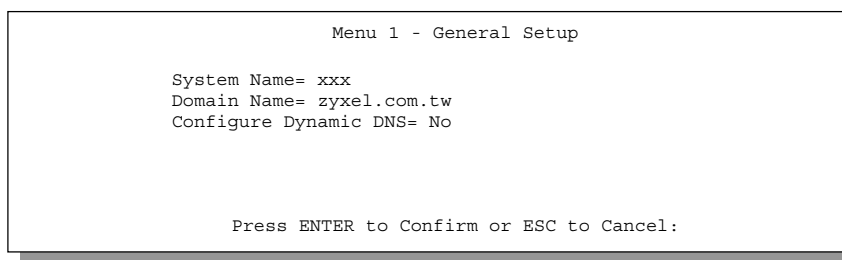
Figure 2-7   Menu 1 – General Setup

The fields for General Setup are as shown below. **System Name** is for identification purposes. However, because some ISPs check this name you should enter your PC's "Computer Name" (Start -> Settings -> Control Panel -> Network. Click the Identification tab, note the entry for the Computer name" field). It is the domain name that will be 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 machine, the domain name can be assigned from the Prestige via DHCP.

Table 2-4   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.	Billy
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 router. 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
Configure Dynamic DNS	Press the [SPACE BAR] to select **Yes** or **No** (default). Select **Yes** to configure **Menu 1.1 – Configure Dynamic DNS** discussed next.	

2.7.1 Dynamic DNS

Dynamic DNS allows you to update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in *NetMeeting*, *CU-SeeMe*, etc.) or access your FTP server or Web site on your own computer using a DNS-like address (e.g. *myhost.dhs.org*, where *myhost* is a name of your

choice) which will never change instead of using your 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 client. The Dynamic DNS Client service provider will give you a password or key. The Prestige at the time of writing supports www.ddns.org and www.dyndns.org clients. You can apply to either of these clients 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.

2.7.2 Configuring Dynamic DNS

To configure Dynamic DNS, go to **Menu 1 – General Setup** and press select **Yes** in the **Configure Dynamic DNS** field.

Pressing [Enter] takes you to **Menu 1.1– Configure Dynamic DNS** as shown next.

```
                    Menu 1.1 - Configure Dynamic DNS

       Service Provider = WWW.DynDNS.ORG
       Active= Yes
       Host= me.ddns.org
       EMAIL= mail@mailserver
       User= username
       Password= ******
       Enable Wildcard= No
                   Press ENTER to confirm or ESC to cancel:
```

Figure 2-8   Configure Dynamic DNS

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

Table 2-5   Configure Dynamic DNS Menu Fields

Field	Description	Example
Service Provider	Enter the name of your Dynamic DNS client.	**www.ddns.org**
Active	Press [SPACE BAR] to toggle between **Yes** or **No**.	**Yes**
Host	Enter the domain name assigned to your Prestige by your Dynamic DNS provider.	**me.ddns.org**
EMAIL	Enter your e-mail address.	**mail@mailserver**
User	Enter your user name.	

Password	Enter the password assigned to you.	
Enable Wildcard	Your Prestige supports DYNDNS Wildcard. Press [SPACE BAR] to toggle between **Yes** or **No** This field is **N/A** when you choose DDNS client as your service provider.	**Yes**

The IP address will be updated when you reconfigure Menu 1 or perform DHCP client renewal.

Please note that:

♦ **The Prestige supports basic DDNS, i.e., insecure login and password.**

♦ **If you have a private WAN IP address, then you can not use this service.**

2.8   WAN Setup

This section describes how to configure the WAN using **Menu 2 – WAN (10 Mbps Ethernet) Setup**. From the Main Menu, enter 2 to open Menu 2.

You only need to configure this menu if your ISP requires MAC address authentication.

```
                        Menu 2 - WAN Setup
                   MAC Address:
                    Assigned By=IP address attached on LAN
                    IP Address= 192.168.1.42



                      Press ENTER to Confirm or ESC to Cancel:
       Press Space Bar to Toggle
```
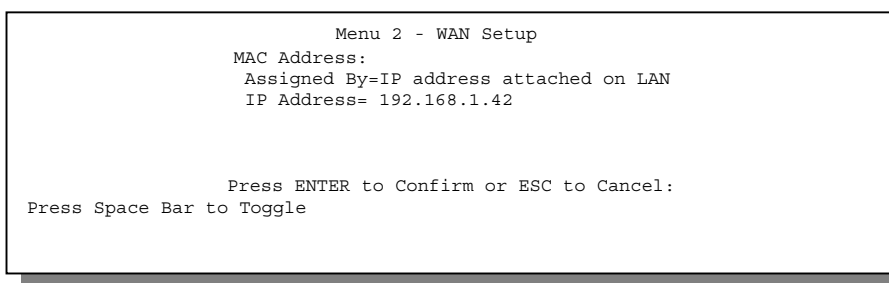
Figure 2-9   Menu 2 – WAN Setup

This menu allows you to configure the WAN port's MAC Address by using either 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 in **Menu 2** or upload a different rom file.

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

Table 2-6   WAN Setup Menu Fields

Field	Description	Examples
MAC Address		
Assigned By	Press the [SPACEBAR] to choose either of the two methods of assigning a MAC Address. Choose **Factory Default** to select the factory assigned default MAC Address. Choose **IP Address attached**	**Factory Default**

	on LAN to use the MAC Address of that workstation whose IP you give in the following field.	
IP Address	This field is applicable only if you choose **IP Address attached on LAN** method. Enter the IP address of the workstation on the LAN whose MAC you are cloning.	

2.9 LAN Setup

This section describes how to configure the LAN using **Menu 3 – LAN Setup (10/100 Mbps Ethernet)**. From the Main Menu, enter 3 to open Menu 3.

```
                         Menu 3 - LAN Setup


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




             Enter Menu Selection Number:
```

Figure 2-10   Menu 3 – LAN Setup

2.9.1 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= 2
               device filters=
            Output Filter Sets:
               protocol filters=
               device filters=


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

Figure 2-11   Menu 3.1 – LAN Port Filter Setup

Menu 3.2 is discussed in the next chapter.

Chapter 3
Internet Access

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

3.1 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.

3.1.1 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 the parameters are satisfactory, you can skip to *section 3.2* to enter the DNS server address(es) if your ISP gives you explicit DNS server address(es). If you wish to change the factory defaults or to learn more about TCP/IP, please read on.

3.1.2 IP Address and Subnet Mask

Similar to the houses on a street that share a common street name, the machines 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 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 3 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.

3.1.3 Private IP Addresses

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

```
10.0.0.0      –   10.255.255.255

172.16.0.0    –   172.31.255.255

192.168.0.0   –   192.168.255.255
```

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

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

3.1.4 RIP Setup

RIP (Routing Information Protocol, RFC 1058 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**.

3.1.5 DHCP Configuration

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows the individual clients (workstations) to obtain the 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 sever 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 machines, e.g., server for mail, FTP, telnet, web, etc., that you may have.

DNS Server Address

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa, 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 machine before you can access it.
There are two ways that an ISP disseminates the DNS server addresses. The first is for an ISP to tell a customer the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP does give you the DNS server addresses, enter them in the **DNS Server** fields in **DHCP Setup.** The second is to leave this field blank, i.e., 0.0.0.0 – in this case the Prestige acts as a DNS proxy.

Example Of Network Properties For LAN Servers With Fixed IP#:

Choose an IP:	192.168.1.2 – 192.168.1.32**;** 192.168.1.65 - 192.168.1.254.
Netmask:	255.255.255.0
Gateway (or default route):	192.168.1.1 (Prestige LAN IP)
DNS server:	192.168.1.1
Domain:	(optional)

3.1.6 IP Multicast

Traditionally, IP packets are transmitted in one of either two ways - Unicast (1 sender – 1 recipient) or Broadcast (1 sender – everybody on the network). Multicast is a third way to deliver IP packets to *a group* of hosts on the network - not everybody.
IGMP (Internet Group Multicast Protocol) is a 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.

3.2   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:
```
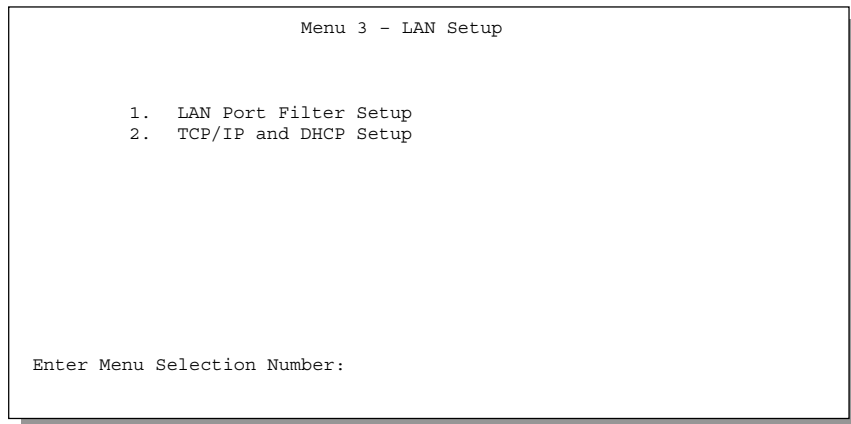
Figure 3-1   Menu 3 – LAN Setup (10/100 Mbps Ethernet)

To edit the TCP/IP and DHCP configuration, enter 2 to open **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

      TCP/IP Setup:
        IP Address= 192.168.1.1
        IP Subnet Mask= 255.255.255.0
        RIP Direction= Both
        Version= RIP-1
        Multicast= IGMP-v2


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

Figure 3-2   Menu 3.2 – TCP/IP and DHCP Ethernet Setup

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

Table 3-1   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.	**None** **Server** (default)
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.	192.168.1.33
Size of Client IP Pool	This field specifies the size, or count, of the IP address pool.	32
Primary DNS Server Secondary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask. Leave these entries at 0.0.0.0 if they are provided by a WAN DHCP server.	

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

Table 3-2   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 from **Both/In Only/Out Only/None.**	**Both** (default)
Version	Press the [SPACE BAR] to select the RIP version from **RIP-1/RIP-2B/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**
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.		

3.3   Internet Access Setup

You will see two different Menu 4 screens depending on whether you chose **Ethernet** or **PPPoE Encapsulation**.

3.3.1 Ethernet Encapsulation

You must choose the **Ethernet** option when the WAN port is used as a regular Ethernet. The PPPoE choice is for a dial-up connection using PPPoE. If you choose **Ethernet** in **Menu 4** you will see the next screen.

```
            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
      Single User Account= Yes




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

Figure 3-3   Menu 4 – Internet Access Setup

The following table describes this screen.

Table 3-3   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	Press the [SPACE BAR] to select **Standard, RR-Toshiba** (RoadRunner Toshiba authentication method) or **RR-Manager** (RoadRunner Manager authentication method). Choose a RoadRunner flavor if your ISP is Time Warner's RoadRunner; otherwise choose **Standard**.
Note: DSL 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 Name	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.
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.
Single User Account	Please see the SUA chapter in the next Part for a more detailed discussion on SUA.

3.3.2 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. DSL, 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 & 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 314 rather than individual PC's, the machines on the LAN do **not** need PPPoE software installed since the P314 does that part of the task. Furthermore, with NAT, all of the LAN's machines will have access.

If you enable PPPoE in Menu 4, you will see the next screen. For more information on PPPoE, please see the Appendices.

```
      Menu 4 - Internet Access Setup

  ISP's Name= ChangeMe
  Encapsulation= PPPoE
    Service Type= N/A
    My Login= baboo
    My Password= ********
    Idle Timeout= 100

  IP Address Assignment= Dynamic
    IP Address= N/A
    IP Subnet Mask= N/A
    Gateway IP Address= N/A
  Single User Account= Yes




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

Figure 3-4   Menu 4 Using PPPoE

Table 3-4   New Fields in Menu 4 (PPPoE) Screen

Field	Description	Examples
Encapsulation	Press the [SPACE BAR] and then press [ENTER] to choose **PPPoE**. The encapsulation method influences your choices for IP Address.	**PPPoE**
Service Type	Enter the PPPoE service name provided to you. PPPoE uses a service name to identify and reach the PPPoE server.	**poellc**
Idle Timeout	This value specifies the time in seconds that elapses before the Prestige automatically disconnects from the PPPoE server.	**100** (default)

3.4   Internet Setup Test

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 **PPPoE** as your encapsulation method. Enter 'Y' to test your setup.

3.5   Basic Setup Complete

Well done! You have successfully connected, installed and set up your Prestige to operate on your network as well as access the Internet.

Part II:

Advanced Applications

Advanced Applications (Chapters 4-6) describe the advanced applications of your Prestige, such as Remote Node Setup, IP Static Routes and SUA.

<div align="right">

Chapter 4
Remote Node Setup

</div>

<div align="right">

This chapter shows you how to configure a remote node.

</div>

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**.

4.1   Remote Node Profile

From the Main Menu, select menu option 11 to open **Menu 11.1 – Remote Node Profile**. There are two variations of this menu depending on whether you choose **Ethernet Encapsulation** or **PPPoE Encapsulation.**

4.1.1 Ethernet Encapsulation

You must 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
           My Password= N/A
           Server IP= N/A




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

Figure 4-1   Menu 11.1 Remote Node Profile for Ethernet Encapsulation

Table 4-1   Fields in Menu 11.1

Field	Description	Examples
Rem Node Name	Enter a descriptive name for the remote node. This field can be up to eight characters.	LAoffice
Active	Press the [SPACE BAR] to toggle between **Yes** and **No** and activate (deactivate) the remote node.	**Yes**
Encapsulation	**Ethernet** is the default encapsulation. Press the [SPACE BAR] if you wish to change to **PPPoE** encapsulation.	**Ethernet**
Service Type	Press the [SPACE BAR] to select from **Standard**, **RR-Toshiba** (RoadRunner Toshiba authentication method) or **RR-Manager** (RoadRunner Manager authentication method). Choose one of the RoadRunner methods if your ISP is Time Warner's RoadRunner; otherwise choose **Standard**.	**Standard**
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**
Outgoing: 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 only for the P314.	**IP**
Edit IP	This field leads to a "hidden" menu. Press the [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 toggle this field to **Yes** and press [ENTER] to open Menu 11.5 to edit the filter sets. See the Remote Node Filter section for more details.	**Yes**

4.1.2 PPPoE Encapsulation

The Prestige supports PPPoE (Point-to-Point Protocol over Ethernet). You can only use PPPoE encapsulation when you're using the Prestige with an xDSL modem as the WAN device. If you change the **Encapsulation** to **PPPoE,** then you will see the next screen. Please see *the Appendices* for more information on PPPoE.

