# *Prestige 316*

***Broadband Sharing Gateway/Wireless LAN***

# User's Guide

Version 3.26
August 2001

ZyXEL
TOTAL INTERNET ACCESS SOLUTION

# Copyright

## DISCLAIMER

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

## TRADEMARKS

Trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

# Federal Communications Commission (FCC) Interference Statement

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

This device may not cause harmful interference.

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

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

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

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and the receiver.

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

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

### NOTICE 1

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

### NOTICE 2

Shielded RS-232C 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-232C 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

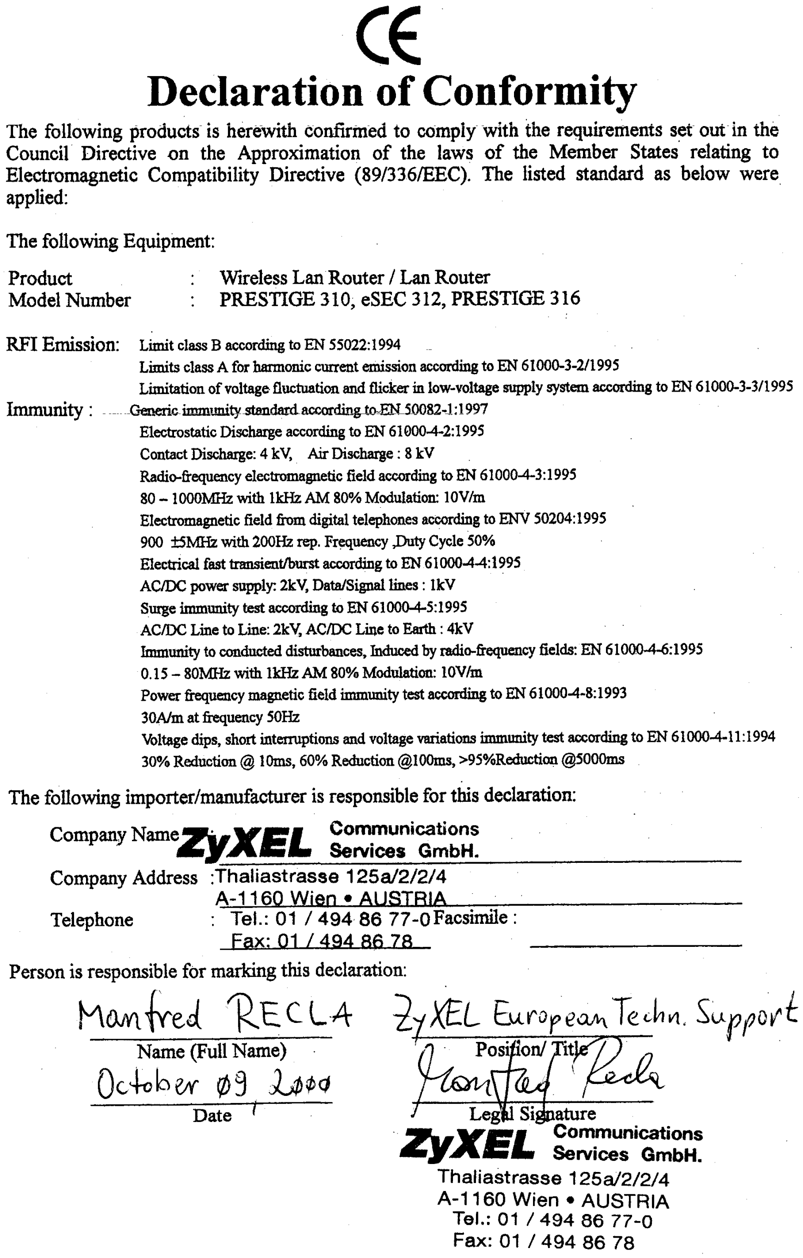
## Prestige 316

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. | 1995 |
| • | 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 | Power magnetism test. | 1993 |
| EN 61000-4-11 | Voltage dips, short interruptions and voltage variations immunity tests. | 1994 |
| ENV 50204 | Electromagnetic field from digital telephones test. | |
| SmartBit | LAN compatibility test. | |



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 | : | Wireless Lan Router / Lan Router |
| Model Number | : | PRESTIGE 310, eSEC 312, PRESTIGE 316 |

RFI Emission: Limit class B according to EN 55022:1994
Limits class A for harmonic current emission according to EN 61000-3-2/1995
Limitation of voltage fluctuation and flicker in 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 61000-4-3:1995
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 disturbances, Induced by radio-frequency fields: EN 61000-4-6:1995
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, 60% 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 marking this declaration:

Manfred RECLA
Name (Full Name)

ZyXEL European Techn. Support
Position/ Title

October 09 2000
Date

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

### Online Registration

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

# Customer Support

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

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

| METHOD<br>LOCATION | E-MAIL SUPPORT/SALES | TELEPHONE/FAX | WEB SITE/ FTP SITE | REGULAR MAIL |
|---|---|---|---|---|
| **WORLDWIDE** | support@zyxel.com.tw<br>support@europe.zyxel.com | +886-3-578-3942 | www.zyxel.com<br>www.europe.zyxel.com | ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, HsinChu, Taiwan 300, R.O.C. |
| | sales@zyxel.com.tw | +886-3-578-2439 | ftp.europe.zyxel.com | |
| **NORTH AMERICA** | support@zyxel.com | +1-714-632-0882<br>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 | 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 | |
| **GERMANY** | support@zyxel.de | +49-2405-6909-0 | www.zyxel.de | ZyXEL Deutschland GmbH. Adenauerstr. 20/A4 D-52146 Wuerselen, Germany |
| | sales@zyxel.de | +49-2405-6909-99 | | |
| **MALAYSIA** | support@zyxel.com.my | +603-795-44-688 | www.zyxel.com.my | Lot B2-06, PJ Industrial Park, Section 13, Jalan Kemajuan, 46200 Petaling Jaya Selangor Darul Ehasn, Malaysia |

# Table of Contents

# List of Figures

# List Of Tables

# Preface

## About Your Router

Congratulations on your purchase of the Prestige 316 Broadband Sharing Gateway with Wireless LAN.

**Online Registration**

Do not forget to register your Prestige (fast, easy online registration at www.zyxel.com for free future product updates and information.

The Prestige 316 is a dual Ethernet Broadband Sharing Gateway integrated with robust network management features that allows access to the Internet via Cable/xDSL modem or broadband router. It is designed for:

- Home offices and small businesses with Cable, xDSL and wireless modem via Ethernet port as Internet access media.
- Wireless LAN connectivity allows you to work anywhere in the coverage area.
- Multiple office/department connections via access devices.
- E-commerce/EDI applications.

Your Prestige 316 is easy to install and configure.

The embedded Web Configurator (eWC) is a web-based utility that allows you to access the Prestige's management settings through the Internet. All functions of the Prestige 316 are 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 Guide

This guide is designed to guide you through the SMT configuration of your Prestige 316 for its various applications.

### Structure of this Guide

This guide is structured as follows:

Part I. *Getting Started* 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* describe the advanced applications of your Prestige, such as NAT, Remote Node Setup and IP Static Routes.

Part III. *Advanced Management* provides information on Prestige Filtering, System Information and Diagnosis, SNMP, Transferring Files, Call Scheduling and Telnet.

Part IV. *Troubleshooting* 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* and *2* to connect your Prestige to your LAN. You can then refer to the appropriate chapters of the guide, depending on your applications.

### Related Documentation

➢ Support CD

More detailed information about the Prestige and examples of its use can be found in our Support CD. This CD contains HTML help on the embedded web configurator, our handy web-based Internet access wizard designed to get you up and running as soon as possible, the Prestige manual in PDF format, Support Notes (that include a General FAQ, an Advanced FAQ, Applications Notes, Troubleshooting, Reference CI Commands) and bundled software.

➢ Read Me First

Our Read Me First was 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 and information on using the Prestige Web Configurator (PWC), our web-based Internet access configuration wizard.

➢ Packing List Card

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

### 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 guide.
- The Prestige 316 may be referred to as the Prestige or the P316 in this guide. Occasionally, SMT screens may refer to the Prestige as a router.

# Part I:

## GETTING STARTED

This part 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.

# Chapter 1
# Getting to Know Your Prestige

*This chapter introduces the main features and applications of the Prestige.*

## 1.1 The Prestige 316 Broadband Sharing Gateway

The Prestige 316 is a dual Ethernet Broadband Sharing Gateway integrated with network management features designed for home offices and small businesses to access the Internet via Cable/xDSL modem or broadband router. By integrating NAT capability, the Prestige 316 provides not only ease of installation and Internet access, but also a complete security solution to protect your Intranet and efficiently manage data traffic on your network. What's more, with the wireless LAN connectivity, users can enjoy the convenience and mobility, working anywhere within the coverage area.

## 1.2 Features of the Prestige 316

The following are the main features of the Prestige 316.

### Broadband Internet Access Sharing

One 10 Mbps Ethernet port for WAN access allows speeds of up to 10 Mbps half duplex data transfer capability for connecting to broadband cable or xDSL modems.

### IEEE 802.11b 11 Mbps Wireless LAN

The 11 Mbps wireless LAN provides mobility and a fast network environment for small and home offices. Users can connect to the local area network without any wiring efforts and enjoy reliable high-speed connectivity.

### Wireless LAN MAC Address Filtering

MAC Address Filtering together with ESSID (Extended Service Set IDentifier) and WEP (Wired Equivalent Privacy) ensure the most secure wireless solution.

### Packet Filtering

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

### PPPoE Support

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

### PPTP Support

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks. PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet.

### 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.

### Auto-negotiating 10/100 Mbps Ethernet

The LAN interface automatically detects if it is on a 10 or a 100 Mbps Ethernet, providing the SOHO and professional users a higher bandwidth.

### Network Address Translation (NAT)

NAT (Network Address Translation - NAT, RFC 1631) allows the translation of an Internet Protocol address used within one network to a different IP address known within another network.

### Port Forwarding

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

### DHCP (Dynamic Host Configuration Protocol)

DHCP (Dynamic Host Configuration Protocol) allows the individual clients (workstations) to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The Prestige has built-in DHCP server capability, enabled by default, which means it can assign IP addresses, an IP default gateway and DNS servers to Windows 9X, Windows NT and other systems that support the DHCP client. The Prestige can also act as a surrogate DHCP server (**DHCP Relay**) where it relays IP address assignment from the actual real DHCP server to the clients.

### Full Network Management

This feature allows you to access SMT (System Management Terminal) through the console port or telnet connection.

### RoadRunner Support

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

### Time and Date Setting

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

### Logging and Tracing

The Prestige has the following logging and tracing features:

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

### Upgrade Prestige Firmware via LAN

The firmware of the Prestige 316 can be upgraded via the LAN.

### Embedded FTP and TFTP Servers

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

### IP Alias

The ability to partition physical network into logical network over the same Ethernet interface is referred as IP Alias functionality.

# 1.3 Applications for Prestige 316

## 1.3.1 Broadband Internet Access via Cable or xDSL Modem

A cable modem or xDSL modem can connect to the Prestige 316 for broadband Internet access via Ethernet port on the modem. The Prestige provides high speed Internet access and secured internal network protection and management as well.

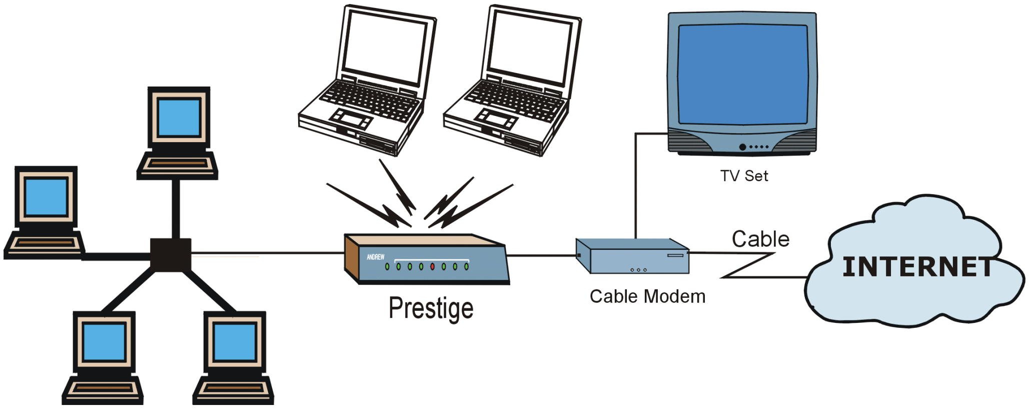


**Figure 1-1 Internet Access via Cable with Wireless LAN Structure**

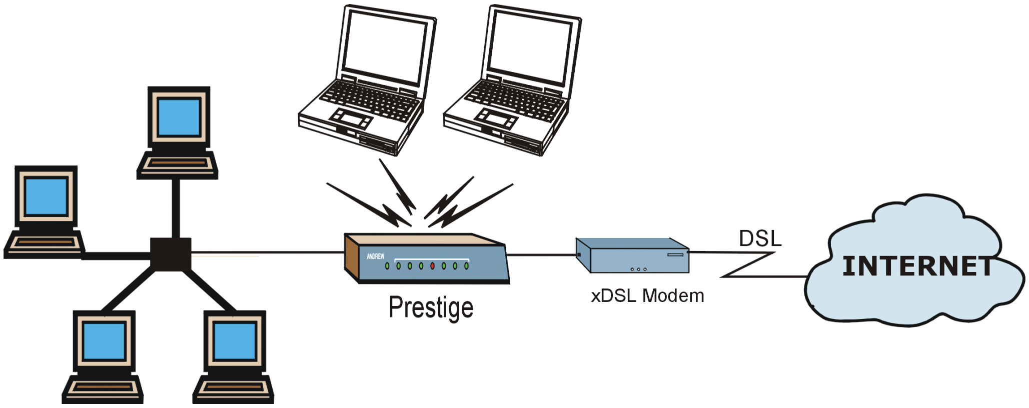


**Figure 1-2 Internet Access via xDSL with Wireless LAN Structure**

You can also use your xDSL modem in the bridge mode for always-on Internet access and high speed data transfer.

## 1.4 Internet Access Configuration Checklist

The following table shows the minimum SMT menu configurations you'll need to make (without changing the default Prestige values) in order to access the Internet. Please also refer to the Support CD that contains HTML help on the embedded web configurator, our handy web-based Internet access wizard designed to get you up and running as soon as possible.

**Table 1-1 Internet Access Configuration Checklist**

| SMT # | FIELD | ACTION |
|---|---|---|
| 1 | System Name | This field is for identification purposes but because some ISPs check this name you should enter your computer's "Computer Name".<br>• In Windows 95/98 click **Start** -> **Settings** -> **Control Panel** -> **Network**. Click the **Identification** tab, note the entry for the **Computer Name** field and enter it as the **System Name**.<br>• In Windows 2000, click **Start** -> **Settings**-> **Control Panel** -> **Network Identification**. Click the **Identification** tab, note the entry for the **Computer Name** field and enter it as the **System Name**. |
| 2 | MAC Address: Assigned By | The default is **Factory Default**, which is the factory assigned default MAC Address. We recommend you choose **IP Address attached on LAN** and enter the IP address of the workstation on the LAN whose MAC you are cloning. |
| 4 | Encapsulation | Choose **PPPoE** if you have a dial-up connection to the Internet (or **PPTP** if you reside in France or Austria); otherwise choose **Ethernet**. Choose from **RR-Manager, RR-Telstra** or **RR-Toshiba** if your ISP is Time Warner's RoadRunner; otherwise choose **Standard**. |
| | PPTP | You need to know your login name, password and connection ID/Name. The latter may not be obligatory for some ISPs, but if it is you must follow the "c:id" and "n:name" format. |
| | PPPoE | You need to know your login name, password and service name. The latter may not be obligatory for some ISPs. |
| | IP Address Assignment | If your ISP did not assign you a fixed IP address, select **Dynamic**, otherwise select **Static** and enter the IP address & subnet mask in the IP address and IP Subnet Mask fields. |
| Once these key fields have been configured, you should be able to enjoy super-fast Internet access with your Prestige! | | |

# Chapter 2
# Hardware Installation and 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.

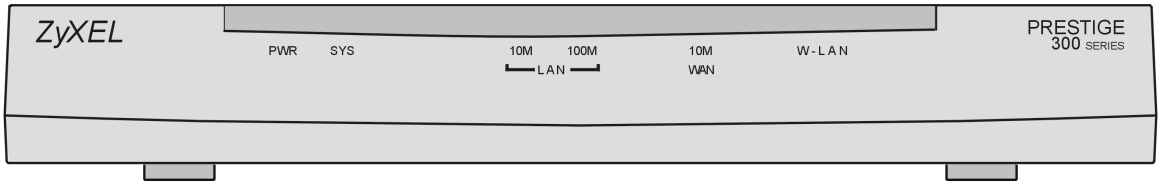


**Figure 2-1 Front Panel**

The following table describes the LED functions:

**Table 2-1 LED Functions**

| LED | FUNCTION | COLOR | STATUS | DESCRIPTION |
|---|---|---|---|---|
| PWR | Power | Green | On | The Prestige is receiving power. |
| 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. |

| LED | FUNCTION | COLOR | STATUS | DESCRIPTION |
|---|---|---|---|---|
| | | | On | The Prestige is connected to a 10 Mbps 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. |
| 10M WAN | WAN | Green | Off | The WAN link is not ready, or has failed. |
| | | | On | The WAN link is ready. |
| | | | Flashing | The 10M WAN link is sending/receiving packets. |
| W-LAN | Wireless LAN | Green | Off | The wireless LAN is not ready, or has failed. |
| | | | On | The wireless LAN is ready. |
| | | | Flashing | The wireless LAN is sending/receiving packets. |

## 2.2 Prestige 316 Rear Panel and Connections

The following figure shows the rear panel connections of your Prestige 316.

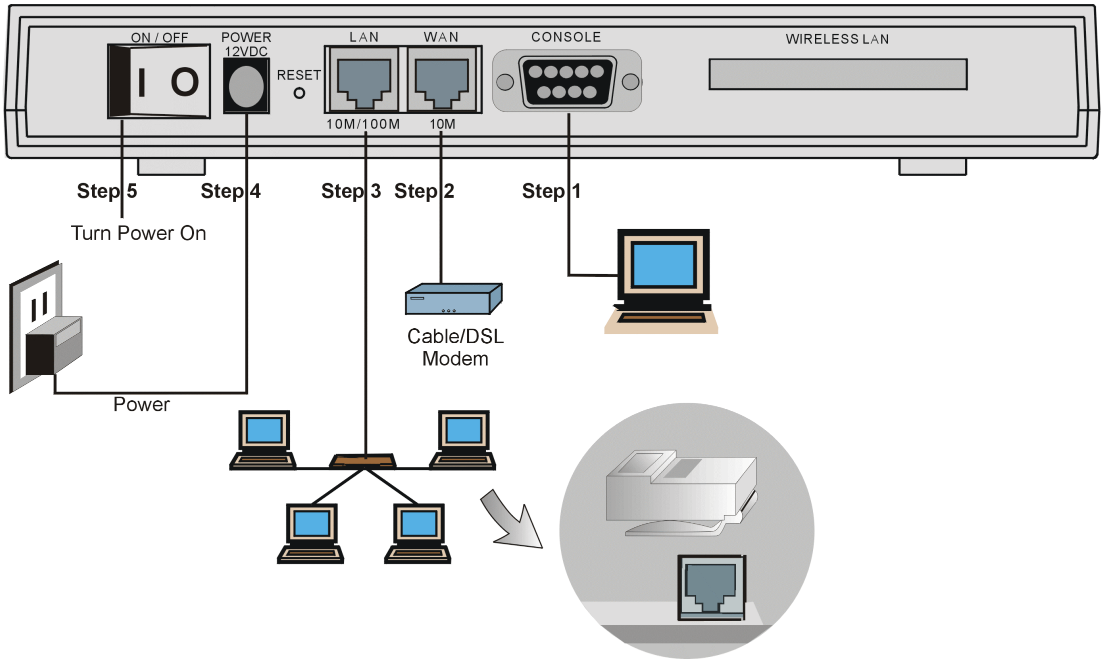


**Figure 2-2 Prestige 316 Rear Panel and Connections**

This section outlines how to connect your Prestige 316 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 xDSL modem to the xDSL wall jack. Please also see the *Appendices* for important safety instructions on making connections to the Prestige.

**Your Prestige comes with the Wireless PC Card already inserted. Do not try to remove it!**

### 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 (smaller) end of the console cable to the console port of the Prestige and the 25-pin (bigger) end to a serial port (COM1, COM2 or other COM port) of your workstation. You can use an extension RS-232C 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 Broadband Modem

**Step 2a.** Connecting the Prestige to the Cable Modem

Connect the WAN port (silver) 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".

**OR**

**Step 2b.** Connecting the Prestige to the xDSL Modem

Connect the WAN port (silver) on the Prestige to the Ethernet port on the xDSL modem using the cable that came with your xDSL modem.

### Step 3. Connecting the Prestige to the LAN

If you have more than one PC, you must use an external hub. Connect the 10/100M LAN port (gold) on the Prestige to a port on the hub using a straight-through Ethernet cable. If you only have one PC, you can connect the Prestige to the PC directly without a hub. For a single PC, connect the 10/100M LAN port on the Prestige to the Network Adapter on the PC using a crossover cable.

### Step 4. Connecting the Power Adapter to Your Prestige

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

### Step 5. Turning On Your Prestige

You can now turn on your Prestige.

**The two ports of the Prestige on the LAN side (Ethernet LAN and Wireless LAN ports) can transparently communicate with each other since there is bridging function between the two ports.**

## 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/xDSL 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 Housing

Your Prestige has rubber pads that fit snugly into grooves, enabling compact, sturdy stacking with airflow between routers. You should not stack more than four routers for maximum stability.

**To keep the Prestige operating at optimal internal temperature, keep the bottom, sides and rear clear of obstructions and away from the exhaust of other equipment.**

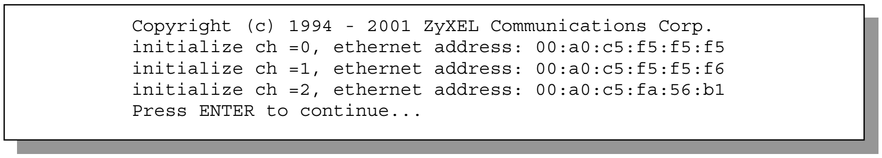
## 2.5 Starting Your Prestige

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.

### 2.5.1 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 next.



```
Copyright (c) 1994 - 2001 ZyXEL Communications Corp.
initialize ch =0, ethernet address: 00:a0:c5:f5:f5:f5
initialize ch =1, ethernet address: 00:a0:c5:f5:f5:f6
initialize ch =2, ethernet address: 00:a0:c5:fa:56:b1
Press ENTER to continue...
```

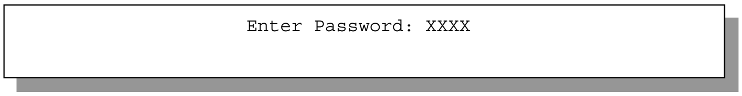
**Figure 2-3 Initial Screen**

#### Entering the Password

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

For your first login, enter the default password **1234**. As you type the password, the screen displays an (X) for each character you type.

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**

### 2.5.2 Prestige 316 SMT Menu Overview

The following figures give you an overview of the various SMT menu screens of your Prestige.

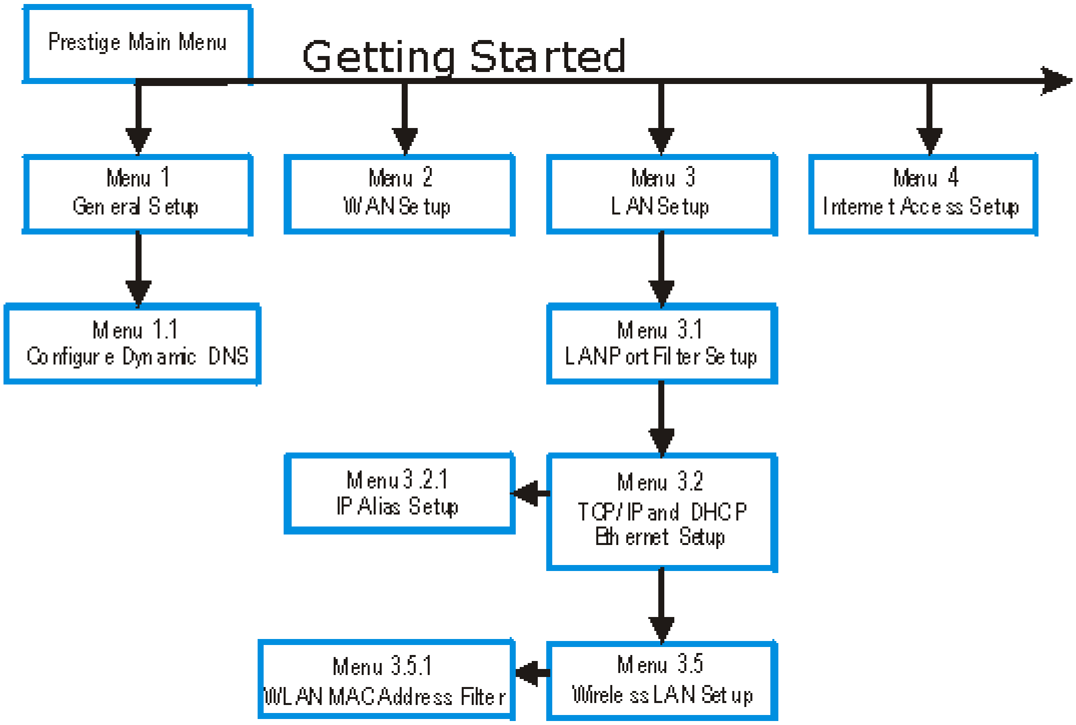


**Figure 2-5 Getting Started SMT Menu Overview**

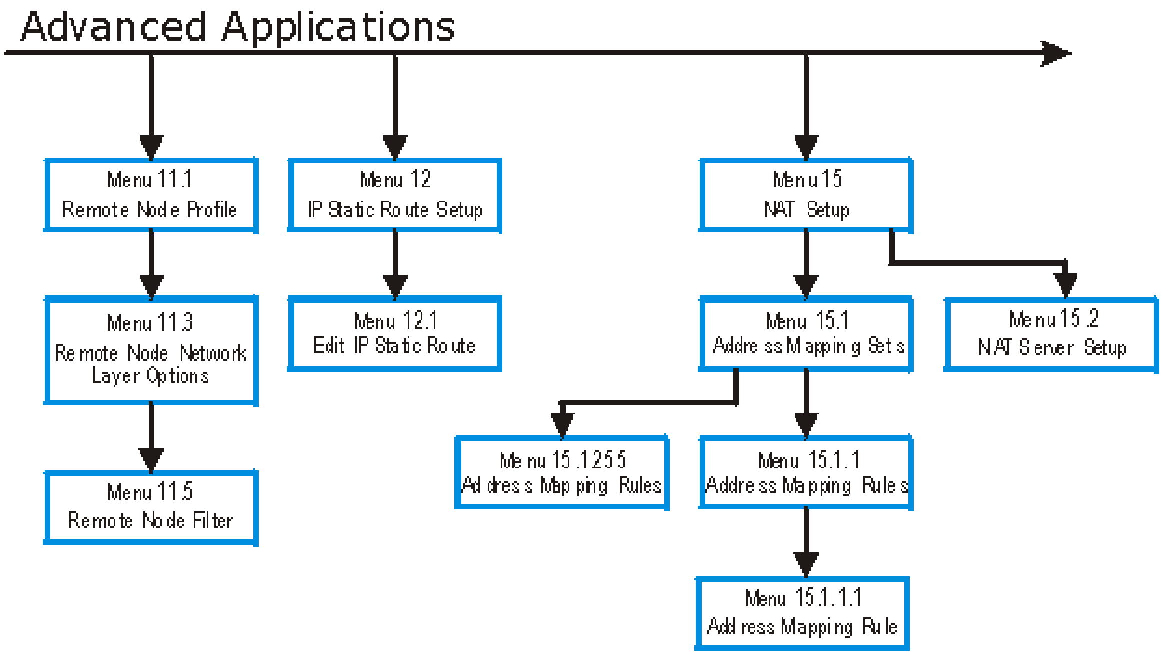


**Figure 2-6 Advanced Applications SMT Menu Overview**

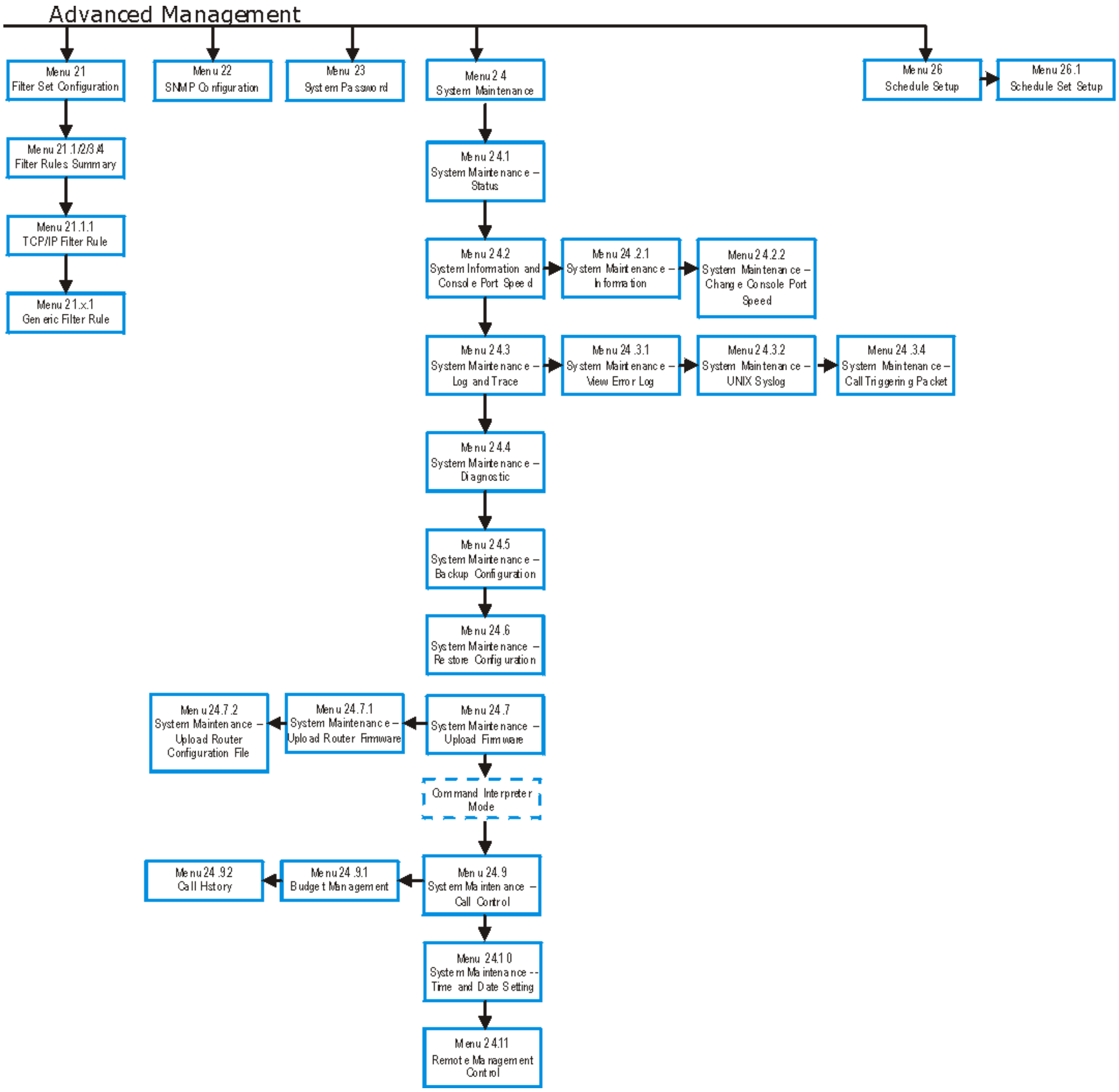


**Figure 2-7 Advanced Management SMT Menu Overview**

## 2.6 Navigating the SMT Interface

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

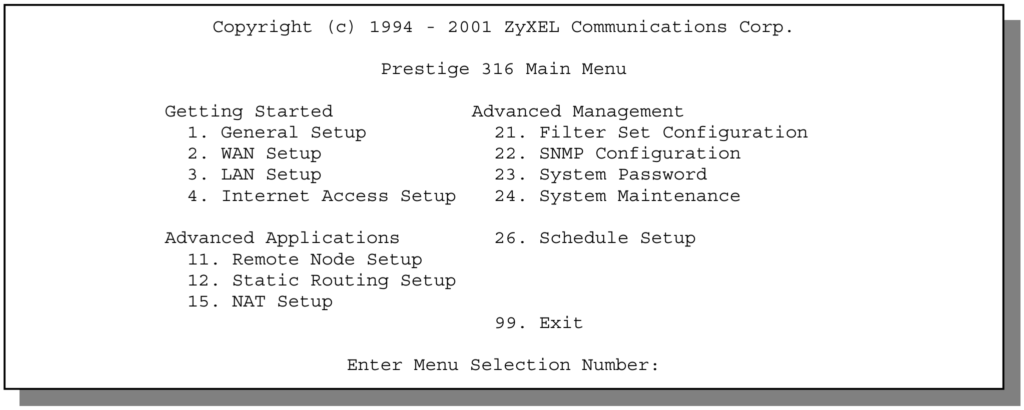
Several operations that you should be familiar with before you attempt to modify the configuration are listed in the next table.

**Table 2-2 Main Menu Commands**

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

### 2.6.1 Main Menu

After you enter the password, the SMT displays the **Prestige 316 Main Menu**, as shown next.



```
                   Copyright (c) 1994 - 2001 ZyXEL Communications Corp.

                                  Prestige 316 Main Menu

              Getting Started              Advanced Management
                1. General Setup             21. Filter Set Configuration
                2. WAN Setup                 22. SNMP Configuration
                3. LAN Setup                 23. System Password
                4. Internet Access Setup     24. System Maintenance

              Advanced Applications          26. Schedule Setup
                11. Remote Node Setup
                12. Static Routing Setup
                15. NAT Setup
                                             99. Exit

                               Enter Menu Selection Number:
```

**Figure 2-8 Prestige 316 Main Menu**

### 2.6.2 System Management Terminal Interface Summary

**Table 2-3 Main Menu Summary**

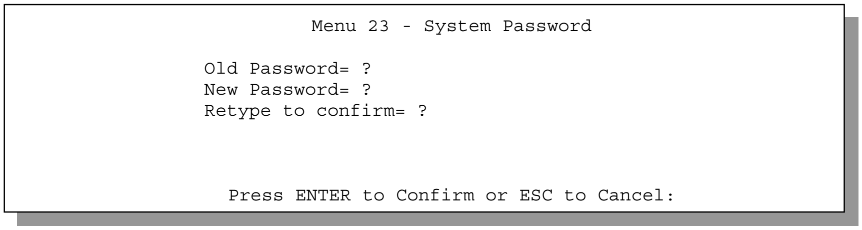
| NO. | MENU TITLE | DESCRIPTION |
|---|---|---|
| 1 | General Setup | Use this menu to set up general information. |
| 2 | WAN Setup | Use this menu to set up the WAN. |
| 3 | LAN Setup | Use this menu to set up the LAN. |
| 4 | Internet Access Setup | A quick and easy way to set up Internet connection. |
| 11 | Remote Node Setup | Use this menu to set up the remote node for LAN-to-LAN connection, including Internet connection. |
| 12 | Static Routing Setup | Use this menu to set up static route. |
| 15 | NAT Setup | Use this menu to configure NAT |
| 21 | Filter Set Configuration | Use this menu to set up filters to provide security. |
| 22 | SNMP Configuration | Use this menu to set up SNMP-related parameters. |

| NO. | MENU TITLE | DESCRIPTION |
|---|---|---|
| 23 | System Password | Use this menu to set up a new password. |
| 24 | System Maintenance | This menu provides system status, diagnostics, firmware upload, etc. |
| 26 | Schedule Setup | This menu allows the Prestige to manage a remote node and dictate when a remote node should be called and for how long. |
| 99 | Exit | To exit from SMT and return to the blank screen. |

## 2.7 Changing the System Password

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

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



```
                         Menu 23 - System Password

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



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

**Figure 2-9 Menu 23 – System Password**

**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 an (X) for each character you type.

## 2.8 Resetting the Prestige

If you have forgotten your password or for some reason cannot access the Prestige you will need to reinstall the configuration (rom) 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 following is the Prestige factory default password and IP address.

- Password: 1234
- IP address: 192.168.1.1

You can erase the current configuration and restore factory defaults in three ways:

1. Upload the default configuration file via teh console port. 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 later in this User's Guide for more information on how to transfer the configuration file to your Prestige using the SMT menus.
2. Use the **RESET** button on the rear panel of the Prestige (see the next section). Use this method for cases when the password or IP address of the Prestige is not known.
3. Use the web configurator to restore defaults (see the web configurator HTML help).

### 2.8.1 Procedure To Use The Reset Button

Make sure the **SYS** LED is on (not blinking) before you begin this procedure.

1. Press the **RESET** button for ten seconds, then release it. If the **SYS** LED begins to blink, the defaults have been restored and the Prestige restarts. Otherwise, go to step 2.
2. Turn the Prestige off.
3. While pressing the **RESET** button, turn the Prestige on.

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

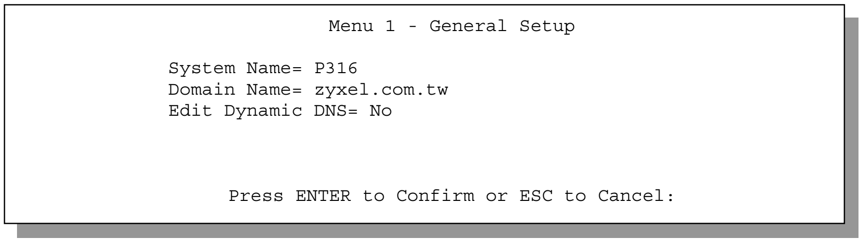
## 2.9 General Setup

**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 next. Fill in the required fields.