```
                     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=
          My Password= ********
                                           Session Options:
                                             Edit Filter Sets= No
                                             Idle Timeout(sec)= 300




                     Press ENTER to Confirm or ESC to Cancel:

        Press Space Bar to Toggle.
```

Figure 4-2   Menu 11.1 Remote Node Profile for PPPoE Encapsulation

The following table describes the fields NOT already described in *Table 4-1* already.

Table 4-2   Fields in Menu 11.1 (PPPoE Encapsulation Specific Only)

Field	Description	Examples
Telco Option: Allocated Budget	The field sets a ceiling for outgoing call time for this remote node. The default is 0, meaning no budget control.	10
Period(hr)	This field is the time period that the budget should be reset. For example, if we are allowed to call this remote node for a maximum of 10 minutes every hour, then the **Allocated Budget** is (10 minutes) and the **Period(hr)** is 1 (hour).	**1**
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*.	**100 seconds** (default)

4.2   Editing TCP/IP Options

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

```
            Menu 11.3 - Remote Node Network Layer Options

                 IP Address Assignment= Dynamic
                 Rem IP Addr: N/A
                 Rem Subnet Mask= N/A
                 My WAN Addr= N/A

                 Single User Account= Yes
                 Metric= N/A
                 Private= N/A
                 RIP Direction= None
                  Version= N/A
                 Multicast= None

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

Figure 4-3   Remote Node Network Layer Options

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

Table 4-3   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 Subnet Mask	If you have a **Static IP Assignment,** enter the subnet mask assigned to you.	
My WAN Addr	If you have a **Static** IP Assignment, enter the gateway IP address assigned to you.	
Single User Account	Use the [SPACE BAR] to toggle **Yes** and **No**. See *the chapter on SUA* for a full discussion of this feature.	**Yes**
Metric	This field is valid only for PPPoE encapsulation. The 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.	3

Field	Description	Example
Private	This field is valid only for **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 broadcasts.	**Yes**
RIP	Press the [SPACE BAR] to select the **RIP direction** from **Both/ None/In Only/Out Only**. Please see section 3.1.4 for more information on RIP. The default for RIP on the WAN side is **None.** It is recommended you do not change this setting.	**None**
Version	Press the [SPACE BAR] to select the RIP version from **RIP-1/RIP-2B/RIP-2M** or **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 **IGMP-v2**. Press [SPACE BAR] to enable IP Multicasting or select **None** to disable it. Please see Part 1 for more information on these two fields.	**None**
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.		

4.3   Remote Node Filter

Move the cursor to the field **Edit Filter Sets** in **Menu 11.1**, then press the [SPACE BAR] to toggle and 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 and to prevent certain packets from triggering calls. You can specify up to 4 filter sets separated by a comma, 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 chapter on filters. Note that for PPPoE encapsulation, you can also specify remote node call filter sets.

```
             Menu 11.5 - Remote Node Filter

      Input Filter Sets:
        protocol filters= 3
           device filters=
      Output Filter Sets:
        protocol filters= 1
           device filters=


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

Figure 4-4   Remote Node Filter (Ethernet Encapsulation)

```
             Menu 11.5 - Remote Node Filter

      Input Filter Sets:
        protocol filters= 3
           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 4-5   Remote Node Filter (PPPoE Encapsulation)

<div align="right">

Chapter 5
IP Static Route Setup

</div>

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

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

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.
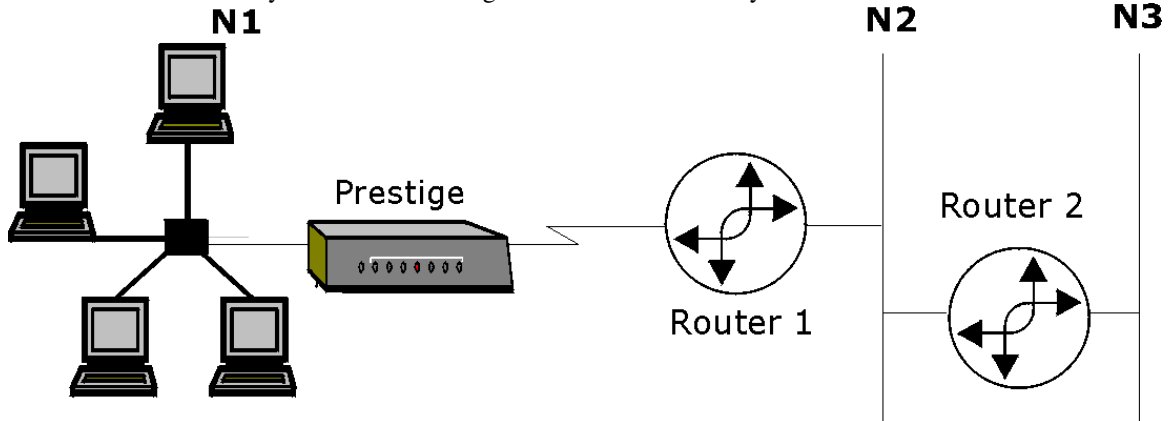
Figure 5-1   Example of Static Routing Topology

5.1   IP Static Route Setup

You configure IP static routes in **Menu 12 – IP Static Route Setup**, 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:
```
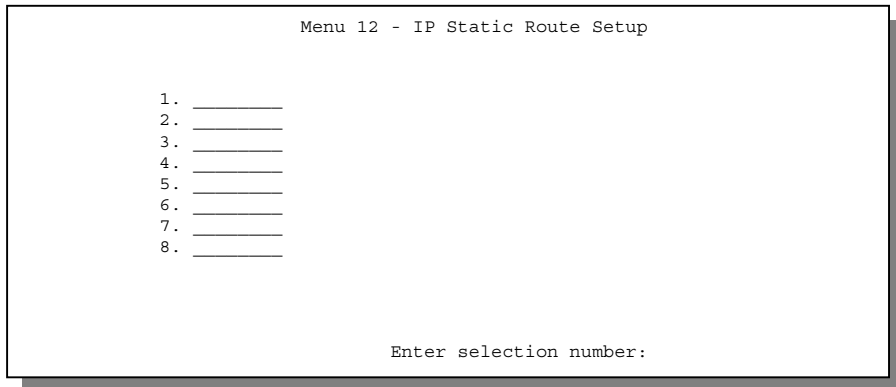
Figure 5-2   Menu 12 – IP Static Route Setup

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:
```
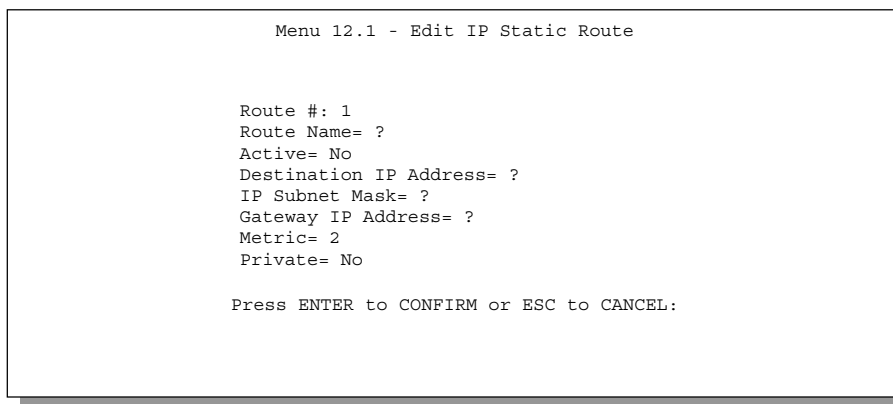
Figure 5-3   Menu 12. 1 – Edit IP Static Route

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

Table 5-1   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 6
SUA Server Setup

This chapter introduces SUA and helps you set up multiple servers behind SUA.

6.1   Single User Account (SUA)

Typically, if there are multiple users on the LAN wanting to concurrently access the Internet, you will have to lease a block of legal, or globally unique, IP addresses from the ISP.

Your Prestige accomplishes address sharing by translating the internal LAN IP addresses to a single address that is globally unique on the Internet. The SUA feature allows you to have the same benefits as having multiple legal addresses, but allows you to have one legal IP address and many local LAN IP addresses that can be used in other domains also, thus conserving the number of global IP addresses.

The Single User Account feature may also be used on connections to remote networks other than the ISP. For example, this feature can be used to simplify the allocation of IP addresses when connecting branch offices to the corporate network.

The IP address for the SUA can be either fixed or dynamically assigned. In addition, you can designate servers, e.g., a web server, on your local network in the client side and make them accessible to outside world.
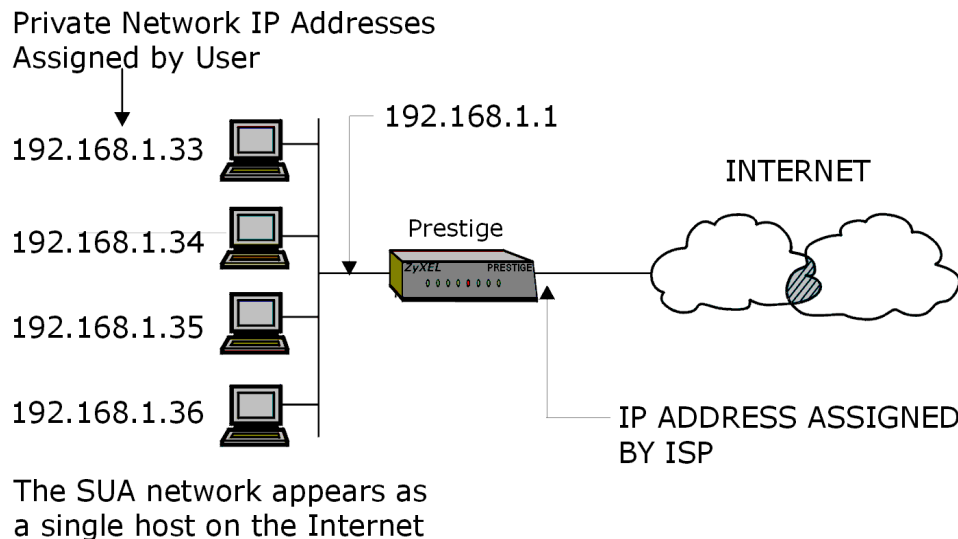
Figure 6-1   An Example of Single User Account Topology

SUA offers the additional benefit of firewall protection. All incoming inquiries will be filtered out by your Prestige and thus preventing intruders from probing your network.

For more information on IP address translation as a solution for IP address depletion problem, refer to RFC 1631, *The IP Network Address Translator (NAT)*.

In summary:

- SUA helps in more efficient IP address management.
- SUA can provide firewall protection. All incoming inquiries will be filtered out by your Prestige.
- UDP and TCP datagrams can be routed. In addition, partial ICMP, including echo (ping) and trace route, is supported.
- SUA is also a cost-effective solution for offices to access the Internet or other remote TCP/IP networks as they have to pay for a single globally unique IP address only.

6.1.1 Single User AccountConfiguration

The steps for configuring your Prestige for Single User Account are identical to conventional Internet access (See configuration instructions in the previous chapter) with the exception that you need to fill in two extra fields in **Menu 4 – Internet Access Setup**, as shown in the following figure. SUA here is applied solely to the output interface and is valid *only* for LAN -– WAN connections and *not* for connections between LANs.

```
        Menu 4 - Internet Access Setup

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

 IP Address Assignment= Dynamic
   IP Address= N/A
   IP Subnet Mask= N/A
   Gateway IP Address= N/A
 Single User Account= Yes  ──────────────→  SUA


  Press ENTER to Confirm or ESC to Cancel:
```
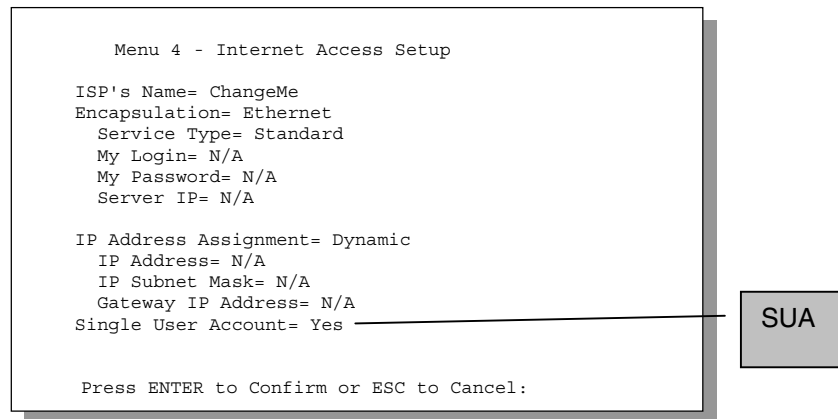
Figure 6-2   Menu 4 – Internet Access Setup for Single User Account

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

Table 6-1   Single User Account Menu Fields

Field	Description
Single User Account	To enable SUA in **Menu 4**, move the cursor to the **Single User Account** field and press [SPACE BAR] to select **Yes** (or **No** to disable SUA).
Press [ENTER] at the message [Press ENTER to Confirm ...] to save your configuration, or press [ESC] at any time to cancel.	