```
                          Menu 1 - General Setup

               System Name= P316
               Domain Name= zyxel.com.tw
               Edit Dynamic DNS= No



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

**Figure 2-10 Menu 1 – General Setup**

The fields for General Setup are as shown next. **System Name** is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name"

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

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

**Table 2-4 General Setup Menu Fields**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| System Name | Choose a descriptive name for identification purposes. It is recommended that 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. | P316 |
| 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 [SPACE BAR]. The domain name you entered is given priority over the ISP-assigned domain name. | zyxel.com.tw |
| Edit Dynamic DNS | Allows you to alias a dynamic IP address to a static hostname, enabling easier access to the host from various locations on the internet. Press [SPACE BAR] to select **Yes** or **No**. | **No/Yes** |

## 2.9.1 Dynamic DNS Basics

Your Prestige 316 supports Dynamic Domain Name Service. 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.

Usually, the Prestige 316 users are asked to use the WAN IP of the Prestige to access internal servers. If this IP is dynamic, it is inconvenient for the users. Now, you do not have to hunt for the IP address whenever you dial up your ISP. With Dynamic DNS service, you can apply a DNS name (e.g., www.zyxel.com.tw) for your web server for example and can access the server using this name regardless of the WAN IP of the Prestige 316.

In a Dynamic DNS service, an IP registry server provides a public central database where information such as email addresses, hostnames, IPs, etc., can be stored and retrieved. The Dynamic DNS server also stores password-protected e-mail addresses along with IPs and hostnames and accepts queries based on e-mail addresses. The Dynamic DNS services act like old-style phone operators: other users call the operators and ask to speak to you. Similarly, every time your computer comes online, you tell the Dynamic DNS server what your current address is and other users will be sent to the right place using DNS.

When the ISP assigns a new IP, you must inform the Dynamic DNS server and it will update its IP-to-DNS entry. Once the IP-to-DNS table is updated, you can continue to use the same DNS name for your web server.

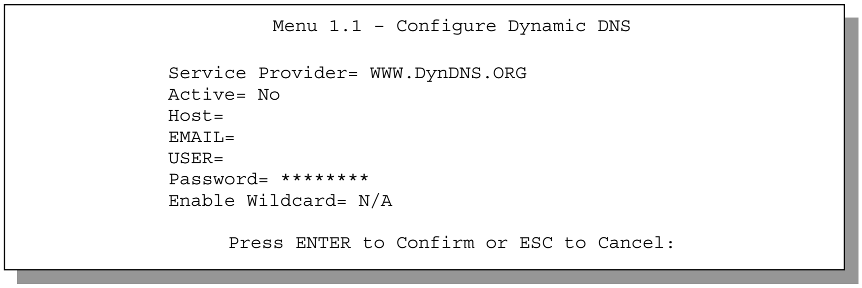
If you want to utilize this service, you must register for this service with the Dynamic DNS client. The Dynamic DNS client service provider will give you a password or key. Currently, ZyNOS supports the WWW.DynDNS.ORG client. You can apply to either of these clients for the DNS and update the WAN IP to it.

### 2.9.2 Configure Dynamic DNS

To configure the dynamic DNS and fill in the required information, follow these steps:

**Step 1.** In Menu 1 select **Yes** in the **Edit Dynamic DNS** field by using [SPACE BAR] and press [ENTER]. This opens **Menu 1.1 – Configure Dynamic DNS**.

**Step 2.** The **Menu 1.1** – **Configure Dynamic DNS** is shown next. Fill in the required fields.



```
                    Menu 1.1 - Configure Dynamic DNS

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

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

**Figure 2-11 Menu 1.1 – Configure Dynamic DNS**

The fields for Configure Dynamic DNS setup are as shown next.

**Table 2-5 Configure Dynamic DNS Menu Fields**

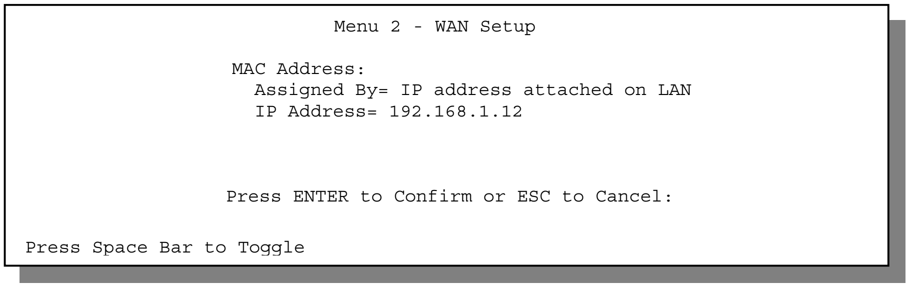
| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Service Provider | This read-only field is the name of the dynamic DNS client. | **WWW.DynDNS.ORG** |
| Active | Press the [SPACE BAR] to choose **Yes** to activate Dynamic DNS. | **No/Yes** |
| Host | Enter the domain name assigned to your Prestige by your dynamic DNS client. | p316.ddns.org |
| EMAIL | Enter your email address here. | yourmail@ yourmailserver |
| USER | Enter your username. | |
| Password | Enter the password assigned to you. | |
| Enable Wildcard | Your Prestige supports the DYNDNS Wildcard feature. | **N/A / Yes/No** |

**If you have a private WAN IP address, we recommend that you do not use Dynamic DNS.**

## 2.10 WAN Setup

This section describes how to configure the WAN using **Menu 2 – WAN Setup**. From the main menu, enter 2 to open Menu 2.

**ZyXEL recommends you configure this menu even if your ISP presently does not require MAC address authentication.**



```
                             Menu 2 - WAN Setup

                   MAC Address:
                     Assigned By= IP address attached on LAN
                     IP Address= 192.168.1.12



                  Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle
```

**Figure 2-12 Menu 2 – WAN Setup**

The MAC address field allows users to configure the WAN port's MAC address by either using the factory default or cloning the MAC address from a workstation on your LAN. 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**

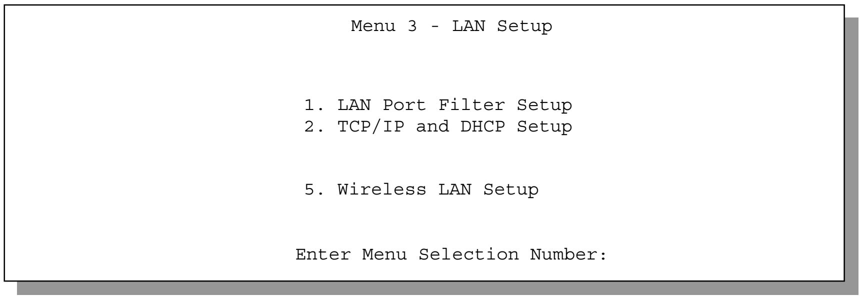
| FIELD | DESCRIPTION | EXAMPLES |
|---|---|---|
| MAC Address<br>Assigned By | Press [SPACE BAR] to choose either of the two methods of assigning a MAC address. Choose Factory Default to select the factory assigned default MAC address. Choose IP Address attached on LAN to use the MAC address of that workstation whose IP you give in the following field. | **Factory Default** |
| 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. | |

**Your Prestige WAN port is always set at half-duplex mode as most cable modems only support half-duplex mode. If your cable modem supports full-duplex mode, then you will be able to manually set it at half-duplex mode. If the Prestige was set at half-duplex and the cable modem was set at full-duplex then the WAN port would not function properly.**

**The Prestige supports full duplex on the LAN port.**

# 2.11 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.

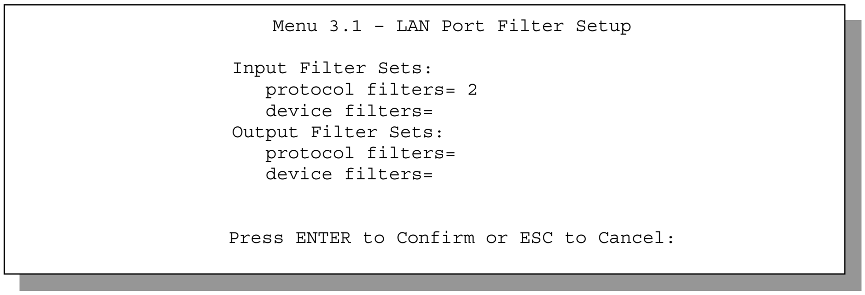


```
                      Menu 3 - LAN Setup



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


                  5. Wireless LAN Setup


                 Enter Menu Selection Number:
```

**Figure 2-13 Menu 3 – LAN Setup**

## 2.11.1 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 2-14 Menu 3.1 – LAN Port Filter Setup**

Menu 3.2 and 3.5 are discussed in another chapter. Please read on.

# 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, also.

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 us 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.

**192.168.1.1 is the default LAN IP address for the Prestige.**

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 do not 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. The Prestige can also act as a surrogate DHCP server (**DHCP Relay**) where it relays IP address assignment from the actual real DHCP server to the clients.

### IP 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 addresses:**

| | |
|---|---|
| Choose an IP: | 192.168.1.2 to 192.168.1.32**;** 192.168.1.65 to 192.168.1.254 |
| Netmask: | 255.255.255.0 |
| Gateway (or default route): | 192.168.1.1 (Prestige LAN IP) |

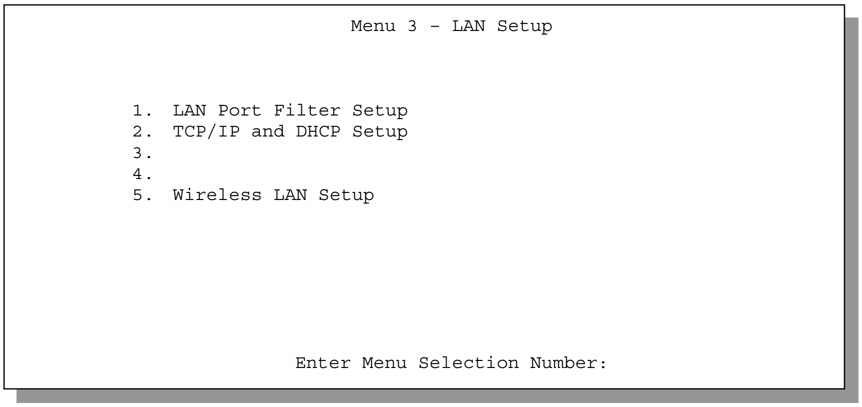
### 3.1.6 IP Multicast

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. Host groups are identified by Class D IP addresses, i.e., those with "1110" as their higher-order bits. In dotted decimal notation, host group addresses range from 224.0.0.0 to 239.255.255.255. Among them, 224.0.0.1 is assigned to the permanent IP hosts group and 224.0.0.2 is assigned to the multicast routers group.

IGMP (Internet Group Management Protocol) is the protocol used to support multicast groups. The latest version is version 2 (see RFC-2236). IP hosts use IGMP to report their multicast group membership to any immediate-neighbor multicast routers so the multicast routers can decide if a multicast packet needs to be forwarded. At start up, the Prestige queries all directly connected networks to gather group membership. After that, the Prestige updates the information by periodic queries. The Prestige implementation of IGMP is also compatible with version 1. The multicast setting can be turned on or off on Ethernet and remote nodes.

## 3.2 TCP/IP and DHCP Ethernet Setup

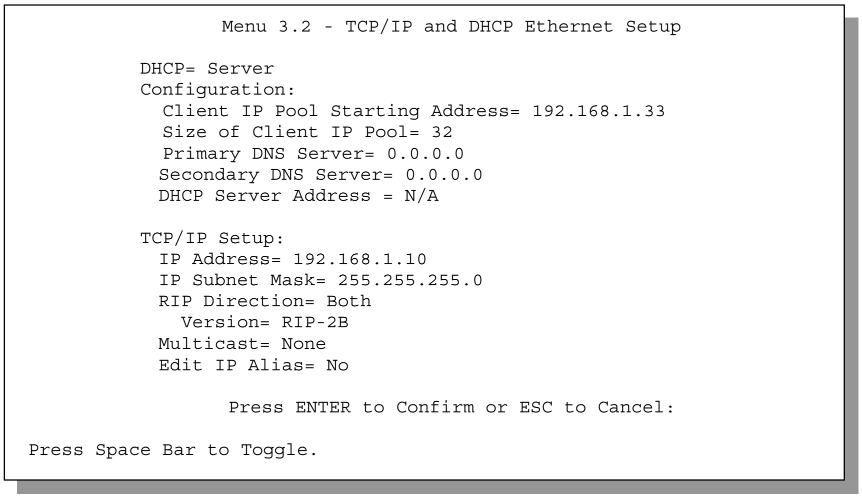
From the main menu, enter 3 to open **Menu 3 – LAN Setup** (10/100 Mbps Ethernet) to configure TCP/IP (RFC-1155) and DHCP Ethernet setup.



```
                        Menu 3 - LAN Setup



          1.  LAN Port Filter Setup
          2.  TCP/IP and DHCP Setup
          3.
          4.
          5.  Wireless LAN 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
             DHCP Server Address = N/A

            TCP/IP Setup:
             IP Address= 192.168.1.10
             IP Subnet Mask= 255.255.255.0
             RIP Direction= Both
               Version= RIP-2B
             Multicast= None
             Edit IP Alias= No

                   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 next 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. The Prestige can also act as a surrogate DHCP server (**Relay**) where it relays IP address assignment from the actual real DHCP server to the clients. | **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<br>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. | |
| DHCP Server Address | The Prestige acts as a surrogate DHCP server when you select **Relay** from the **DHCP** field. This field is **N/A** when the **DHCP** field is **Server** or **None**. | **N/A** |

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

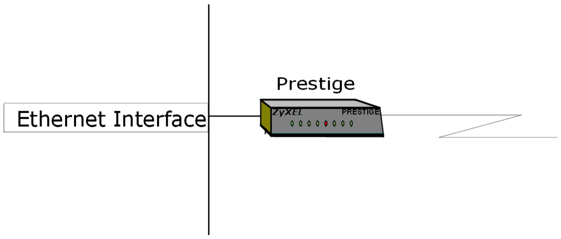
**Table 3-2 LAN TCP/IP Setup Menu Fields**

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

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Multicast | Turn on/off IGMP support by selecting from **IGMP-v2/IGMP-v1/ None**. | **None** (default) |
| Edit IP Alias | Toggle [SPACE BAR] to choose **Yes** or **No**. | **No** (default) |
| 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 IP Alias

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



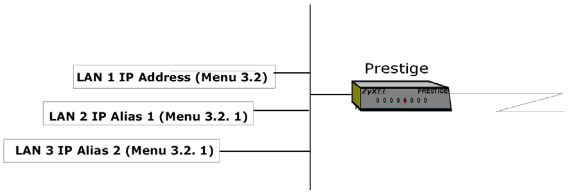

Prestige
LAN 1 IP Address (Menu 3.2)
LAN 2 IP Alias 1 (Menu 3.2. 1)
LAN 3 IP Alias 2 (Menu 3.2. 1)

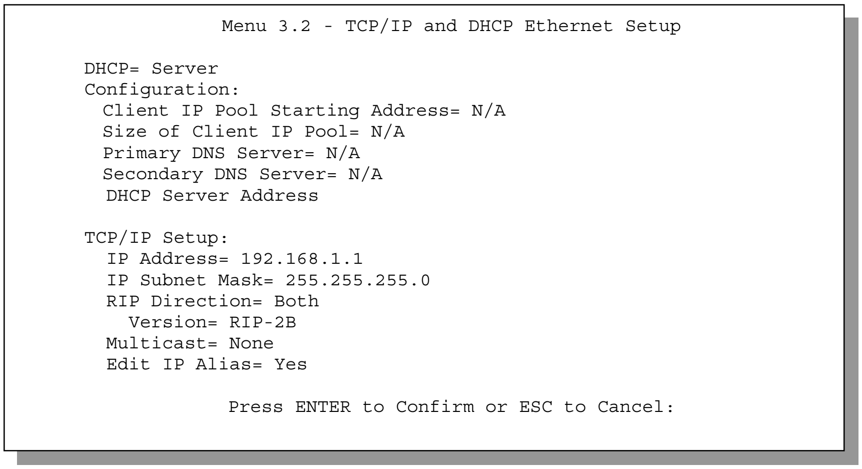
**Figure 3-3 Physical Network**

**Figure 3-4 Partitioned Logical Networks**

Use Menu 3.2.1 to configure IP Alias on your Prestige.

## 3.4 IP Alias Setup

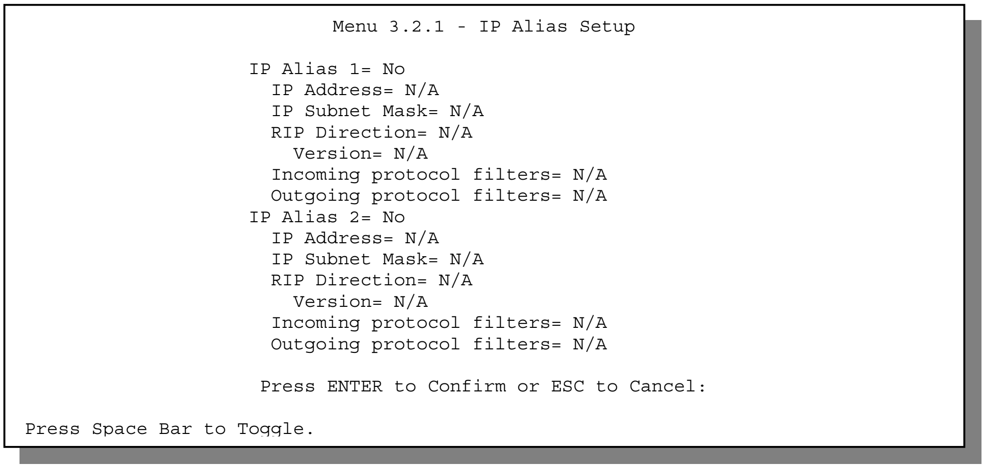
You must use **Menu 3.2** to configure the first network and move the cursor to **Edit IP Alias** field and toggle [SPACE BAR] to choose **Yes** and press [ENTER] to configure the second and third network.



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

      DHCP= Server
      Configuration:
        Client IP Pool Starting Address= N/A
        Size of Client IP Pool= N/A
        Primary DNS Server= N/A
        Secondary DNS Server= N/A
        DHCP Server Address

      TCP/IP Setup:
        IP Address= 192.168.1.1
        IP Subnet Mask= 255.255.255.0
        RIP Direction= Both
          Version= RIP-2B
        Multicast= None
        Edit IP Alias= Yes

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

Figure 3-5 Menu 3.2 – TCP/IP and DHCP Ethernet Setup

Pressing [ENTER] opens **Menu 3.2.1** – **IP Alias Setup**, as shown next.



```
                           Menu 3.2.1 - IP Alias Setup

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

                       Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 3-6 Menu 3.2.1 – IP Alias Setup

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

**Table 3-3 IP Alias Setup Menu Fields**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| IP Alias 1/2 | Choose **Yes** to configure the LAN network for the Prestige. | **Yes** |
| IP Address | Enter the IP address of your Prestige in dotted decimal notation. | **192.168.2.1** |
| IP Subnet Mask | Your Prestige will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Prestige. | **255.255.255.0** |
| RIP Direction | Press [SPACE BAR] to select the RIP direction from **Both/In Only/Out Only.** | **Both** |
| Version | Press [SPACE BAR] to select the RIP version from **RIP-1/RIP-2B/RIP-2M.** | **RIP-1** |
| Incoming Protocol Filters | Enter the filter set(s) you wish to apply to the incoming traffic between this node and the Prestige. | |
| Outgoing Protocol Filters | Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the Prestige. | |
| When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel. | | |

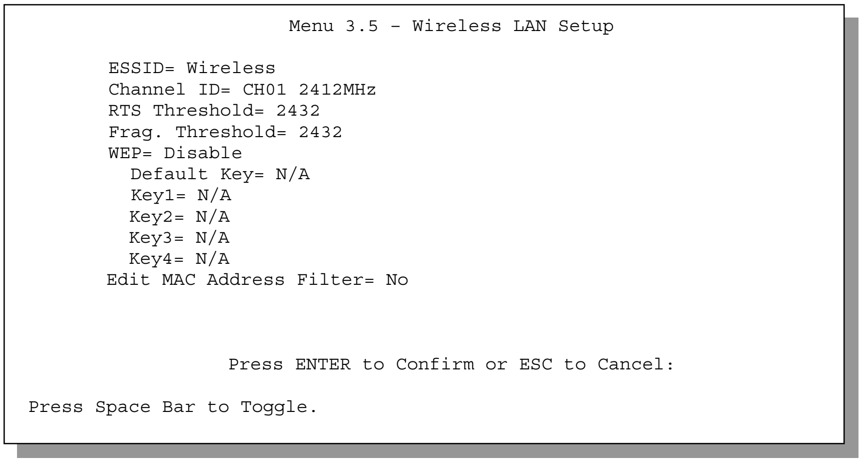
## 3.5 Wireless LAN Setup

The next-generation wireless LAN device – 11 Mbps wireless LAN brings Ethernet-like performance to the wireless realm. Fully compliant with the IEEE802.11(b) Direct Sequence Spread Spectrum (DSSS) standard, the 11 Mbps wireless LAN also provides powerful features such as WEP security.

As a minimum security precaution, we recommend that you change the ESSID setting of all devices on your network to a unique value, not the default value. A further improvement in security can be obtained by using Wired Equivalent Privacy (WEP) data encryption. However, there may be a significant degradation of the data throughput on the wireless link when WEP is enabled.

**If you are configuring the Prestige from a wireless computer and you change the Prestige's ESSID or WEP settings, you will lose your wireless connection when you press [ENTER] to confirm. You must then change the wireless settings of your computer to match the Prestige's new settings.**

From the main menu, enter 3 to open **Menu 3** – **LAN Setup** to configure the Wireless LAN setup. To edit the wireless LAN configuration, enter 5 to open **Menu 3.5** – **Wireless LAN Setup** as shown next.



```
                         Menu 3.5 - Wireless LAN Setup

         ESSID= Wireless
         Channel ID= CH01 2412MHz
         RTS Threshold= 2432
         Frag. Threshold= 2432
         WEP= Disable
           Default Key= N/A
           Key1= N/A
           Key2= N/A
           Key3= N/A
           Key4= N/A
         Edit MAC Address Filter= No



                    Press ENTER to Confirm or ESC to Cancel:

  Press Space Bar to Toggle.
```

**Figure 3-7 Menu 3.5 – Wireless LAN Setup**

Follow the instructions in the next table on how to configure the wireless LAN parameters.

**Table 3-4 Wireless LAN Setup Menu Fields**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| ESSID | (Extended Service Set IDentification) The ESSID identifies the Service Set the station is to connect to. Wireless clients associating to the Access Point must have the same ESSID. Enter a descriptive name (up to 32 characters) for the wireless LAN. | **Wireless** |
| Channel ID | This allows you to set the operating frequency/channel depending on your particular region. Use the  [SPACE BAR] to select a channel.<br>• CH01 2412 MHz / CH02 2417 MHz ~ CH11 2462 MHz (North America/FCC)<br>• CH01 2412 MHz / CH02 2417 MHz ~ CH13 2472 MHz (Europe CE/ ETSI)<br>• CH01 2412 MHz / CH02 2417 MHz ~ Ch14 2484 MHz (Japan)<br>• CH10 2457 MHz / CH11 2462 MHz (Spain)<br>• CH10 2457 MHz / CH11 2462 MHz ~ CH13 2472 MHz (France) | **CH01 2412 MHz** |
| RTS Threshold | (Request To Send) The threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will | 2432 (default) |

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| RTS Threshold | (Request To Send) The threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to zero turns on the RTS/CTS handshake. Enter a value between **0** and **2432**. | 2432 (default) |
| Frag. Threshold | The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter a value between **256** and **2432**. | 2432 (default) |
| WEP | (Wired Equivalent Privacy) To prevent unauthorized wireless stations from accessing data transmitted over the network, the Prestige 316 offers a data encryption, known as WEP to help encrypt wireless data transmitted via wireless medium. **Disable** allows wireless adapters to communicate with the Access Points without any data encryption. Select **64-bit WEP**[1] or **128-bit WEP** to allow data encryption. Although WEP is functional at 5.5 and 11 Mbps, there is significant performance degradation when using WEP at these rates. | **64-bit WEP** |
| Default Key | This allows you to select one WEP key as an active key to encrypt wireless data transmission. | **1** |
| Key1 to Key4 | If you chose **64-bit** WEP, then enter any 5 characters (ASCII string) or 10 hexadecimal digits ("0-9", "A-F") preceded by 0x for each Key (1-4).<br>If you chose **128-bit WEP**, then enter 13 characters (ASCII string) or 26 hexadecimal digits ("0-9", "A-F") preceded by 0x for each Key (1-4).<br>There are four data encryption keys to secure your data from eavesdropping by unauthorized wireless users. The values must be set up exactly the same on the Access Points as they are on the wireless client stations. The same value must be assigned to Key 1 on both the Access Point and the client adapters, the same value must be assigned to Key 2 on both the Access Point and the client stations and so on, for all four WEP keys. | ******** |
| Edit MAC Address Filter | Press the [SPACE BAR] once to select **Yes** to go to **Menu 3.5.1 - WLAN MAC Address Filter** discussed next. | **No** |

[1] The 64-bit WEP data encryption method, allows for a five-character (40-bit) input. Additionally, 24 factory-set bits are added to the forty-bit input to generate a 64-bit encryption key. (The 24 factory-set bits are not user-configurable). This encryption key will be used to encrypt/decrypt all data transmitted via the wireless interface. Some vendors refer to the 64-bit WEP data encryption as 40-bit WEP data encryption since the user-configurable portion of the encryption key is 40 bits wide.

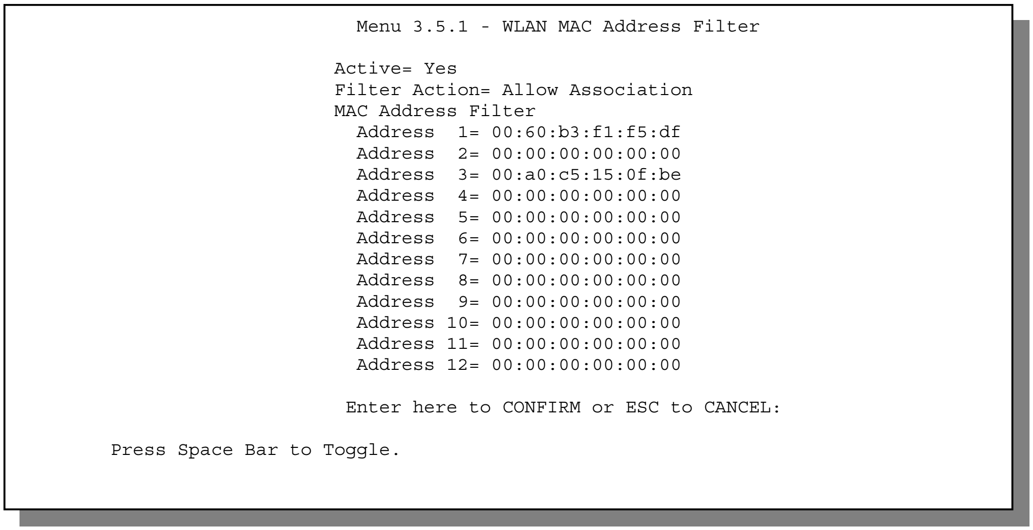
| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| When you have completed this menu, press [ENTER] at the prompt "Press ENTER to Confirm…" to save your configuration, or press [ESC] at any time to cancel. | | |

**The Prestige LAN Ethernet and wireless ports can transparently communicate with each other (transparent bridge).**

## 3.5.1 WLAN MAC Address Filter

In **Menu 3.5- Wireless LAN Setup** press the [SPACE BAR] once in the **Edit MAC Address Filter** field to select **Yes** and go to **Menu 3.5.1 - WLAN MAC Address Filter**.

A client computer is identified by the (unique) MAC address of its network card. Program the Prestige (the AP) with a list of MAC addresses associated with the client computers allowed or denied access to the AP.



```
                              Menu 3.5.1 - WLAN MAC Address Filter

                            Active= Yes
                            Filter Action= Allow Association
                            MAC Address Filter
                              Address  1= 00:60:b3:f1:f5:df
                              Address  2= 00:00:00:00:00:00
                              Address  3= 00:a0:c5:15:0f:be
                              Address  4= 00:00:00:00:00:00
                              Address  5= 00:00:00:00:00:00
                              Address  6= 00:00:00:00:00:00
                              Address  7= 00:00:00:00:00:00
                              Address  8= 00:00:00:00:00:00
                              Address  9= 00:00:00:00:00:00
                              Address 10= 00:00:00:00:00:00
                              Address 11= 00:00:00:00:00:00
                              Address 12= 00:00:00:00:00:00

                             Enter here to CONFIRM or ESC to CANCEL:

         Press Space Bar to Toggle.
```

**Figure 3-8 Menu 3.5.1 - WLAN MAC Address Filter**

**Table 3-5 Menu 3.5.1 - WLAN MAC Address Filter**

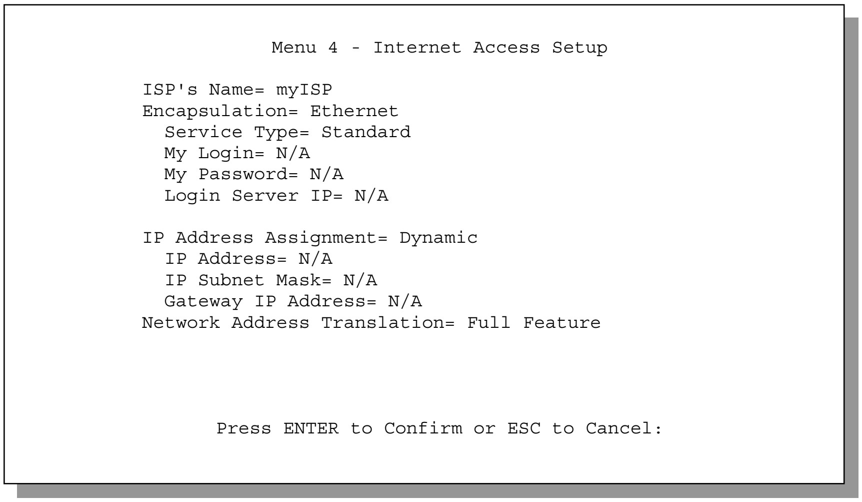
| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Active | Press the [SPACE BAR] to select **Yes** to make the wireless LAN MAC address filter active. | **Yes** |
| Filer Action | Press the [SPACE BAR] to select **Allow Association** or **Deny Association** and then enter the MAC addresses of the client computers in the **Address** fields. **Allow Association** means the client computers will be allowed access to the Prestige. **Deny Association** means those computers will be denied access to the Prestige | **Deny Association** |
| MAC Address Filter<br>Address 1 ~ 12 | Enter the MAC addresses of the client computers that are allowed or denied access to the Prestige in these **Address** fields. | **Deny Association** |
| 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. | | |

## 3.6 Internet Access Setup

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

### 3.6.1 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**, the following Menu 4 screen appears.



```
                    Menu 4 - Internet Access Setup

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

            IP Address Assignment= Dynamic
              IP Address= N/A
              IP Subnet Mask= N/A
              Gateway IP Address= N/A
            Network Address Translation= Full Feature




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

**Figure 3-9 Menu 4 – Internet Access Setup**

The following table describes this screen.

**Table 3-6 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 [SPACE BAR] and then press [ENTER] to choose **Ethernet**. The encapsulation method influences your choices for IP Address. |
| Service Type | This is applicable only when you choose Ethernet as your encapsulation method. Press the [SPACE BAR] to select **Standard**, **RR-Toshiba** (RoadRunner Toshiba authentication method) or **RR-Manager** (RoadRunner Manager authentication method). Choose a RoadRunner flavor if your ISP is Time Warner's RoadRunner; otherwise choose **Standard** or **RR-Telstra**. |
| NOTE: xDSL users must choose the **Standard** option only. The **Server IP**, **My Login IP** and **My Password** fields are not applicable in this case. | |
| My Login | Enter the login name given to you by your ISP. |
| My Password | Enter the password associated with the login name above. |
| Login Server IP | The Prestige will find the RoadRunner Server IP if this field is left blank. If it does not, then you must enter the authentication server IP address. |

| FIELD | DESCRIPTION |
|---|---|
| IP Address Assignment | If your ISP did not assign you a fixed IP address, select Dynamic, otherwise select Static and enter the IP address and subnet mask in the following fields. |
| IP Address | Enter the (fixed) IP address assigned to you by your ISP (Static *IP Address Assignment* is selected in the previous field). |
| IP Subnet Mask | Enter the subnet mask associated with your static IP. |
| Gateway IP Address | Enter the gateway IP address associated with your static IP. |
| Network Address Translation | Please see the NAT chapter for a more detailed discussion on this topic. |

### 3.6.2 PPTP Encapsulation

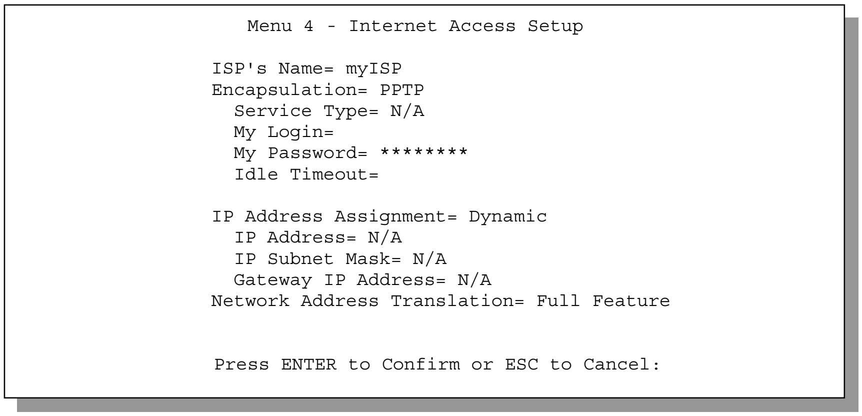
The Prestige supports PPTP (Point-to-Point Tunneling Protocol). PPTP is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet.