When SUA is disabled, the Prestige sends packets from your LAN computers to the remote computer on the WAN using real source and destination IPs - no port translation is performed. If the LAN computers use private IPs (Private Networks IPs: 10.0.0.0 ~ 10.255.255.255; 172.16.0.0. ~ 172.31.255.255; 192.168.0.0. ~ 192.168.255.255) and SUA is disabled, outgoing packets are routed by the Prestige but are never returned.

Only legal IPs are valid on the Internet. Computers on your LAN must use legal IPs when SUA is disabled.

6.2   Multiple Servers behind SUA

If you wish, you can make inside servers for different services, e.g., web or FTP, visible to the outside users, even though SUA makes your whole inside network appear as a single machine to the outside world. A service is identified by the port number, e.g., web service is on port 80 and FTP on port 21.

As an example, if you have a web server at 192.168.1.2 and an FTP server 192.168.1.3, then you need to specify for port 80 (web) the server at IP address 192.168.1.2 and for port 21 (FTP) another at IP address 192.168.1.3.

Please note that a server can support more than one service, e.g., a server can provide both FTP and DNS service, while another provides only web service. Also, since you need to specify the IP address of a server in the Prestige, a server must have a fixed IP address and not be a DHCP client whose IP address potentially changes each time it is powered on.

In addition to the servers for specific services, SUA 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 server is not defined, the service request is simply discarded.

To make a server visible to the outside world, specify the port number of the service and the inside IP address of the server in **Menu 15, Multiple Server Configuration**.

Please note that the default filters protect the services running on the P314 (web, telnet, ftp, etc). These services are NOT protected by the SUA! Moreover, SUA protection is compromised once servers are specified in menu 15.

```
             Menu 15 - Multiple Server Configuration

          Port #                  IP  Address
          ----                    ---------------
        1.Default                 0.0.0.0
        2. 0                      0.0.0.0
        3. 0                      0.0.0.0
        4. 0                      0.0.0.0
        5. 0                      0.0.0.0
        6. 0                      0.0.0.0
        7. 0                      0.0.0.0
        8. 0                      0.0.0.0
        9. 0                      0.0.0.0
       10. 0                      0.0.0.0
       11. 0                      0.0.0.0
       12. 1026                   RR Reserved
             Press ENTER to Confirm or ESC to Cancel:
```

Figure 6-3   Menu 15

**For more information on configuring supporting applications behind SUA refer to the
ZyNOS Support Note documentation on your Support Disc.**

6.2.1 Configuring a Server behind SUA

Follow the steps below to configure a server behind SUA:

Step 1   Enter 15 in the Main Menu to go to **Menu 15 – Multiple Server Configuration.**

Step 2   Enter the service port number in the **Port #** field and the inside IP address of the server in the **IP Address** field.

Step 3   Press [ENTER] at the "Press ENTER to confirm …" prompt to save your configuration after you define all the servers or press ESC at any time to cancel.

The most often used port numbers are:

Table 6-2   Services vs. Port number

Services	Port Number
FTP (File Transfer Protocol)	21
Telnet	23
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol, version 3)	110
PPTP (Point-to-Point Tunneling Protocol)	1723

Part III:

Advanced Management

Chapters 7 – 11 provide information on Prestige Filtering, System Information and Diagnosis, Transferring Files and Telnet.

<div align="right">

Chapter 7
Filter Configuration
</div>

<div align="right">

This chapter shows you how to create and apply filter(s).
</div>

7.1   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 LAN 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 **PPPoE** encapsulation. Outgoing packets must undergo data filtering before they encounter call filtering as shown in the following figure.
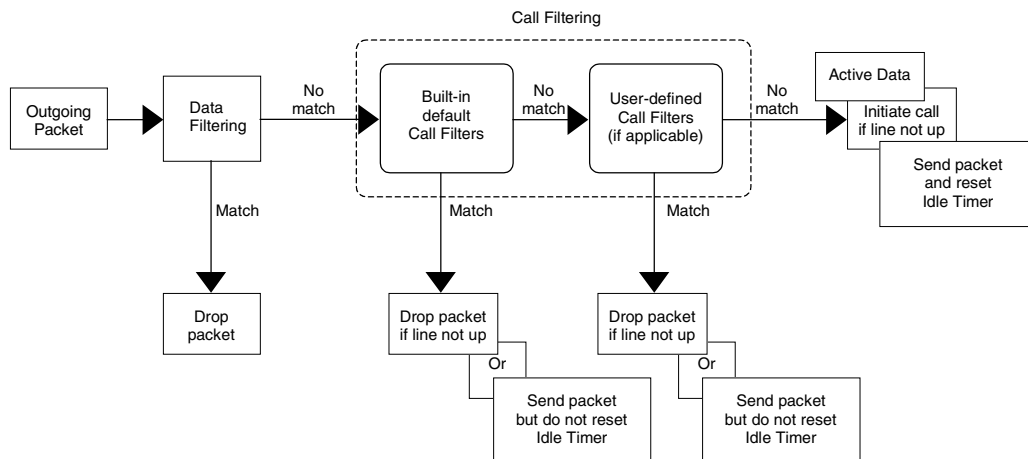
Figure 7-1   Outgoing Packet Filtering Process

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.

7.1.1 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 <u>cannot</u> 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.

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

The following diagram illustrates the logic flow when executing a filter rule.
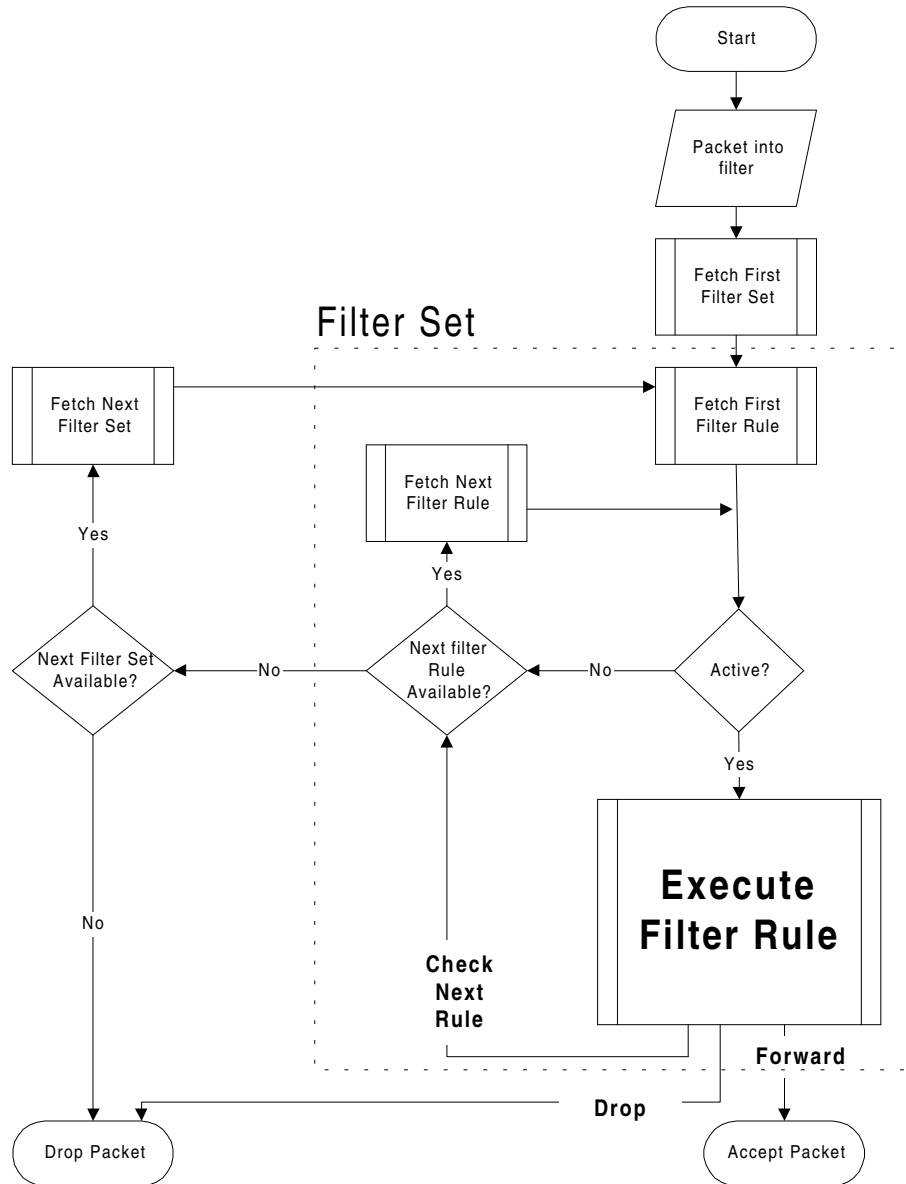
Figure 7-2   Filter Rule Process

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.

7.2 Configuring a Filter Set

To configure a filter set, follow the procedure below.

Step 1. Select option **21. Filter Set Configuration** from the Main Menu to open **Menu 21.1**

```
                    Menu 21 - Filter Set Configuration

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


                  Enter Filter Set Number to Configure= 0

                  Edit Comments= N/A

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

Figure 7-3   Menu 21 – Filter Set Configuration

Step 2. Select the filter set you wish to configure (no. 1-12) and press [ENTER].
Step 3. Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].
Step 4. Press [ENTER] at the message: [Press ENTER to confirm] to open **Menu 21.1 – Filter Rules Summary**.

```
                   Menu 21.1 - Filter Rules Summary

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


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



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

Figure 7-4   NetBIOS_WAN Filter Rules Summary

```
                   Menu 21.2 - Filter Rules Summary

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

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

Figure 7-5   NetBIOS _LAN Filter Rules Summary

```
                   Menu 21.3 - Filter Rules Summary

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

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

Figure 7-6   Tel_FTP_Web_WAN Filter Rules Summary

7.2.1 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 7-1   Abbreviations Used in the Filter Rules Summary Menu

Abbreviations	Description	Display
#	Refers to the filter rule number (1-6).	
A	Shows whether the rule is active or not.	[Y] means the filter rule is active. [N] means the filter rule is inactive.
Type	Refers to the type of filter rule. This shows GEN for generic, or IP for TCP/IP	[GEN] for Generic. [IP] for TCP/IP.
Filter Rules	The filter rule parameters will be displayed here (see below).	
M	Refers to **More**. More in a set behaves like a logical AND i.e., the set is only matched if ALL rules in it are matched. [Y] means an action can not yet be taken as there are more rules to check, which are concatenated with the present rule to form a rule chain. When the rule chain is complete an action can be taken. [N] means you can now 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. If More is **Yes**, then **Action Matched** and **Action Not Matched** will be **N/A.**	[Y] means there are more rules to check. [N] means there are no more rules to check.
m	Refers to **Action Matched**. [F] means to forward the packet immediately and skip checking the remaining rules.	[F] means to forward the packet. [D] means to drop the packet. [N] means check the next rule.
n	Refers to **Action Not Matched.** [F] means to forward the packet immediately and skip checking the remaining rules.	[F] means to forward the packet. [D] means to drop the packet. [N] means check the next rule.

The protocol dependent filter rules abbreviation are listed as follows:

● If the filter type is IP, the following abbreviations listed in the following table will be used.

Table 7-2   Abbreviations Used If Filter Type Is IP

Abbreviation	Description
Pr	Protocol
SA	Source Address
SP	Source Port number
DA	Destination Address
DP	Destination Port number

● If the filter type is GEN (generic), the following abbreviations listed in the following table will be used.

Table 7-3   Abbreviations Used If Filter Type Is GEN

Abbreviation	Description
Off	Offset
Len	Length

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

7.2.2 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.

7.2.3 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 a TCP/IP rule, select TCP/IP Filter Rule from the Filter Type field and press [ENTER] to open **Menu 21.1.1 – TCP/IP Filter Rule**, as shown below.

```
            Menu 21.1.1 - TCP/IP Filter Rule

        Filter #: 1,1
        Filter Type= TCP/IP Filter Rule
        Active= Yes
        IP Protocol= 6      IP Source Route= No
        Destination: IP Addr= 0.0.0.0
                     IP Mask= 0.0.0.0
                     Port #= 137
                     Port # Comp= Equal
             Source: IP Addr= 0.0.0.0
                     IP Mask= 0.0.0.0
                     Port #=
                     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.
```

Figure 7-7   Menu 21.1.1.1 – TCP/IP Filter Rule

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

Table 7-4   TCP/IP Filter Rule Menu Fields

Field	Description	Option
Active	This field activates/deactivates the filter rule.	**Yes/No**
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.	**Yes/No**
Destination: IP Addr	Enter the destination IP Address of the packet you wish to filter. This field is disregarded if it is 0.0.0.0.	IP address
Destination: IP Mask	Enter the IP mask to apply to the Destination: IP Addr.	IP mask
Destination: Port #	Enter the destination port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is disregarded if it is 0.	0-65535
Destination: Port # Comp	Select the comparison to apply to the destination port in the packet against the value given in Destination: Port #.	**None/Less/Greater/ Equal/Not Equal]**

Field	Description	Option
Source: IP Address	Enter the source IP Address of the packet you wish to filter. This field is disregarded if it is 0.0.0.0.	IP Address
Source: IP Mask	Enter the IP mask to apply to the Source: IP Addr.	IP Mask
Source: Port #	Enter the source port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is disregarded if it is 0.	0-65535
Source: Port # Comp	Select the comparison to apply to the source port in the packet against the value given in Source: Port #.	**None/Less/Greater/ Equal/Not Equal**
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**
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 More is **Yes**, then Action Matched and Action Not Matched will be **N/A**.	**Yes/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** **Action Not Matched** **Both**
Action Matched	Select the action for a matching packet.	**Check Next Rule** **Forward** **Drop**
Action Not Matched	Select the action for a packet not matching the rule.	**Check Next Rule** **Forward** **Drop**
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 diagram illustrates the logic flow of an IP filter.