**The Prestige 316 supports only one PPTP server connection at any given time.**

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

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

If you enable PPTP in Menu 4, you will see the next screen.



```
                 Menu 4 - Internet Access Setup

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

              IP Address Assignment= Dynamic
                IP Address= N/A
                IP Subnet Mask= N/A
                Gateway IP Address= N/A
              Network Address Translation= Full Feature


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

**Figure 3-10 Menu 4 Using PPTP**

**Table 3-7 New Fields in Menu 4 (PPTP) Screen**

| FIELD | DESCRIPTION | EXAMPLES |
|---|---|---|
| Encapsulation | Press [SPACE BAR] and then press [ENTER] to choose PPTP. The encapsulation method influences your choices for IP address. | PPTP |
| Idle Timeout | This value specifies the time in seconds that elapses before the Prestige automatically disconnects from the PPTP server. | 100 (default) |

## 3.6.3 PPPoE Encapsulation

The Prestige supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC-2516) specifying how a personal computer (PC) interacts with a broadband modem (i.e., xDSL, cable, wireless, etc.) connection.

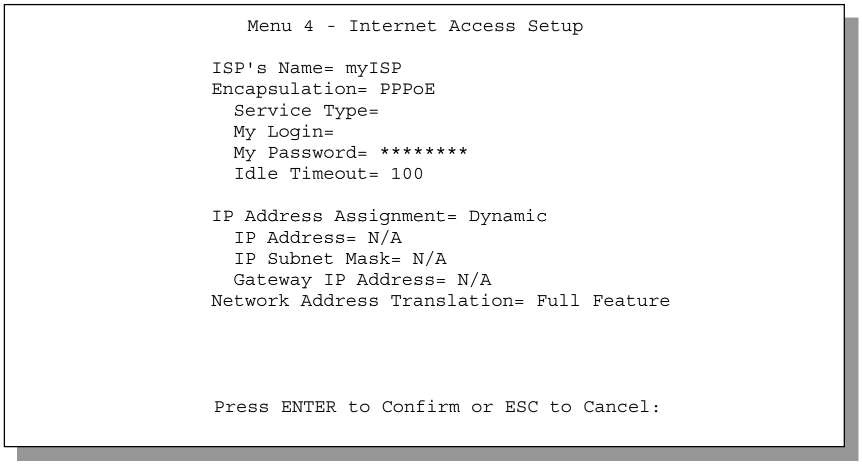
For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (e.g., Radius). For the user, PPPoE provides a login and authentication method that the existing Microsoft™ Dial-Up Networking software can activate and therefore requires no new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

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

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

By implementing PPPoE directly on the Prestige 316 rather than individual PC's, the machines on the LAN do **not** need PPPoE software installed, since the Prestige 316 does that part of the task.

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= myISP
                 Encapsulation= PPPoE
                   Service Type=
                   My Login=
                   My Password= ********
                   Idle Timeout= 100

                 IP Address Assignment= Dynamic
                   IP Address= N/A
                   IP Subnet Mask= N/A
                   Gateway IP Address= N/A
                 Network Address Translation= Full Feature




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

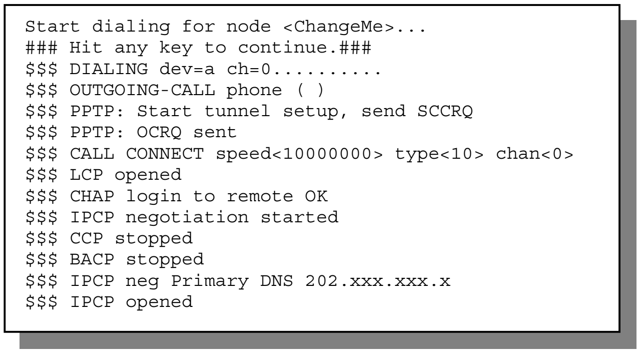
**Figure 3-11 Menu 4 Using PPPoE**

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

| FIELD | DESCRIPTION | EXAMPLES |
|---|---|---|
| Encapsulation | Press [SPACE BAR] and then press [ENTER] to choose PPPoE. The encapsulation method influences your choices for IP address. | PPPoE |
| Service Name | 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) |

## 3.7 Internet Test Setup

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



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

**Figure 3-12 Sample Internet Setup Test**

## 3.8 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 describe the advanced applications of your Prestige, such as Remote Node Setup IP Static routes and NAT.

# Chapter 4
# Remote Node Setup

*This chapter shows you how to configure a remote node.*

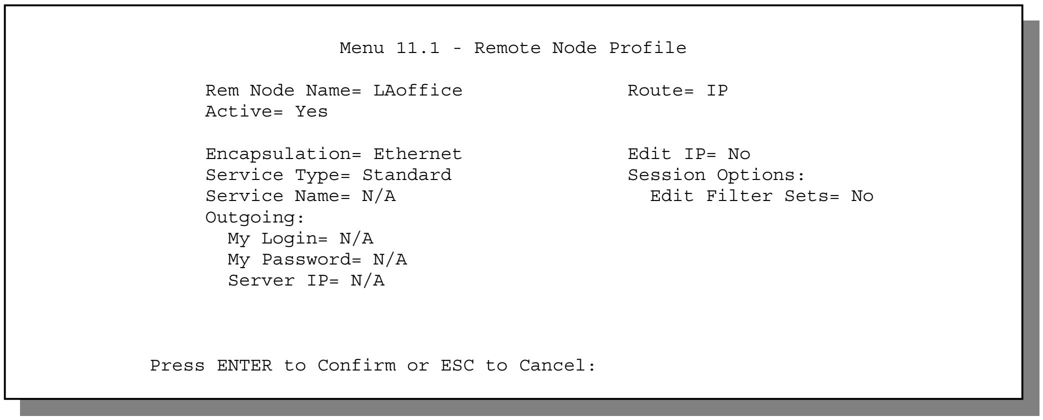
A remote node is required for placing calls to a remote gateway. A remote node represents both the remote gateway and the network behind it across a WAN connection. Note that when you use Menu 4 to set up Internet access, you are actually configuring a remote node. We will show you how to configure **Menu 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 option 11 to open **Menu 11.1 – Remote Node Profile**. There are three variations of this menu depending on whether you choose **Ethernet Encapsulation, PPTP 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= LAoffice               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

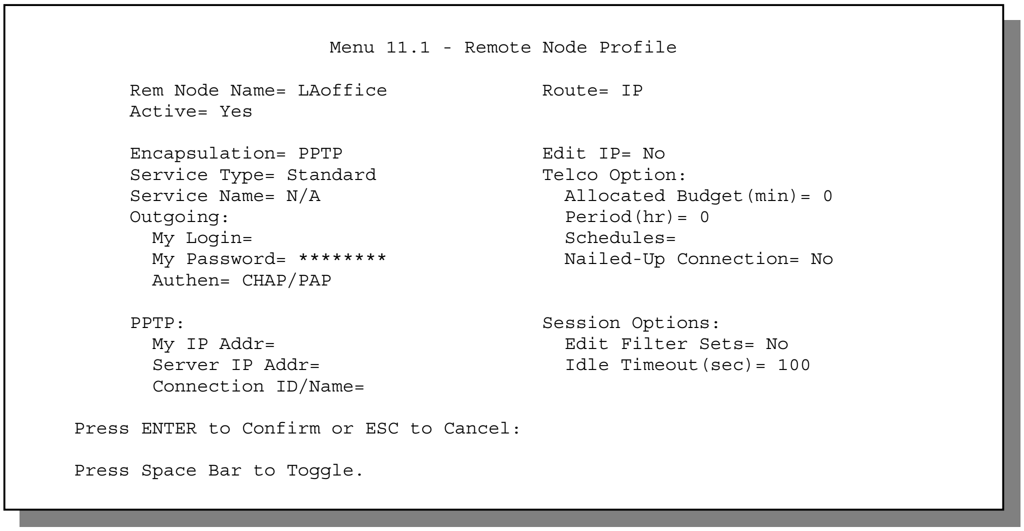
Table 4-1 Fields in Menu 11.1

| 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 [SPACE BAR] to toggle between **Yes** and **No** and activate (deactivate) the remote node. | **Yes** |
| Encapsulation | **Ethernet** is the default encapsulation. Press [SPACE BAR] if you wish to change to **PPTP**/**PPPoE** encapsulation. | **Ethernet** |
| Service Type | Press [SPACE BAR] to select from **Standard**, **RR-Toshiba** (RoadRunner Toshiba authentication method) **RR-Manager** (RoadRunner Manager authentication method), or **RR-Telstra** (RoadRunner Telstra authentication method). Choose one of the RoadRunner methods if your ISP is Time Warner's RoadRunner; otherwise choose **Standard**. | **Standard** |
| Service 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 **PPTP**/**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 | Enter the password assigned by your ISP when the Prestige calls this | ***** |

| FIELD | DESCRIPTION | EXAMPLES |
|---|---|---|
| Outgoing: My Password | Enter the password assigned by your ISP when the Prestige calls this remote node. Valid for **PPTP**/**PPPoE** encapsulation only. | ***** |
| Outgoing: 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 Prestige 316. | **IP** |
| Edit IP | This field leads to a “hidden” menu. Press [SPACE BAR] to select **Yes** and press [ENTER] to go to **Menu 11.3 – Remote Node Network Layer Options**. | **Yes** |
| Session Options: Edit Filter sets | This field leads to another “hidden” menu. Use [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 PPTP Encapsulation

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



```
                          Menu 11.1 - Remote Node Profile

           Rem Node Name= LAoffice              Route= IP
           Active= Yes

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

           PPTP:                                Session Options:
             My IP Addr=                          Edit Filter Sets= No
             Server IP Addr=                      Idle Timeout(sec)= 100
             Connection ID/Name=

      Press ENTER to Confirm or ESC to Cancel:

      Press Space Bar to Toggle.
```

**Figure 4-2 Menu 11.1 Remote Node Profile for PPTP Encapsulation**

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

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

| FIELD | DESCRIPTION | EXAMPLES |
|---|---|---|
| Encapsulation | Toggle [SPACE BAR] to choose **PPTP/PPPoE**. You must also go to **Menu 11.3** to check the IP address setting once you have selected the encapsulation method. | **PPTP/ PPPoE** |
| Authen | This field sets the authentication protocol used for outgoing calls. Your Prestige supports two authentication protocols: PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol).<br>• **PAP** sends the user name and password in plain text.<br>• **CHAP** scrambles the password before it is sent over the wire.<br>Generally speaking, CHAP is more secure than PAP, however, PAP is readily available on more platforms. The recommendation is to use CHAP whenever possible.<br>Options for this field are:<br>• **CHAP/PAP** – your Prestige will try CHAP when CHAP is requested by the Remote Node or PAP when PAP is requested by the Remote Node.<br>• **CHAP** – use CHAP only.<br>• **PAP** – use PAP only. | **CHAP/PAP / CHAP / PAP** |
| PPTP: My IP Addr | Enter the IP address of the WAN Ethernet port. | 10.0.0.140 (default) |
| PPTP: Server IP Addr | Enter the IP address of the ANT modem. | 10.0.0.138 (default) |
| PPTP: Connection ID/ Name | Enter the connection ID or name in the ANT. It must follow the “c:id” and “n:name” format. This field is optional and depends on the requirements of your xDSL modem. | N:myISP |
| Telco Option: Allocated Budget (min) | This field sets a ceiling for outgoing call time for this remote node. The default for this field is 0 meaning no budget control. | 10 |
| Telco Option: 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 |
| Telco Option: Schedules | You can apply up to 4 schedule sets here. For more details, please refer to the chapter on *Call Schedule Setup*. | |

| FIELD | DESCRIPTION | EXAMPLES |
|---|---|---|
| Telco Option: Nailed-Up Connection | This field specifies if you want to make the connection to this remote node a nailed-up connection. For more details, please see ahead. | |
| Session Options: Idle Timeout (sec) | 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 PPTP/PPPoE connection.<br>**NOTE:** This option only applies when the Prestige initiates the call. | **100 seconds** (default) |

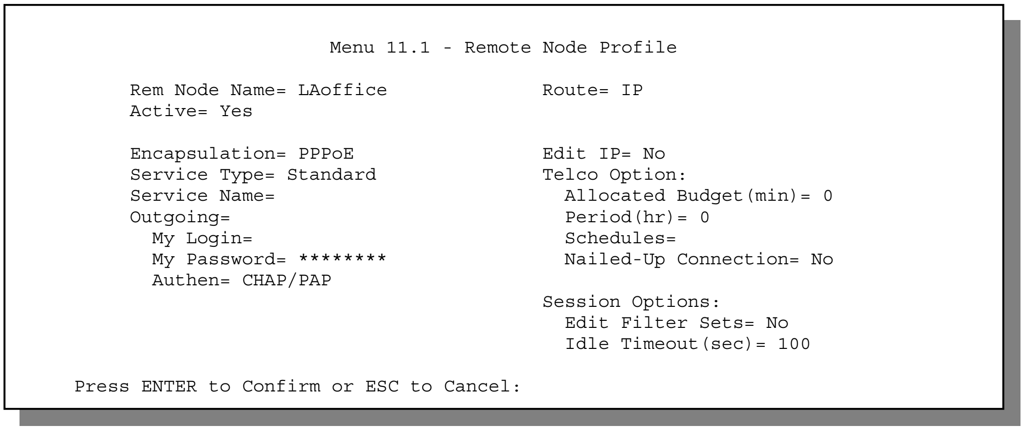
### Nailed-Up Connection

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

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

## 4.1.3 PPPoE Encapsulation

The Prestige supports PPPoE (Point-to-Point Protocol over Ethernet). You can only use PPPoE encapsulation when you are using the Prestige with a 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.



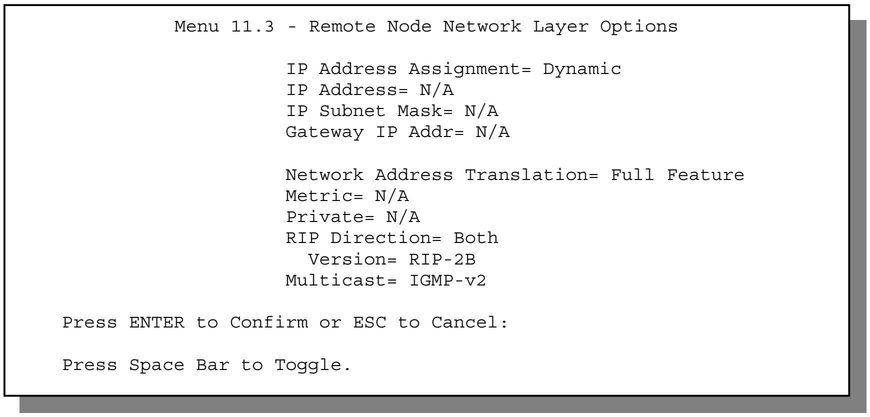
```
                           Menu 11.1 - Remote Node Profile

         Rem Node Name= LAoffice              Route= IP
         Active= Yes

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

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

**Figure 4-3 Menu 11.1 Remote Node Profile for PPPoE Encapsulation**

## 4.2 Editing TCP/IP Options

### 4.2.1 Ethernet Encapsulation

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



```
              Menu 11.3 - Remote Node Network Layer Options

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

                        Network Address Translation= Full Feature
                        Metric= N/A
                        Private= N/A
                        RIP Direction= Both
                          Version= RIP-2B
                        Multicast= IGMP-v2

    Press ENTER to Confirm or ESC to Cancel:

    Press Space Bar to Toggle.
```

**Figure 4-4 Remote Node Network Layer Options**

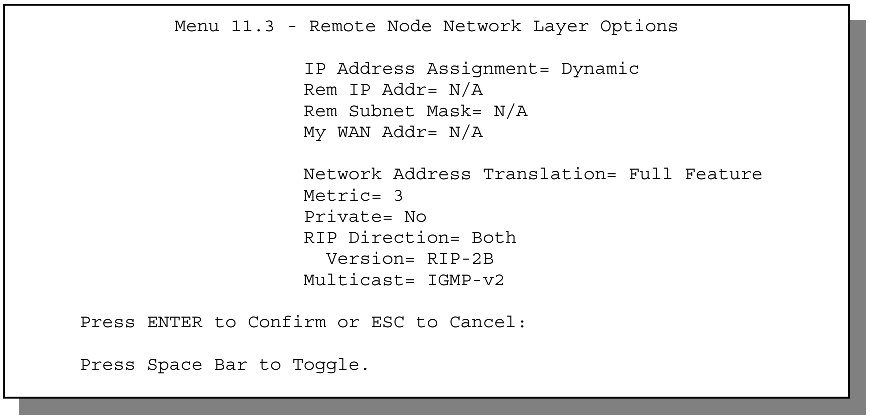
The next table gives you instructions about configuring remote node network layer options.

### 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 and subnet mask in the following fields. | **Dynamic** |
| IP Address | If you have a **Static IP Assignment,** enter the IP address assigned to you by your ISP. | |
| IP Subnet Mask | If you have a **Static IP Assignment,** enter the subnet mask assigned to you. | |
| Gateway IP Addr | If you have a **Static IP Assignment**, enter the gateway IP address assigned to you. | |
| Network Address Translation | Use [SPACE BAR] to toggle between **Full Feature, SUA Only** and **None**. See a previous section for a full discussion of this feature. | **Full Feature** |
| Metric | 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. This field is **N/A** if *Encapsulation* field is **Ethernet**. | **3** |
| 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. This field is **N/A** if *Encapsulation* field is **Ethernet**. | **Yes** |
| RIP Direction | Press [SPACE BAR] to select the **RIP direction** from **Both/None/In Only** /**Out Only**. Please see a previous section 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 [SPACE BAR] to select the RIP version from **RIP-1/RIP-2B/RIP-2M** and **N/A.** | **RIP-2B** |
| Multicast | Turn on/off IGMP support and select the version from **IGMP-v2/ IGMP-v1/None**. | **None** |
| Once you have completed filling in the Remote Node 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. | | |

### 4.2.2 PPTP/PPPoE Encapsulation

Make sure that **Encapsulation** is set to **PPTP/PPPoE** in Menu 11.1. Move the cursor to the **Edit IP** field in **Menu 11.1**, then press [SPACE BAR] to toggle and set the value to **Yes**. Press [ENTER] to open **Menu 11.3 – Remote Node 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

                           Network Address Translation= Full Feature
                           Metric= 3
                           Private= No
                           RIP Direction= Both
                             Version= RIP-2B
                           Multicast= IGMP-v2

      Press ENTER to Confirm or ESC to Cancel:

      Press Space Bar to Toggle.
```

**Figure 4-5 Remote Node Network Layer Options**

The next table gives you instructions about configuring remote node network layer options not covered in Table 5-3.

**Table 4-4 Remote Node Network Layer Options Menu Fields**

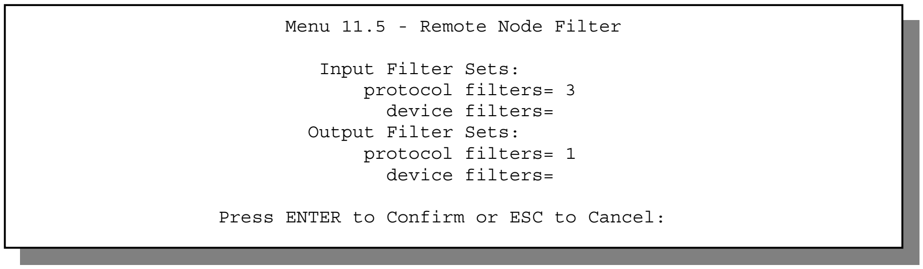
| FIELD | DESCRIPTION |
|---|---|
| Rem IP Addr | If you have a Static IP Assignment, enter the IP address assigned to the remote node. |
| Rem Subnet Mask | If you have a **Static IP Assignment,** enter the subnet mask assigned to the remote node. |
| My WAN Addr | Some implementations, especially the UNIX derivatives require the WAN link to have a separate IP network number from the LAN and each end must have a unique address within the WAN network number. If this is the case, enter the IP address assigned to the WAN port of your Prestige.<br>**NOTE:** This is the address assigned to your local Prestige, not the remote router. |

## 4.3 Remote Node Filter

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

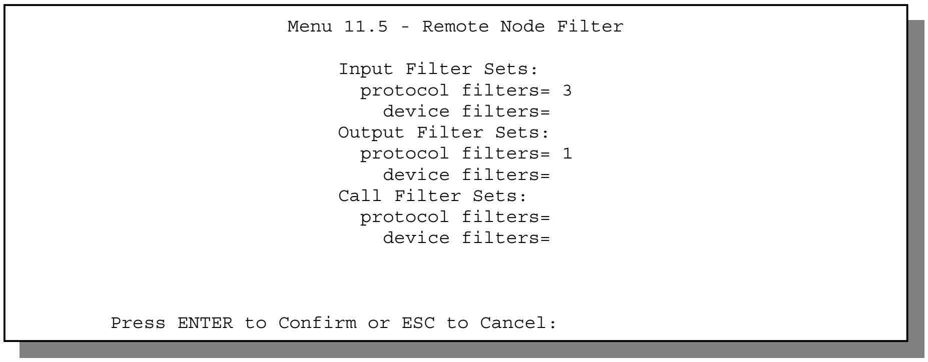
Use **Menu 11.5** to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the Prestige and to prevent certain packets from triggering calls. You can specify up to four filter sets separated by a comma, e.g., 1, 5, 9, 12, in each **filter** field.

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 PPTP and 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=

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

**Figure 4-6 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=
                                device filters=



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

**Figure 4-7 Remote Node Filter (PPTP/PPPoE Encapsulation)**

# Chapter 5
# IP Static Route Setup

*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 does not 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.

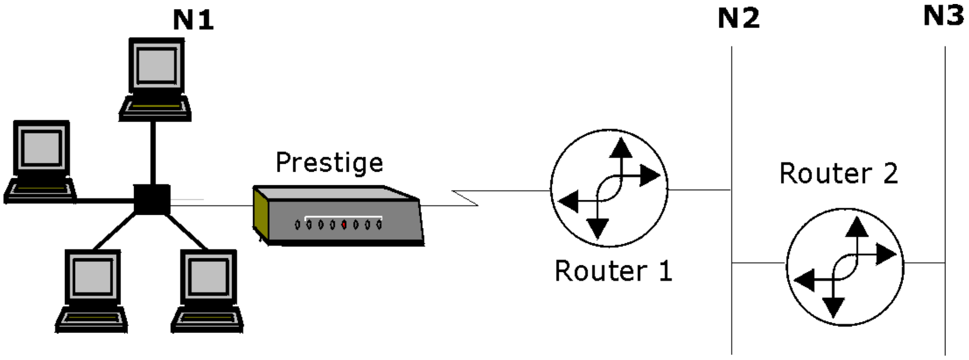
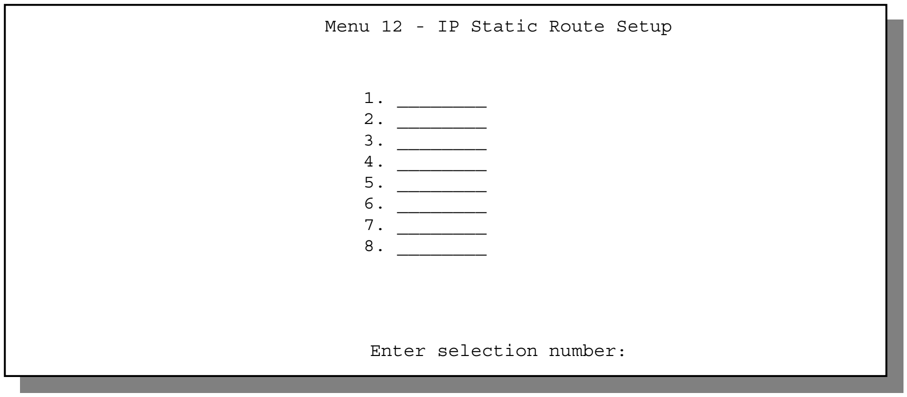


**Figure 5-1 Example of Static Routing Topology**

## 5.1 IP Static Route Setup

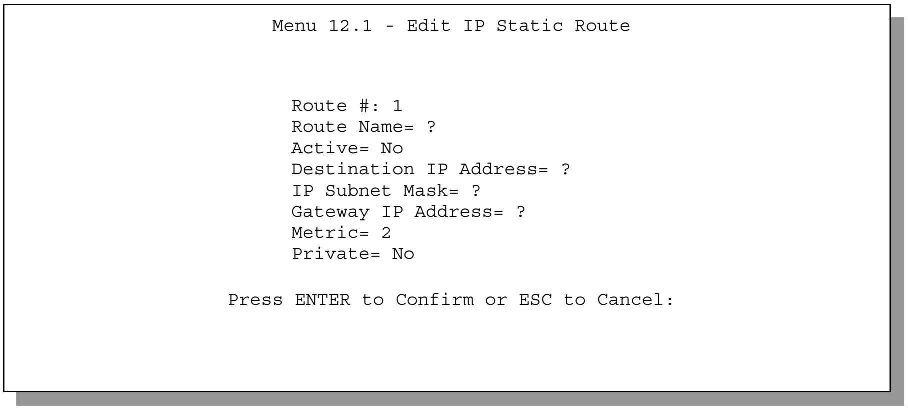
You configure IP static routes in **Menu 12.1**, by selecting one of the IP static routes as shown next. Enter 12 from the main menu.



```
                         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 Network Address Translation (NAT)

*This chapter discusses how to configure NAT on the Prestige.*

## 6.1 Introduction

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

### 6.1.1 NAT Definitions

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

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

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

**Table 6-1 NAT Definitions**

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

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

### 6.1.2 What NAT Does

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

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, e.g., a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping – see *Table 6-2*), NAT offers the additional benefit of firewall protection. If no server is defined in these cases, all incoming inquiries will be filtered out by your Prestige, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631*, *The IP Network Address Translator (NAT).*

### 6.1.3 How NAT Works

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

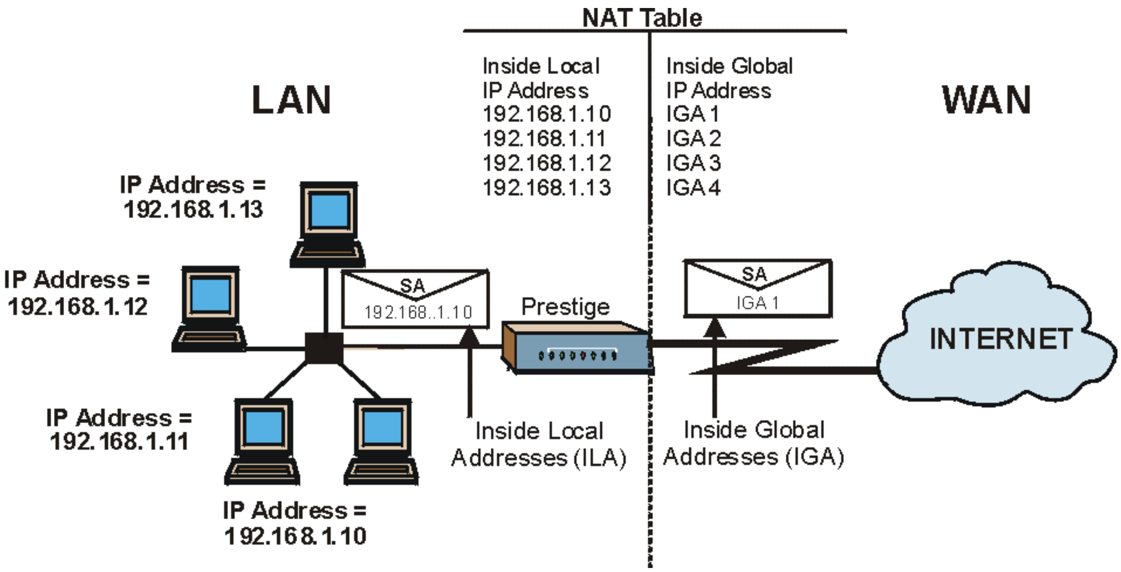


**Figure 6-1 How NAT Works**

### 6.1.4 NAT Application

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

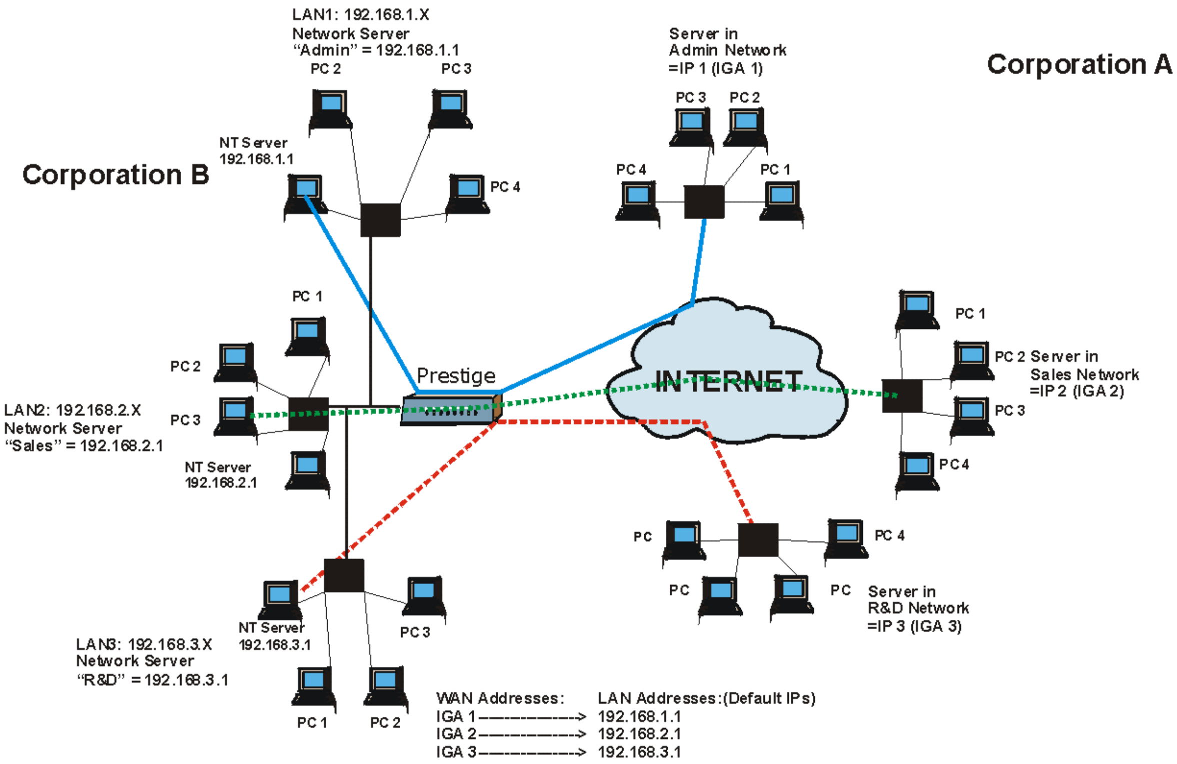


**Figure 6-2 NAT Application With IP Alias**

### 6.1.5 NAT Mapping Types

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

1. **One to One**: In One-to-One mode, the Prestige maps one local IP address to one global IP address.
2. **Many to One**: In Many-to-One mode, the Prestige maps multiple local IP addresses to one global IP address. This is equivalent to SUA (i.e., PAT, port address translation), ZyXEL's Single User Account feature (**SUA Only**).
3. **Many to Many Overload**: In Many-to-Many Overload mode, the Prestige maps the multiple local IP addresses to shared global IP addresses.
4. **Many to Many No Overload**: In Many-to-Many No Overload mode, the Prestige maps the each local IP addresses to unique global IP addresses.

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

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

The following table summarizes these types.

**Table 6-2 NAT Mapping Types**

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

## 6.2 Using NAT

### 6.2.1 SUA (Single User Account) Versus NAT

SUA (Single User Account) is a ZyNOS implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. See section *6.3.1* for a detailed description of the NAT set for SUA.

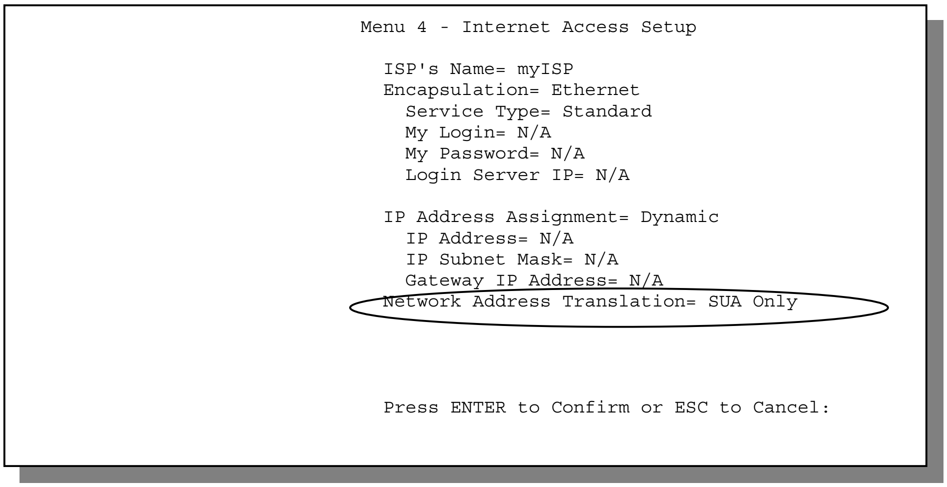
The Prestige also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types as outlined in *Table 6-2*.

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

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

### 6.2.2 Applying NAT

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



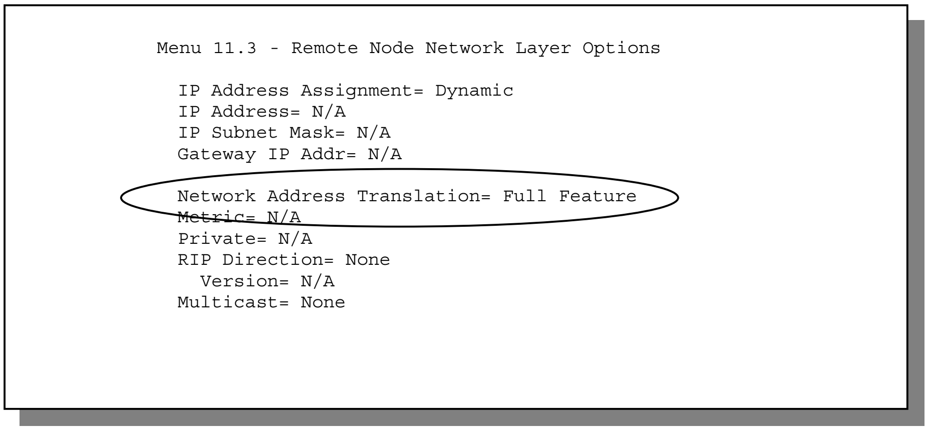
```
                        Menu 4 - Internet Access Setup

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

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



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

**Figure 6-3 Menu 4 — Applying NAT for Internet Access**

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

**Step 1.** Enter 11 from the main menu.

**Step 2.** Move the cursor to the **Edit IP** field, press the [SPACE BAR] to select **Yes** and then press [ENTER] to bring up **Menu 11.3 - Remote Node Network Layer Options.**



```
                    Menu 11.3 - Remote Node Network Layer Options

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

                      Network Address Translation= Full Feature
                      Metric= N/A
                      Private= N/A
                      RIP Direction= None
                        Version= N/A
                      Multicast= None
```

**Figure 6-4 Menu 11.3 — Applying NAT to the Remote Node**

The following table describes the options for Network Address Translation.

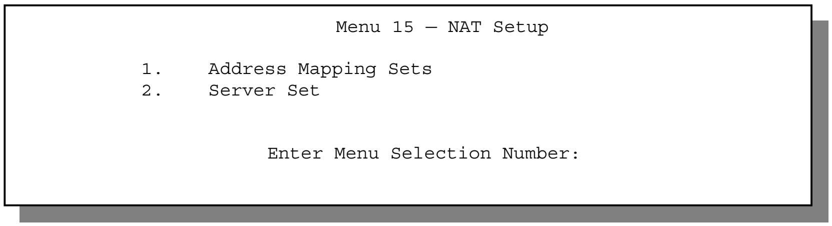
**Table 6-3 Applying NAT in Menus 4 & 11.3**

| FIELD | OPTIONS | DESCRIPTION |
|---|---|---|
| Network Address Translation | **Full Feature** | When you select this option the SMT will use Address Mapping Set 1 (menu 15.1 - see section *6.3.1* for further discussion). You can configure any of the mapping types described in *Table 6-2*. Choose **Full Feature** if you have multiple public WAN IP addresses for your Prestige. |
| | **None** | NAT is disabled when you select this option. |
| | **SUA Only** | When you select this option the SMT will use Address Mapping Set 255 (menu 15.1 - see section *6.3.1*). Choose **SUA Only** if you have just one public WAN IP address for your Prestige. |

## 6.3 NAT Setup

Use the Address Mapping Sets menus and submenus to create the mapping table used to assign global addresses to computers on the LAN. You can see two NAT Address Mapping sets in menu 15.1. You can only configure **Set 1**. **Set 255** is used for SUA. When you select **Full Feature** in menu 4 or 11.3, the SMT will use **Set 1**, which supports all mapping types as outlined in *Table 6-2.* When you select **SUA Only**, the SMT will use the pre-configured **Set 255** (read only).

The Server Set is a list of LAN side servers mapped to external ports. To use this set (one set for the Prestige 10), a server rule must be set up inside the NAT Address Mapping set. Please see *section 6.4* for further information on these menus. To configure NAT, enter 15 from the main menu to bring up the following screen.

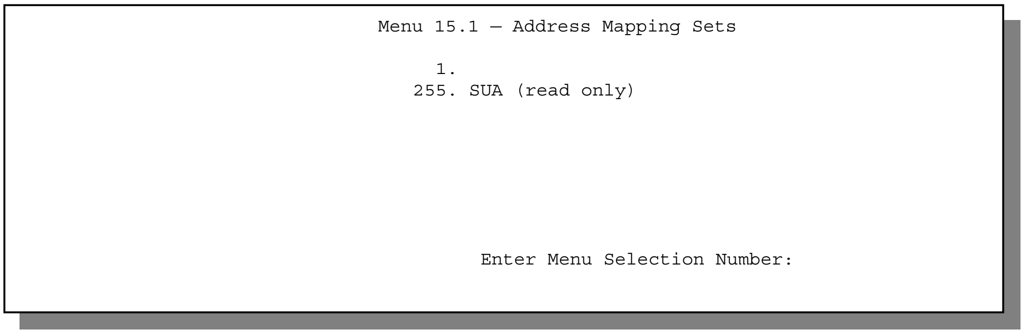


```
                    Menu 15 — NAT Setup

          1.    Address Mapping Sets
          2.    Server Set


                Enter Menu Selection Number:
```

Figure 6-5 Menu 15 — NAT Setup

### 6.3.1 Address Mapping Sets

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

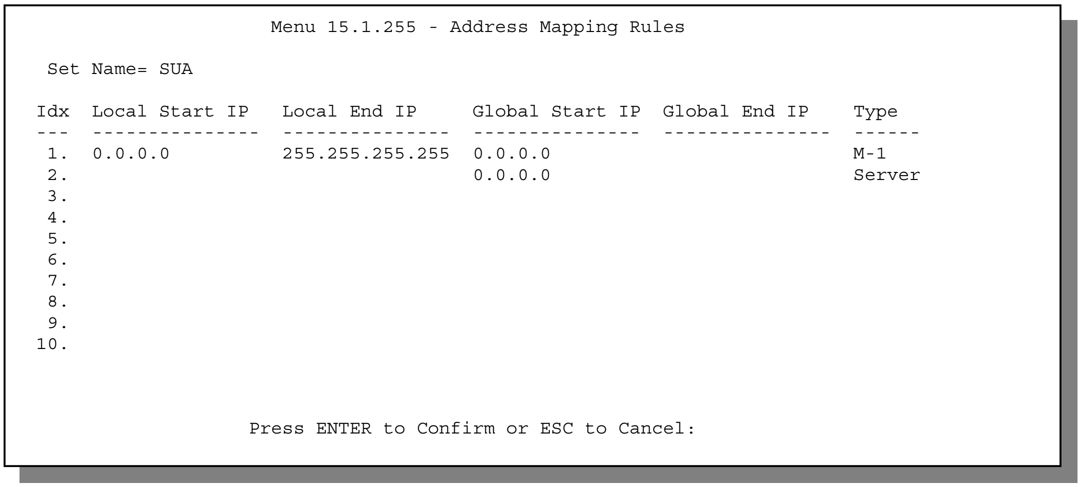


```
                         Menu 15.1 — Address Mapping Sets

                              1.
                            255. SUA (read only)







                                     Enter Menu Selection Number:
```

Figure 6-6 Menu 15.1 — Address Mapping Sets

### SUA Address Mapping Set

Enter 255 to display the next screen (see also *section 6.2.1)*. The fields in this menu cannot be changed.



```
                     Menu 15.1.255 - Address Mapping Rules

 Set Name= SUA

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



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

**Figure 6-7 Menu 15.1.255 — SUA Address Mapping Rules**

The following table explains the fields in this screen.