Packet
into IP Filter

Filter Active? — No

Yes

Apply SrcAddrMask
to Src Addr

Check Src
IP Addr — Not Matched

Matched

Apply DestAddrMask
to Dest Addr

Check Dest
IP Addr — Not Matched

Matched

Check
IP Protocol — Not Matched

Matched

Check Src &
Dest Port — Not Matched

Matched

More? — Yes

No

Action Matched

Action Not Matched

Check Next Rule

Check Next Rule

Drop   Forward

Drop   Forward

Drop Packet

Check Next Rule

Accept Packet

Figure 7-8   Executing an IP Filter

7.2.4 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 **Menu 21.4.1** and press [ENTER] to open 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.
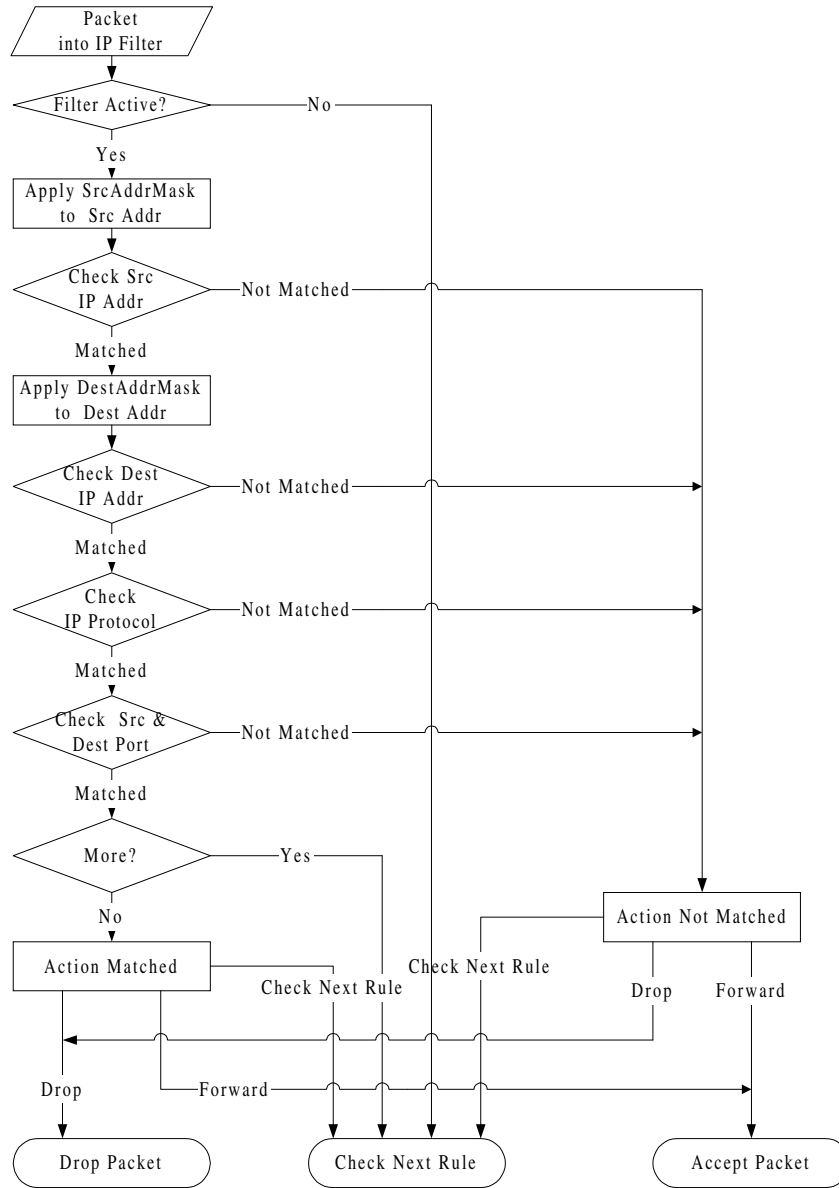```

**Figure 7-9        Menu 21.4.1 – Generic Filter Rule**

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

**Table 7-5        Generic Filter Rule Menu Fields**

| Field | Description | Option |
|---|---|---|
| Filter # | This is the filter set, filter rule coordinates, i.e., 2,3 refers to the second filter set and the third rule of that set. | |
| Filter Type | Use the [SPACE BAR] to toggle between both types of rules. Parameters displayed below each type will be different. | **Generic Filter Rule/ TCP/IP Filter Rule** |
| Active | Select **Yes** to turn on the filter rule. | **Yes/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. | Default = 0 |
| 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. | Default = 0 |
| 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 More is **Yes**, then Action Matched and Action Not Matched will be **No**. | **Yes/No** |
| Log | Select the logging option from the following:<br>● **None** – No packets will be logged.<br>● **Action Matched** – Only packets that match the rule parameters will be logged.<br>● **Action Not Matched** – Only packets that do not match the rule parameters will be logged.<br>● **Both** – All packets will be logged. | **None**<br><br>**Action Matched**<br><br>**Action Not Matched**<br><br>**Both** |
| Action Matched | Select the action for a matching packet. | **Check Next Rule**<br><br>**Forward**<br><br>**Drop** |
| Action Not Matched | Select the action for a packet not matching the rule. | **Check Next Rule**<br><br>**Forward**<br><br>**Drop** |

> 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**.

## 7.3 Example Filter

Let's look at the first rule in the third default ZyXEL filter set, TELNET_FTP_Web_WAN (*see Figure* 7-6) as an example. Please see our PNC Disk for more example filters. This filter is designed to block outside users telnetting into the Prestige.
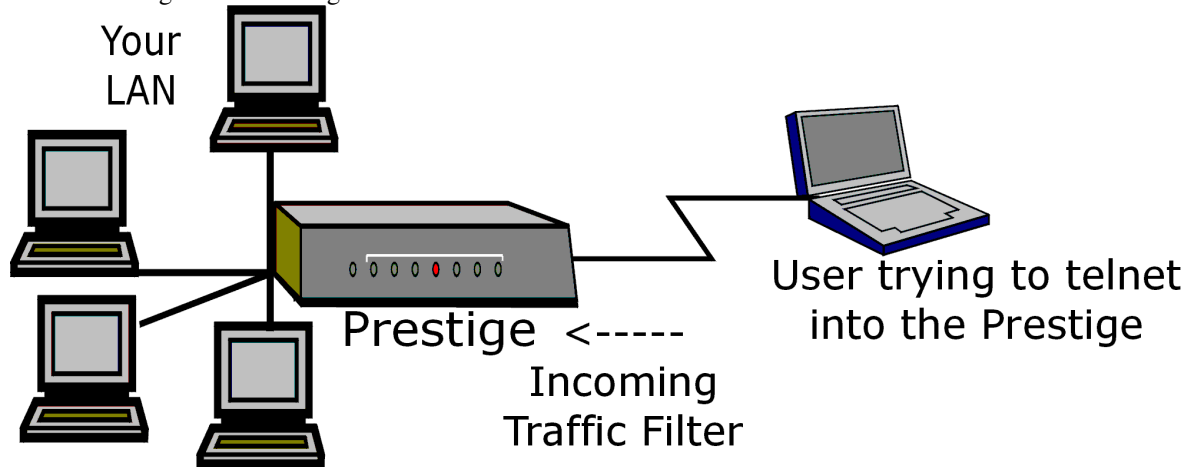


**Figure 7-10     Telnet Filter Example**

**Step 1.**   Enter **21** from the Main Menu to open **Menu 21 – Filter Set Configuration**.

**Step 2.**   Enter the index of the filter set you wish to configure (in this case, 3) and press [ENTER].

**Step 3.**   Enter a descriptive name or comment in the **Edit Comments** field (in this case TELNET_FTP_Web_WAN) and press [ENTER].

**Step 4.**   Press [ENTER] at the message: [Press ENTER to confirm] to open **Menu 21.3.1 – Filter Rules Summary**.

**Step 5.**   Enter **1** to configure the first filter rule (the only filter rule of this set). Make the entries in this menu as shown in the following figure.

```
                Menu 21.3.1 - TCP/IP Filter Rule

        Filter #: 3,1
        Filter Type= TCP/IP Filter Rule
        Active= Yes
        IP Protocol= 6        IP Source Route= No
        Destination: IP Addr= 0.0.0.0
                     IP Mask= 0.0.0.0
                     Port #= 23
                     Port # Comp= Equal
             Source: IP Addr= 0.0.0.0
                     IP Mask= 0.0.0.0
                     Port #= 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 the [SPACE BAR] to choose this filter rule type. The first filter rule type determines all subsequent filter types within a set.

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

6 is the TCP protocol.

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

No more rules to check to block telnet.

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

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

Select **Check Next Rule** here so that the next rule is checked if the destination is not the telnet port.

Figure 7-11   Example Filter

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

```
                    Menu 21.3 - Filter Rules Summary

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



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

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

M = N means an action can be taken immediately, i.e., we don't need more rules to block telnet. The action is to drop the packet if the action is matched (**m = D**) and the next rule is checked (**n = N**) if the action is not matched.

Figure 7-12   Example Filter Rules Summary – Menu 21.3

Configure the next filter rules in this set in the same way. After you've created the filter set, you must apply it.

Step 1.   Enter **11** from the main menu to go to Menu 11.

Step 2.   Go to the **Edit Filter Sets** field, press the [SPACE BAR] to toggle **Yes** to **No** and press [ENTER].

Step 3.   This brings you to Menu 11.5. Apply the TELNET_FTP_Web_WAN filter set (filter set 3) as shown in *Figure 7-15*.

Step 4.   Press [ENTER] to confirm after you enter the set numbers and to leave Menu 11.5.

7.4   Filter Types and SUA

There are two classes of filter rules, **Generic Filter** (Device) rules and Protocol Filter (**TCP/IP**) rules. Generic Filter rules act on the raw data from/to LAN and WAN. Protocol Filter rules act on the IP packets. Generic and TCP/IP filter rules are discussed in more detail in the next section. When SUA (Single User Account) 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 SUA for outgoing packets and after

SUA 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 diagram illustrates this.
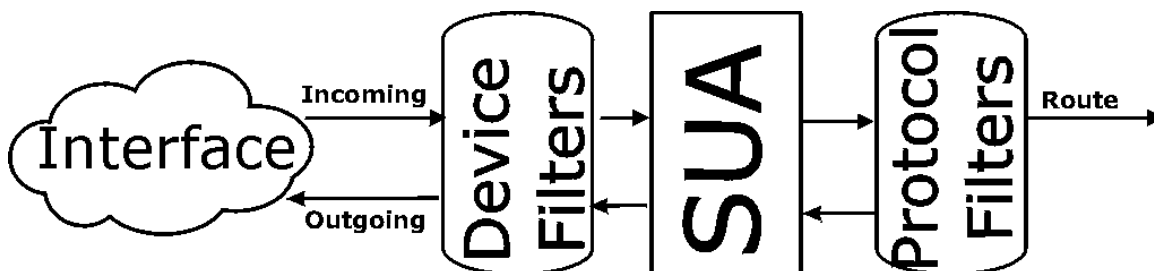
Figure 7-13   Protocol and Device Filter Sets

7.5   Applying a Filter and Factory Defaults

This section shows you where to apply the filter(s) after you design it (them). Sets of factory default filter rules have been configured in Menu 21 to prevent NetBIOS traffic from triggering calls, and block incoming telnet, FTP and HTTP connections.

7.5.1 LAN Traffic

LAN traffic filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to **Menu 3.1** (shown next) 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. The factory default set, NetBIOS_LAN, can be inserted in **protocol filters –**field under **Input Filter Sets** in **Menu 3.1** to block NetBIOS traffic to the Prestige from the LAN.

```
             Menu 3.1 – LAN Port Filter Setup

        Input Filter Sets:
          protocol filters= 2
             device filters=
        Output Filter Sets:
          Protocol filters=
             device filters=


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

Apply
Default Filter
2 here.
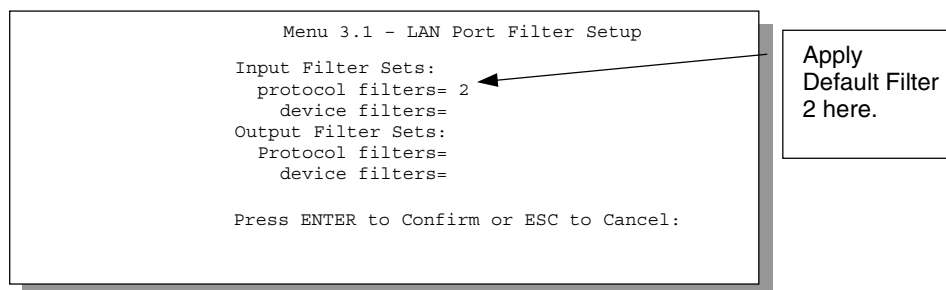
Figure 7-14   Filtering LAN Traffic

7.5.2 Remote Node Filters

Go to Menu 11.5 (shown below – 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. The factory default filter set, NetBIOS_WAN, can be applied in Menu 11.5 to block local NetBIOS traffic from triggering calls to the ISP (when you are using **PPPoE** encapsulation only). Enter "1" in the **protocol filters** field under **Call Filter Sets** when using PPPoE encapsulation and in **protocol filters** under **Output Filter Sets – protocol filters** when using Ethernet encapsulation. Filter set "3", Telnet_WAN, blocks telnet connections from the WAN Port to help prevent security breaches. Filter set "4", FTP_WAN, blocks FTP connections from the WAN Port. Apply them as shown in the following figure.