**The fields in Menu 15.1.255 are read-only.**

**Table 6-4 SUA Address Mapping Rules**

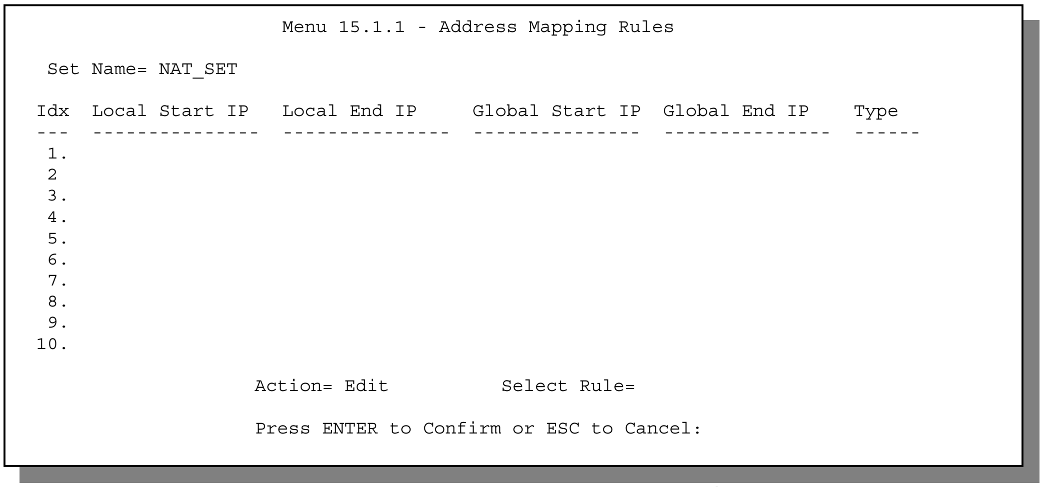
| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Set Name | This is the name of the set you selected in menu 15.1 or enter the name of a new set you want to create. | **SUA** |
| Idx | This is the index or rule number. | 1 |
| Local Start IP<br>Local End IP | **Local Start IP** is the starting local IP address (ILA) (see *Figure 6-1)*. **Local End IP** is the ending local IP address (ILA). If the rule is for all local IPs, then the Start IP is 0.0.0.0 and the End IP is 255.255.255.255. | 0.0.0.0<br>255.255.255.255 |
| Global Start IP | This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global Start IP**. | 0.0.0.0 |
| Global End IP | This is the ending global IP address (IGA). | **N/A** |
| Type | These are the mapping types discussed above (see *Table 6-2*). **Server** allows us to specify | **Server** |

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Type | These are the mapping types discussed above (see *Table 6-2*). **Server** allows us to specify multiple servers of different types behind NAT to this machine. See later for some examples. | **Server** |
| Once you have finished configuring a rule in this menu, press [ENTER] at the message “Press ENTER to Confirm…” to save your configuration, or press [ESC] to cancel. | | |

## User-Defined Address Mapping Sets

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

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



```
                         Menu 15.1.1 - Address Mapping Rules

   Set Name= NAT_SET

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

                      Action= Edit          Select Rule=

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

**Figure 6-8 Menu 15.1.1 — First Set**

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

## Ordering Your Rules

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

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

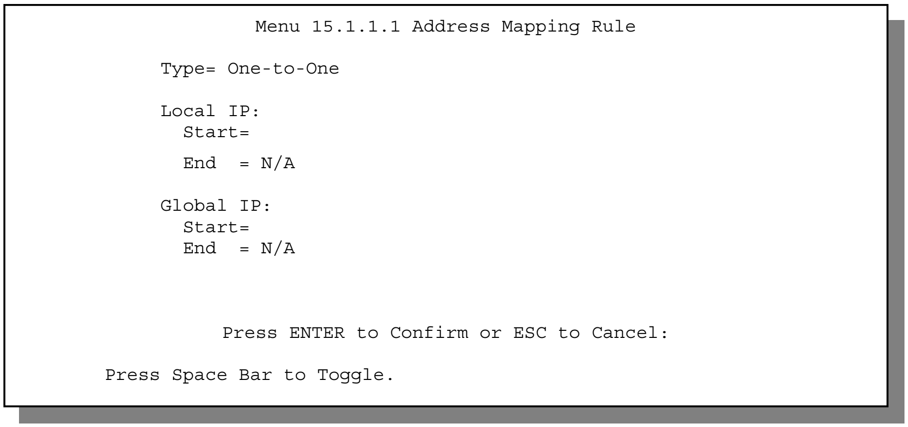
**Table 6-5 Fields in Menu 15.1.1**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Set Name | Enter a name for this set of rules. This is a required field. If this field is left blank, the entire set will be deleted. | NAT_SET |
| Action | The default is **Edit**. **Edit** means you want to edit a selected rule (see following field). **Insert Before** means to insert a rule before the rule selected. The rules after the selected rule will then be moved down by one rule. **Delete** means to delete the selected rule and then all the rules after the selected one will be advanced one rule. **None** disables the **Select Rule** item. | **Edit** |
| Select Rule | When you choose **Edit**, **Insert Before** or **Delete** in the previous field the cursor jumps to this field to allow you to select the rule to apply the action in question. | 1 |

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

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

**The IP Start Address field should contain the first address in a range of contiguous IP addresses. The IP End Address field should contain the last address in the corresponding range of contiguous address.**



```
                      Menu 15.1.1.1 Address Mapping Rule

              Type= One-to-One

              Local IP:
                Start=
                End  = N/A

              Global IP:
                Start=
                End  = N/A



                   Press ENTER to Confirm or ESC to Cancel:

          Press Space Bar to Toggle.
```

**Figure 6-9 Menu 15.1.1.1 — Editing/Configuring an Individual Rule in a Set**

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

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Type | Press the [SPACE BAR] to toggle through a total of five types. These are the mapping types discussed in *Table 6-2*. **Server** allows you to specify multiple servers of different types behind NAT to this computer. See *section 6.5.3 below* for an example. | **One-to-One** |
| Local IP | Only local IP fields are **N/A** for server; Global IP fields MUST be set for **Server**. | |
| Start | This is the starting local IP address (ILA). | 0.0.0.0 |
| End | This is the ending local IP address (ILA). If the rule is for all local IPs, then put the Start IP as 0.0.0.0 and the End IP as 255.255.255.255. This field is **N/A** for One-to-One and Server types. | N/A |
| Global IP | | |
| Start | This is the starting global IP address (IGA). If you have a dynamic IP, enter 0.0.0.0 as the **Global IP Start**. Note that **Global IP Start** can be set to 0.0.0.0 only if the types are **Many-to-One** or **Server**. | 0.0.0.0 |
| End | This is the ending global IP address (IGA). This field is **N/A** for **One-to-One**, **Many-to-One** and **Server types**. | N/A |
| Once you have finished configuring a rule in this menu, press [ENTER] at the message "Press ENTER to Confirm…" to save your configuration, or press [ESC] to cancel. | | |

## 6.4 NAT Server Sets – Port Forwarding

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

Use **Menu 15 - NAT Setup** to forward incoming service requests to the server(s) on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers. Entry 12 (port 1026) is non-editable (see *Figure 6-10*).

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

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

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

**Table 6-7 Services & Port Numbers**

| SERVICES | PORT NUMBER |
|---|---|
| ECHO | 7 |
| FTP (File Transfer Protocol) | 21 |
| Telnet | 23 |
| SMTP (Simple Mail Transfer Protocol) | 25 |
| DNS (Domain Name System) | 53 |
| Finger | 79 |
| HTTP (Hyper Text Transfer protocol or WWW, Web) | 80 |
| POP3 (Post Office Protocol) | 110 |
| NNTP (Network News Transport Protocol) | 119 |
| SNMP (Simple Network Management Protocol) | 161 |
| SNMP trap | 162 |
| PPTP (Point-to-Point Tunneling Protocol) | 1723 |

### 6.4.1 Configuring a Server behind NAT

Follow these steps to configure a server behind NAT:

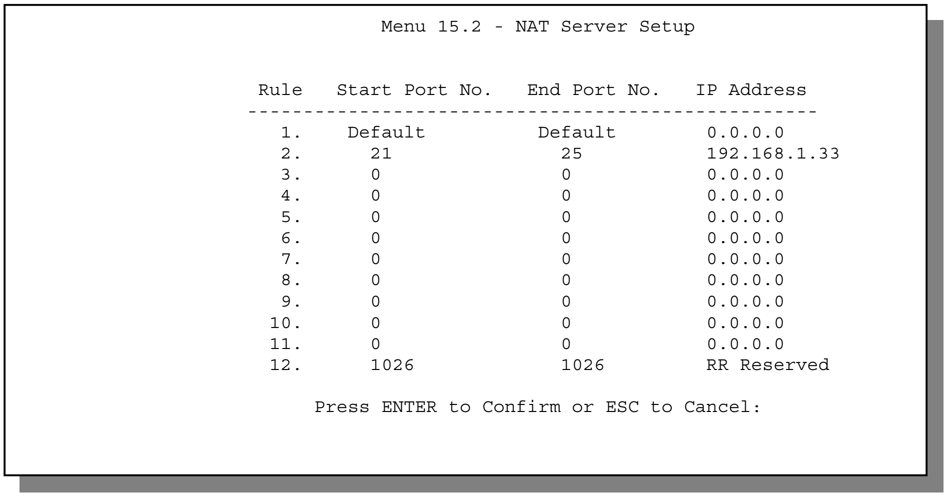
**Step 1.** Enter 15 in the main menu to go to **Menu 15 - NAT Setup.**

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

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

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

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



```
                         Menu 15.2 - NAT Server Setup


             Rule   Start Port No.   End Port No.   IP Address
            ---------------------------------------------------
               1.    Default          Default        0.0.0.0
               2.      21               25           192.168.1.33
               3.      0                0            0.0.0.0
               4.      0                0            0.0.0.0
               5.      0                0            0.0.0.0
               6.      0                0            0.0.0.0
               7.      0                0            0.0.0.0
               8.      0                0            0.0.0.0
               9.      0                0            0.0.0.0
              10.      0                0            0.0.0.0
              11.      0                0            0.0.0.0
              12.      1026             1026         RR Reserved

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

Figure 6-10 Menu 15.2 — NAT Server Setup

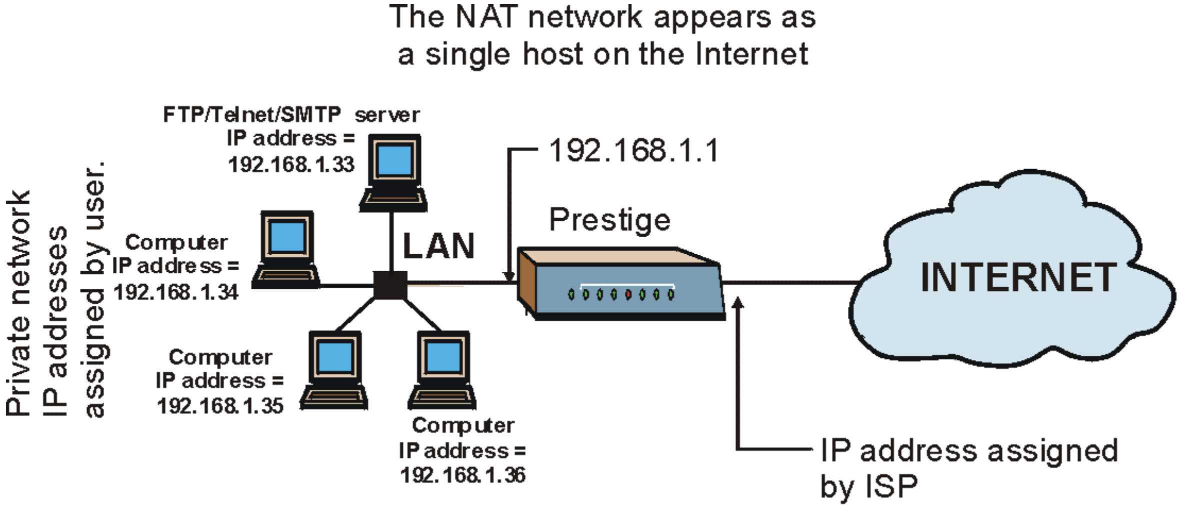


Figure 6-11 Multiple Servers Behind NAT Example

# 6.5 General NAT Examples

## 6.5.1 Internet Access Only

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

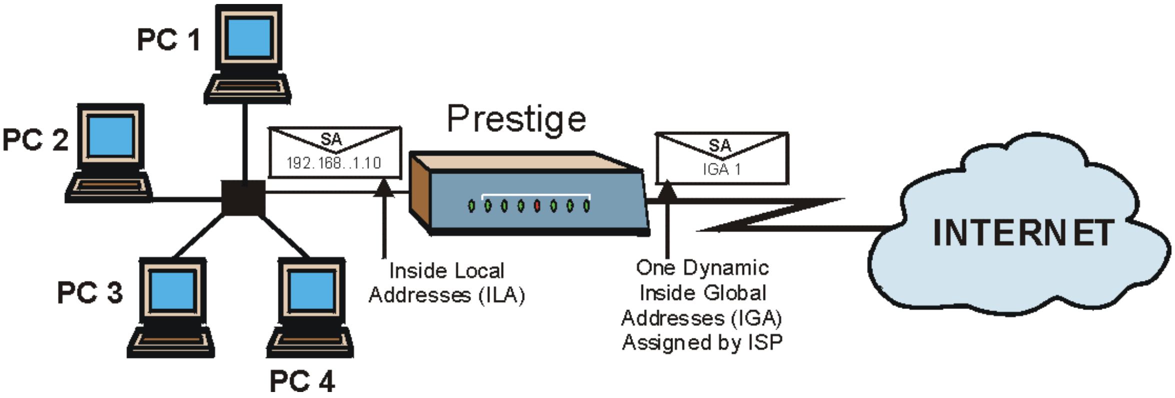
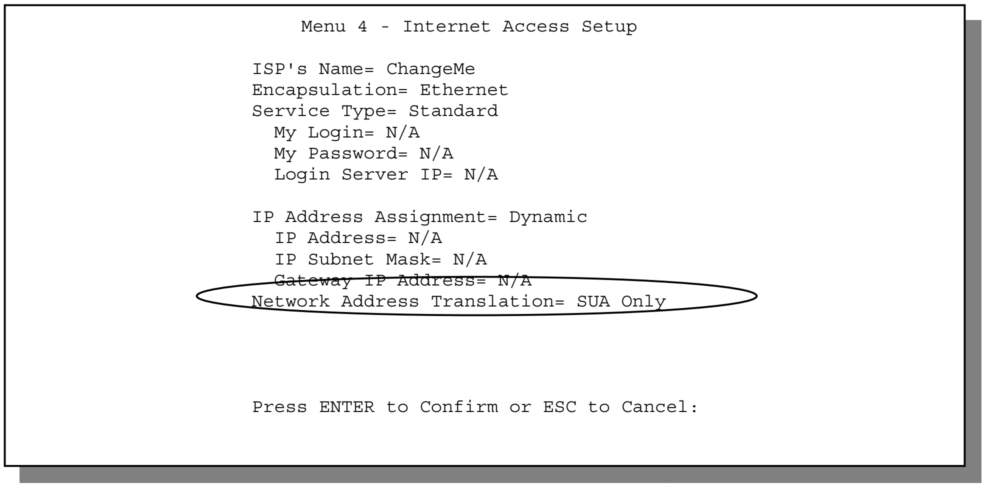


Figure 6-12 NAT Example 1



```
                 Menu 4 - Internet Access Setup

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

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



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

Figure 6-13 Menu 4 — Internet Access & NAT Example

From menu 4 shown above, simply choose the **SUA Only** option from the **Network Address Translation** field. This is the Many-to-One mapping discussed in *section 6.1.5*. The **SUA Only** read-only option from the **Network Address Translation** field in menus 4 and 11.3 is specifically pre-configured to handle this case.

## 6.5.2 Example 2: Internet Access with an Inside Server

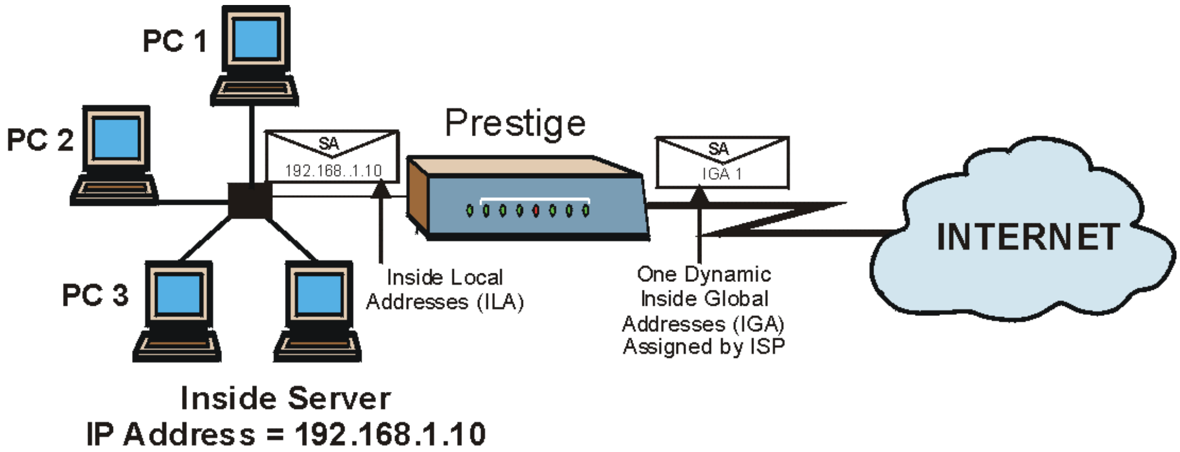
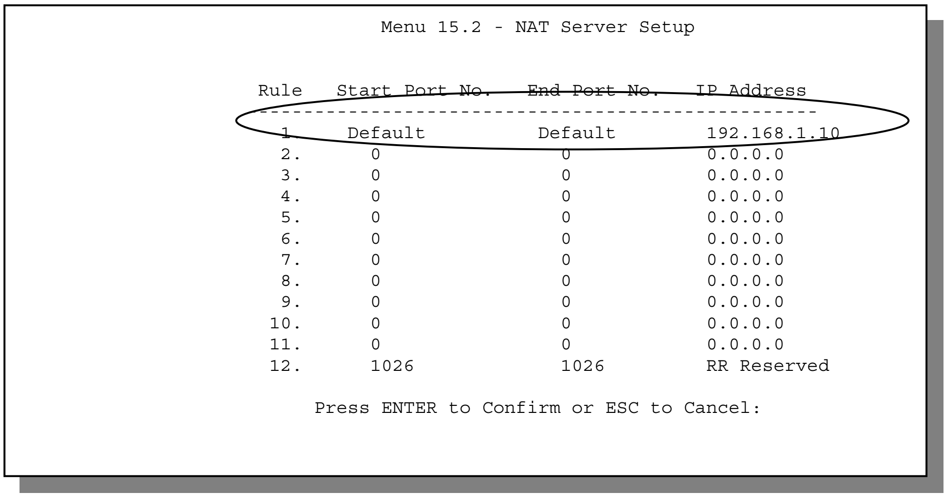


**Figure 6-14 NAT Example 2**

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



```
                    Menu 15.2 - NAT Server Setup

          Rule   Start Port No.   End Port No.   IP Address
          ---------------------------------------------------
            1.     Default          Default        192.168.1.10
            2.     0                0              0.0.0.0
            3.     0                0              0.0.0.0
            4.     0                0              0.0.0.0
            5.     0                0              0.0.0.0
            6.     0                0              0.0.0.0
            7.     0                0              0.0.0.0
            8.     0                0              0.0.0.0
            9.     0                0              0.0.0.0
           10.     0                0              0.0.0.0
           11.     0                0              0.0.0.0
           12.     1026             1026           RR Reserved

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

**Figure 6-15 Menu 15.2 — Specifying an Inside Server**

## 6.5.3 Example 3: Multiple Public IP Addresses With Inside Servers

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

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

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

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

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

The example situation looks somewhat like this:

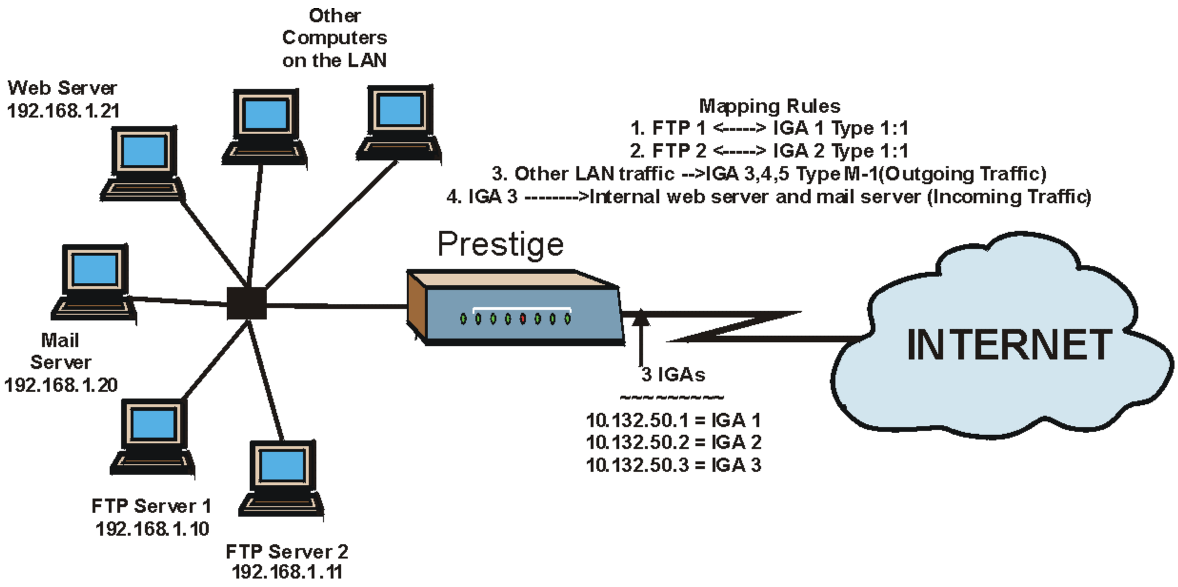

Other Computers on the LAN
Web Server 192.168.1.21
Mapping Rules
1. FTP 1 <-----> IGA 1 Type 1:1
2. FTP 2 <-----> IGA 2 Type 1:1
3. Other LAN traffic -->IGA 3,4,5 Type M-1(Outgoing Traffic)
4. IGA 3 -------->Internal web server and mail server (Incoming Traffic)
Prestige
INTERNET
Mail Server 192.168.1.20
3 IGAs
~~~~~~~~~
10.132.50.1 = IGA 1
10.132.50.2 = IGA 2
10.132.50.3 = IGA 3
FTP Server 1 192.168.1.10
FTP Server 2 192.168.1.11

**Figure 6-16 NAT Example 3**

**Step 1.** In this case you need to configure Address Mapping Set 1 from **Menu 15.1 - Address Mapping Sets.** Therefore you must choose the **Full Feature** option from the **Network Address Translation** field (in menu 4 or menu 11.3) in *Figure 6-17*.

**Step 2.** Then enter 15 from the main menu.

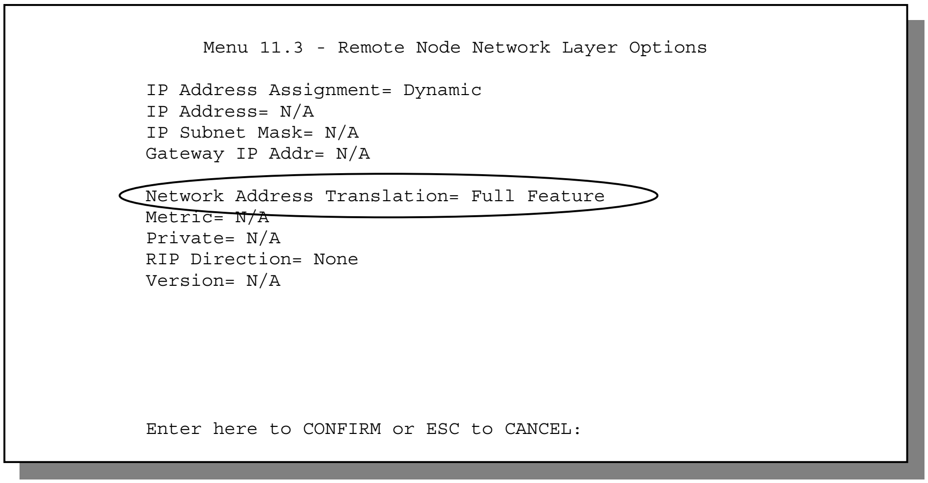
**Step 3.** Enter 1 to configure the Address Mapping Sets.

**Step 4.** Enter 1 to begin configuring this new set. Enter a Set Name, choose the **Edit Action** and then enter 1 for the **Select Rule** field. Press [ENTER] to confirm.

**Step 5.** Select **Type** as **One-to-One** (direct mapping for packets going both ways), and enter the local **Start IP** as 192.168.1.10 (the IP address of FTP Server 1), the global **Start IP** as 10.132.50.1 (our first IGA). (See *Figure 6-18).*

**Step 6.** Repeat the previous step for rules 2 to 4 as outlined above.

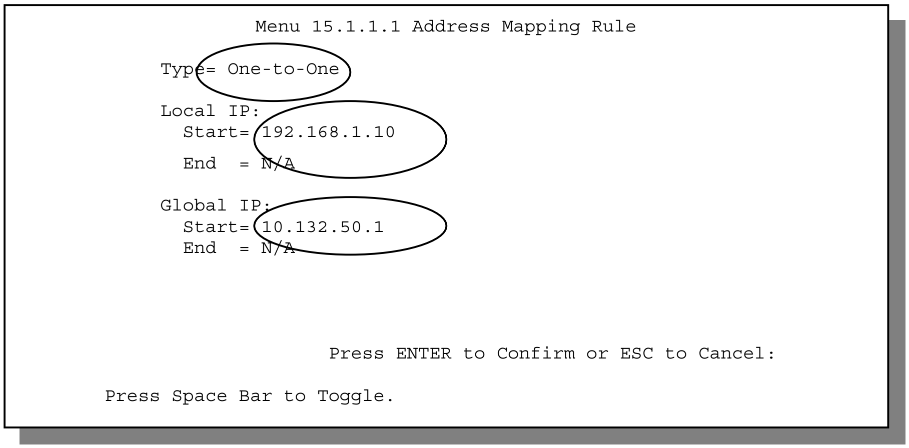
**Step 7.** When finished, menu 15.1.1 should look like as shown in *Figure 6-19.*
~~~~~~~~~



```
                 Menu 11.3 - Remote Node Network Layer Options

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

            Network Address Translation= Full Feature
            Metric= N/A
            Private= N/A
            RIP Direction= None
            Version= N/A





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

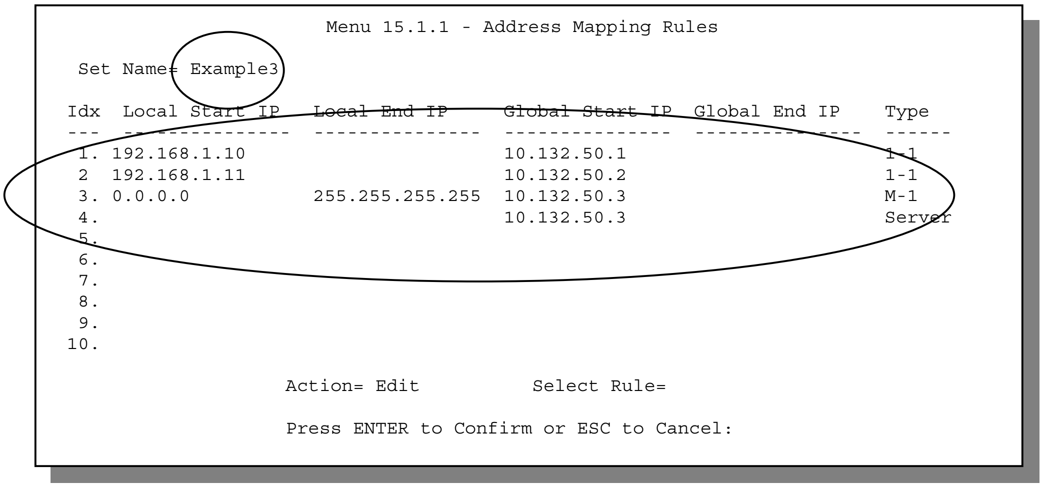
Figure 6-17 Example 3: Menu 11.3

The following figure shows how to configure the first rule.



```
                    Menu 15.1.1.1 Address Mapping Rule

            Type= One-to-One

            Local IP:
              Start= 192.168.1.10

              End  = N/A

            Global IP:
              Start= 10.132.50.1
              End  = N/A



                           Press ENTER to Confirm or ESC to Cancel:

         Press Space Bar to Toggle.
```

Figure 6-18 Example 3: Menu 15.1.1.1



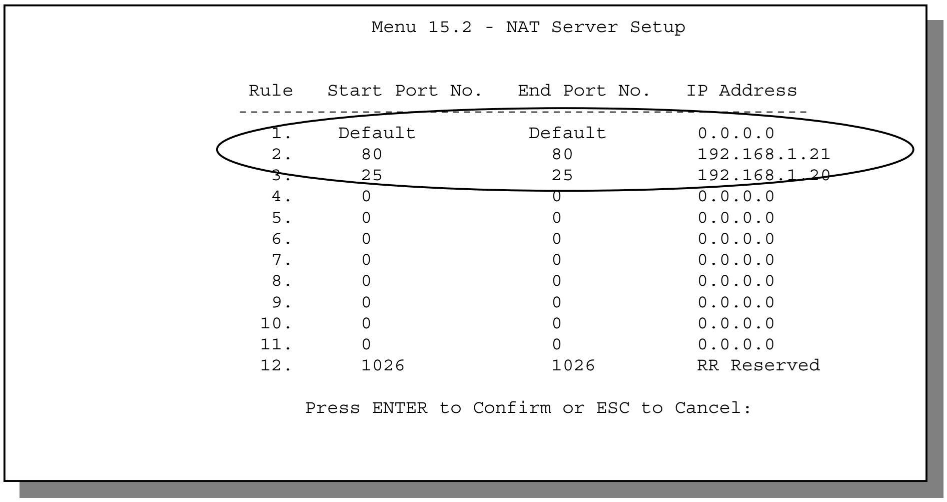
```
                          Menu 15.1.1 - Address Mapping Rules

  Set Name= Example3

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

                    Action= Edit          Select Rule=

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

Figure 6-19 Example 3: Final Menu 15.1.1

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

**Step 8.** Enter 15 from the main menu.

**Step 9.** Now enter 2 from this menu and configure it as shown in *Figure 6-20*.



```
                          Menu 15.2 - NAT Server Setup


              Rule   Start Port No.   End Port No.   IP Address
             ---------------------------------------------------
                1.    Default          Default        0.0.0.0
                2.      80               80           192.168.1.21
                3.      25               25           192.168.1.20
                4.      0                0            0.0.0.0
                5.      0                0            0.0.0.0
                6.      0                0            0.0.0.0
                7.      0                0            0.0.0.0
                8.      0                0            0.0.0.0
                9.      0                0            0.0.0.0
               10.      0                0            0.0.0.0
               11.      0                0            0.0.0.0
               12.      1026             1026         RR Reserved

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

Figure 6-20 Example 3: Menu 15.2

### 6.5.4 Example 4: NAT Unfriendly Application Programs

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

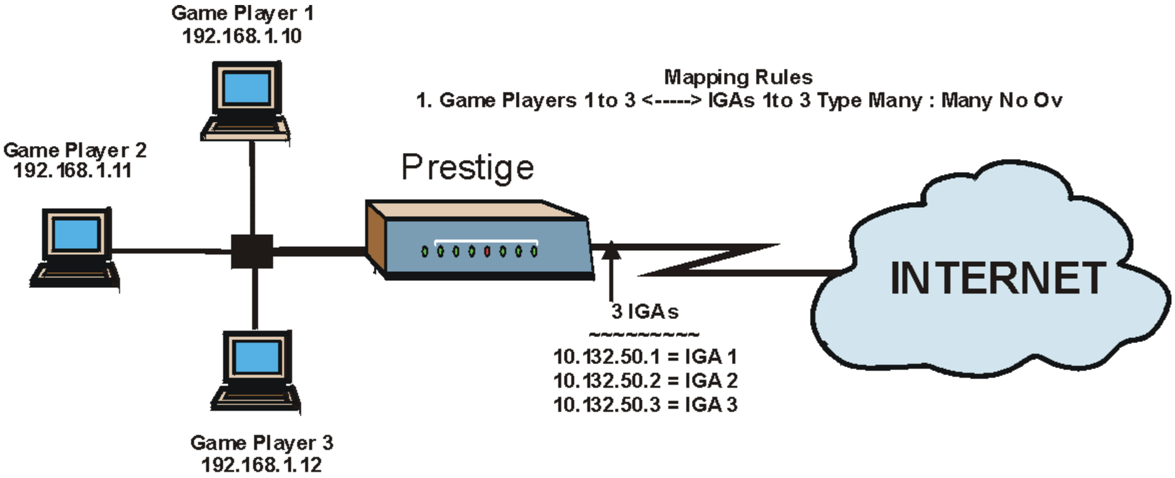
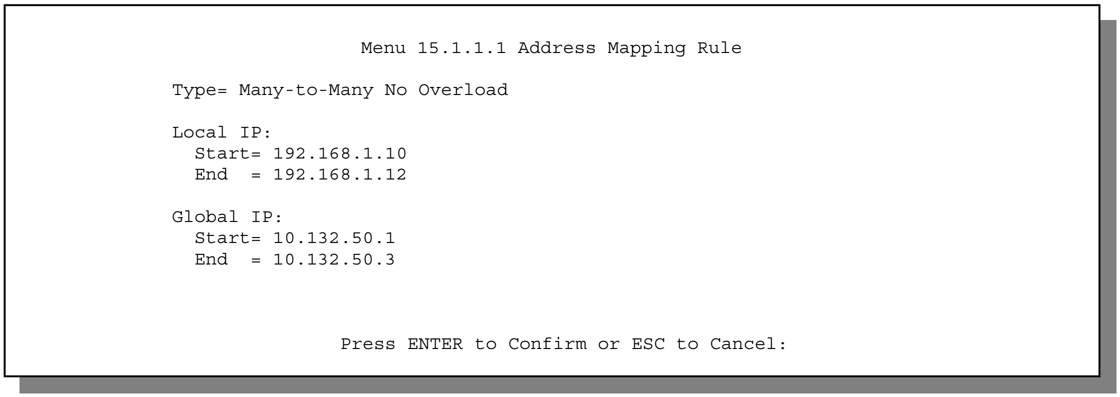


**Figure 6-21 NAT Example 4**

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

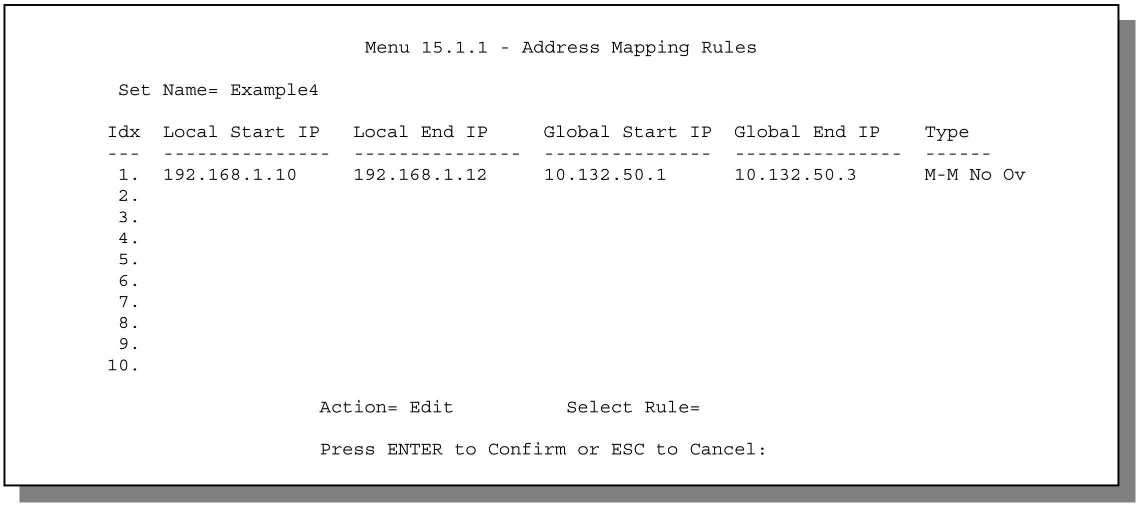
Follow the steps outlined in example 3 above to configure these two menus as follows.