```
                   Menu 11.5 - Remote Node Filter

           Input Filter Sets:
             protocol filters= 3
                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:
```

Apply Default Filters 1 and 3 here. Enter 1 in **protocol filters** under **Output Filter Sets** when using Ethernet encapsulation and under **Call Filter Sets** when using PPPoE Encapsulation**.**

Figure 7-15   Filtering Remote Node Traffic

Chapter 8
System Information and Diagnosis

This chapter talks you through 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. This chapter describes how to use these tools in detail.

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.  Firmware Upload
            8.  Command Interpreter Mode
            9.  Call Control




                Enter Menu Selection Number:
```
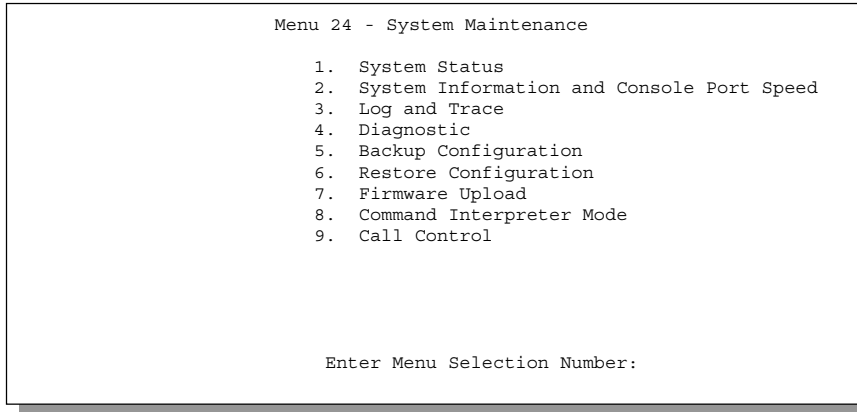
Figure 8-1   Menu 24 – System Maintenance

8.1   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 figure below. 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.

To get to the System Status:

Step 1:   Enter number 24 to go to Menu 24 – System Maintenance.

Step 2:   In this menu, enter number 1 to open **System Maintenance – Status**.

Step 3:   There are three commands in **Menu 24.1 – System Maintenance – Status**. Entering 1 drops the 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. The upper right corner of the screen shows the time and date according to the format you set in Menu 24.10.

```
                       Menu 24.1 - System Maintenance - Status
 Port   Status        TxPkts    RxPkts     Cols    Tx B/s   Rx B/s    Up Time
   WAN  10M/Half          67       289        0        74       64    2:20:56
   LAN  10M/Half         299       220        0        74       64    2:20:54

 Port    Ethernet Address     IP Address              IP Mask      DHCP
   WAN   00:a0:c5:21:8c:a3    x.y.155.97          255.255.255.0    Client
   LAN   00:a0:c5:21:8c:a2    192.168.1.1         255.255.255.0    Server


    System up Time:    2:21:02

    Name: 314.baboo.zyxel.com
    Routing: IP
    ZyNOS F/W Version: V3.20(CA.0)b3 | 6/12/2000

                      Press Command:

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

Figure 8-2   Menu 24.1 – System Maintenance – Status

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

Table 8-1   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.
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= 314; Domain Name= baboo.zyxel.com Name= 314.baboo.zyxel.com
ZyNOS F/W Version	The ZyNOS Firmware version and the date created.

8.2   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:

Step 4:   Enter **24** to go to **Menu 24 – System Maintenance**.

Step 5:   Enter **2** to open, **Menu 24.2** – **System Information and Console Port Speed**.

Step 6:   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 8-3   Menu 24.2 – System Information and Console Port Speed

8.2.1   System Information

System Information gives you information about your system as shown below. More specifically, it gives you information on your routing protocol, Ethernet address, IP address, etc.

```
                    Menu 24.2.1 - System Maintenance - Information
                         Name: xxx.baboo.mickey.com
                         Routing: IP
                         ZyNOS F/W Version: V3.20(CA.0)b3 | 6/12/2000




                         LAN
                           Ethernet Address: 00:a0:c5:21:8c:a2
                           IP Address: 192.168.1.1
                           IP Mask: 255.255.255.0
                           DHCP: Server



                         Press ESC or RETURN to Exit
```

Figure 8-4   Menu 24.2.1 – System Maintenance – Information

Table 8-2   Fields in System Maintenance

Field	Description
Name	This is the Prestige's system name + domain name assigned in Menu 1. E.G., System Name= xxx; Domain Name= baboo.mickey.com; Name= xxx.baboo.mickey.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 IP mask of the Prestige.
DHCP	This field shows the DHCP setting of the Prestige.

8.2.2 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. Use the [SPACE BAR] to select the desired speed in **Menu 24.2.2**, as shown below.

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

                   Console Port Speed: 115200




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

Figure 8-5   Menu 24.2.2 – System Maintenance – Change Console Port Speed

8.3   Log and Trace

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

8.3.1 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 open **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 8-6   Examples of Error and Information Messages

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

```
 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 8-7   Examples of Error and Information Messages

8.3.2 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 – UNIX Syslog** as shown next.

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

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

                 Types:
                 CDR= No
                 Packet triggered= No
                 Filter log= No
                 PPP log= No
               Press ENTER to Confirm or ESC to Cancel:
 Press Space Bar to Toggle.
```

Figure 8-8   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 8-3   System Maintenance Menu Syslog Parameters

Parameter	Description
UNIX Syslog:	
Active	Press the [SPACE BAR] to turn on or off syslog.
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.
Types:	
CDR	Call Detail Record (CDR) logs all data phone line activity if set to **Yes**.
Packet triggered	The first 48 bytes or octets and protocol type of the triggering packet is sent to the UNIX syslog server when this field is set to **Yes**.
Filter log	No filters are logged when this field is set to **No**. Filters with the individual filter Log Filter field set to **Yes** (Menu 21.x.x) are logged when this field is set to **Yes**.
PPP log	PPP events are logged when this field is set to **Yes**.

Your Prestige sends four types of syslog messages. Some examples (not P314 specific) of these syslog messages with their message formats are shown next:

1. CDR

CDR Message Format

SdcmdSyslogSend(SYSLOG_CDR, SYSLOG_INFO, String);
String = board xx line xx channel xx, call xx, str
board = the hardware board ID
line = the WAN ID in a board
Channel = channel ID within the WAN
call = the call reference number which starts from 1 and increments by 1 for each new call
str = C01 Outgoing Call dev xx ch xx (dev:device No. ch:channel No.)
            L02   Tunnel Connected(L2TP)
            C02 OutCall Connected xxxx (means connected speed) xxxxx (means Remote Call Number)
 	
            L02 Call Terminated
            C02 Call Terminated

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

2. Packet triggered

Packet triggered Message Format

sdcmdSyslogSend(SYSLOG_PKTTRI, SYSLOG_NOTICE, String);
            String = Packet trigger: Protocol=xx Data=xxxxxxxxxx…..x
            Protocol: (1:IP 2:IPX 3:IPXHC 4:BPDU 5:ATALK 6:IPNG)
            Data: We will send forty-eight Hex characters to the server

```
Jul 19 11:28:39 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=4500003c100100001f010004c0a86614ca849a7b08004a5c0200010061626364656667686696a6b6c6d6e6f
7071727374
Jul 19 11:28:56 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600220008cd40000020405
b4
Jul 19 11:29:06 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=45000028240140001f06ac12c0a86614ca849a7b0427001700195b451d143013500400007760000
```

3. Filter log

Filter log Message Format

SdcmdSyslogSend(SYSLOG_FILLOG, SYSLOG_NOTICE, String);
String = IP[Src=xx.xx.xx.xx Dst=xx.xx.xx.xx prot spo=xxxx dpo=xxxx] S04>R01mD
 	
IP[…] is the packet header and S04>R01mD means filter set 4 (S) and rule 1 (R), match (m) drop (D).
            Src: Source Address
            Dst: Destination Address
            prot: Protocol ("TCP", "UDP", "ICMP")
spo: Source port
dpo: Destination port

```
Mar 03 10:39:43 202.132.155.97 ZyXEL:
GEN[ffffffffffffnordff0080] }S05>R01mF
Mar 03 10:41:29 202.132.155.97 ZyXEL:
GEN[00a0c5f502fnord010080] }S05>R01mF
Mar 03 10:41:34 202.132.155.97 ZyXEL:
IP[Src=192.168.2.33 Dst=202.132.155.93 ICMP]}S04>R01mF
Mar 03 11:59:20 202.132.155.97 ZyXEL:
GEN[00a0c5f502fnord010080] }S05>R01mF
Mar 03 12:00:31 202.132.155.97 ZyXEL:
GEN[ffffffffffffnordff0080] }S05>R01mF
Mar 03 12:00:52 202.132.155.97 ZyXEL:
GEN[ffffffffffff0080] }S05>R01mF
Mar 03 12:00:57 202.132.155.97 ZyXEL:
GEN[00a0c5f502010080] }S05>R01mF
Mar 03 12:01:01 202.132.155.97 ZyXEL:
IP[Src=192.168.2.33 Dst=202.132.155.93 TCP spo=01170  dpo=00021]}S04>R01mF
Mar 03 12:01:06 202.132.155.97 ZyXEL:
IP[Src=192.168.2.33 Dst=202.132.155.93 TCP spo=01170  dpo=00021]}S04>R01mF
```

4. PPP log

PPP log Message Format
sdcmdSyslogSend(SYSLOG_PPPLOG, SYSLOG_NOTICE, String);
String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto Shutdown
Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP / IPXCP

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

8.3.3 Call-Triggering Packet

Call-Triggering Packet displays information about the packet that triggered the dial-out call in an easy readable format (for PPPoE Encapsulation only). Equivalent information is available in **Menu 24.1** in hex format. An example is shown next.

```
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 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 8-9   Call-Triggering Packet Example

8.4   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 8-10   Menu 24.4 – System Maintenance – Diagnostic

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

Step 1. From the Main Menu, select option 24 to open **Menu 24 – System Maintenance**.

Step 2. From this menu, select option 4. This will open **Menu 24.4 – System Maintenance – Diagnostic**.

8.4.1 WAN DHCP

DHCP functionality can be enabled on the LAN or WAN as shown in *Figure 8-11*. LAN DHCP has already been discussed previously. 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 renew the assigned WAN IP address, subnet mask and default gateway in a fashion similar to winipcfg.
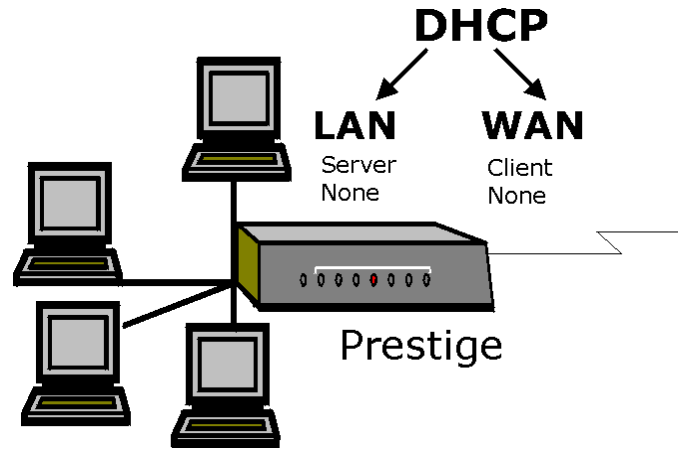
Figure 8-11   WAN & LAN DHCP

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

Table 8-4   System Maintenance Menu Diagnostic

Selection 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 your Internet Setup. You can also test this after configuring **Menu 4 – Internet Access Setup**.
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 9
Transferring Files

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

9.1 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 name of P314.ROM or similar. Once you have customized the Prestige's setting, they can be saved back to PC/workstation under a filename of your choosing. Choose something meaningful, e.g., "MyP314.cfg".

The ZyNOS firmware file (sometimes referred to as the ras file) is the file that contains the ZyXEL Network Operating System firmware and usually is the router model name with a *.bin extension, e.g., P314.bin.

With serial (XMODEM) transfer, the filenames on the PC are your choice. With many ftp and tftp clients, they are as well as seen next.

```
ftp> put P314.bin ras
```
This is a sample ftp session showing the transfer of the PC file "P314.bin" to the Prestige.

```
ftp> get rom-0 MyP314.cfg
```
This is a sample ftp session saving the current configuration to the PC file MyP314.cfg.

If your [t]ftp client does <u>not</u> allow you 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 to 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 <u>not </u>on the Prestige, i.e., on your workstation, local network or ftp site and so the name (but not the extension) will vary. The AT command is the command you enter after you press "Y" when prompted in the SMT menu to go into debug mode. After uploading new firmware see the **ZyNOS F/W Version** field in **Menu 24.2.1** (Figure 8-4   Menu 24.2.1 – System Maintenance – Information) to check you have uploaded the correct firmware version.

Table 9-1   Filename Conventions

File Type	Internal Name	External Name	Description	AT Command
Configuration File	Rom-0	*.rom	This is the router 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 baud rate and default password), the error log and the trace log.	ATLC
Firmware	Ras	*.bin	This is the generic name for the ZyNOS firmware on the Prestige.	ATUR

9.1.1 Firmware Development

It is important to upgrade your firmware regularly, especially if there are problems. If you discover an unexpected behavior, or bug, see if your problem is mentioned in the release notes. Load it according to instructions (e.g., see if the default configuration file is needed also). If the problem still exists, e-mail or call tech support.

9.2   Backup Configuration

Option 5 from **Menu 24 – System Maintenance** allows you to backup the current Prestige configuration to your workstation. Backup is highly recommended once your Prestige is functioning properly. FTP and TFTP are the preferred methods for backing up your current workstation 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 9.1*).

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

The following screen is what you see in Menu 24.5 when connected to the Prestige via console port.

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

Figure 9-1   Menu 24.5 – System Maintenance – Backup Configuration (Console Port)

The following screen is what you see in Menu 24.5 when you telnet into the Prestige.

```
             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.
```

Figure 9-2   Menu 24.5 – System Maintenance – Backup Configuration (Telnet)

9.3   Restore Configuration

Menu 24.6 -– System Maintenance – Restore Configuration allows you to restore the configuration via the console port.

FTP and TFTP are the preferred methods for restoring your current workstation configuration to your Prestige since FTP and TFTP are faster. Please note that the system reboots automatically after the file transfer is complete. The following screen is what you see in Menu 24.5 when connected to the Prestige via console port.

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

Figure 9-3   Menu 24.6 – System Maintenance – Restore Configuration (Console Port)

The following screen is what you see in Menu 24.5 when you telnet into the Prestige.

```
            Menu 24.6 -- System Maintenance - Restore Configuration

To transfer the firmware and configuration file, follow the procedure
below:

1. Launch the FTP client on your 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 9-4   Menu 24.6 – System Maintenance – Restore Configuration (Telnet)

9.4   Upload Firmware

Menu 24.7 -– System Maintenance – Upload Firmware allows you to upgrade the firmware and the configuration file via the console port. There are two components in the system: the router firmware and the configuration file, as shown below.

```
        Menu 24.7 -- System Maintenance - Upload Firmware

            1. Upload Router Firmware
            2. Upload Router Configuration File



                Enter Menu Selection Number:
```

Figure 9-5   Menu 24.7 – System Maintenance – Upload Firmware

9.4.1 Uploading the Router Firmware

Menu 24.7.1 shows you the instructions for uploading the router firmware. Follow the procedure below to upload the file:

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

Step 2.   Enter atur after Enter Debug Mode message.

Step 3.   Wait for the Starting XMODEM upload message before activating Xmodem upload on your terminal.

Step 4.   After successful firmware upload, enter atgo to restart the Prestige.

```
        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 9-6   Menu 24.7.1 – System Maintenance – Upload Router Firmware

The screen for Menu 24.7.1 when you telnet into the Prestige (*see Figure 9-8)* is the same except for the following additional message.

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

9.4.2 Uploading Router Configuration File

The configuration data, system-related data, the error log and the trace log are all stored in the configuration file. Please be aware that uploading the configuration file replaces everything contained within.

> Menu 24.6 **replaces the current configuration with your customized configuration you backed up previously.** Menu 24.7.2 **shows you the instructions for uploading the Router Configuration file that replaces the current configuration file with the default configuration file, i.e., P314.rom. You will lose all configurations that you had before and the speed of the console port will be reset to the default of 9600 bps with 8 data bit, no parity and 1 stop bit (8n1). You will need to change your serial communications software to the default before you can connect to the Prestige again. The password will be reset to the default of 1234, also.**

Follow the procedure below to upload the configuration file:

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

Step 2. Enter `atlc` after the `Enter Debug Mode` message.

Step 3. Wait for the `Starting XMODEM upload` message before activating Xmodem upload on your terminal.

Step 4. After successful firmware upload, enter `atgo` to restart the Prestige.

```
    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 9-7   Menu 24.7.2 – System Maintenance – Upload Router Configuration File

The screen for Menu 24.7.2 when you telnet into the Prestige (*see Figure 9-9*) is the same except for the following additional message.

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

9.5   TFTP File Transfer

In addition to the direct console port connection, 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 workstation must have both telnet and TFTP clients. To transfer the firmware and the configuration file, follow the next procedure:

Step 1.   Use telnet from your workstation 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 workstation 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 workstation. The file name for the firmware is `ras` and for the configuration file, is `rom-0` (rom-zero, not capital o).

Note: If you upload the firmware to the Prestige, it will reboot automatically when the file transfer is completed (the SYS LED will flash).

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 workstation, "put" the other way around, and "binary" to set binary transfer mode.

9.5.1 Example TFTP Command

The following is an example tftp command:

`TFTP [-i] host put p314.bin ras`

where "i" specifies binary image transfer mode (use this mode when transferring binary files), "host" is the Prestige IP address, "put" transfers the file source on the workstation (p314.bin – name of the firmware on the workstation) to the file destination on the remote host (ras – name of the firmware on the Prestige).

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

Table 9-2   Third Party TFTP Clients –General fields

Host	Enter the IP address of the Prestige. 192.168.1.1 is the Prestige default IP address when shipped.
Send/Fetch	Press "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.

TFTP over WAN will not work if:

1. You have applied a filter in Menu 3.1 (LAN) or in Menu 11.5 (WAN) to block Telnet service.

2. You have an SMT console session running.

9.6 FTP File Transfer

In addition to uploading the firmware and configuration via the console port and TFTP client, you can also upload the Prestige firmware and configuration files using FTP. To use this feature, your workstation 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 Router Firmware


   To upload the router firmware, 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 firmwarefilename ras" where "firmwarefilename" is the name
   of your firmware upgrade file on your workstation and "ras" is the
   remote file name on the router.
   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 router firmware using TFTP (note
   that you must remain on this menu to upload router firmware using TFTP),
   please see your router manual.


                        Press ENTER to Exit:
```
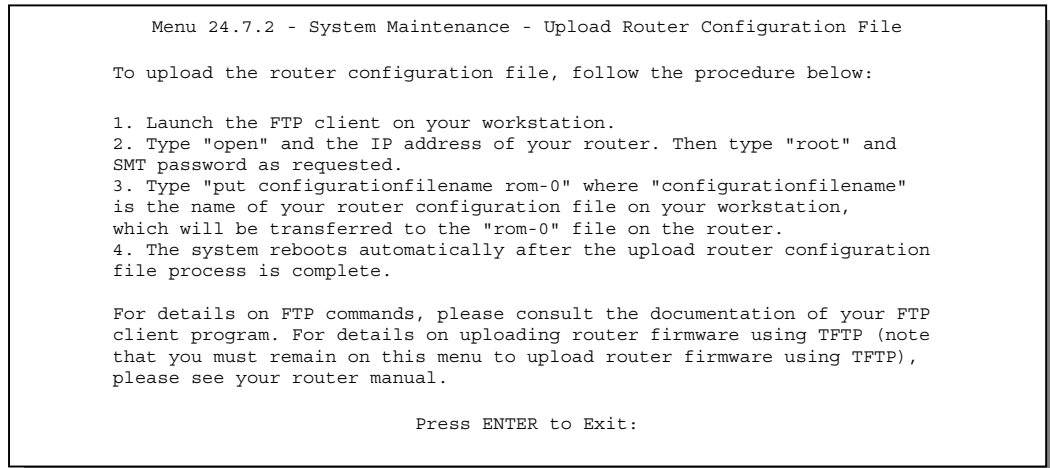
Figure 9-8   Telnet into Menu 24.7.1

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

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

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

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

                        Press ENTER to Exit:
```

Figure 9-9   Telnet into Menu 24.7.2 – System Maintenance

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

9.6.1 Using the FTP Command from the DOS Prompt

Step 1.   Launch the FTP client on your workstation.

Step 2.   Type open and the IP address of your Prestige.

Step 3.   You may press [ENTER] when prompted for a username.

Step 4.   Type root and your SMT password as requested. The default is 1234.

Step 5.   Type bin to set transfer mode to binary.

Step 6.   Use "put" to transfer files from the workstation to the Prestige, e.g., put p314.bin ras transfers the firmware on your computer (p314.bin) to the Prestige and renames it "ras". Similarly put p314.rom rom-0 transfers the configuration file on your computer (p314.rom) to the Prestige and renames it "rom-0". See *section 9.1* for more information on filename conventions.

Step 7.   Type quit to exit the ftp prompt.

```
Connected to 314.x.x.x
220 P314 FTP version 1.0 ready at Thu Jan 20 18:00:02 2000
User (314.x.x.x:(none)): <Enter>
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put p314e.bin ras
200 Port command okay
150 Opening data connection for STOR ras
226 File received OK
ftp: 327680 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

Figure 9-10   FTP Session Example

The system reboots after a successful upload.

The following table describes some of the fields that you may see in third party FTP clients.

Table 9-3   Third Party FTP Clients – General fields

Host Address	Enter the address of the host server.	Parameters for Prestige
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.	Normal
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode.	Binary
Initial Remote Directory	Specify the default remote directory (path).	
Initial Local Directory	Specify the default local directory (path).	

Please note that FTP over WAN will not work if you have applied a filter in Menu 11.5 to block FTP service from the WAN.

Chapter 10
System Maintenance & Information

This chapter leads you through SMT menus 24.8 to 24.9
and also discusses bootbase commands.

10.1 Command Interpreter Mode

This option allows you to enter command interpreter mode, a "DOS prompt" type command interface, which allows more advanced system diagnosis and troubleshooting (beyond the scope of this guide). See our PNC supporting disk or the ZyXEL web site at www.zyxel.com 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 Upload
                    8.  Command Interpreter Mode
                    9.  Call Control




                    Enter Menu Selection Number:
```

Figure 10-1   Command Mode in Menu 24

```
             Copyright (c) 1994 - 2000 ZyXEL Communications Corp.
             ras> ?
             Valid commands are:
             sys           exit          device        ether
             poe           ip            ppp           hdap
             ras>
```

Figure 10-2   Valid Commands

10.2 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 **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. Call Control** 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:
```
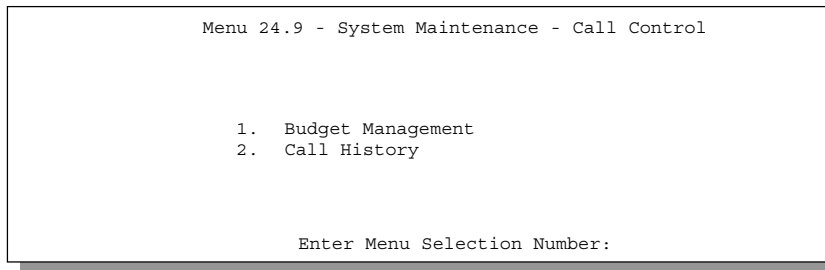
Figure 10-3   Call Control

10.2.1 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):
```
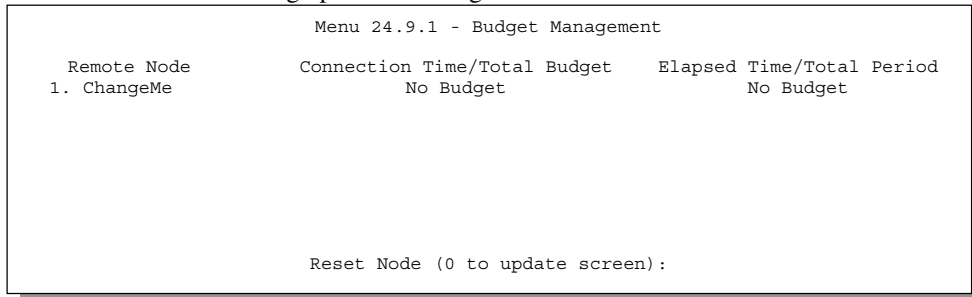
Figure 10-4   Budget Management

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 10-1   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 gone by.
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 gone by.

10.2.2 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 10-5   Call History

Table 10-2   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.

10.3 Boot Commands

When you reboot your Prestige, you will be 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) already discussed in *Chapter 9*.

```
Bootbase Version: V1.05 | 4/14/2000 13:58:03
RAM: Size = 4096 Kbytes
FLASH: Intel 8M

ZyNOS Version: V3.20(CA.0)b3 | 6/12/2000 18:00:34

Press any key to enter debug mode within 3 seconds.
..................................................
```

Figure 10-6   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
ATWBx,y         write address x with  8-bit value y
ATWWx,y         write address x with 16-bit value y
ATWLx,y         write address x with 32-bit value 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
AT%Tx           Enable Hardware Test Program at boot up
ATBTx           block0 write enable (1=enable, other=disable)
ATRTw,x,y(,z)   RAM test level w, from address x to y (z iterations)
ATWEa(,b,c,d)   write MAC addr, Country code, EngDbgFlag, FeatureBit to flash ROM
ATCUx           write Country code to flash ROM
ATCB            copy from FLASH ROM to working buffer
ATCL            clear working buffer
ATSB            save working buffer to FLASH ROM
ATBU            dump manufacturer related data in working buffer
ATSH            dump manufacturer related data in ROM
ATWMx           set MAC address in working buffer
ATCOx           set country code in working buffer
ATFLx           set EngDebugFlag in working buffer
ATSTx           set ROMRAS address in working buffer
ATSYx           set system type in working buffer
ATVDx           set vendor name in working buffer
ATPNx           set product name in working buffer
ATFEx,y,...     set feature bits in working buffer
ATMP            check & dump memMapTab
ATDOx,y         download from address x for length y to PC via XMODEM
ATTD            download router configuration to PC via XMODEM
ATUPx,y         upload to RAM address x for length y from PC via XMODEM
ATUR            upload router firmware to flash ROM
ATLC            upload router configuration file to flash ROM
ATUXx(,y)       xmodem upload from flash block x to y
ATERx,y         erase flash rom from block x to y
ATWFx,y,z       copy data from addr x to flash addr y, length z
ATXSx           xmodem select: x=0: CRC mode(default); x=1: checksum mode
ATLOa,b,c,d     Int/Trap Log Cmd
```

Figure 10-7   Boot Module Commands

Chapter 11
Telnet Configuration and Capabilities

This chapter covers the Telnet Configuration and Capabilities of the Prestige.

11.1 About Telnet Configuration

Before the Prestige is properly setup for TCP/IP, the only option for configuring it is through the console port. Once your Prestige is configured, you can use telnet to configure it remotely as shown below.
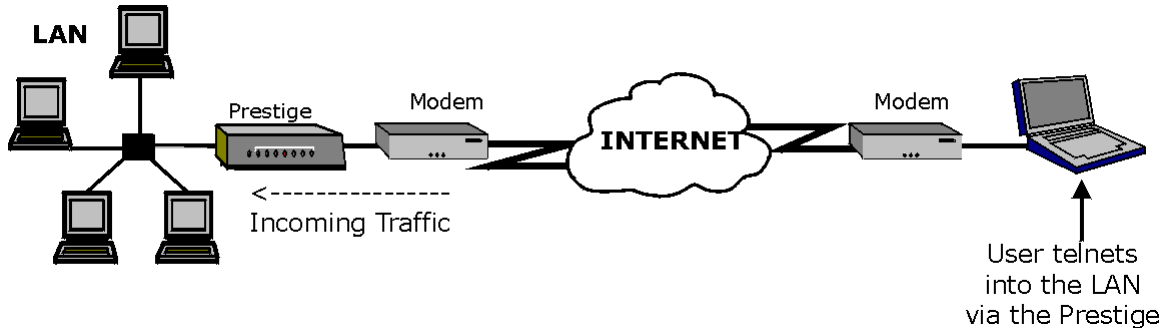
Figure 11-1   Telnet Configuration on a TCP/IP Network

11.2 Telnet Under SUA

When Single User Account (SUA) is enabled and an inside server is specified, telnet connections from the outside will be forwarded to the inside server. So to configure the Prestige via telnet from the outside, you must first telnet to the inside server, and then telnet from the server to the Prestige using its inside LAN IP address. If no inside server is specified, telnetting to the SUA's IP address will connect to the Prestige directly.