```
                    Menu 15.1.1.1 Address Mapping Rule

        Type= Many-to-Many No Overload

        Local IP:
          Start= 192.168.1.10
          End  = 192.168.1.12

        Global IP:
          Start= 10.132.50.1
          End  = 10.132.50.3



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

Figure 6-22 Example 4: Menu 15.1.1.1 — Address Mapping Rule

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



```
                         Menu 15.1.1 - Address Mapping Rules

          Set Name= Example4

         Idx  Local Start IP   Local End IP     Global Start IP  Global End IP    Type
         ---  ---------------  ---------------  ---------------  ---------------  ------
          1.  192.168.1.10     192.168.1.12     10.132.50.1      10.132.50.3      M-M No Ov
          2.
          3.
          4.
          5.
          6.
          7.
          8.
          9.
         10.
                         Action= Edit          Select Rule=

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

Figure 6-23 Example 4: Menu 15.1.1 — Address Mapping Rules

# Part III:

## ADVANCED MANAGEMENT

Advanced Management provides information on Prestige Filtering, SNMP, System Information and Diagnosis, Firmware and Configuration Maintenance, System Maintenance and Management, Call Scheduling and Telnet.

# Chapter 7
# Filter Configuration

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

## 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 Ethernet side. Call filtering is used to determine if a packet should be allowed to trigger a call. Remote node call filtering is only applicable when using **PPTP** or **PPPoE** encapsulation. Outgoing packets must undergo data filtering before they encounter call filtering as shown in the following figure.

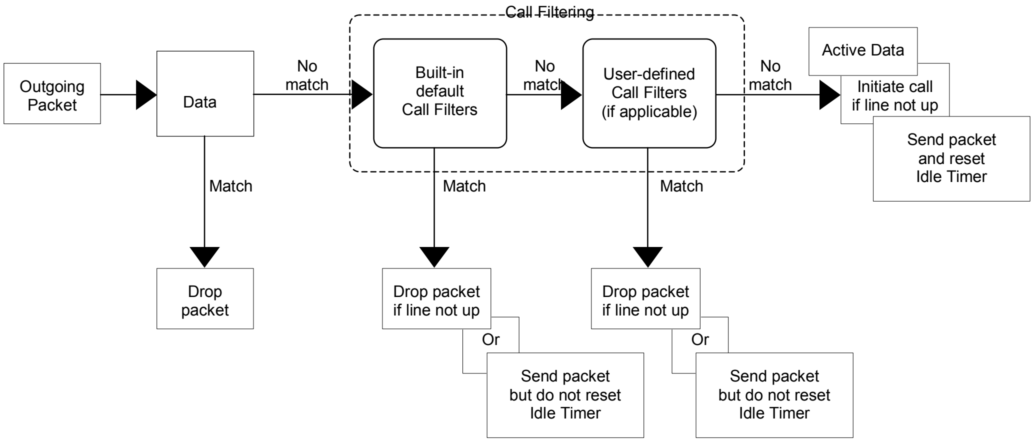

Call Filtering
Outgoing Packet
Data
No match
Built-in default Call Filters
No match
User-defined Call Filters (if applicable)
No match
Active Data
Initiate call if line not up
Send packet and reset Idle Timer
Match
Match
Match
Drop packet
Drop packet if line not up
Or
Send packet but do not reset Idle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

**Figure 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 cannot mix device filter rules and protocol filter rules within the same set. You can apply up to four filter sets to a particular port to block multiple types of packets. With each filter set having up to six rules, you can have a maximum of 24 rules active for a single port.

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.

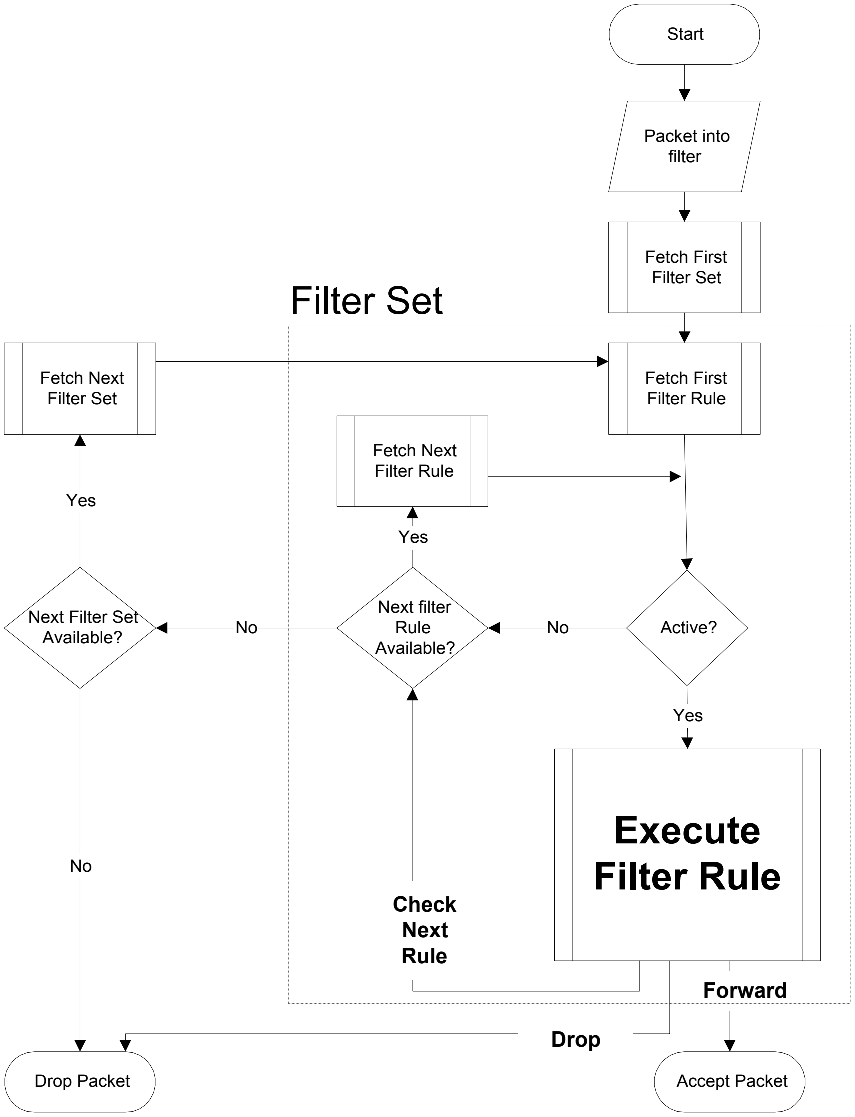


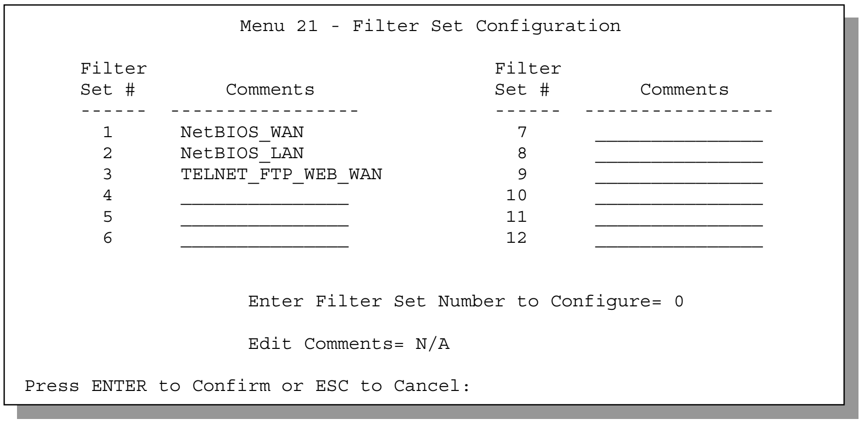
**Figure 7-2 Filter Rule Process**

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 procedures stated next.

**Step 1.** Select option **21. Filter Set Configuration** from the main menu to open **Menu 21**.



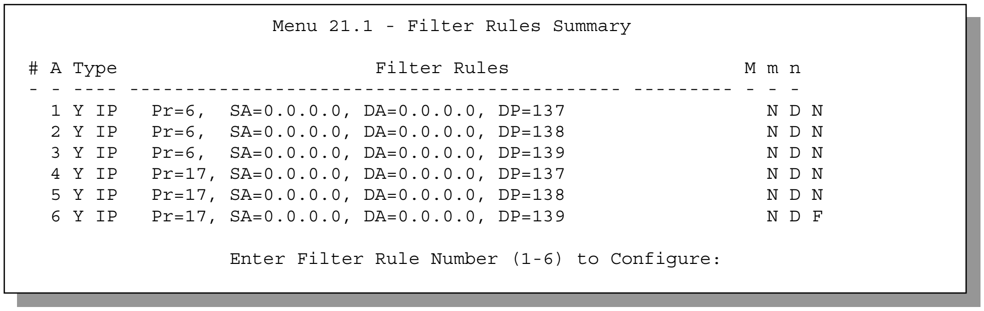
```
                      Menu 21 - Filter Set Configuration

       Filter                                  Filter
       Set #        Comments                   Set #        Comments
       ------  -----------------               ------  -----------------
         1      NetBIOS_WAN                      7      _______________
         2      NetBIOS_LAN                      8      _______________
         3      TELNET_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 to 12) and press [ENTER].

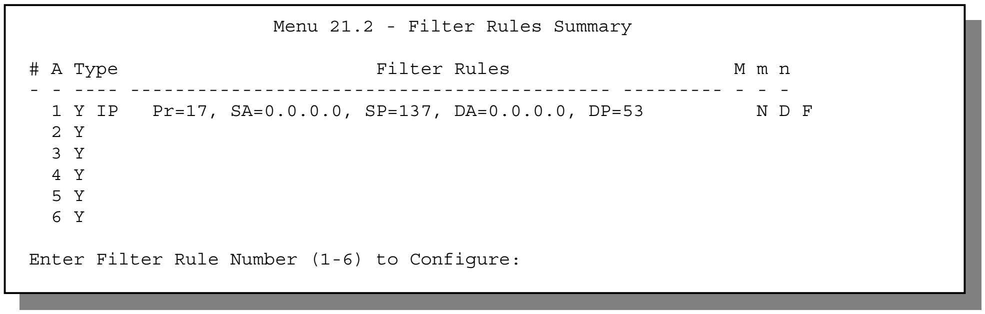
**Step 3.** Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].

**Step 4.** Press [ENTER] at the message: “Press ENTER to Confirm...” to open **Menu 21.1** – **Filter Rules Summary**.



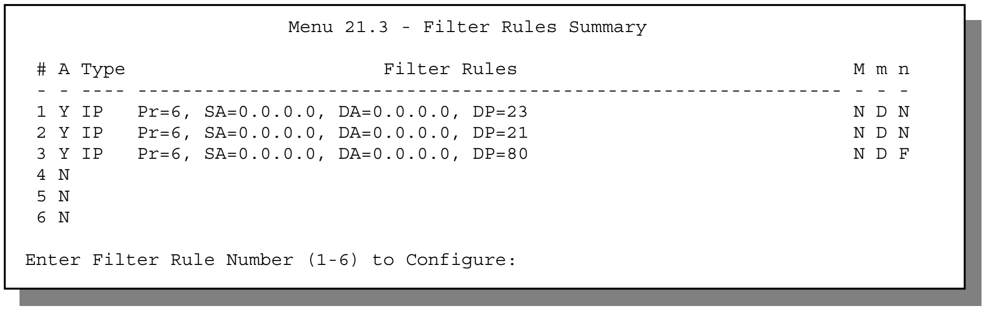
```
                       Menu 21.1 - Filter Rules Summary

 # 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:
```

**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 Y
   3 Y
   4 Y
   5 Y
   6 Y

 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 Telnet_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 table contains a brief description of the abbreviations used in the previous menus.

**Table 7-1 Abbreviations Used in the Filter Rules Summary Menu**

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

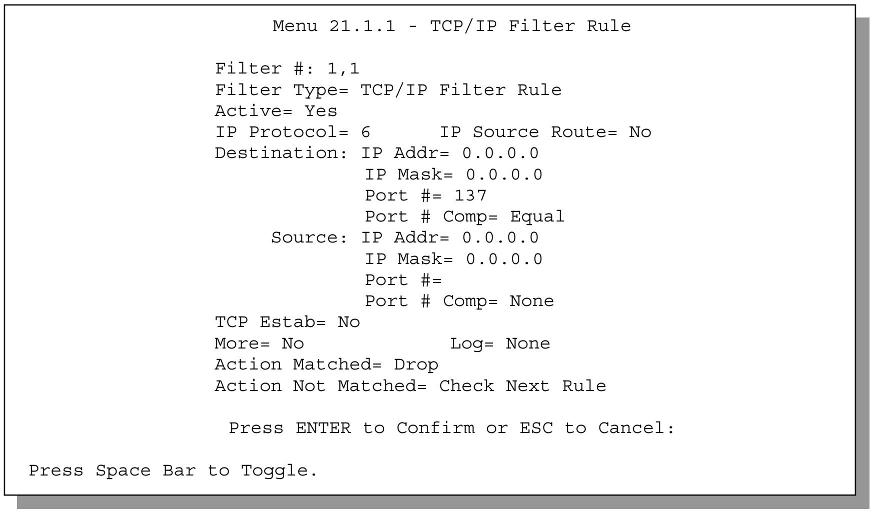
To configure a filter rule, type its number in **Menu 21.1 – Filter Rules Summary** and press [ENTER] to open **Menu 21.1.1** for the rule.

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 next.



```
                    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 – 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 | OPTIONS |
|---|---|---|
| Filter # | This is the filter set, filter rule coordinates, i.e., 2, 3 refers to the second filter set and the third filter rule of that set. | |
| Filter Type | Use [SPACE BAR] to toggle between types of rules. Parameters displayed for each type will be different. | **TCP/IP Filter Rule, Generic Filter Rule** |
| 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** to **255** |
| IP Source Route | If **Yes**, the rule applies to packet with IP source route option; or 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* field. | IP mask |

| FIELD | DESCRIPTION | OPTIONS |
|---|---|---|
| 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** to **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** |
| Source: IP Addr | 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* field. | 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** to **65535** |
| Source: Port # Comp | Select the comparison to apply to the source port in the packet against the value given in *Source: Port #* field. | **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; or 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; or else the packet is disposed of according to the action fields.<br>If *More* is **Yes**, then *Action Matched* and *Action Not Matched* fields will be **N/A**. | **Yes/No** |
| Log | Select the logging option from the following:<br>● **None** – No packet 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>**Action Matched**<br>**Action Not Matched**<br>**Both** |
| Action Matched | Select the action for a matching packet. This field is **N/A** if the previously configured *More* field is **Yes**. | **Check Next Rule, Forward, Drop, N/A** |
| Action Not Matched | Select the action for a packet not matching the rule. This field is **N/A** if the previously configured *More* field is **No**. | **Check Next Rule/ Forward/Drop/ N/A** |

| FIELD | DESCRIPTION | OPTIONS |
|---|---|---|
| Once you have completed filling in **Menu 21.1.1 – 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 – Filter Rules Summary**. | | |

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

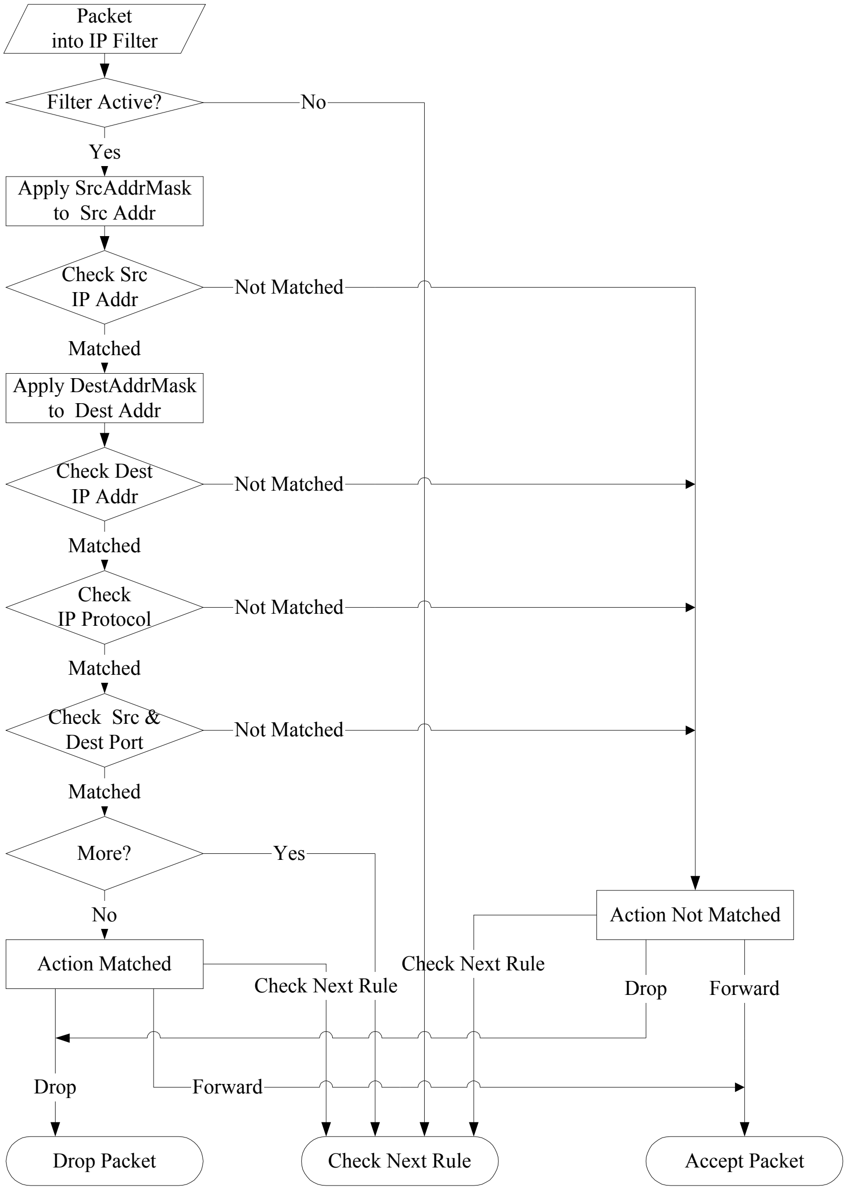


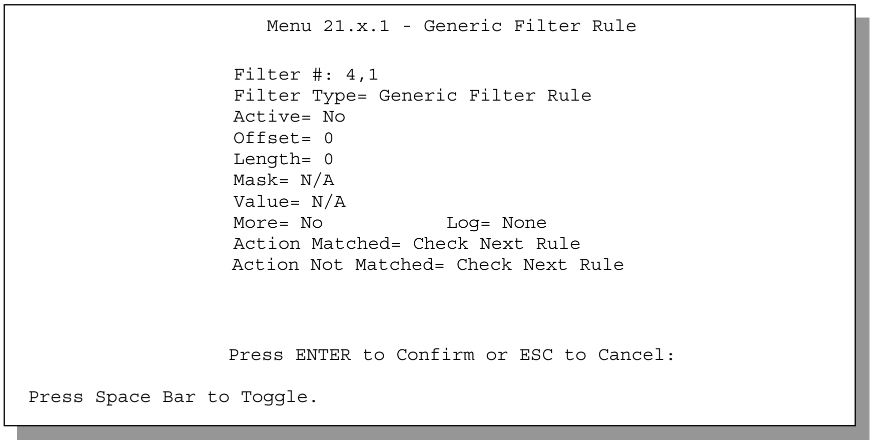
**Figure 7-8 Executing an IP Filter**

### 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.x.1** and press [ENTER] to open **Menu 21.x.1 - Generic Filter Rule**, as shown next.



```
                         Menu 21.x.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.x.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 | OPTIONS |
|---|---|---|
| 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 [SPACE BAR] to select a rule. 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. | **0** (default) |
| Length | Enter the byte count of the data portion in the packet that you wish to compare. The range for this field is 0 to 8. | **0** (default) |
| Mask | Enter the mask (in Hexadecimal) to apply to the data portion before comparison. | |
| Value | Enter the value (in Hexadecimal) to compare with the data portion. | |
| More | If **Yes**, a matching packet is passed to the next filter rule before an action is taken; or else the packet is disposed of according to the action fields.<br>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 packet 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>**Action Matched**<br>**Action Not Matched**<br>**Both** |
| Action Matched | Select the action for a matching packet. This field is **N/A** if previously configured **More** field is **Yes**. | **Check Next Rule, Forward, Drop, N/A** |
| Action Not Matched | Select the action for a packet not matching the rule. This field is **N/A** if previously configured **More** field is **Yes**. | **Check Next Rule, Forward, Drop, N/A** |

Once you have completed filling in **Menu 21.x.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** – **Filter Rules Summary**.

## 7.3 Example Filter

Let us look at the third default ZyXEL filter, TELNET_FTP_WAN (*see Figure* 7-6) as an example. This filter is designed to block outside users from telnetting into the Prestige.

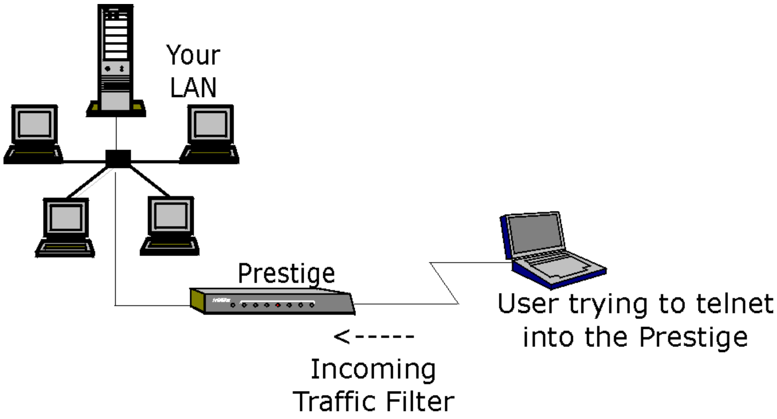


**Figure 7-10 Telnet Filter Example**

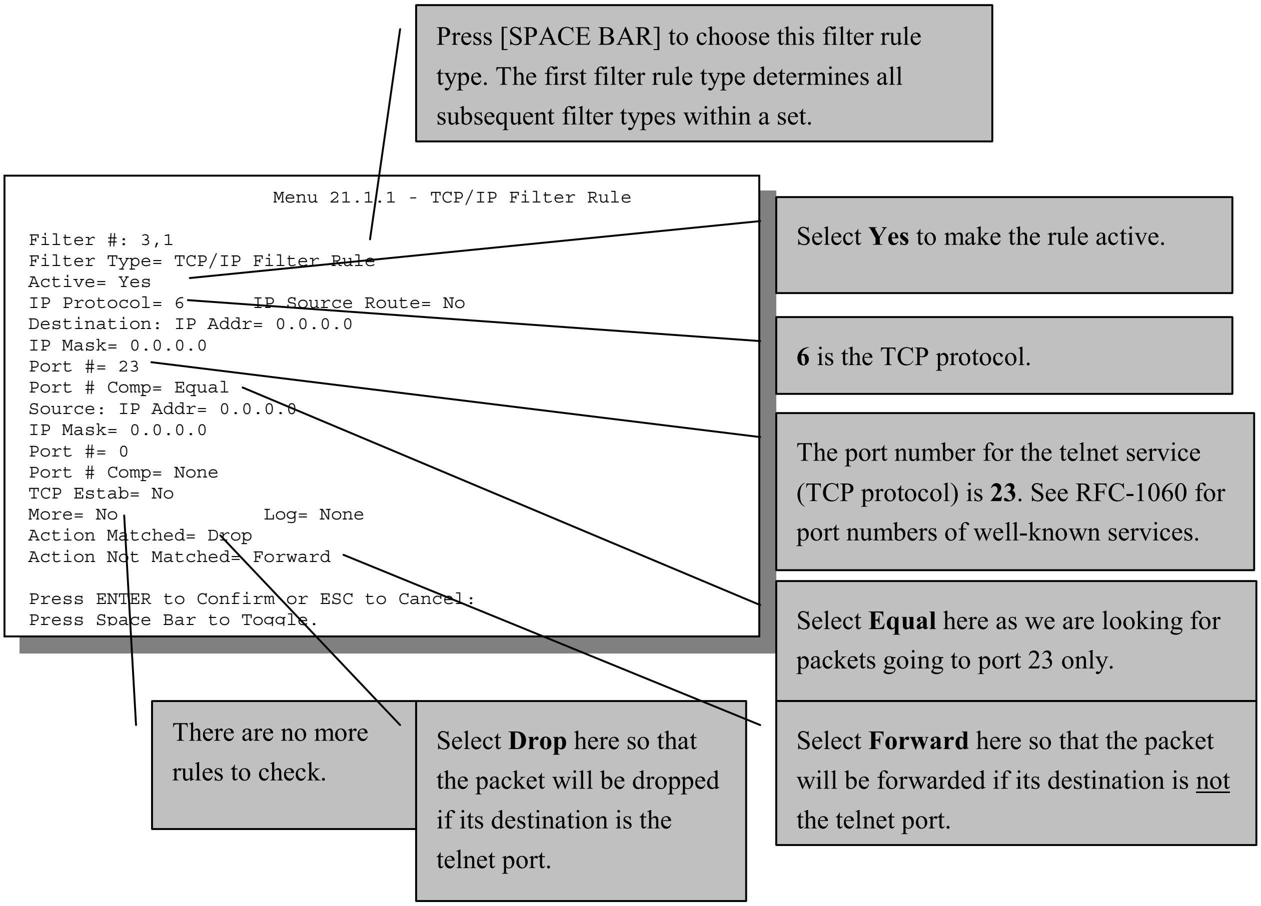
**Step 1.** Enter 21 from the main menu to open **Menu 21** – **Filter Set Configuration**.

**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_WAN) and press [ENTER].

**Step 4.** Press [ENTER] at the message: "Press Enter to Confirm..." to open **Menu 21.1** – **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 21.1.1 - 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= Forward

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

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

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

**6** is the TCP protocol.

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

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

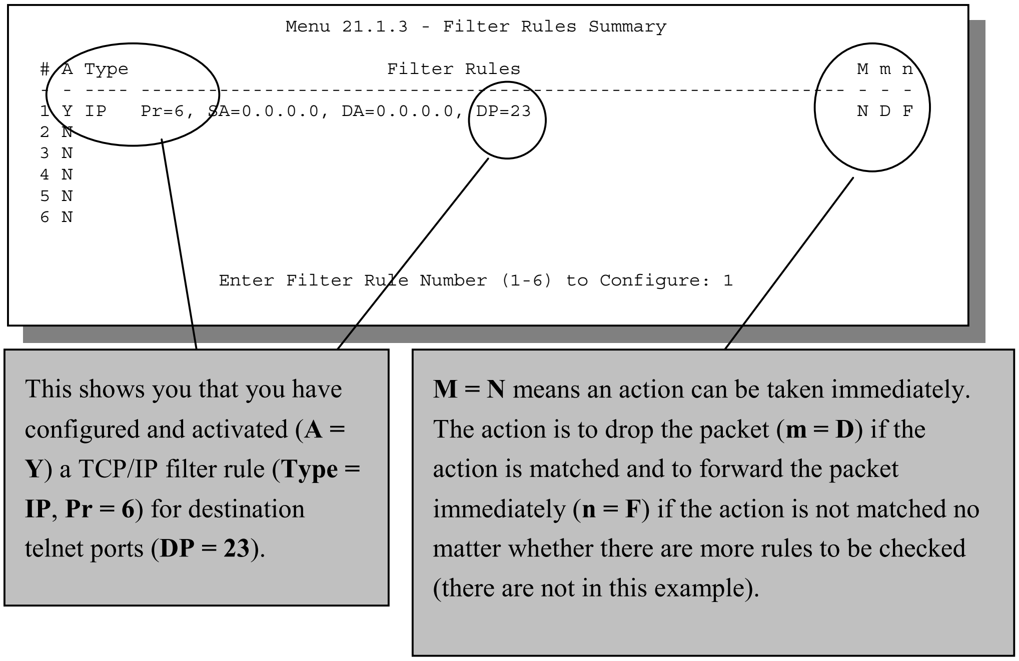
There are no more rules to check.

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

Select **Forward** here so that the packet will be forwarded if its destination is not the telnet port.

**Figure 7-11 Sample Filter – Menu 21.1.1**

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



```
                         Menu 21.1.3 - 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 F
 2 N
 3 N
 4 N
 5 N
 6 N


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

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

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

**Figure 7-12 Sample Filter Rules Summary – Menu 21.1.3**

After you have 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 [SPACE BAR] to select **No** and press [ENTER].

**Step 3.** This brings you to menu 11.5. Apply the TELNET_FTP_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.

**Step 5.** Press [ENTER] to confirm and leave menu 11.

## 7.4 Filter Types and NAT

There are two classes of filter rules, **Generic Filter** (Device) rules and Protocol Filter (**TCP/IP**) rules. Generic Filter rules act on the raw data from/to LAN and WAN. 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/NAT (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/NAT for outgoing packets and after SUA/NAT for incoming packets. On the other hand, the generic, or device filters are applied to the raw packets that appear on the wire. They are applied at the point when the Prestige is receiving and sending the packets; i.e., the interface. The interface can be an Ethernet port or any other hardware port. The following diagram illustrates this.

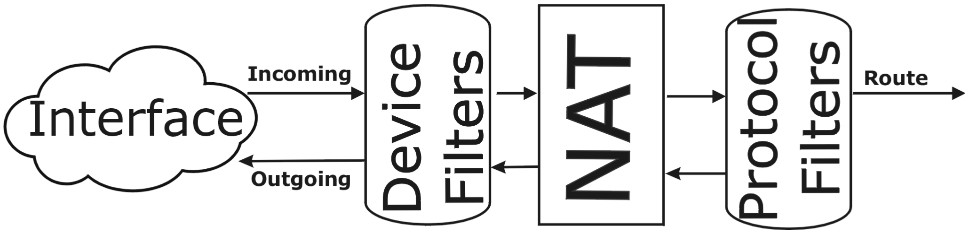


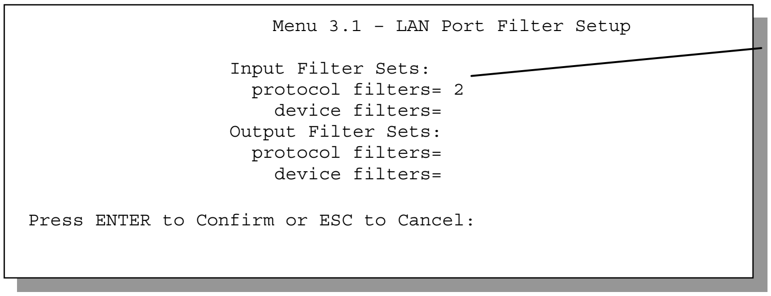
**Figure 7-13 Protocol and Device Filter Sets**

## 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 the *Protocol Filters* field under **Input Filter Sets** in **Menu 3.1** to block NetBIOS traffic to the Prestige from the LAN.



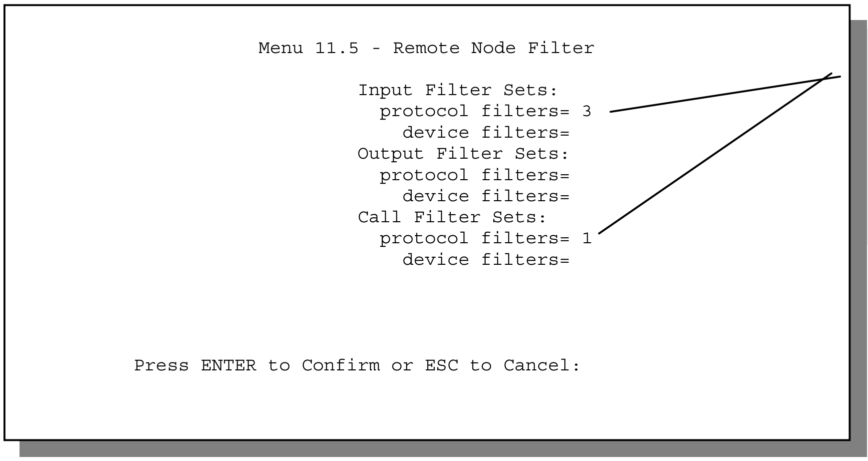
```
                        Menu 3.1 - LAN Port Filter Setup

                    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 next – note that call filter sets are only present for PPTP/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 PPTP/PPPoE encapsulation only). Enter “1” in the **protocol filters** field under **Call Filter Sets** when using PPTP/PPPoE encapsulation and in **protocol filters** field under **Output Filter Sets** when using Ethernet encapsulation**.** Filter set “3”, Telnet_FTP_WAN, blocks telnet and FTP connections from the WAN Port to help prevent security breaches. 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=
                                 device filters=
                             Call Filter Sets:
                               protocol filters= 1
                                 device filters=




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

Apply default filters 1, 3 here. Enter 1 in **protocol filters** under **Output Filter Sets** when using Ethernet encapsulation.

**Figure 7-15 Filtering Remote Node Traffic (PPTP/PPPoE Encapsulation)**

# Chapter 8
# SNMP Configuration

*This chapter discusses SNMP (Simple Network Management Protocol) for network management and monitoring.*

## 8.1 About SNMP

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

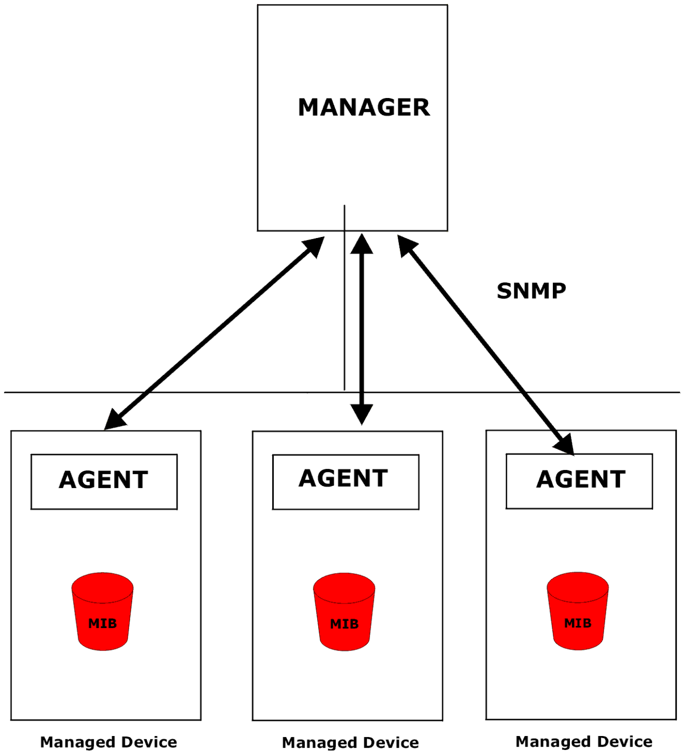


**Figure 8-1 SNMP Management Model**

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

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

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

SNMP itself is a simple request/response protocol based on the manager/agent model

**Table 8-1 General SNMP Commands**

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

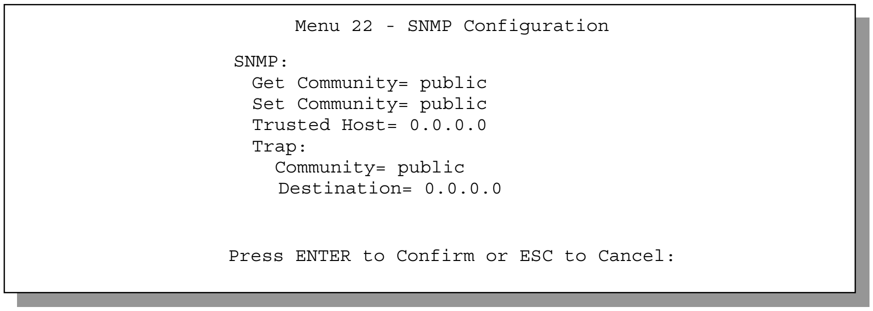
## 8.2 Supported MIBs

The Prestige supports MIB II that is defined in RFC-1213 and RFC-1215. The Prestige can also respond with specific data from the ZyXEL private MIB (ZYXEL-MIB). The focus of the MIBs is to let administrators collect statistic data and monitor status and performance.

The Prestige acts as an SNMP agent. Users must implement their own GUI on SNMP platform (SNMP manager).

## 8.3 Configuring SNMP

To configure SNMP, select **SNMP Configuration** (enter 22) from the main menu to open **Menu 22 - SNMP Configuration**, as shown in the figure below. The “community” for Get, Set and Trap fields is simply SNMP’s terminology for password.



```
                    Menu 22 - SNMP Configuration

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


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

**Figure 8-2 Menu 22 — SNMP Configuration**

The following table describes the SNMP configuration parameters.

**Table 8-2 SNMP Configuration Menu Fields**

| FIELD | DESCRIPTION | DEFAULT |
|---|---|---|
| Get Community | Enter the **Get Community**, which is the password for the incoming Get- and GetNext- requests from the management station. | public (default) |
| Set Community | Enter the **Set Community**, which is the password for incoming Set- requests from the management station. | public (default) |
| Trusted Host | If you enter a trusted host, your Prestige will only respond to SNMP messages from this address. If you leave the field set to 0.0.0.0 (default), your Prestige will respond to all SNMP messages it receives, regardless of source. | 0.0.0.0 (default) |
| Trap: Community | Enter the trap community, which is the password sent with each trap to the SNMP manager. | public (default) |
| Trap: Destination | Enter the IP address of the station to send your SNMP traps to. | 0.0.0.0 (default) |
| Once you have completed filling in **Menu 22 - SNMP Configuration**, press [ENTER] at the message “Press ENTER to Confirm” to save your configuration, or press [ESC] to cancel. | | |

## 8.4 SNMP Traps

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

**Table 8-3 SNMP Traps**

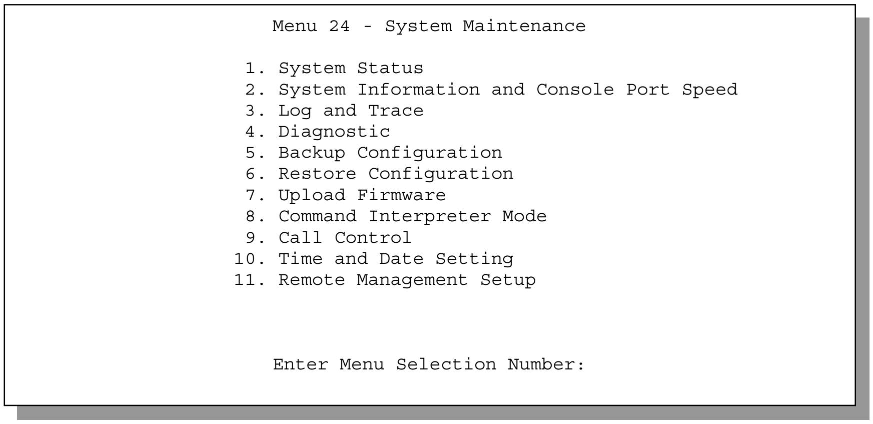
| TRAP # | TRAP NAME | DESCRIPTION |
|---|---|---|
| 0 | coldStart (defined in *RFC-1215*) | A trap is sent after booting (power on). |
| 1 | warmStart (defined in *RFC-1215*) | A trap is sent after booting (software reboot). |
| 4 | authenticationFailure (defined in *RFC-1215*) | A trap is sent to the manager when receiving any SNMP get or set requirements with wrong community (password). |
| 6 | whyReboot (defined in ZYXEL-MIB) | A trap is sent with the reason of restart before rebooting when the system is going to restart (warmstart). |
| 6a | For intentional reboot : | A trap is sent with the message "System reboot by user!" if reboot is done intentionally, (e.g. download new files, CI command "sys reboot", etc.). |
| 6b | For fatal error : | A trap is sent with the message of the fatal code if the system reboots because of fatal errors. |

# Chapter 9
# 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 24 in the main menu to open **Menu 24 – System Maintenance**, as shown next.



```
                    Menu 24 - System Maintenance

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



                    Enter Menu Selection Number:
```

**Figure 9-1 Menu 24 – System Maintenance**

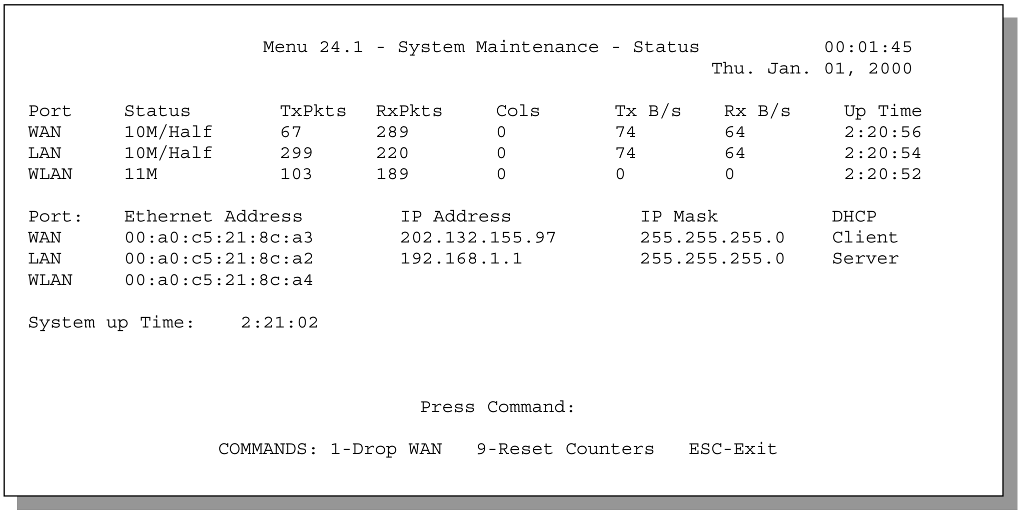
## 9.1 System Status

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

### 9.1.1 To get to the System Status:

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

The next table describes the fields present in **Menu 24.1 – System Maintenance – Status**. It should be noted that these fields are READ-ONLY and are meant 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           00:01:45
                                                             Thu. Jan. 01, 2000

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
WLAN     11M           103     189        0          0         0          2:20:52

Port:    Ethernet Address         IP Address           IP Mask           DHCP
WAN      00:a0:c5:21:8c:a3        202.132.155.97       255.255.255.0     Client
LAN      00:a0:c5:21:8c:a2        192.168.1.1          255.255.255.0     Server
WLAN     00:a0:c5:21:8c:a4

System up Time:    2:21:02


                                   Press Command:

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

**Figure 9-2 Menu 24.1 – System Maintenance – Status**

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

**Table 9-1 System Maintenance – Status Menu Fields**

| FIELD | DESCRIPTION |
|---|---|
| Port | The WAN or LAN port. |
| Status | Shows the port speed and duplex setting if you are using **Ethernet Encapsulation** and **down** (line is down), **idle** (line (PPP) idle), **dial** (starting to trigger a call) and |

| FIELD | DESCRIPTION |
|---|---|
| Status | Shows the port speed and duplex setting if you are 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 are using **PPTP**/**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. |
| 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. |
| 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. |
| WLAN | |
| Ethernet Address | The wireless LAN port Ethernet address. |
| IP Address | The same value as the LAN port's IP address. |
| IP Mask | The same value as the LAN port's IP mask. |
| DHCP | The same value as the LAN port's DHCP role. |
| System up Time | The total time the Prestige has been on. |
| Name | This is the Prestige's system name + domain name assigned in menu 1. e.g., System Name= xxx;  Domain Name= baboo.mickey.com.<br>Name= xxx.baboo.mickey.com |
| ZyNOS F/W | The ZyNOS Firmware version and the date created. |

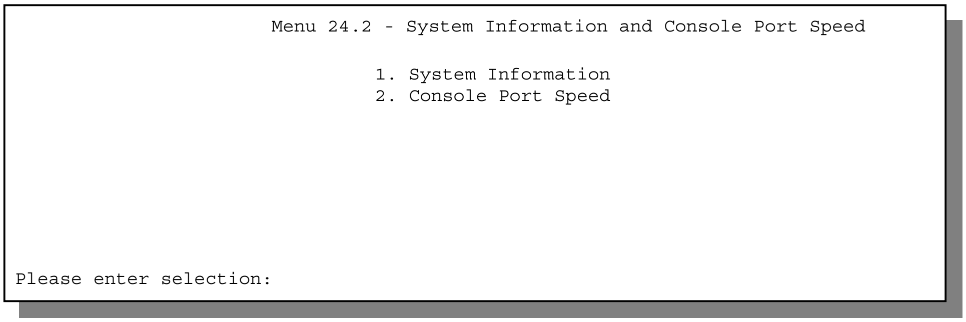
| FIELD | DESCRIPTION |
|---|---|
| Version | |
| You may enter 1 to drop the PPPoE/PPTP connection, 9 to reset the counters or [ESC] to return to menu 24. | |

## 9.2 System Information and Console Port Speed

This section describes your system and allows you to choose different console port speeds. To get to **Menu 24.2 - System Information and Console Port Speed**:

1. Enter 24 to go to **Menu 24 – System Maintenance**.
2. Enter 2 to open **Menu 24.2 – System Information and Console Port Speed**.

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

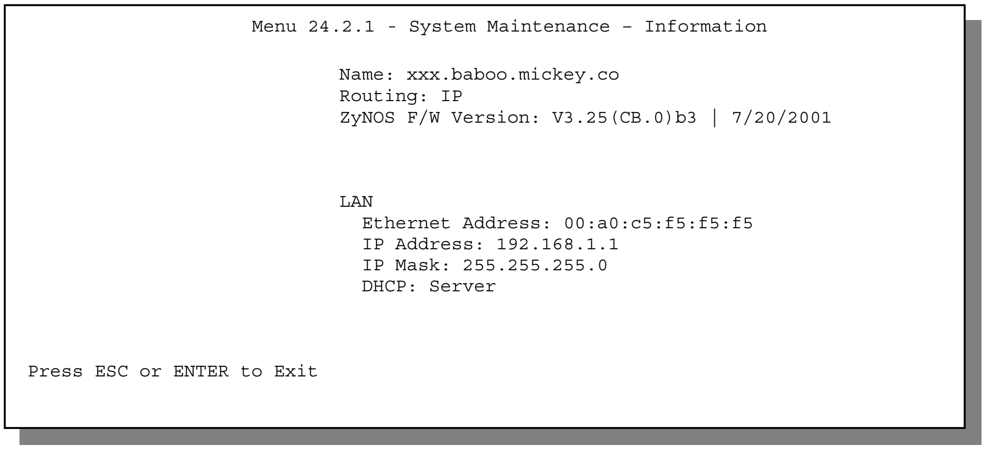


```
                        Menu 24.2 - System Information and Console Port Speed

                                 1. System Information
                                 2. Console Port Speed









Please enter selection:
```

**Figure 9-3 Menu 24.2 – System Information and Console Port Speed**

### 9.2.1 System Information

System Information gives you information about your system as shown next. 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.co
                           Routing: IP
                           ZyNOS F/W Version: V3.25(CB.0)b3 | 7/20/2001



                           LAN
                             Ethernet Address: 00:a0:c5:f5:f5:f5
                             IP Address: 192.168.1.1
                             IP Mask: 255.255.255.0
                             DHCP: Server



Press ESC or ENTER to Exit
```

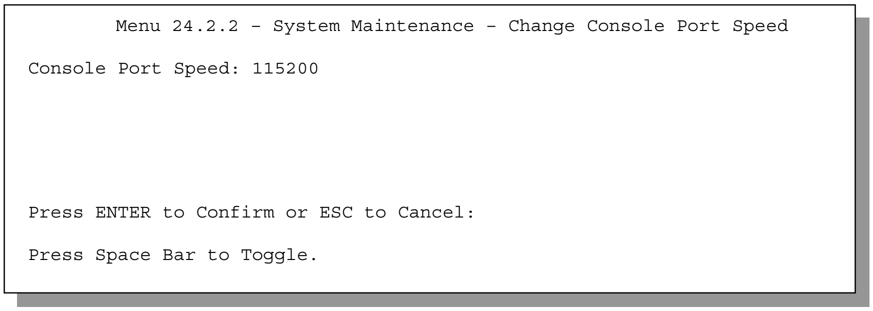
**Figure 9-4 Menu 24.2.1 System Maintenance – Information**

**Table 9-2 Fields in System Maintenance**

| FIELD | DESCRIPTION |
|---|---|
| Name | This is the Prestige's system name plus domain name assigned in Menu 1. E.g., System Name= xxx; Domain Name= baboo.mickey.com<br>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. |

## 9.2.2 Console Port Speed

You can change the speed of the console port through **Menu 24.2.2 – System Maintenance – Change Console Port Speed**. Your Prestige supports 9600 (default), 19200, 38400, 57600, and 115200 bps for the console port. Use [SPACE BAR] to select the desired speed in **Menu 24.2.2**, as shown next.



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

Console Port Speed: 115200





Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

**Figure 9-5 Menu 24.2.2 – System Maintenance – Change Console Port Speed**

# 9.3 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.

## 9.3.1 Viewing Error Log

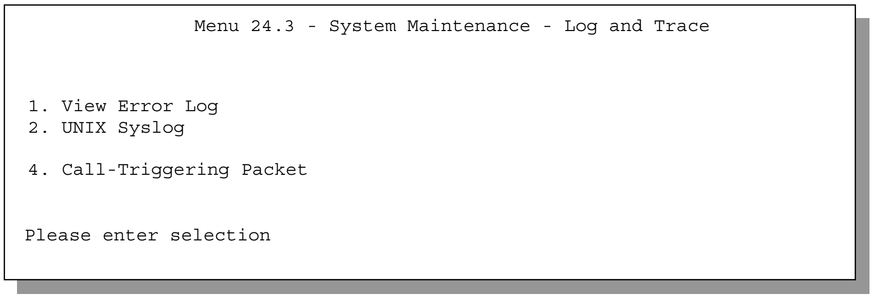
The first place you should look for clues when something goes wrong is the error/trace log. Follow the procedures next to view the local error/trace log:

**Step 1.** Select 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.

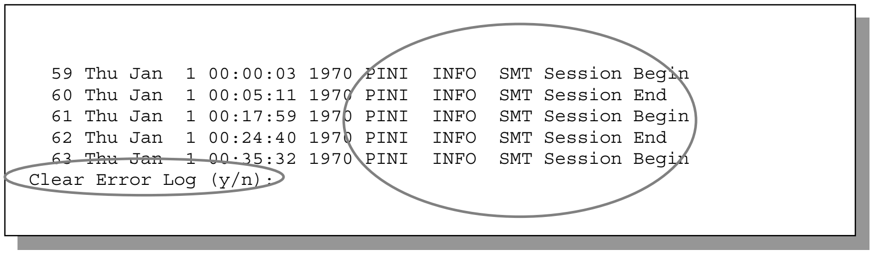
After the Prestige finishes displaying, you will have the option to clear the error log.



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



 1. View Error Log
 2. UNIX Syslog

 4. Call-Triggering Packet


Please enter selection
```

**Figure 9-6 Log and Trace**

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

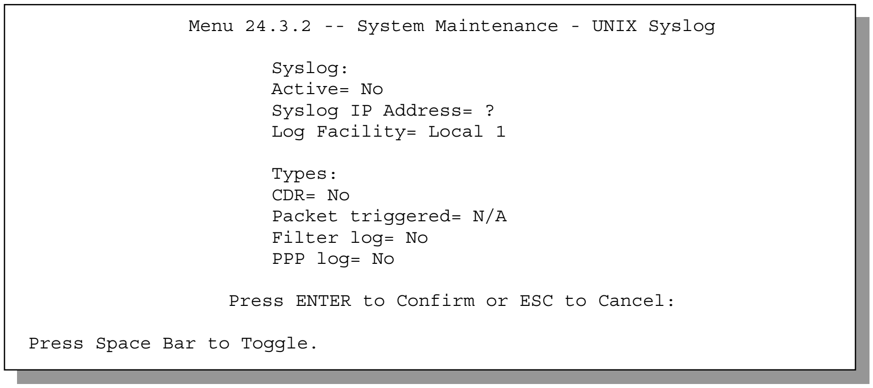


```
   59 Thu Jan  1 00:00:03 1970 PINI  INFO  SMT Session Begin
   60 Thu Jan  1 00:05:11 1970 PINI  INFO  SMT Session End
   61 Thu Jan  1 00:17:59 1970 PINI  INFO  SMT Session Begin
   62 Thu Jan  1 00:24:40 1970 PINI  INFO  SMT Session End
   63 Thu Jan  1 00:35:32 1970 PINI  INFO  SMT Session Begin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

**Figure 9-7 Examples of Error and Information Messages**

## 9.3.2 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

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

                           Types:
                           CDR= No
                           Packet triggered= N/A
                           Filter log= No
                           PPP log= No

                   Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

**Figure 9-8 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 9-3 System Maintenance Menu Syslog Parameters**

| FIELD | DESCRIPTION |
|---|---|
| Syslog: | |
| Active | Press [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 [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 details. |
| 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* 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**. |
| 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. | |

Your Prestige sends four types of syslog messages. Some examples (not Prestige 316 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=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a6b6c6d6e6f707172
7374

Jul 19 11:28:56 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600220008cd40000020405b4

Jul 19 11:29:06 192.168.102.2 ZyXEL: Packet Trigger: Protocol=1,
Data=45000028240140001f06ac12c0a86614ca849a7b0427001700195b451d1430135004000077600000
```

## 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[ffffffffffnordff0080] }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[ffffffffffnordff0080] }S05>R01mF

Mar 03 12:00:52 202.132.155.97 ZyXEL:

GEN[ffffffffffff0080] }S05>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

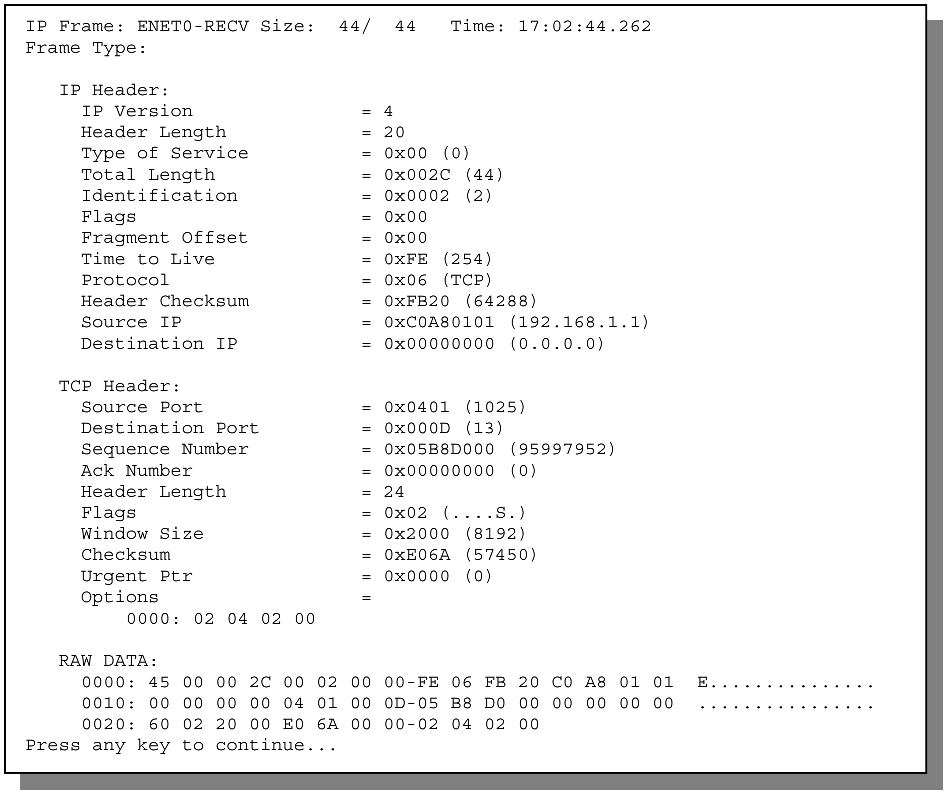
```
Jul 19 11:42:44 192.168.102.2 ZyXEL: ppp:LCP Closing
Jul 19 11:42:49 192.168.102.2 ZyXEL: ppp:IPCP Closing
Jul 19 11:42:54 192.168.102.2 ZyXEL: ppp:CCP Closing
```

## 9.3.3 Call-Triggering Packet

Call-Triggering Packet is a packet-parsing tool that displays information about the packet that triggered the dial-out call in an easy readable format.

**This feature is available for PPTP/PPPoE Encapsulation only.**

An example is shown next.

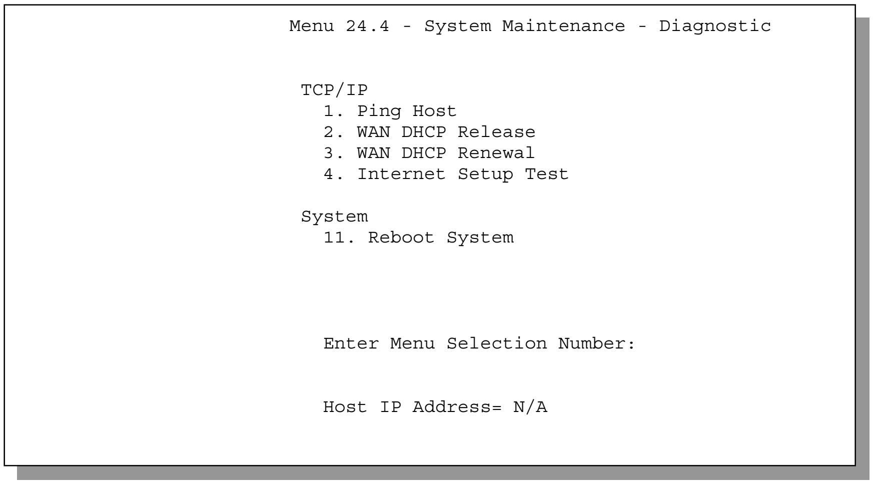


```
IP Frame: ENET0-RECV Size:  44/  44   Time: 17:02:44.262
Frame Type:

   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 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 9-9 Call-Triggering Packet Example**

## 9.4 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 9-10 Menu 24.4 – System Maintenance – Diagnostic**

Follow the procedures next 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**.

## 9.4.1 WAN DHCP

DHCP functionality can be enabled on the LAN or WAN as shown in *Figure 9-11*. 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 11.1 is **Ethernet**) or "none", i.e., you have a static IP. The **WAN DHCP Release** and **Renewal** fields in menu 24.4 conveniently allow you to release and/or renew the assigned WAN IP address, subnet mask and default gateway in a fashion similar to `winipcfg` (Windows 95/98) or `ipconfig` (Windows NT/2000).

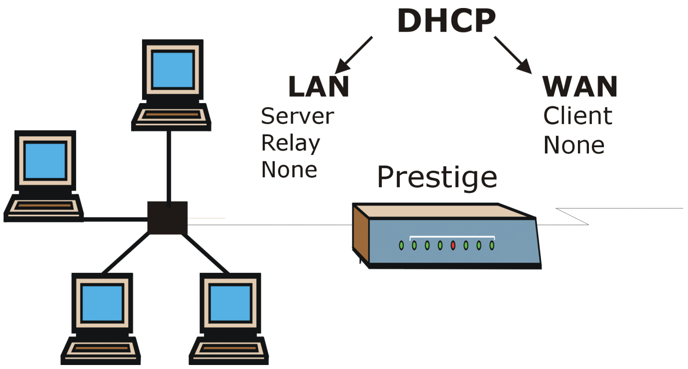


**Figure 9-11 WAN and LAN DHCP**

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

**Table 9-4 System Maintenance Menu Diagnostic**

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

# Chapter 10
# Firmware and Configuration Maintenance

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

## 10.1 Filename Conventions

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

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

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

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

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

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

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

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

**Table 10-1 Filename Conventions**

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

## 10.2 Backup Configuration

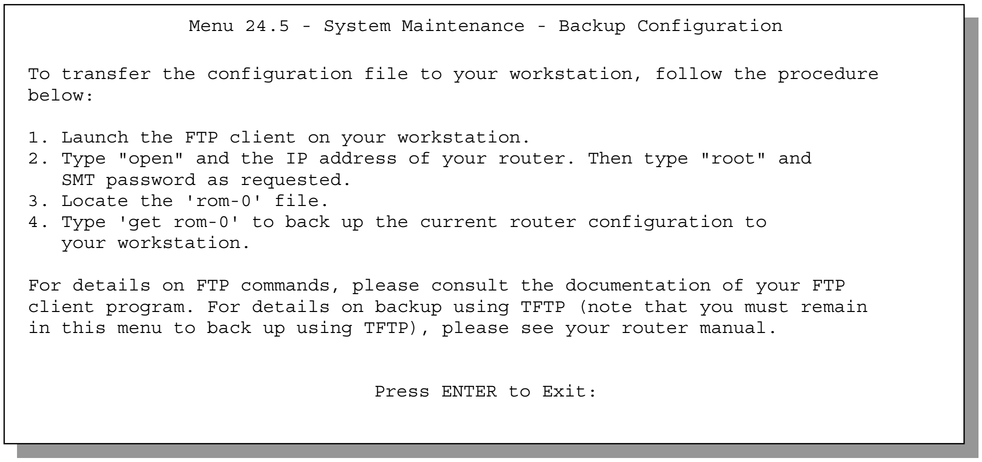
**The Prestige displays different messages explaining different ways to backup, restore and upload files in menus 24.5, 24.6, 24. 7.1 and 24.7.2 when you use the serial/console port and when you telnet in.**

Option 5 from **Menu 24 - System Maintenance** allows you to backup the current Prestige configuration to your computer. Backup is highly recommended once your Prestige is functioning properly. FTP and TFTP are the preferred methods for backing up your current configuration to your computer since FTP and TFTP are faster. You can also perform backup and restore using menu 24 through the console port. Any serial communications program should work fine; however, you must use Xmodem protocol to perform the download/upload and you don't have to rename the files (see *section 10.1*).

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

### 10.2.1 Backup Configuration

Follow the instructions as shown in the next screen.



```
                Menu 24.5 - System Maintenance - Backup Configuration

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

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

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


                               Press ENTER to Exit:
```

**Figure 10-1 Telnet into Menu 24.5**

### 10.2.2 Using the FTP Command from the DOS Prompt

**Step 1.** Launch the FTP client on your computer.

**Step 2.** Enter “open”, followed by a space and the IP address of your Prestige.

**Step 3.** Press [ENTER] when prompted for a username.

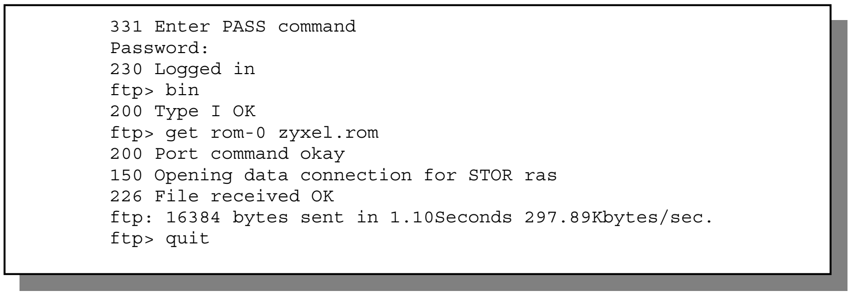
**Step 4.** Enter your password as requested (the default is “1234”).

**Step 5.** Enter “bin” to set transfer mode to binary.

**Step 6.** Use “get” to transfer files from the Prestige to the computer, for example, “get rom-0 config.rom” transfers the configuration file on the Prestige to your computer and renames it “config.rom”. See earlier in this chapter for more information on filename conventions.

**Step 7.** Enter “quit” to exit the ftp prompt.

### 10.2.3 Example of FTP Commands from the DOS Prompt



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

**Figure 10-2 FTP Session Example**

### 10.2.4 Third Party FTP Clients

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

**Table 10-2 General Commands for Third Party FTP Clients**

| COMMAND | DESCRIPTION |
|---|---|
| Host Address | Enter the address of the host server. |
| Login Type | Anonymous.<br>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.<br>Normal.<br>The server requires a unique User ID and Password to login. |
| Transfer Type | Transfer files in either ASCII (plain text format) or in binary mode. |
| Initial Remote Directory | Specify the default remote directory (path). |
| Initial Local Directory | Specify the default local directory (path). |

### 10.2.5 TFTP and FTP over WAN Will Not Work When

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

- The IP address in the **Secured Client IP** field (menu 24.11) does not match the client IP address. If it does not match, the Prestige will disconnect the Telnet session immediately.
- There is an SMT console session running.

### 10.2.6 Backup Configuration Using TFTP

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

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

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

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

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

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

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

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

### 10.2.7 TFTP Command Example

The following is an example tftp command:

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

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

### 10.2.8 Third Party TFTP Clients

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

**Table 10-3 General Commands for Third Party TFTP Clients**

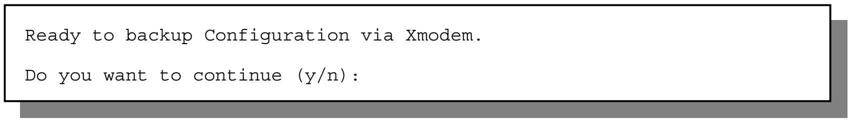
| COMMAND | DESCRIPTION |
|---|---|
| Host | Enter the IP address of the Prestige. 192.168.1.1 is the Prestige’s default IP address when shipped. |
| Send/Fetch | Use “Send” to upload the file to the Prestige and “Fetch” to back up the file on your computer. |
| Local File | Enter the path and name of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

Refer to *section 10.2.5* to read about configurations that disallow TFTP and FTP to work over WAN.

### 10.2.9 Backup Via Console Port

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

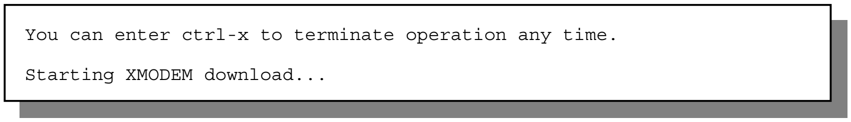
**Step 1.** Display menu 24.5 and enter “y” at the following screen.



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

**Figure 10-3 System Maintenance — Backup Configuration**

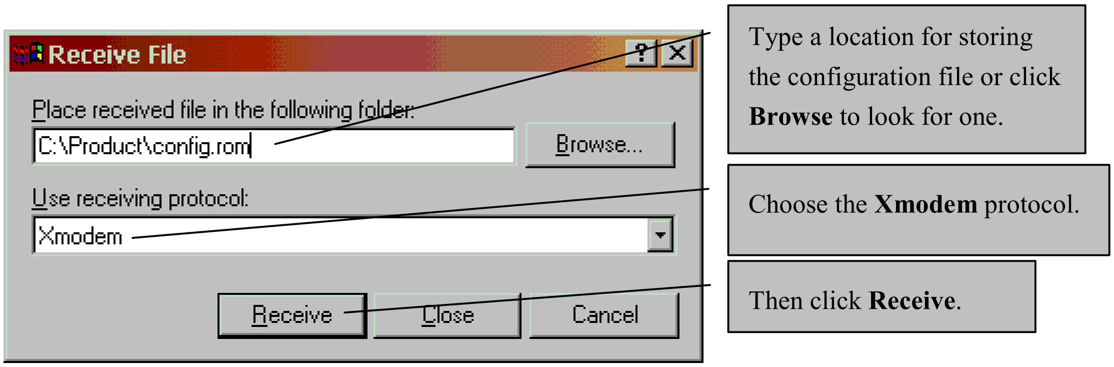
**Step 2.** The following screen indicates that the Xmodem download has started.



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

**Figure 10-4 System Maintenance — Starting Xmodem Download Screen**

**Step 3.** Run the HyperTerminal program by clicking **Transfer**, then **Receive File** as shown in the following screen.



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

Use receiving protocol: Xmodem

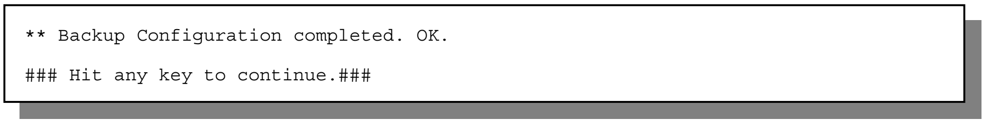
Type a location for storing the configuration file or click **Browse** to look for one.

Choose the **Xmodem** protocol.

Then click **Receive**.

**Figure 10-5 Backup Configuration Example**

**Step 4.** After a successful backup you will see the following screen. Press any key to return to the SMT menu.



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

**Figure 10-6 Successful Backup Confirmation Screen**

## 10.3 Restore Configuration

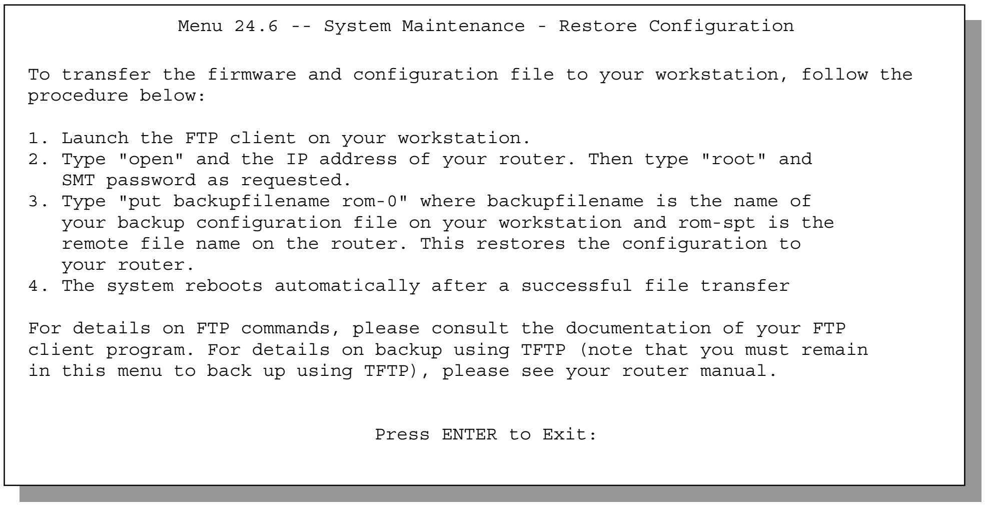
This section shows you how to restore a previously saved configuration. Note that this function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

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

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

### 10.3.1 Restore Using FTP or TFTP

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



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

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

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

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


                                Press ENTER to Exit:
```

**Figure 10-7Telnet into Menu 24.6**

**Step 1.** Launch the FTP client on your computer.

**Step 2.** Enter “open”, followed by a space and the IP address of your Prestige.

**Step 3.** Press [ENTER] when prompted for a username.

**Step 4.** Enter your password as requested (the default is “1234”).

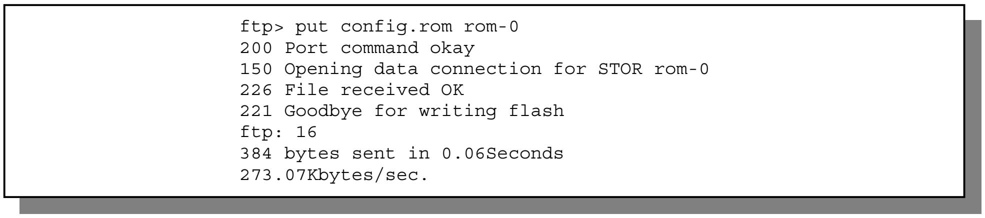
**Step 5.** Enter “bin” to set transfer mode to binary.

**Step 6.** Find the “rom” file (on your computer) that you want to restore to your Prestige.

**Step 7.** Use “put” to transfer files from the Prestige to the computer, for example, “put config.rom rom-0” transfers the configuration file on the Prestige to your computer and renames it “config.rom”. See earlier in this chapter for more information on filename conventions.

**Step 8.** Enter “quit” to exit the ftp prompt. The Prestige will automatically restart after a successful restore process.

## 10.3.2 Restore Using FTP or TFTP Session Example



```
ftp> put config.rom rom-0
200 Port command okay
150 Opening data connection for STOR rom-0
226 File received OK
221 Goodbye for writing flash
ftp: 16
384 bytes sent in 0.06Seconds
273.07Kbytes/sec.
```

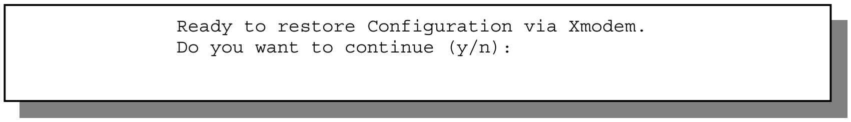
**Figure 10-8 Restore Using FTP or TFTP Session Example**

Refer to *section 10.2.5* to read about configurations that disallow TFTP and FTP to work over WAN.

## 10.3.3 Restore Via Console Port

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

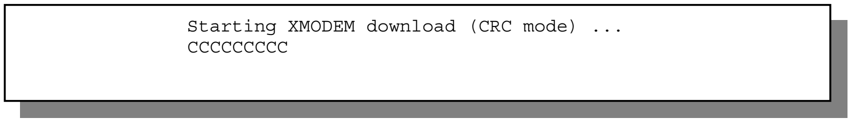
**Step 1.** Display menu 24.6 and enter “y” at the following screen.



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

**Figure 10-9 System Maintenance — Restore Configuration**

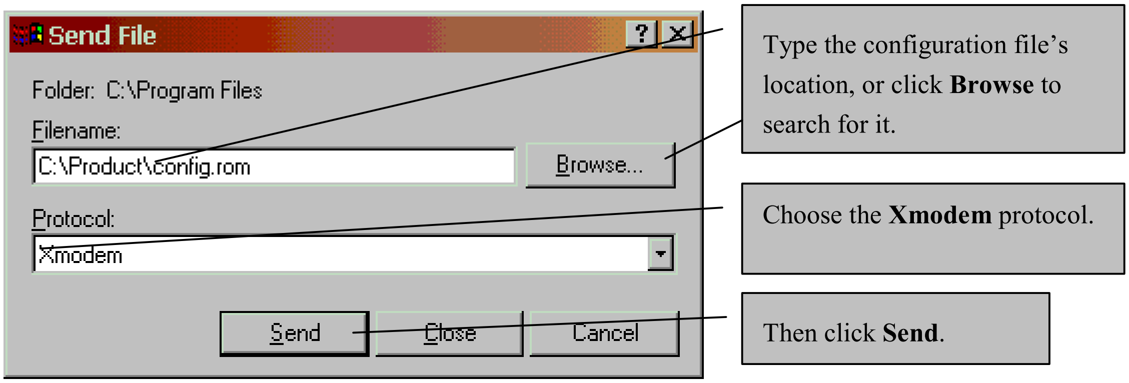
**Step 2.** The following screen indicates that the Xmodem download has started.



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

**Figure 10-10 System Maintenance — Starting Xmodem Download Screen**

**Step 3.** Run the HyperTerminal program by clicking **Transfer**, then **Receive File** as shown in the following screen.



Folder: C:\Program Files

Filename: C:\Product\config.rom

Protocol: Xmodem

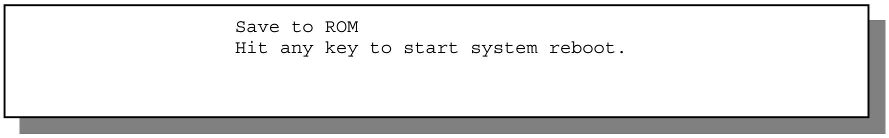
Type the configuration file's location, or click **Browse** to search for it.

Choose the **Xmodem** protocol.

Then click **Send**.

**Figure 10-11 Restore Configuration Example**

**Step 4.** After a successful restoration you will see the following screen. Press any key to restart the Prestige and return to the SMT menu.



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

**Figure 10-12 Successful Restoration Confirmation Screen**

## 10.4 Uploading Firmware and Configuration Files

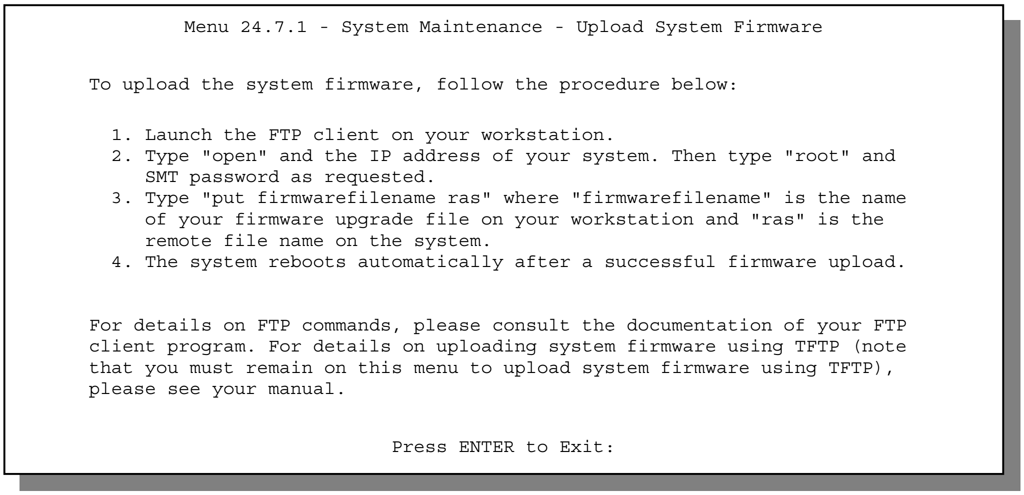
This section shows you how to upload firmware and configuration files. You can upload configuration files by following the procedure in the previous *Restore Configuration* section or by following the instructions in **Menu 24.7.2 - System Maintenance - Upload Router Configuration File** (for console port).

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

### 10.4.1 Firmware File Upload

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

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

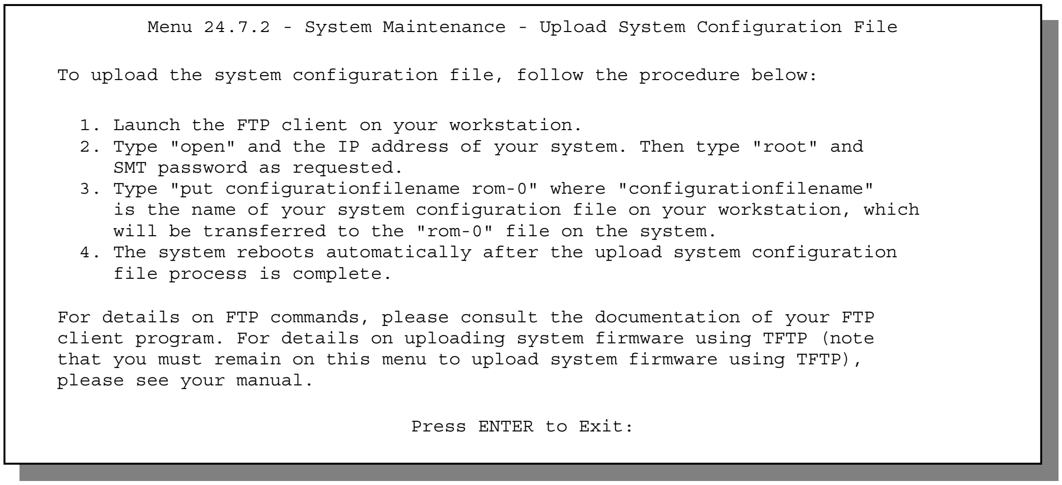


```
                 Menu 24.7.1 - System Maintenance - Upload System Firmware


        To upload the system firmware, follow the procedure below:

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


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

                                   Press ENTER to Exit:
```

**Figure 10-13 Telnet Into Menu 24.7.1 — Upload System Firmware**

### 10.4.2 Configuration File Upload

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



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

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

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

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

                               Press ENTER to Exit:
```

**Figure 10-14 Telnet Into Menu 24.7.2 — System Maintenance**

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

### 10.4.3 FTP File Upload Command from the DOS Prompt Example

**Step 1.** Launch the FTP client on your computer.

**Step 2.** Enter “open”, followed by a space and the IP address of your Prestige.

**Step 3.** Press [ENTER] when prompted for a username.

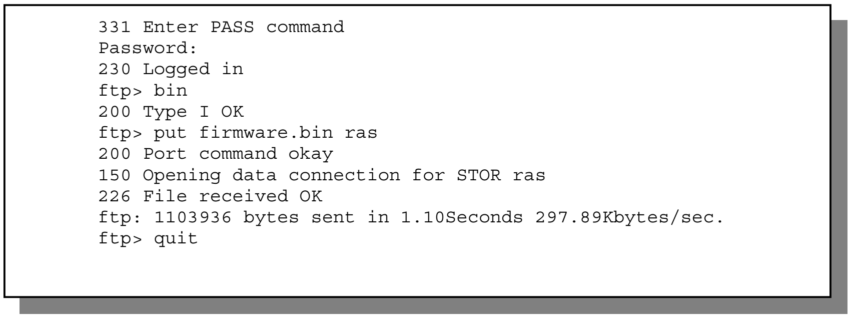
**Step 4.** Enter your password as requested (the default is “1234”).