11.3 Telnet Capabilities

11.3.1 Single Administrator

To prevent confusion and discrepancy on the configuration, your Prestige only allows one administrator to log in at any time. Your Prestige also gives priority to the console port over telnet. If you have already connected to your Prestige via telnet or PNC, you will be logged out if another user logs in to the Prestige via the console port.

11.3.2 System Timeout

There is a system timeout of 5 minutes (300 seconds) for either the console port or telnet. Your Prestige will automatically log you out if you do nothing in this timeout period, except when it is continuously updating the status in Menu 24.1 or when "sys stdio" has been changed on the command line.

11.3.3 Telnet Blocking

Telnet over the WAN doesn't work when:

1. You have applied a filter in Menu 3.1 (LAN) or in Menu 11.5 (WAN) to block Telnet service.

2. You have an SMT console session running.

Part IV:

Troubleshooting, Appendices, Glossary and Index

Chapter 12 provides information about solving common problems, followed by some Appendices, a Glossary of Terms and an Index.

<div align="right">

Chapter 12
Troubleshooting

</div>

This chapter covers the potential problems you may run into and the possible remedies. After each problem description, some instructions are provided to help you to diagnose and to solve the problem. Please see our supporting disk for further information.

12.1 Problems Starting Up the Prestige

Table 12-1   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 technical support.	
Cannot access the Prestige via the console port.	1. Check to see if the Prestige is connected to your computer's serial 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 is the default speed on leaving the factory. Try other speeds in case the speed has been changed.
		No parity, 8 Data bits, 1 Stop bit, Data Flow set to None.

12.2   Problems with the LAN Interface

Table 12-2   Troubleshooting the LAN Interface

Problem	Corrective Action
Can't ping any workstation on the LAN.	Check the 10M/100M LEDs on the front panel. One of these LEDs for each port connected should be on. If they are both off, check the cables between your Prestige 4-Port Switch and the computer. Use a straight through Ethernet cable (white tag) to connect each computer to the 10/100M LAN ports on the Prestige. If you have more than four computers, you must use an external hub. Connect LAN port 4 on the Prestige to a port on the external hub using a straight through Ethernet cable (white tag) and press the **Uplink** button. If you do not press the **Uplink** button (LAN port 4) or use LAN ports 1 to 3 to daisy chain the Prestige to an external hub, then you must use a crossover cable.
	Verify that the IP address and the subnet mask are consistent between the Prestige and the workstations.

12.3 Problems with the WAN Interface

Table 12-3   Troubleshooting the WAN Interface

Problem	Corrective Action
Cannot get WAN IP from the ISP.	The WAN IP 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** (recommended).
	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**.
Can't connect to a remote node or ISP.	Check Menu 24.1 to verify the line status. If it indicates **Down**, then refer to the section on the line problems.

12.4 Problems with Internet Access

Table 12-4   Troubleshooting Internet Access

Problem	Corrective Action
Cannot access the Internet.	Connect your cable/xDSL modem with the Prestige using appropriate cable.
	Check with the manufacturer of your cable/xDSL modem about the cable requirement because for some modems you may require crossover cable and for others regular patch cable.
	Verify your settings in Menu 3.2 and Menu 4.

12.5 Problems with Telnet

Problem	Corrective Action
Cannot Telnet into the Prestige.	Telnet doesn't work if:
	1. You have applied a filter in Menu 3.1 (LAN) or in Menu 11.5 (WAN) to block Telnet service.
	2. You have an SMT console session running.

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.
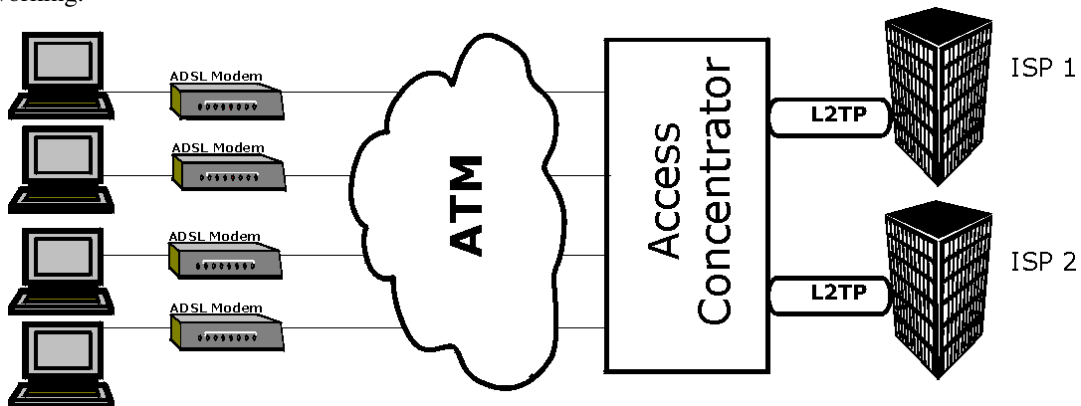
Diagram 1   Single-PC per Modem Hardware Configuration

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.

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.
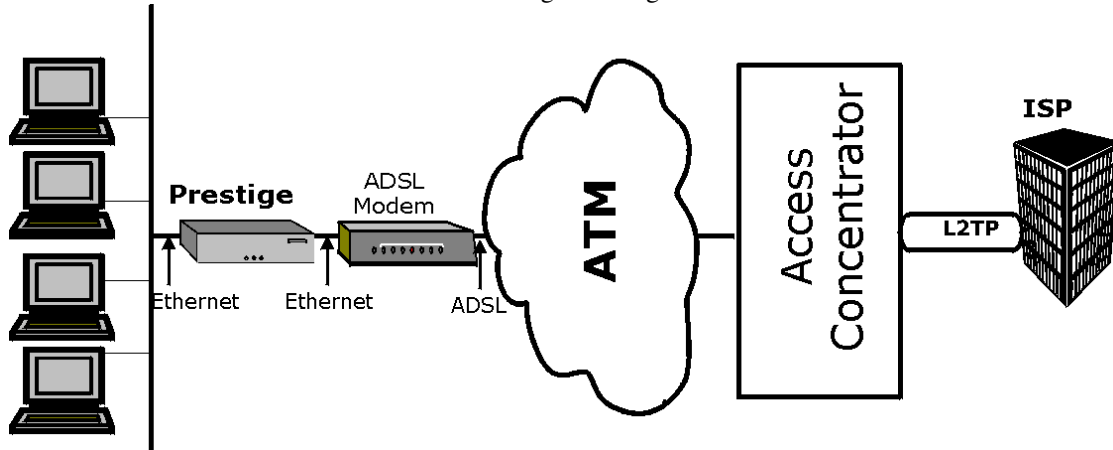
Diagram 2   Prestige as a PPPoE Client

Appendix B
Hardware Specifications

Power Specification	I/P AC 120V / 60Hz ; O/P DC 12V 1200 mA
MTBF	100000 hrs
Operation Temperature	0º C ~ 40º C
Ethernet Specification for WAN	10 Mbit Half Duplex
Ethernet Specification for 4-Port LAN	10/100 Mbit Half / Full Auto-negotiation
Console Port RS – 232	Pin 1 = NON ; Pin 2 = DTE-RXD; Pin 3 = DTE-TXD; Pin 4 = DTE-DTR; Pin 5 = GND; Pin 6 = DTE-DSR; Pin 7 = DTE-RTS; Pin 8 = DTE-CTS; Pin 9 = NON. See Figure below.

Pin1

Pin 9

Pin 6
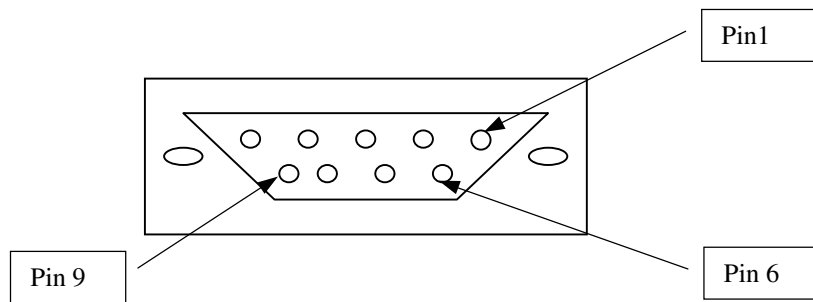
WAN/LAN Cable Pin Layout:				
Straight-Through			Crossover	
(Switch)	(Adapter)		(Switch)	(Switch)
1 IRD +	1 OTD +		1 IRD +	1 IRD +
2 IRD -	2 OTD -		2 IRD -	2 IRD -
3 OTD +	3 IRD +		3 OTD +	3 OTD +
6 OTD -	6 IRD -		6 OTD -	6 OTD -

Appendix C
Important Safety Instructions

The following safety instructions apply to the Prestige:

1. Be sure to read and follow all warning notices and instructions.
2. The maximum recommended ambient temperature for the Prestige is 40ºC (104ºF). Care must be taken to allow sufficient air circulation or space between units when the Prestige is installed inside a closed rack assembly. The operating ambient temperature of the rack environment might be greater than room temperature.
3. Installation in a rack without sufficient airflow can be unsafe.
4. Racks should safely support the combined weight of all equipment.
5. The connections and equipment that supply power to the Prestige should be capable of operating safely with the maximum power requirements of the Prestige. In case of a power overload, the supply circuits and supply wiring should not become hazardous. The input rating of the Prestige is printed on the nameplate.
6. The AC adapter must plug in to the right supply voltage, i.e. 120VAC adapter for North America and 230VAC adapter for Europe. Make sure that the supplied AC voltage is correct and stable. If the input AC voltage is over 10% lower than the standard may cause the Prestige to malfunction.
7. Installation in restricted access areas must comply with Articles 110-16, 110-17, and 110-18 of the National Electrical Code, ANSI/NFPA 70.
8. Do not allow anything to rest on the power cord of the AC adapter and do not locate the product where anyone can walk on the power cord.
9. Do not service the product by yourself. Opening or removing covers can expose you to dangerous high voltage points or other risks. Refer all servicing to qualified service personnel.
10. Generally, when installed after the final configuration, the product must comply with the applicable safety standards and regulatory requirements of the country in which it is installed. If necessary, consult the appropriate regulatory agencies and inspection authorities to ensure compliance.
11. A rare condition can create a voltage potential between the earth grounds of two or more buildings. If products installed in separate building are interconnected, the voltage potential can cause a hazardous condition. Consult a qualified electrical consultant to determine whether or not this phenomenon exists and, if necessary, implement corrective action before interconnecting the products. If the equipment is to be used with telecommunications circuit, take the following precautions:
    - Never install telephone wiring during a lightning storm.
    - Never install telephone jacks in a wet location unless the jack is specially designed for wet locations.
    - Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
    - Use caution when installing or modifying telephone lines (other than a cordless telephone) during an electrical storm. There is a remote risk of electric shock from lightning.

Appendix D
Power Adapter Specs

AC Power Adapter Specifications
North America
AC Power Adapter model MW48-1201200 Input power: AC120Volts/60Hz Output power: DC12Volts/1.2A Power consumption: 9 W Plug: North American standards Safety standards: UL, CUL (UL 1310, CSA C22.2 No.233-M91)
AC Power Adapter model AD48-1201200DUY Input power: AC120Volts/60Hz Output power: DC12Volts/1.2A Power consumption: 9 W Plug: North American standards Safety standards: UL, CUL (UL1950, CSA C22.2 NO. 234-M90)
European Union
AC Power Adapter model AD-1201200DV Input power: AC230Volts/50Hz, Output power: DC12Volts/1.2A Power consumption: 9 W Plug: European Union standards Safety standards: TUV, CE (EN 60950)
AC Power Adapter model JAD-121200E Input power: AC230Volts/50Hz, Output power: DC12Volts/1.2A Power consumption: 9 W Plug: European Union standards Safety standards: TUV, CE (EN 60950)
UK
AC Power Adapter model AD-1201200DK Input power: AC230Volts/50Hz, Output power: DC12Volts/1.2A Power consumption: 9 W Plug: United Kingdom standards Safety standards: TUV, CE (EN 60950, BS7002)

Japan
AC Power Adapter model JOD-48-1124 Input power: AC100Volts/ 50/60Hz/ 27VA Output power: DC12Volts/1.2A Power consumption: 9 W Plug: Japan standards Safety standards: T-Mark
Australia and New Zealand
AC Power Adapter model AD-1201200DS Input power: AC240Volts/50Hz/0.2A Output power: DC12Volts/1.2A Power consumption: 9 W Plug: Australia and New Zealand standards Safety standards: NATA (AS 3260)