**Step 5.** Enter “bin” to set transfer mode to binary.

**Step 6.** Use “put” to transfer files from the computer to the Prestige, for example, put firmware.bin ras transfers the firmware on your computer (firmware.bin) to the Prestige and renames it “ras”. Similarly put config.rom rom-0 transfers the configuration file on your computer (config.rom) to the Prestige and renames it “rom-0”. Likewise get rom-0 config.rom transfers the configuration file on the Prestige to your computer and renames it “config.rom.” See earlier in this chapter for more information on filename conventions.

**Step 7.** Enter “quit” to exit the ftp prompt.

### 10.4.4 FTP Session Example of Firmware File Upload



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

**Figure 10-15 FTP Session Example of Firmware File Upload**

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

Refer to *section 10.2.5* to read about configurations that disallow TFTP and FTP to work over LAN.

### 10.4.5 TFTP File Upload

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

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

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

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

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

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

**Step 5.** Use the TFTP client (see the example below) to transfer files between the Prestige and the computer. The file name for the firmware is "ras".

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

### 10.4.6 TFTP Upload Command Example

The following is an example tftp command:

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

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

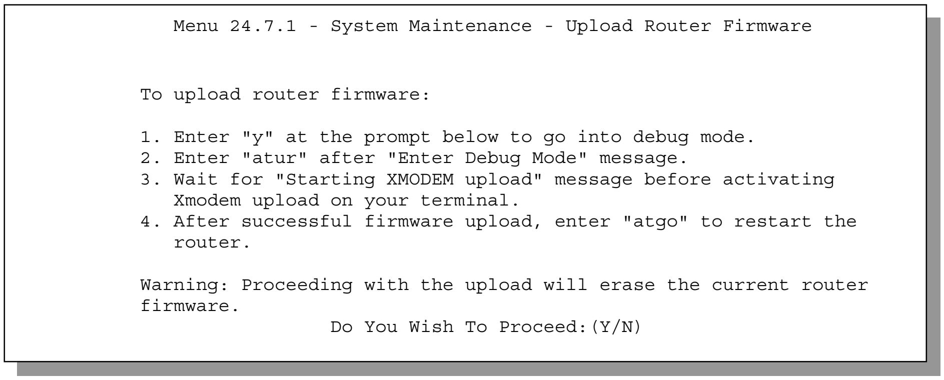
Commands that you may see in third party TFTP clients are listed earlier in this chapter.

### 10.4.7 Uploading Via Console Port

FTP or TFTP are the preferred methods for uploading firmware to your Prestige. However in the event of your network being down, uploading files is only possible with a direct connection to your Prestige via the console port. Uploading files via the console port under normal conditions is not recommended since FTP or TFTP is faster. Any serial communications program should work fine; however, you must use the Xmodem protocol to perform the download/upload.

### 10.4.8 Uploading a Firmware File Via Console Port

**Step 1.** Select 1 from **Menu 24.7 – System Maintenance – Upload Firmware** to display **Menu 24.7.1 - System Maintenance - Upload Router Firmware**, then follow the instructions as shown in the following screen.



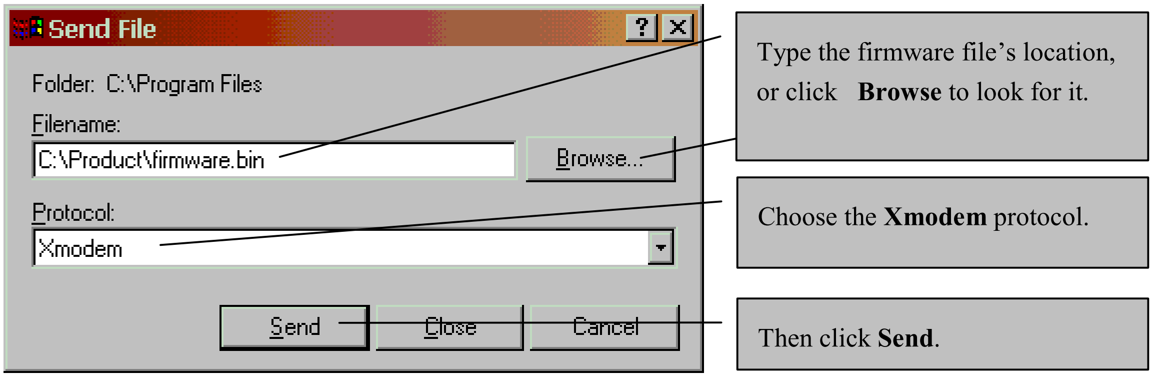
```
               Menu 24.7.1 - System Maintenance - Upload Router Firmware


            To upload router firmware:

            1. Enter "y" at the prompt below to go into debug mode.
            2. Enter "atur" after "Enter Debug Mode" message.
            3. Wait for "Starting XMODEM upload" message before activating
               Xmodem upload on your terminal.
            4. After successful firmware upload, enter "atgo" to restart the
               router.

            Warning: Proceeding with the upload will erase the current router
            firmware.
                             Do You Wish To Proceed:(Y/N)
```

**Figure 10-16 Menu 24.7.1 as seen using the Console Port**

**Step 2.** After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

### 10.4.9 Example Xmodem Firmware Upload Using HyperTerminal

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



Filename: C:\Product\firmware.bin

Protocol: Xmodem

Type the firmware file's location, or click **Browse** to look for it.

Choose the **Xmodem** protocol.

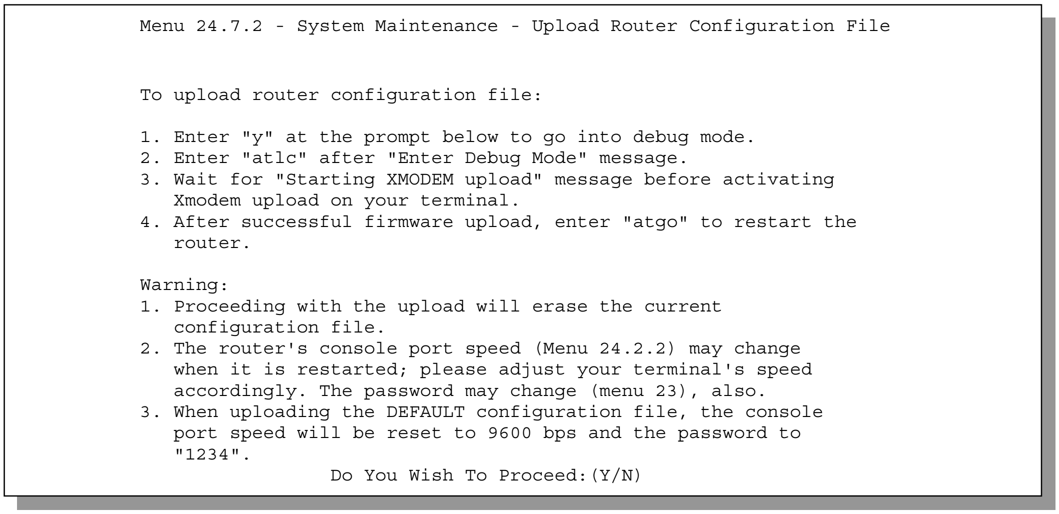
Then click **Send**.

**Figure 10-17 Example Xmodem Upload**

After the firmware upload process has completed, the Prestige will automatically restart.

## 10.4.10 Uploading a Configuration File Via Console Port

**Step 1.** Select 2 from **Menu 24.7 – System Maintenance – Upload Firmware** to display **Menu 24.7.2 - System Maintenance - Upload Router Configuration File**. Follow the instructions as shown in the next screen.



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


            To upload router configuration file:

            1. Enter "y" at the prompt below to go into debug mode.
            2. Enter "atlc" after "Enter Debug Mode" message.
            3. Wait for "Starting XMODEM upload" message before activating
               Xmodem upload on your terminal.
            4. After successful firmware upload, enter "atgo" to restart the
               router.

            Warning:
            1. Proceeding with the upload will erase the current
               configuration file.
            2. The router's console port speed (Menu 24.2.2) may change
               when it is restarted; please adjust your terminal's speed
               accordingly. The password may change (menu 23), also.
            3. When uploading the DEFAULT configuration file, the console
               port speed will be reset to 9600 bps and the password to
               "1234".
                             Do You Wish To Proceed:(Y/N)
```

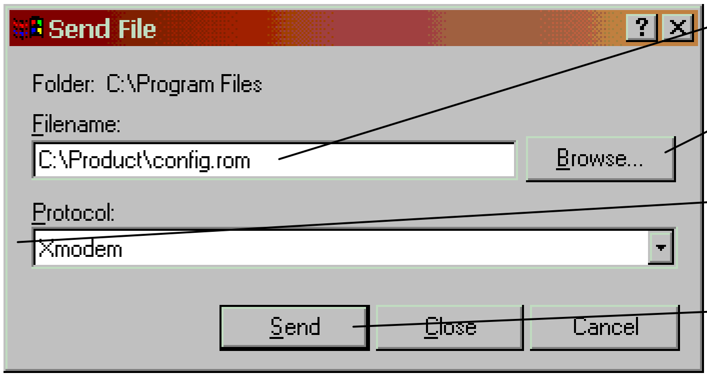
**Figure 10-18 Menu 24.7.2 as seen using the Console Port**

**Step 2.** After the "Starting Xmodem upload" message appears, activate the Xmodem protocol on your computer. Follow the procedure as shown previously for the HyperTerminal program. The procedure for other serial communications programs should be similar.

**Step 3.** Enter “atgo” to restart the Prestige.

### 10.4.11 Example Xmodem Configuration Upload Using HyperTerminal

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



Send File

Folder: C:\Program Files

Filename: C:\Product\config.rom

Protocol: Xmodem

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

Choose the **Xmodem** protocol.

Then click **Send**.

**Figure 10-19 Example Xmodem Upload**

After the configuration upload process has completed, restart the Prestige by entering "atgo".

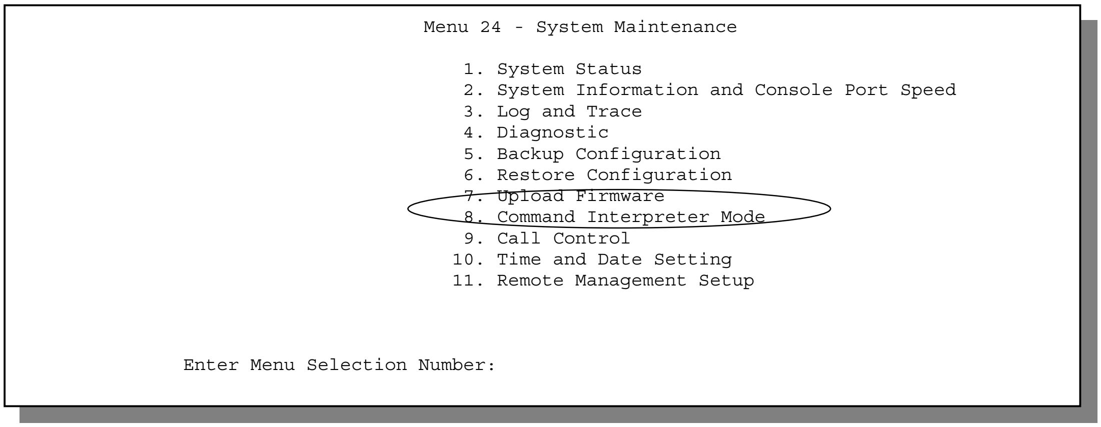
Refer to *section 10.2.5* to read about configurations that disallow TFTP and FTP to work over LAN.

# Chapter 11
# System Maintenance and Management

*This chapter leads you through SMT Menus 24.8 to 24.11.*

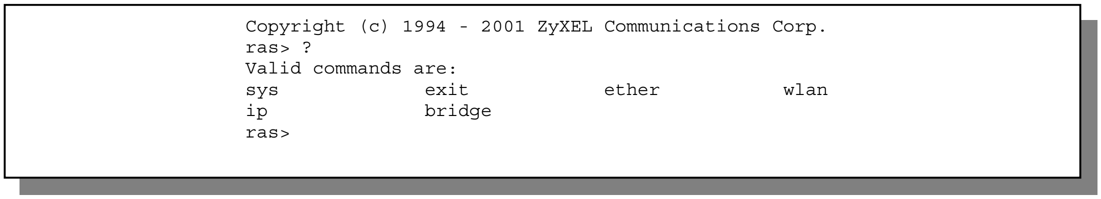
## 11.1 Command Interpreter Mode

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 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. Enter "exit" to return to the SMT main menu when finished.



```
                                    Menu 24 - System Maintenance

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



                     Enter Menu Selection Number:
```

**Figure 11-1 Command Mode in Menu 24**



```
Copyright (c) 1994 - 2001 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys             exit            ether           wlan
ip              bridge
ras>
```

**Figure 11-2 Valid CI Commands**

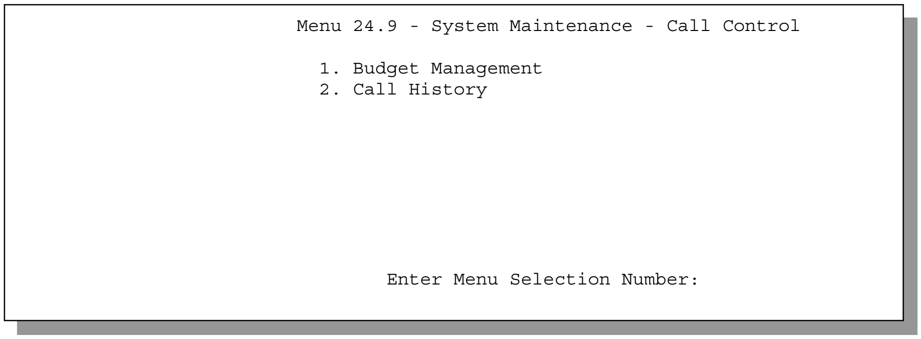
## 11.2 Call Control Support

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 **PPTP**/**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.

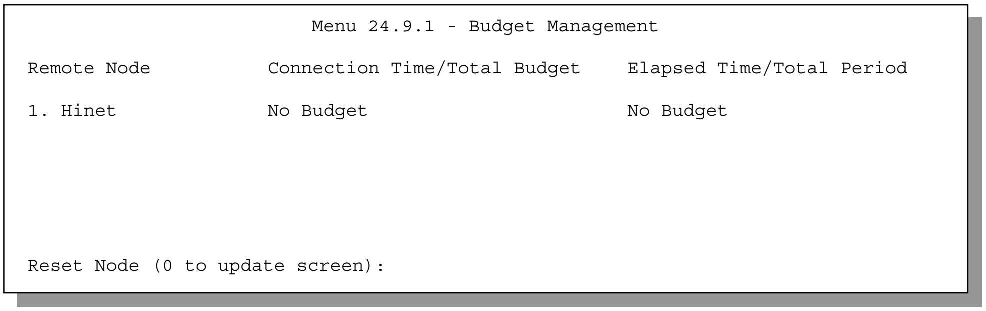


```
        Menu 24.9 - System Maintenance - Call Control

          1. Budget Management
          2. Call History









                Enter Menu Selection Number:
```

**Figure 11-3 Call Control**

### 11.2.1 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. Hinet             No Budget                       No Budget





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

**Figure 11-4 Budget Management**

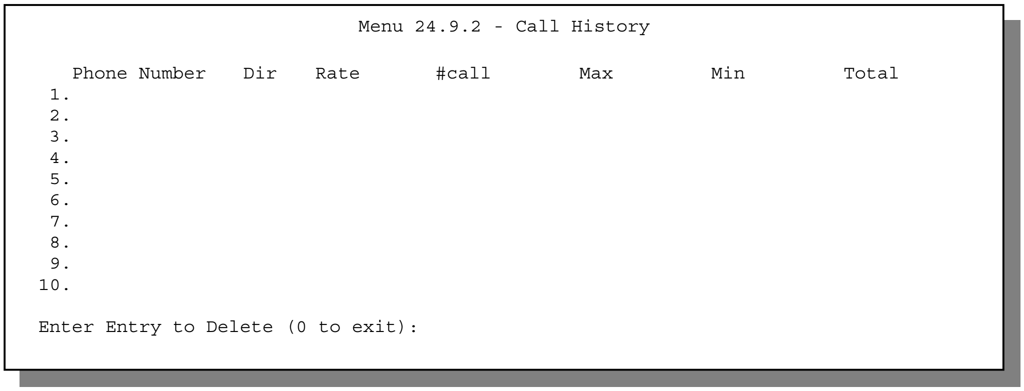
The total budget is the time limit on the accumulated time for outgoing calls to a remote node. When this limit is reached, the call will be dropped and further outgoing calls to that remote node will be blocked. After each period, the total budget is reset. The default for the total budget is 0 minutes 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 11-1 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). | 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. 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. |

## 11.2.2 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 11-5 Call History**

**Table 11-2 Call History Fields**

| FIELD | DESCRIPTION |
|---|---|
| Phone Number | The PPTP/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. |

## 11.3 Time and Date Setting

There is no Real Time Chip (RTC) in the Prestige, so we have a software mechanism to get the current time and date from an external server when you power up your Prestige. **Menu 24.10** does just that – it allows you to update the time and date settings of your Prestige. The real time is then displayed in the Prestige error logs. If you do not choose a time service protocol that your timeserver will send when the Prestige powers up you can enter the time manually but each time the system is booted, the time and date will be reset to **2000/01/01 00:00:00**.

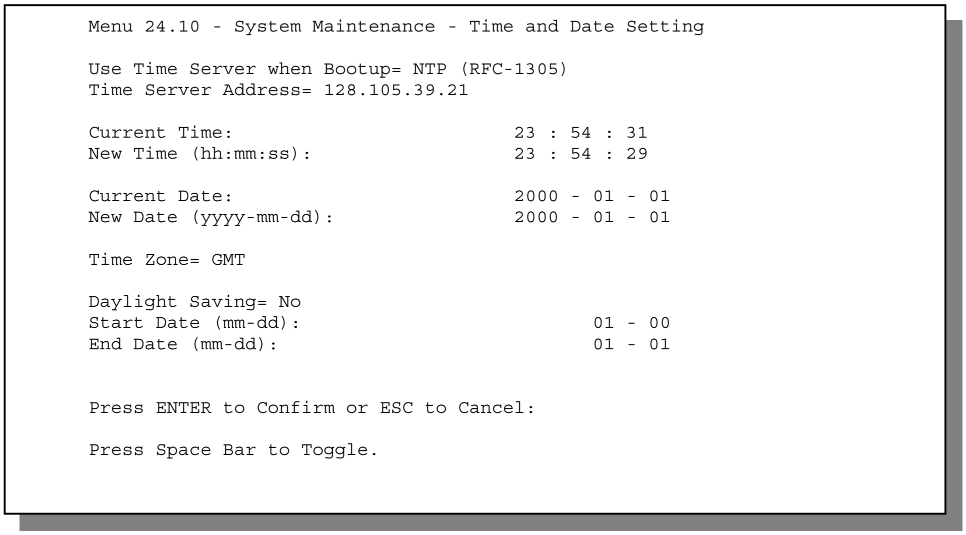
### 11.3.1 How Often Does the Prestige Update the Time?

The Prestige updates the time in three instances:

i. On leaving menu 24.10 after making changes.

ii. When the Prestige boots up and there is a time server configured in Menu 24.10.

iii. The time is also updated at 24-hour intervals after booting.



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

Use Time Server when Bootup= NTP (RFC-1305)
Time Server Address= 128.105.39.21

Current Time:                       23 : 54 : 31
New Time (hh:mm:ss):                23 : 54 : 29

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

Time Zone= GMT

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


Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

**Figure 11-6 System Maintenance – Time and Date Setting**

**Table 11-3 Time and Date Setting Fields**

| FIELD | DESCRIPTION |
|---|---|
| Use Time Server when Bootup | Enter the time service protocol that your time server will send when the Prestige powers up. Choices are **Daytime (RFC-867)**, **Time (RFC-868)**, **NTP (RFC-1305)** and **None**. The main differences between them are the format, e.g., the **Daytime (RFC-867)** format is day/month/date/year/time zone of the server while the **Time (RFC-868)** format gives a 4-byte integer giving the total number of seconds since **1970/1/1** at 0:0:0. The **NTP (RFC-1305)** format is similar. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. If you select **None** (this is the default value), you can |

| FIELD | DESCRIPTION |
|---|---|
| Use Time Server when Bootup | Enter the time service protocol that your time server will send when the Prestige powers up. Choices are **Daytime (RFC-867)**, **Time (RFC-868)**, **NTP (RFC-1305)** and **None**. The main differences between them are the format, e.g., the **Daytime (RFC-867)** format is day/month/date/year/time zone of the server while the **Time (RFC-868)** format gives a 4-byte integer giving the total number of seconds since **1970/1/1** at 0:0:0. The **NTP (RFC-1305)** format is similar. Not all time servers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. If you select **None** (this is the default value), you can enter the time manually but each time the system is booted, the time and date will be reset to **2000/1/1 0:0:0**. |
| Time Server IP Address | Enter the IP address of your time server. Check with your ISP/network administrator if you are unsure of this information. |
| Current Time: New Time | Enter the new time in hour, minute and second format. |
| Current Date: New Date | Enter the new date in month, date and year format. |
| Time Zone= GMT+0800 | Press [SPACE BAR] to set the time difference between your time zone and Greenwich Mean Time (GMT). Be aware if/when daylight savings time alters this time difference for your time zone. |
| Daylight Saving | Press [SPACE BAR] once to select **Yes** and then press [ENTER} to enable daylight savings time. |
| Start Date (mm-dd) | Enter the date that daylight savings takes effect in month-date format here. |
| End Date (mm-dd) | Enter the date that daylight savings ends in month-date format here. |
| Once you have filled in the new time and date, press [ENTER] to save the setting and press [ESC] to return to menu 24. | |

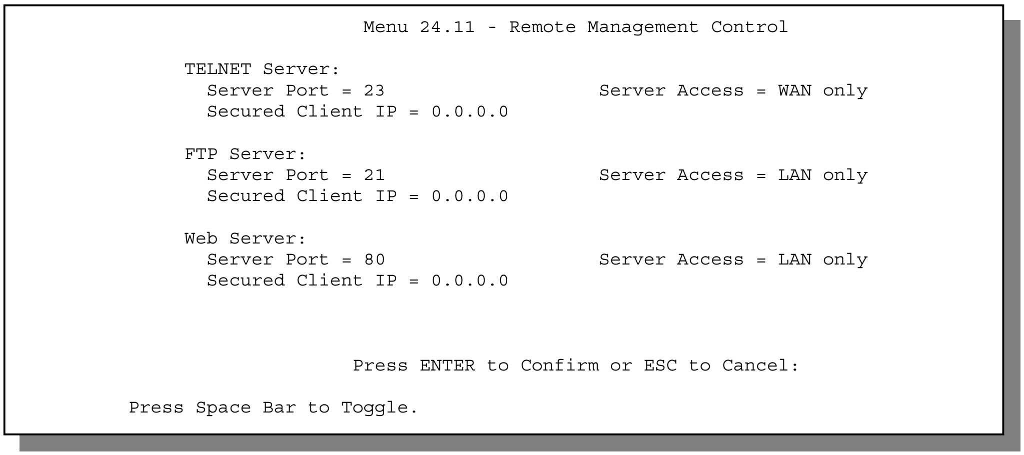
## 11.4 Remote Management Setup

Remote management setup is for managing Telnet, Web and FTP services. You can customize the service port, access interface, and the secured client IP address to enhance security and flexibility.

You may manage your Prestige from a remote location, via the Internet (**WAN only**), via the **LAN only**, **Both** (LAN & WAN) or neither (**Disable**).

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

Enter 11 from menu 24 to bring up **Menu 24.11 – Remote Management Control**.



```
                    Menu 24.11 - Remote Management Control

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

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

          Web Server:
            Server Port = 80                   Server Access = LAN only
            Secured Client IP = 0.0.0.0



                       Press ENTER to Confirm or ESC to Cancel:

     Press Space Bar to Toggle.
```

**Figure 11-7 Menu 24.11 – Remote Management Control**

**Table 11-4 Menu 24.11 – Remote Management Control**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Servers | These read-only labels denote the kind of server (Telnet, FTP or Web) that you may remotely manage via LAN, WAN, both or neither. | |
| Server Port | Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. If you wish to run such a server from your location, you will have to change the default service port number. Type in the new service port number here that corresponds to the new port number you configured on the server. | 23 |
| Server Access | Select the access interface (if any) by pressing the [SPACE BAR], then [ENTER] to choose from: **LAN only**, **WAN only**, **ALL** or **Disable**. | **LAN only** |
| Secured Client IP | The default value for **Secured Client IP** is 0.0.0.0, which means you don’t care which host is trying to use a service (Telnet, FTP or Web).<br>If you enter an IP address in this field, the Prestige will check if the client IP address matches the value here when a (Telnet, FTP or Web) session is up. If it does not match, the Prestige will disconnect the session immediately.<br>If the **Server Access** field is set to **Disable**, then this field is **N/A**. | 0.0.0.0 |

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel. | | |

### 11.4.1 Remote Management Limitations

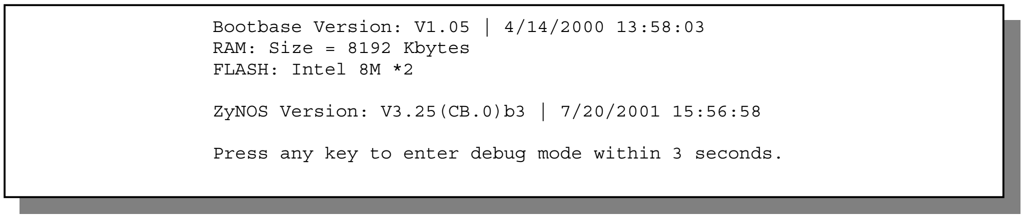
Remote management over LAN or WAN will not work when:

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

## 11.5 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 a previous section.

**To access the Boot Commands, a serial terminal connection like the console port (HyperTerminal) is required.**



```
Bootbase Version: V1.05 | 4/14/2000 13:58:03
RAM: Size = 8192 Kbytes
FLASH: Intel 8M *2

ZyNOS Version: V3.25(CB.0)b3 | 7/20/2001 15:56:58

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

**Figure 11-8 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 follow; e.g., ATBA3 will give a console port speed of 9.6 Kbps. ATSE displays the seed that is used to generate a password to turn on the debug flag in the firmware. The ATSH command shows product-related information such as boot module version, vendor name, product model, RAS code revision, etc. ATGO allows you to continue booting the system. Most other commands aid in advanced troubleshooting and should only be used by qualified engineers.

```
======= Debug Command Listing =======
AT              just answer OK
ATHE            print help
ATBAx           change baudrate. 1:38.4k, 2:19.2k, 3:9.6k 4:57.6k 5:115.2k
ATENx,(y)       set BootExtension Debug Flag (y=password)
ATSE            show the seed of password generator
ATTI(h,m,s)     change system time to hour:min:sec or show current time
ATDA(y,m,d)     change system date to year/month/day or show current date
ATDS            dump RAS stack
ATDT            dump Boot Module Common Area
ATDUx,y         dump memory contents from address x for length y
ATRBx           display the  8-bit value of address x
ATRWx           display the 16-bit value of address x
ATRLx           display the 32-bit value of address x
ATGO(x)         run program at addr x or boot router
ATGR            boot router
ATGT            run Hardware Test Program
ATRTw,x,y(,z)   RAM test level w, from address x to y (z iterations)
ATSH            dump manufacturer related data in ROM
ATDOx,y         download from address x for length y to PC via XMODEM
ATTD            download router configuration to PC via XMODEM
ATUR            upload router firmware to flash ROM
ATLC            upload router configuration file to flash ROM
ATXSx           xmodem select: x=0: CRC mode(default); x=1: checksum mode
AT              just answer OK
```

**Figure 11-9 Boot Module Commands**

# Chapter 12
# Call Scheduling

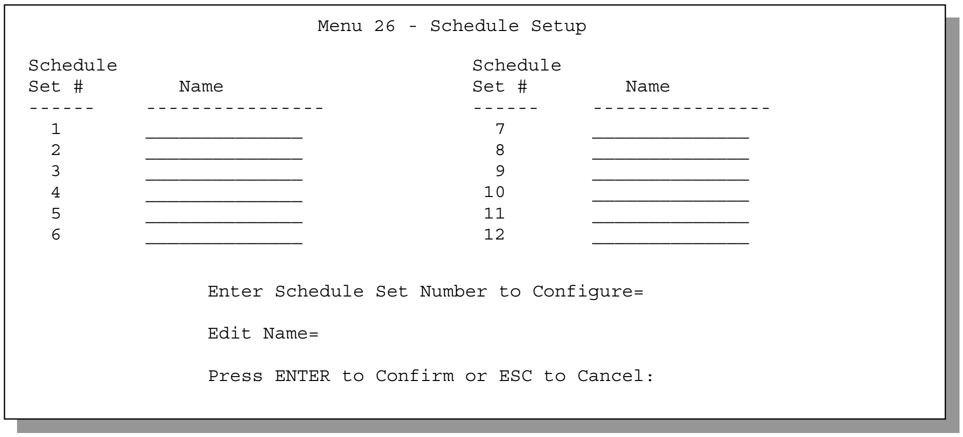
*This chapter shows you how to set up call time periods for remote nodes.*

## 12.1 Introduction

The call scheduling feature allows the Prestige to manage a remote node and dictate when a remote node should be called and for how long. This feature is similar to the scheduler in a video cassette recorder where you record programs at times that you specify. You can apply up to four schedule sets in **Menu 11.1 - Remote Node Profile**.

## 12.2 Schedule Setup

From the main menu, enter 26 to access **Menu 26 - Schedule Setup** as shown next.



```
                          Menu 26 - Schedule Setup

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

                Enter Schedule Set Number to Configure=

                Edit Name=

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

**Figure 12-1 Schedule Setup**

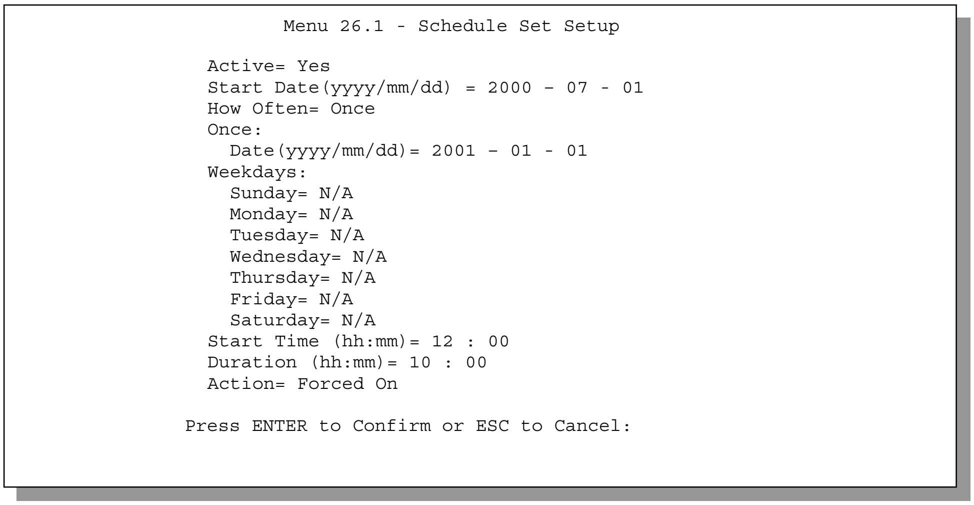
Lower numbered sets take precedence over higher numbered sets thereby avoiding scheduling conflicts. For example, if sets 1, 2, 3 and 4 are applied in the remote node then set 1 will take precedence over sets 2, 3 and 4 as the Prestige, by default, applies the lowest numbered set first. Set 2 will take precedence over sets 3 and 4, and so on.

You can design up to 12 schedule sets but you can only apply up to four schedule sets for a remote node.

**To delete a schedule set, choose the set number and either delete the name or press [SPACE BAR] once in Edit Name field and then press [ENTER] in the DELETE PROFILE field.**

## 12.3 Schedule Set Setup

To setup a schedule set, select the schedule set you want to setup from menu 26 (1-12), press [ENTER] and then type in a name for the set. Press [ENTER] to display **Menu 26.1 - Schedule Set Setup** as shown next.



```
                    Menu 26.1 - Schedule Set Setup

             Active= Yes
             Start Date(yyyy/mm/dd) = 2000 – 07 - 01
             How Often= Once
             Once:
               Date(yyyy/mm/dd)= 2001 – 01 - 01
             Weekdays:
               Sunday= N/A
               Monday= N/A
               Tuesday= N/A
               Wednesday= N/A
               Thursday= N/A
               Friday= N/A
               Saturday= N/A
             Start Time (hh:mm)= 12 : 00
             Duration (hh:mm)= 10 : 00
             Action= Forced On

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

**Figure 12-2 Schedule Set Setup**

If a connection has already been established, your Prestige will not drop it. Once the connection is dropped manually or it times out (the time configured in the **Duration** field expires), then that remote node can't be triggered again until the next configured start time.