Glossary of Terms

10BaseT	The 10-Mbps baseband Ethernet specification that uses two pairs of twisted-pair cabling (Category 3 or 5): one pair for transmitting data and the other for receiving data.
ARP	Address Resolution Protocol is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network.
Authenticity	Proof that the information came from the person or location that reportedly sent it. One example of authenticating software is through digital signatures.
Backbone	A high-speed line or series of connections that forms a major pathway within a network.
Bandwidth	This is the capacity on a link usually measured in bits-per-second (bps).
Bit	(Binary Digit) -- A single digit number in base-2, in other words, either a 1 or a zero. The smallest unit of computerized data.
Byte	A set of bits that represent a single character. There are 8 bits in a Byte.
CDR	Call Detail Record. This is a name used by telephone companies for call related information.
CHAP	Challenge Handshake Authentication Protocol is an alternative protocol that avoids sending passwords over the wire by using a challenge/response technique.
Client	A software program that is used to contact and obtain data from a Server software program on another computer. Each Client program is designed to work with one or more specific kinds of Server programs and each Server requires a specific kind of Client. A Web Browser is a specific kind of Client.
Crossover Ethernet cable	A cable that wires a pin to its opposite pin, for example, RX+ is wired to TX+. This cable connects two similar devices, for example, two data terminal equipment (DTE) or data communications equipment (DCE) devices.
CSU/DSU	Channel Service Unit/Data Service Unit. CSUs (channel service units) and DSUs (data service units) are actually two separate devices, but they are used in conjunction and often combined into the same box. The devices are part of the hardware you need to connect computer equipment to digital transmission lines. The Channel Service Unit device connects with the digital communication line and provides a termination for the digital signal. The Data Service Unit device, sometimes called a digital service unit, is the hardware component you need to transmit digital data over the hardware channel. The device converts signals from bridges, routers, and multiplexors into the bipolar digital signals used by the digital lines. Multiplexors mix voice signals and data on the same line.
DCE	Data Communications Equipment is typically a modem or other type of communication device. The DCE sits between the DTE (data terminal equipment) and a transmission circuit such as a phone line.
DHCP	Dynamic Host Configuration Protocol automatically assigns IP addresses to clients when they log on. DHCP centralizes IP address management on central computers

	that run the DHCP server program. DHCP leases addresses for a period of time which means that addresses are made available to assign to other systems.
DNS	Domain Name System. A database of domain names and their IP addresses. DNS is the primary naming system for many distributed networks, including the Internet.
Domain Name	The unique name that identifies an Internet site. Domain Names always have 2 or more parts, separated by dots. The part on the left is the most specific and the part on the right is the most general.
DRAM	Dynamic RAM that stores information in capacitors that must be refreshed periodically.
DSL	Digital Subscriber Line technologies enhances the data capacity of the existing twisted-pair wire that runs between the local telephone company switching offices and most homes and offices. There are actually seven types of DSL service, ranging in speeds from 16 Kbits/sec to 52 Mbits/sec. The services are either symmetrical (traffic flows at the same speed in both directions), or asymmetrical (the downstream capacity is higher than the upstream capacity). DSL connections are point-to-point dedicated circuits, meaning that they are always connected. There is no dial-up. There is also no switching, which means that the line is a direct connection into the carrier's frame relay, ATM (Asynchronous Transfer Mode), or Internet-connect system.
DSLAM	A Digital Subscriber Line Access Multiplexer (DSLAM) is a network device, usually at a telephone company central office, that receives signals from multiple customer Digital Subscriber Line connections and puts the signals on a high-speed backbone line using multiplexing techniques. Depending on the product, DSLAM multiplexers connect DSL lines with some combination of asynchronous transfer mode ATM, frame relay, or IP networks.
DTE	Originally, the DTE (data terminal equipment) meant a dumb terminal or printer, but today it is a computer, or a bridge or router that interconnects local area networks.
EMI	ElectroMagnetic Interference. The interference by electromagnetic signals that can cause reduced data integrity and increased error rates on transmission channels.
Ethernet	A very common method of networking computers in a LAN. There are a number of adaptations to the IEEE 802.3 Ethernet standard, including adaptations with data rates of 10 Mbits/sec and 100 Mbits/sec over coaxial cable, twisted-pair cable and fiber-optic cable. The latest version of Ethernet, Gigabit Ethernet, has a data rate of 1 Gbit/sec.
FAQ	(Frequently Asked Questions) -- FAQs are documents that list and answer the most common questions on a particular subject.
FCC	The FCC (Federal Communications Commission) is in charge of allocating the electromagnetic spectrum and thus the bandwidth of various communication systems.
Flash Memory	The nonvolatile storage that can be electrically erased and reprogrammed so that data can be stored, booted and rewritten as necessary.
FTP	File Transfer Protocol is an Internet file transfer service that operates on the Internet and over TCP/IP networks. FTP is basically a client/server protocol in which a system running the FTP server accepts commands from a system running an FTP client. The service allows users to send commands to the server for uploading and downloading files. FTP is popular on the Internet because it allows for speedy transfer of large files between two systems.

Gateway	A gateway is a computer system or other device that acts as a translator between two systems that do not use the same communication protocols, data formatting structures, languages, and/or architecture.
HDLC	HDLC (High-level Data Link Control) is a bit-oriented (the data is monitored bit by bit), link layer protocol for the transmission of data over synchronous networks.
Host	Any computer on a network that is a repository for services available to other computers on the network. It is quite common to have one host machine provide several services, such as WWW and USENET.
HTTP	Hyper Text Transfer Protocol. The most common protocol used on the Internet. HTTP is the primary protocol used for web sites and web browsers. It is also prone to certain kinds of attacks.
IANA	Internet Assigned Number Authority acts as the clearinghouse to assign and coordinate the use of numerous Internet protocol parameters such as Internet addresses, domain names, protocol numbers, and more. The IANA Web site is at http://www.isi.edu/iana.
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and are not directly apparent to the application user.
Integrity	Proof that the data is the same as originally intended. Unauthorized software or people have not altered the original information.
internet	(Lower case i) Any time you connect 2 or more networks together, you have an internet.
Internet	(Upper case I) The vast collection of inter-connected networks that all use the TCP/IP protocols and that evolved from the ARPANET of the late 60's and early 70's. The Internet now (July 1995) connects roughly 60,000 independent networks into a vast global internet
Intranet	A private network inside a company or organization that uses the same kinds of software that you would find on the public Internet, but that is only for internal use.
IP	Internet Protocol (currently IP version 4, or IPv4), is the underlying protocol for routing packets on the Internet and other TCP/IP-based networks.
IPCP (PPP)	IP Control Protocol allows changes to IP parameters such as the IP address.
ISP	Internet Service Providers provide connections into the Internet for home users and businesses. There are local, regional, national, and global ISPs. You can think of local ISPs as the gatekeepers into the Internet.
LAN	Local Area Network is a shared communication system to which many computers are attached. A LAN, as its name implies, is limited to a local area. This has to do more with the electrical characteristics of the medium than the fact that many early LANs were designed for departments, although the latter accurately describes a LAN as well. LANs have different topologies, the most common being the linear bus and the star configuration.

Linux	A version of the UNIX operating system designed to run on IBM Compatible computers.
MAC	On a local area network (LAN) or other network, the MAC (Media Access Control) address is your computer's unique hardware number. (On an Ethernet LAN, it's the same as your Ethernet address.) The MAC layer frames data for transmission over the network, then passes the frame to the physical layer interface where it is transmitted as a stream of bits.
Name Resolution	The allocation of an IP address to a host name. See DNS.
NAT	Network Address Translation is the translation of an Internet Protocol address used within one network to a different IP address known within another network - see also SUA.
NDIS	Network Driver Interface Specification is a Windows specification for how communication protocol programs (such as TCP/IP) and network device drivers should communicate with each other.
NetBIOS	Network Basic Input / Output System. NetBIOS is an extension of the DOS BIOS that enables a PC to connect to and communicate with a LAN.
Network	Any time you connect 2 or more computers together so that they can share resources, you have a computer network. Connect 2 or more networks together and you have an internet.
NIC	Network Interface Card. A board that provides network communication capabilities to and from a computer system. Also called an adapter.
Node	Any single computer connected to a network
Packet Filter	A filter that scans packets and decides whether to let them through.
PAP	Password Authentication Protocol PAP is a security protocol that requires users to enter a password before accessing a secure system. The user's name and password are sent over the wire to a server, where they are compared with a database of user account names and passwords. This technique is vulnerable to wiretapping (eavesdropping) because the password can be captured and used by someone to log onto the system.
Password encryption	A system of encrypting electronic files using a single key or password. Anyone who knows the password can decrypt the file.
POP	Post Office Protocol. This is a common protocol used for sending, receiving, and delivering mail messages.
Port (H/W)	An interface on a computer for connecting peripherals or devices to the computer. A printer port, for example, is an interface that is designed to have a printer connected to it. Ports can be defined by specific hardware (such as a keyboard port) or through software.
Port	An Internet port refers to a number that is part of a URL, appearing after a colon (:) right after the domain name. Every service on an Internet server listens on a particular port number on that server. Most services have standard port numbers, e.g. Web servers normally listen on port 80.
POTS	Plain Old Telephone Service is the analog telephone service that runs over copper twisted-pair wires and is based on the original Bell telephone system. Twisted-pair

	wires connect homes and businesses to a neighborhood central office. This is called the local loop. The central office is connected to other central offices and long-distance facilities.
PPP	Point to Point Protocol. PPP encapsulates and transmits IP (Internet Protocol) datagrams over serial point-to-point links. PPP works with other protocols such as IPX (Internetwork Packet Exchange). The protocol is defined in IETF (Internet Engineering Task Force) RFC 1661 through 1663. PPP provides router-to-router, host-to-router, and host-to-host connections.
Promiscuous Packet Capture	Actively capturing packet information from a network. Most computers only collect packets specifically addressed to them. Promiscuous packet capture acquires all network traffic it can regardless of where the packets are addressed.
Protocol	A "language" for communicating on a network. Protocols are sets of standards or rules used to define, format, and transmit data across a network. There are many different protocols used on networks. For example, most web pages are transmitted using the HTTP protocol.
Proxy Server	A server that performs network operations in lieu of other systems on the network. Proxy Servers are most often used as part of a firewall to mask the identity of users inside a corporate network yet still provide access to the Internet. When a user connects to a proxy server, via a web browser or other networked application, he submits commands to the proxy server. The server then submits those same commands to the Internet, yet without revealing any information about the system that originally requested the information. Proxy servers are an ideal way to also have all users on a corporate network channel through one point for all external communications. Proxy servers can be configured to block certain kinds of connections and stop some hacks.
PSTN	Public Switched Telephone Network was put into place many years ago as a voice telephone call-switching system. The system transmits voice calls as analog signals across copper twisted cables from homes and businesses to neighborhood COs (central offices); this is often called the local loop. The PSTN is a circuit-switched system, meaning that an end-to-end private circuit is established between caller and callee.
PVC	Permanent Virtual Circuit. A PVC is a logical point-to-point circuit between customer sites. PVCs are low-delay circuits because routing decisions do not need to be made along the way. Permanent means that the circuit is preprogrammed by the carrier as a path through the network. It does not need to be set up or torn down for each session.
RFC	An RFC (Request for Comments) is an Internet formal document or standard that is the result of committee drafting and subsequent review by interested parties. Some RFCs are informational in nature. Of those that are intended to become Internet standards, the final version of the RFC becomes the standard and no further comments or changes are permitted. Change can occur, however, through subsequent RFCs.
RIP	Routing Information Protocol is an interior or intra-domain routing protocol that uses the distance-vector routing algorithms. RIP is used on the Internet and is common in the NetWare environment as a method for exchanging routing information between routers.

Router	A device that connects two networks together. Routers monitor, direct, and filter information that passes between these networks. Because of their location, routers are a good place to install traffic or mail filters. Routers are also prone to attacks because they contain a great deal of information about a network.
SAP	In NetWare, the SAP (Service Advertising Protocol) broadcasts information about available services on the network that other network devices can listen to. A server sends out SAP messages every 60 seconds. A server also sends out SAP messages to inform other devices that it is closing down. Workstations use SAP to find services they need on the network.
Server	A computer, or a software package, that provides a specific kind of service to client software running on other computers.
SNMP	System Network Management Protocol is a popular management protocol defined by the Internet community for TCP/IP networks. It is a communication protocol for collecting information from devices on the network.
SOCKS	A protocol that handles TCP traffic through proxy servers.
SSL (Secured Socket Layer)	Technology that allows you to send information that only the server can read. SSL allows servers and browsers to encrypt data as they communicate with each other. This makes it very difficult for third parties to understand the communications.
STP	Twisted-pair cable consists of copper-core wires surrounded by an insulator. Two wires are twisted together to form a pair, and the pair form a balanced circuit. The twisting prevents interference problems. STP (shielded twisted-pair) provides protection against external crosstalk.
Straight through Ethernet cable	A cable that wires a pin to its equivalent pin. This cable connects two dissimilar devices, for example, a data terminal equipment (DTE) device and a data communications equipment (DCE) device. A straight through Ethernet cable is the most common cable used.
SUA	Single User Account – The Prestige's SUA (Single User Account) feature allows multiple user Internet access for the cost of a single ISP account - see also NAT.
TCP	Transmission Control Protocol handles flow control and packet recovery and IP providing basic addressing and packet-forwarding services.
Telnet	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
Terminal	A device that allows you to send commands to a computer somewhere else. At a minimum, this usually means a keyboard and a display screen and some simple circuitry.
Terminal Software	Software that pretends to be (emulates) a physical terminal and allows you to type commands to a computer somewhere else.
TFTP	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP (File Transfer Protocol), but it is scaled back in functionality so that it requires fewer resources to run. TFTP uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
UDP	UDP is a connectionless transport service that dispenses with the reliability services

---

	provided by TCP. UDP gives applications a direct interface with IP and the ability to address a particular application process running on a host via a port number without setting up a connection session.
UNIX	A widely used operating system in large networks.
URL	(Uniform Resource Locator) URL is an object on the Internet or an intranet that resides on a host system. Objects include directories and an assortment of file types, including text files, graphics, video, and audio. A URL is the address of an object that is normally typed in the Address field of a Web browser. The URL is basically a pointer to the location of an object.
VPN	Virtual Private Network. These networks use public connections (such as the Internet) to transfer information. That information is usually encrypted for security purposes.
WAN	Wide Area Networks link geographically dispersed offices in other cities or around the globe. Just about any long-distance communication medium can serve as a WAN link, including switched and permanent telephone circuits, terrestrial radio systems, and satellite systems.
WWW	(World Wide Web) -- Frequently used when referring to "The Internet", WWW has two major meanings - first, loosely used: the whole constellation of resources that can be accessed using Gopher, FTP, HTTP, telnet, USENET, WAIS and some other tools. Second, the universe of hypertext servers (HTTP servers).

Index