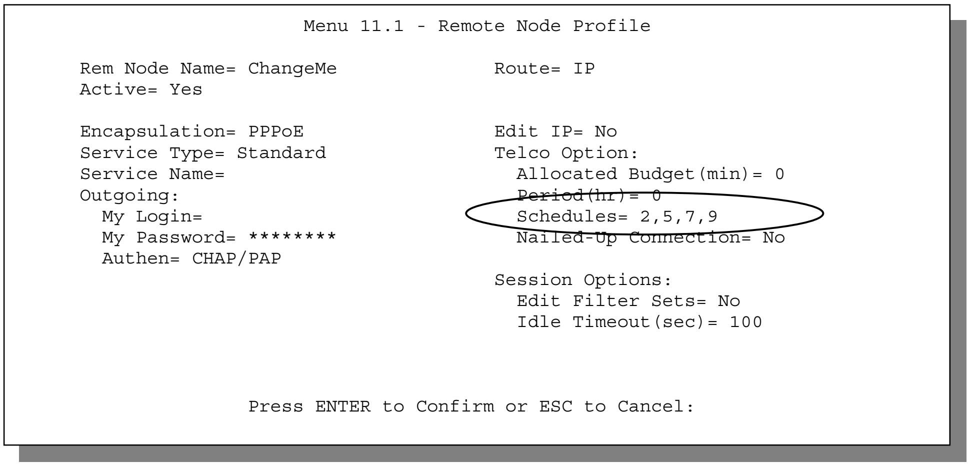
**Table 12-1 Schedule Set Setup Fields**

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| Active | Choose **Yes** to activate and **No** to deactivate the schedule set. | **Yes**<br>(default) |
| Start Date | Enter the start date that you wish the set to take effect in year - month-day format. Valid dates are from the present to February 5, 2036. | 2000 – 07 – 01 |
| How Often | Choose **Once** or **Weekly**. Both these options are mutually | **Once** |

| FIELD | DESCRIPTION | EXAMPLE |
|---|---|---|
| How Often | Choose **Once** or **Weekly**. Both these options are mutually exclusive. If **Once** is selected, then fill in the date it will occur. If **Weekly** is selected, then fill in the weekdays when call should occur. When **Once** is selected, the schedule rule deletes automatically after the scheduled time elapses. | **Once**<br>(default) |
| Once:<br>Date | If you select **Once** in the **How Often** field above, enter the date the set should activate in year-month-day format.<br>If you select **Weekly** in the **How Often** field above, this field is **N/A**. | 2001 – 01 – 01 |
| Weekday:<br>Day | If you select **Weekly** in the **How Often** field above, then choose the day(s) the set should activate (and recur). Individual **Day** parameters are active when their fields read **Yes** and inactive when their fields read **No** or **N/A**. | **N/A**<br>(default) |
| Start Time | Enter the start time that you wish the schedule set to take effect in hour : minute format. | 12 : 00 |
| Duration | Enter the maximum duration allowed in hour : minute format for this scheduled connection. | 10 : 00 |
| Action | Choose an action. Choices are:<br>**Forced On** means that the connection is maintained whether or not there is a demand call on the line and will persist for the time period specified in the **Duration** field.<br>**Forced Down** means that the connection is blocked whether or not there is a demand call on the line.<br>**Enable Dial-On-Demand** means that this schedule permits a demand call on the line.<br>**Disable Dial-On-Demand** means that this schedule prevents a demand call on the line. | **Forced On** |

## 12.4 Applying Schedule Sets to Remote Nodes

Once your schedule sets are configured, you must apply them to the desired remote node(s). Enter menu 11 from the main menu and enter a node number to edit. In menu 11.1 press the [SPACE BAR] to select **PPPoE** in the **Encapsulation** field. You can apply up to four schedule sets, separated by commas, for one remote node. Enter the schedule set numbers in the **Schedule Sets** field. In the following example schedule sets 2, 5, 7 and 9 are applied.



```
                         Menu 11.1 - Remote Node Profile

    Rem Node Name= ChangeMe              Route= IP
    Active= Yes

    Encapsulation= PPPoE                 Edit IP= No
    Service Type= Standard               Telco Option:
    Service Name=                          Allocated Budget(min)= 0
    Outgoing:                              Period(hr)= 0
      My Login=                            Schedules= 2,5,7,9
      My Password= ********                Nailed-Up Connection= No
      Authen= CHAP/PAP
                                         Session Options:
                                           Edit Filter Sets= No
                                           Idle Timeout(sec)= 100



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

**Figure 12-3 Applying Schedule Sets to a Remote Node Example (PPPoE Encapsulation)**

# Chapter 13
# Telnet Configuration and Capabilities

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

## 13.1 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 next.

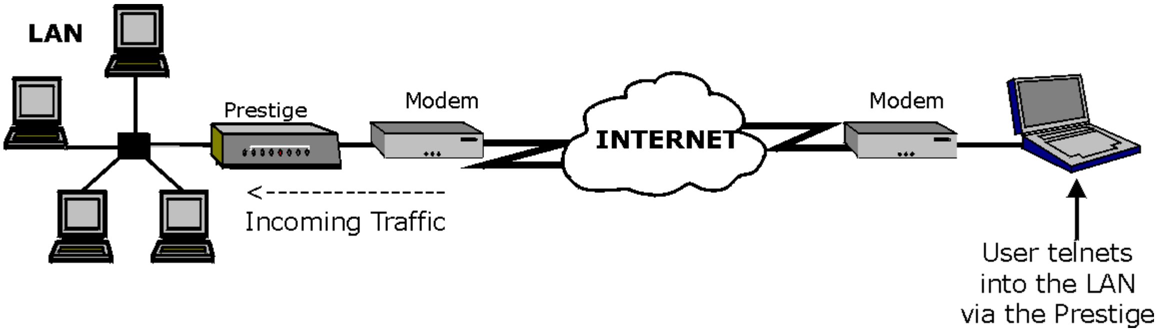


**Figure 13-1 Telnet Configuration on a TCP/IP Network**

## 13.2 Telnet Under NAT

When NAT 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 NAT’s IP address will connect to the Prestige directly. See the NAT chapter for details on port forwarding.

## 13.3 Telnet Capabilities

### 13.3.1 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, you will be logged out if another user logs in to the Prestige via the console port.

### 13.3.2 System Timeout

There is a system timeout of five minutes (300 seconds) for either the console port, web session, 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.

# Part IV:

## TROUBLESHOOTING, APPENDICES, GLOSSARY AND INDEX

Part 4 provides information about solving common problems, followed by some Appendices, a Glossary of Terms and an Index.

# Chapter 14
# Troubleshooting

*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.*

## 14.1 Problems Starting Up the Prestige

**Table 14-1 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.<br>If the error persists, you may have a hardware problem. In this case, you should contact your vendor. | |
| Cannot access the Prestige via the console port. | 1. Check to see if the Prestige is connected to your computer's 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 Control set to None. |

## 14.2 Problems With the LAN Interface

**Table 14-2 Troubleshooting the LAN Interface**

| PROBLEM | CORRECTIVE ACTION |
|---|---|
| Cannot ping any computer on the LAN. | Check the 10M/100M LEDs on the front panel. One of these LEDs should be on. If they are both off, check the cables between your Prestige and hub or the station. |
| | Verify that the IP addresses and the subnet masks of the Prestige and the computers on the LAN are on the same subnet. |
| The wireless workstations cannot connect to the network. | Check that the W-LAN LED is on. If this LED is off, this means that the wireless LAN is encountering some problems. Turn off your Prestige and check the wireless workstation associated with your Prestige. Check: |
| | The wireless workstation is not out-of-range of your Prestige. |
| | The link quality/signal strength using the workstation's wireless utility. To avoid interference problems, try the other channels in Menu 3.5. |
| | The ESSID used by other wireless workstations must match that of your Prestige. The wireless workstations' network type must be set at Infrastructure. |
| | The WEP keys setting on other wireless workstations must match that of your Prestige. |

## 14.3 Problems With the WAN Interface

**Table 14-3 Troubleshooting the WAN Interface**

| PROBLEM | CORRECTIVE ACTION |
|---|---|
| Cannot get WAN IP address from the ISP. | The WAN IP address is provided when the ISP recognizes the user as an authorized user after verifying the MAC address or Host Name or User ID.<br>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.**<br>In case the ISP does not allow you to use a new MAC, you can clone the MAC from the LAN as the WAN MAC and send it to the ISP using **Menu 2 – WAN Setup**. |
| | If the ISP checks the Host Name, enter host name in the *System Name* 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**, **My Login** and **My Password** in **Menu 4 – Internet Access Setup**. |
| Cannot connect to a remote node or ISP. | Check Menu 24.1 to verify the line status. If it indicates **Down**, then contact your server provider. |

## 14.4 Problems With Internet Access

**Table 14-4 Troubleshooting Internet Access**

| PROBLEM | CORRECTIVE ACTION |
|---|---|
| Cannot access the Internet. | Connect your cable/xDSL modem with the Prestige using the appropriate type of cable.<br>Check with the manufacturer of your cable/xDSL modem about the cable requirement because some modems you may require a crossover cable and for others straight through cable. |
| | Verify your settings in **Menu 3.2** and **Menu 4**. |

## 14.5 General Instructions

If you have other problems you can try the following options:

- Check **Menu 24.1 – System Maintenance – Status, Menu 24.2.1 – System Maintenance – Information** and **Menu 24.3 – System Maintenance – Log and Trace** in order to locate the problem.
- Check the Troubleshooting section in the Support Notes.
- Use Debug commands to diagnose problems. In general, ZyXEL recommends that you use these commands with the direction of your customer support representative.

### 14.5.1 When Contacting Customer Support Representative

When you contact your customer support representative have the following information ready:

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

# Appendix A
# Wireless LAN and IEEE 802.11

A wireless LAN (WLAN) provides a flexible data communications system that you can use to access various services (navigating the Internet, email, printer services, etc.) without the use of wires. In effect a wireless LAN environment provides you the freedom to stay connected to the network while in the coverage area.

## Benefits of a Wireless LAN

1. Access to network services in areas otherwise hard or expensive to wire, such as historical buildings, buildings with asbestos materials and classrooms.
2. Doctors and nurses can access a complete patient's profile on a handheld or notebook computer upon entering a patient's room.
3. It allows flexible workgroups a lower total cost of ownership for networks that are frequently reconfigured.
4. Conference room users can access the network as they move from meeting to meeting- accessing up-to-date information that facilitates the ability to communicate decisions "on the fly".
5. It provides campus-wide networking coverage, allowing enterprises the roaming capability to set up easy-to-use wireless networks that transparently covers an entire campus.

## IEEE 802.11

The 1997 completion of the IEEE 802.11 standard for wireless LANs (WLANs) was a first important step in the evolutionary development of wireless networking technologies. The standard was developed to maximize interoperability between differing brands of wireless LANs and to introduce a variety of performance improvements and benefits. On September 16, 1999, the 802.11b provided much higher data rates of up to 11Mbps, while maintaining the 802.11 protocol.

The IEEE 802.11 specifies three different transmission methods for the PHY, the layer responsible for transferring data between nodes. Two of the methods use spread spectrum RF signals, Direct Sequence Spread Spectrum (DSSS) and Frequency-Hopping Spread Spectrum (FHSS), in the 2.4 to 2.4825 GHz unlicensed ISM (Industrial, Scientific and Medical) band. The third method is infrared technology, using very high frequencies, just below visible light in the electromagnetic spectrum to carry data.

## Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless nodes or stations (STA), which is called a Basic Service Set (BSS). In the most basic form, a wireless LAN connects a set of computers with wireless adapters. Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an Ad-hoc network or Independent Basic Service Set (IBSS). See the following diagram of an example of an Ad-hoc wireless LAN.

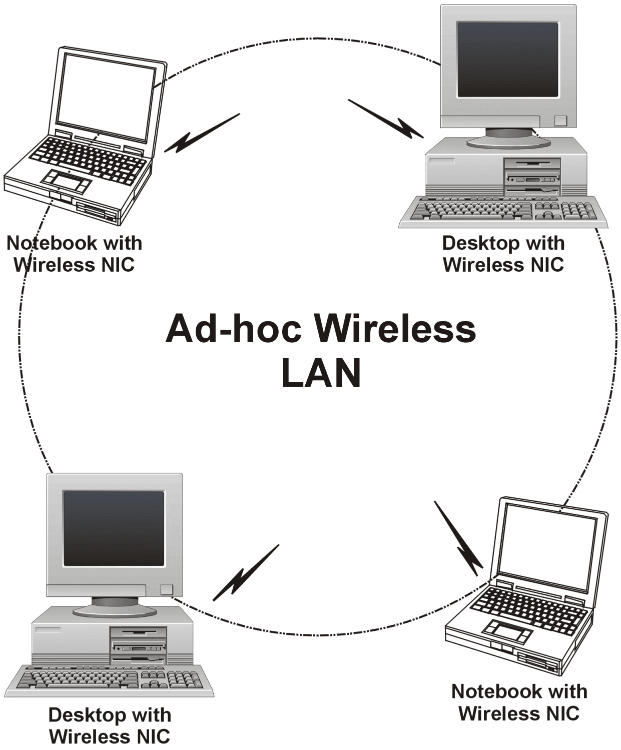

Notebook with Wireless NIC
Desktop with Wireless NIC
Ad-hoc Wireless LAN
Desktop with Wireless NIC
Notebook with Wireless NIC

**Diagram 1 Peer-to-Peer Communication in an Ad-hoc Network**

## Infrastructure Wireless LAN Configuration

For Infrastructure WLANs, multiple Access Points (APs) link the WLAN to the wired network and allow users to efficiently share network resources. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood. Multiple Access Points can provide wireless coverage for an entire building or campus. All communications between stations or between a station and a wired network client go through the Access Point.

The Extended Service Set (ESS) shown in the next figure consists of a series of overlapping BSSs (each containing an Access Point) connected together by means of a Distribution System (DS). Although the DS could be any type of network, it is almost invariably an Ethernet LAN. Mobile nodes can roam between Access Points and seamless campus-wide coverage is possible.

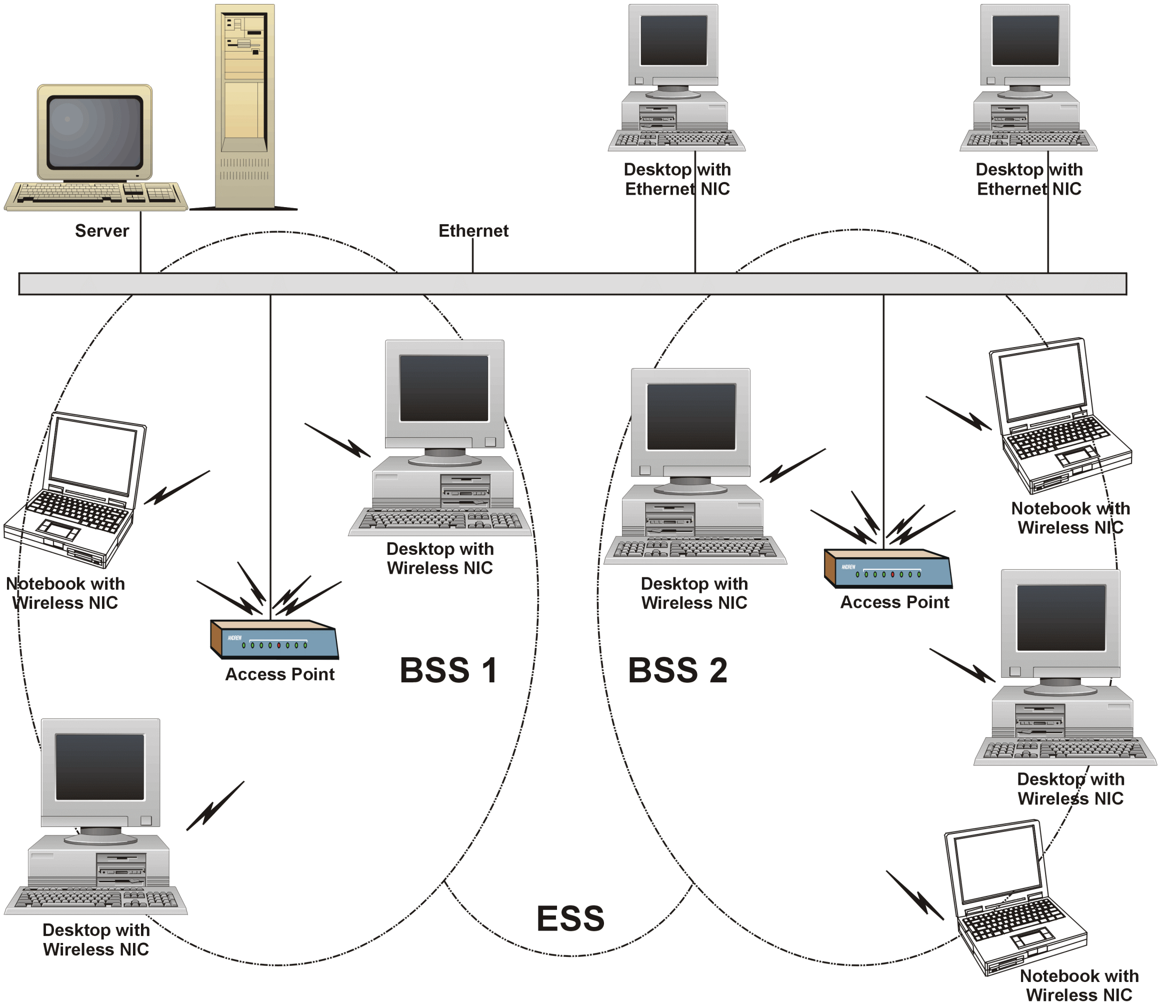

Server
Ethernet
Desktop with Ethernet NIC
Desktop with Ethernet NIC
Notebook with Wireless NIC
Access Point
Desktop with Wireless NIC
BSS 1
Desktop with Wireless NIC
Access Point
BSS 2
Notebook with Wireless NIC
Desktop with Wireless NIC
Desktop with Wireless NIC
ESS
Notebook with Wireless NIC
Desktop with Wireless NIC

**Diagram 2 ESS Provides Campus-Wide Coverage**

# Appendix B PPPoE

## PPPoE in Action

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

## Benefits of PPPoE

PPPoE offers the following benefits:

1. It provides you with a familiar dial-up networking (DUN) user interface.
2. It lessens the burden on the carriers of provisioning virtual circuits all the way to the ISP on multiple switches for thousands of users. For GSTN (PSTN and ISDN), the switching fabric is already in place.
3. It allows the ISP to use the existing dial-up model to authenticate and (optionally) to provide differentiated services.

## Traditional Dial-up Scenario

The following diagram depicts a typical hardware configuration where the computers use traditional dial-up networking.

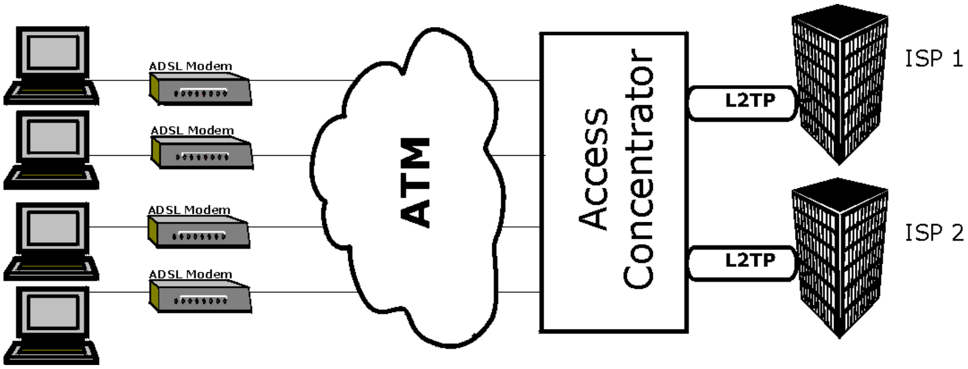


**Diagram 3 Single-computer per Modem Hardware Configuration**

## How PPPoE Works

The PPPoE driver makes the Ethernet appear as a serial link to the COMPUTER and the COMPUTER runs PPP over it, while the modem bridges the Ethernet frames to the Access Concentrator (AC). Between the AC and an ISP, the AC is acting as a L2TP (Layer 2 Tunneling Protocol) LAC (L2TP Access Concentrator) and tunnels the PPP frames to the ISP. The L2TP tunnel is capable of carrying multiple PPP sessions.

With PPPoE, the VC (Virtual Circuit) is equivalent to the dial-up connection and is between the modem and the AC, as opposed to all the way to the ISP. However, the PPP negotiation is between the COMPUTER and the ISP.

## Prestige as a PPPoE Client

When using the Prestige as a PPPoE client, the computers on the LAN see only Ethernet and are not aware of PPPoE. This alleviates the administrator from having to manage the PPPoE clients on the individual computers.

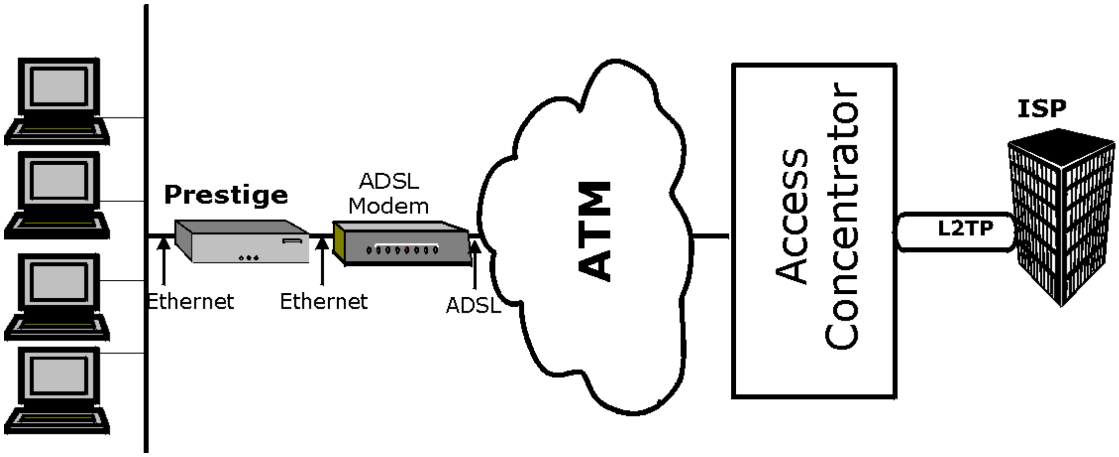
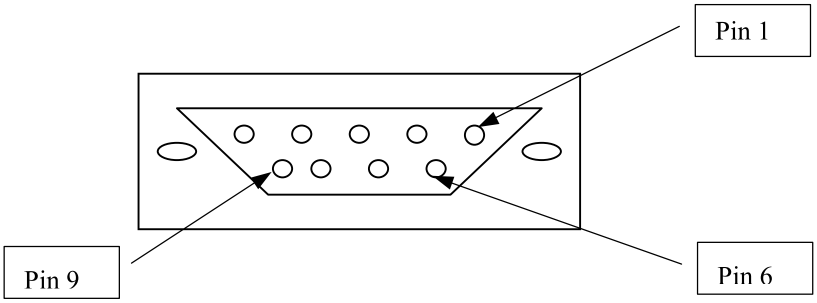


**Diagram 4 Prestige as a PPPoE Client**

# Appendix C Hardware Specifications

| | |
|---|---|
| Power Specification | I/P AC 120V / 60Hz; O/P DC 12V 1200 mA |
| MTBF (Mean Time Between Failure) | 100000 hrs |
| Operating Temperature | 0º C ~ 40º C |
| Ethernet Specification for WAN | 10 Mbit Half Duplex |
| Ethernet Specification for LAN | 10/100 Mbit Half / Full Auto-negotiation |
| Console Port RS–232C | 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 next figure. |



| WAN/LAN Cable Pin Layout:<br>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 D
# 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 non-insulated 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

12. In order to limit Radio Frequency (RF) exposure, the following rules should be applied:

    - Install the antenna in a location where a distance of 20 cm from the antenna may be maintained.
    - While installing the antenna in the location, please do not turn on the power of wireless card.
    - While the device is working (transmitting or receiving), please do not touch or move the antenna.
    - Do not operate a portable transmitter near unshielded blasting caps or in an explosive environment unless it is a type especially qualified for such use.

13. For laptop computer users, in order to comply with the FCC RF exposure limits, it is recommended when using a laptop with a wireless LAN adapter card that the card's integrated antenna should not be positioned closer than 5 cm (2 inches) from your body or nearby persons for extended periods of time while it is transmitting (or operating). If the antenna is positioned less than 5 cm (2 inches) from the user, it is recommended that the user limit exposure time.

# Appendix E PPTP

## PPTP Basics

PPTP (Point-to-Point Tunneling Protocol) is a Microsoft™ proprietary protocol (RFC-2637 for PPTP is informational only) to tunnel PPP frames.

## Transporting PPP Frames From a COMPUTER to a Broadband Modem Over Ethernet

A solution is to build PPTP into the ANT (ADSL Network Termination) where PPTP is used only over the short haul between the COMPUTER and the modem over Ethernet. For the rest of the connection, the PPP frames are transported with PPP over AAL5 (RFC-2364). The PPP connection, however, is still between the COMPUTER and the ISP. The various connections in this setup are depicted in the following diagram. The drawback of this solution is that it requires one separate ATM VC per destination.

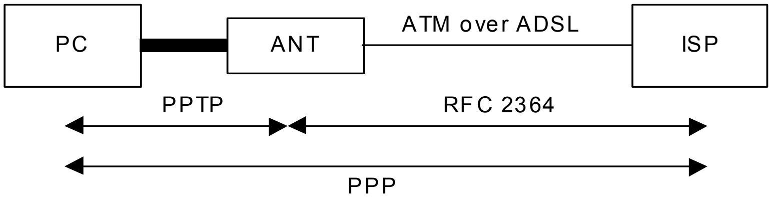


**Diagram 3 PPTP Setup**

## PPTP and the Prestige

When the Prestige is deployed in such a setup, it appears as a COMPUTER to the ANT (ADSL Network Termination).

In Windows® VPN or PPTP Pass-Through feature, the PPTP tunneling is created from Windows® 95, 98 and NT clients to an NT server in a remote location. The pass-through feature allows users on the network to access a different remote server using the Prestige's Internet connection. In NAT mode, the Prestige is able to pass the PPTP packets to the internal PPTP server (i.e., NT server) behind NAT. Users need to forward PPTP packets to port 1723 by configuring the server in **Menu 15 – NAT Setup**. In the case above as the PPTP connection is initialized by the remote PPTP client, the user must configure the PPTP clients. For the Prestige the PPTP connection is initialized by the Prestige and hence, there is no need to configure the remote PPTP clients.

## PPTP Protocol Overview

PPTP is very similar to L2TP, since L2TP is based on both PPTP and L2F (Cisco's Layer 2 Forwarding). Conceptually, there are three parties in PPTP, namely the PNS (PPTP Network Server), the PAC (PPTP Access Concentrator) and the PPTP user. The PNS is the box that hosts both the PPP and the PPTP stacks and forms one end of the PPTP tunnel. The PAC is the box that dials/answers the phone calls and relays the PPP frames to the PNS. The PPTP user is not necessarily a PPP client; it can be a PPP server as well. Both the PNS and the PAC must have IP connectivity; however, the PAC must in addition have dial-up capability. The phone call is between the user and the PAC and the PAC tunnels the PPP frames to the PNS. The PPTP user is unaware of the tunnel between the PAC and the PNS.

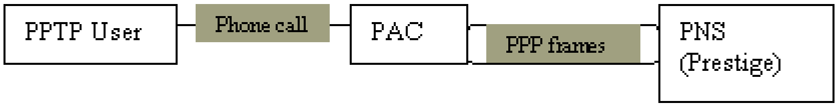


**Diagram 4 PPTP Protocol Overview**

Microsoft™ includes PPTP as a part of the Windows® O/S. In Microsoft™'s implementation, the COMPUTER and hence the Prestige 316 is the PNS that requests the PAC (the ANT) to place an outgoing call over AAL5 to an RFC-2364 server.

## Control and PPP Connections

Each PPTP session has distinct control connection and PPP data connection.

### Control Connection

The control connection runs over TCP. Similar to L2TP, a tunnel control connection is first established before call control messages can be exchanged. Please note that a tunnel control connection supports multiple call sessions.

The following diagram depicts the message exchange of a successful call setup between a COMPUTER and an ANT.

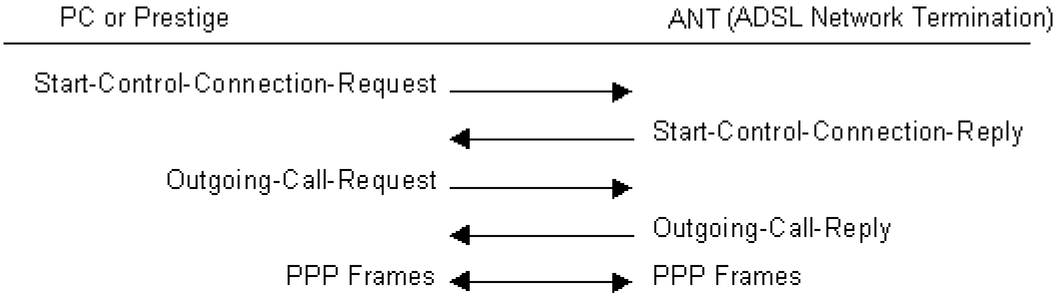

PC or Prestige
ANT (ADSL Network Termination)
Start-Control-Connection-Request
Start-Control-Connection-Reply
Outgoing-Call-Request
Outgoing-Call-Reply
PPP Frames
PPP Frames

**Diagram 5. Control Connection**

### PPP Data Connection

The PPP frames are tunneled between the PNS and PAC over GRE (General Routing Encapsulation, RFC-1701, 1702). The individual calls within a tunnel are distinguished using the Call ID field in the GRE header.

# Appendix F
# Power Adapter Specifications

| NORTH AMERICAN PLUG STANDARDS | | |
|---|---|---|
| **AC Power Adapter Model** | MW48-1201200 | AD48-1201200DUY |
| **Input Power** | AC120Volts/60Hz/22W | AC120Volts/60Hz/0.25A |
| **Output Power** | DC12Volts/1.2A | DC12Volts/1.2A |
| **Power Consumption** | 9 W | 9 W |
| **Safety Standards** | UL, CUL (UL1310, CSA C22.2 No. 233-M91) | |
| **EUROPEAN PLUG STANDARDS** | | |
| **AC Power Adapter Model** | AD-1201200DV | JAD-121200E |
| **Input Power** | AC230Volts/50Hz/0.2A | AC230Volts/50Hz |
| **Output Power** | DC12Volts/1.2A | DC12Volts/1.2A |
| **Power Consumption** | 9 W | 9 W |
| **Safety Standards** | TUV, CE (EN 60950) | |
| | **UNITED KINGDOM PLUG STANDARDS** | **JAPANESE PLUG STANDARDS** |
| **AC Power Adapter Model** | AD-1201200DK | JOD-48-1124 |
| **Input Power** | AC230Volts/50Hz/0.2A | AC100Volts/ 50/60Hz/ 27VA |
| **Output Power** | DC12Volts/1.2A | DC12Volts/1.2A |
| **Power Consumption** | 9 W | 9 W |
| **Safety Standards** | TUV, CE (EN 60950, BS7002) | T-Mark (Japan Dentori) |
| **AUSTRALIAN AND NEW ZEALAND PLUG STANDARDS** | | |
| **AC Power Adapter Model** | AD-1201200DS or AD-121200DS | |
| **Input Power** | AC240Volts/50Hz/0.2A | |
| **Output Power** | DC12Volts/1.2A | |
| **Power Consumption** | 9 W | |
| **Safety Standards** | NATA (AS 3260) | |

# Glossary

| | |
|---|---|
| **100Base-T** | Uses two pairs of twisted-pair wire with a maximum distance of 100 meters between the hub and the workstation. |
| **10Base-T** | 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. |
| **802.11** | The IEEE standard that specifies Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. |
| **802.11b** | The IEEE standard that specifies Higher-Speed Physical Layer Extension in the 2.4 GHz Band for 5.5 and 11 megabit per second wireless LANs. |
| **802.3** | The IEEE standard that specifies carrier sense media access control and physical layer specifications for Ethernet LANs. |
| **Access Control** | The prevention of unauthorized usage of resources. |
| **Access Point (AP)** | Any entity that has station functionality and provides access to the distribution services, via the wireless medium (WM) for associated stations. |
| **ADSL** | Asymmetrical Digital Subscriber Line is an asymmetrical technology which means that the downstream data rate of the line is much higher than the upstream data rate. ADSL operates in a frequency range that is above the frequency range of voice services, so the two systems can operate over the same cable. |
| **Advanced Mobile Phone Service (AMPS)** | Advanced analog mobile service. Uses a 50 MHz segment of the 800 MHz band to provide 832 analog channels. Two service providers are each assigned one half of the channels in each service area. Analog cellular systems that are similar to AMPs but not compatible include Total Access Communications System (TACS) in the United Kingdom, China and other countries, and Nordic Mobile Telephone (NMT) in the Scandinavian countries. |
| **Analog** | An electrical circuit that is represented by means of continuous, variable physical quantities (such as voltages and frequencies), as opposed to discrete representations (like the 0/1, off/on representation of digital circuits). |
| **ARP** | Address Resolution Protocol is a protocol for mapping an Internet Protocol address (IP address) to a physical computer address that is recognized in the local network. |
| **Authentication** | The service used to establish the identity of one station as a member of the set of stations authorized to associate with another station. |
| **Authenticity** | Proof that the information came from the person or location that reportedly sent it. One example of authenticating software is through digital signatures. |

| | |
|---|---|
| **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 one or a zero. The smallest unit of computerized data. |
| **Boot Module Commands** | Boot Module Commands, available in the debug mode via SMT (some devices may not have SMTs), help you initialize the configuration of the basic functions and features of your device(s) such as uploading firmware, changing the console port speed and viewing product-related information. |
| **Bridge** | A device used to connect LANs by forwarding packets across connections at the Media Access Control (MAC) layer. |
| **Bridging** | Bridging provides LAN to LAN frame forwarding services between two or more LANs. Frames from one LAN are forwarded across a bridge to a connected LAN, although filtering can be employed to selectively forward frames. Bridging works similar to the way repeaters work except that bridges forward frames based on their MAC (Medium Access Control) addresses which are hardware-level addresses of NICs (Network Interface Cards). |
| **Broadband** | Refers to telecommunication that provides multiple channels of data over a single communications medium. |
| **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. |
| **CO** | Central Office. A CO is a facility that serves local telephone subscribers. In the CO, subscribers' lines are joined to switching equipment that allows them to connect to each other for both local and long distance calls. |
| **COE** | Central Office Equipment. COE is where home and office phone lines terminate and connect to a much larger switching system. |
| **Command Line Interface** | A command line interface is a computer environment in which you enter predefined commands on the command line to modify, configure and display information about a device or devices. A command line is the line on the display screen where a command is expected. Generally, the command line is the line that contains the most recently displayed command prompt. An interface is a set of commands (for example, a ZyXEL Command Line Interface) or menus (for example, a ZyXEL web configurator) used to communicate with a program. A command-driven interface is an interface in |

| | |
|---|---|
| | which you enter commands. |
| **CPE** | Customer Premise Equipment. CPE is privately-owned telecommunication equipment at an organization’s site that is attached to the telecommunication network. CPE includes routers, modems, PBXs, telephones, key systems, facsimile products, voice processing equipment and video communication equipment. |
| **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. |
| **Device Filters** | Device Filters decide whether or not to allow passage of a data packet and/or to make a call. Device filters act on raw data from/to LAN and WAN and serve as a limited firewall to your device. |
| **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. |
| **Digital** | The use of a binary code to represent information, such as 0/1, or on/off. |
| **Digital AMPS (D-AMPS)** | First digital cellular service in the U.S. Provides 416 1.25 MHz channel pairs. Supports three subscribers per channel with TDMA and a variable number of subscribers per channel with CDMA. |
| **Direct Sequence Spread Spectrum (DSSS)** | A type of spread spectrum radio transmission that spreads its signal continuously over a wide frequency band. |
| **Directional Antennae** | An antenna that concentrates transmission power into a direction thereby increasing coverage distance at the expense of coverage angle. Directional antenna types include yagi, patch and parabolic dish. |
| **DNS** | Domain Name System links names to IP addresses. When you access Web sites on |

| | |
|---|---|
| | the Internet you can type the IP address of the site or the DNS name. When you type a domain name in a Web browser a query is sent to the primary DNS server defined in your Web browser's configuration dialog box. The DNS server converts the name you specified to an IP address and returns this address to your system. Thereafter, the IP address is used in all subsequent communications. |
| **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 (Random Access Memory) stores information in capacitors that must be refreshed periodically. |
| **DSL** | Digital Subscriber Line technologies enhance 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. |
| **Embedded Web Configurator** | This is an HTML-based configurator that usually includes an Internet Access Wizard and menus for configuring key settings and features. |
| **EMI** | ElectroMagnetic Interference. The interference by electromagnetic signals that can cause reduced data integrity and increased error rates on transmission channels. |
| **ESSID** | (Extended Service Set IDentification) The ESSID identifies the Service Set the station is to connect to. Wireless clients associating to the Access Point must have the same ESSID. |
| **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. |
| **General Packet Radio Service (GPRS)** | A packet-based data transmission technology that will initially provide data transfer rates of up to 115 Kbps. GPRS will work with CDMA and TDMA and it supports both the IP and X.25 communication protocols. |
| **Gigahertz (GHz)** | One billion cycles per second. A unit of measure for frequency. |
| **Global System for Mobile Communication** | GSM operates in the 900, 1,800 and 1,900 MHz frequency bands. GSM 1,800 is widely used in Europe and throughout many parts of the world. In the U.S., GSM 1,900 is the same as COMPUTERS 1,900; thus, these two technologies are compatible. |
| **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. |
| **Hertz (Hz)** | Cycles per second. A unit of measure for frequency. |
| **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 clearing house to assign and coordinate the use of numerous Internet protocol parameters such as Internet addresses, domain names, protocol numbers, and more.  Use a search engine to find the current IANA web site. |
| **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. |
| **ICOMPUTERP (PPP)** | IP Control Protocol allows changes to IP parameters such as the IP address. |
| **IMTS** | (Improved Mobile Telephone Service) First analog wireless telephone service in the U.S. Limited to six calls at one time in each service area. |
| **Institute of Electrical and Electronic Engineers (IEEE)** | A professional society serving electrical engineers through its publications, conferences and standards development activities. The body responsible for the Ethernet 802.3 and wireless LAN 802.11 specifications. |
| **Internet** | (Upper case “I”).  The vast collection of inter-connected networks that use TCP/IP protocols evolved from the ARPANET (Advanced Research Projects Agency Network) of the late 1960’s and early 1970’s. |
| **internet** | (Lower case “i”).  Any time you connect two or more networks together, you have an internet. |
| **Internet Worm** | See Worm. |
| **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. |
| **Intruder** | Person or software interested in breaking computer security to access, modify, or damage data. Also see Cracker. |
| **IP** | Internet Protocol.  (Currently IP version 4 or IPv4).  The underlying protocol for routing packets on the Internet and other TCP/IP-based networks. |
| **IP Alias** | Internet Protocol Alias allows you to partition a physical network into different logical networks over the same Ethernet interface. |
| **IP Pool** | Internet Protocol Pool refers to the collective group of IP addresses located in any particular place (for example, LAN, WAN, Ethernet, etc.). |
| **IPX** | Internetwork Packet eXchange The native NetWare internetworking protocol is IPX (Internetwork Packet Exchange). Like IP (Internet Protocol), IPX is an internetworking protocol that provides datagram services. |
| **IRC** | Internet Relay Chat. IRC was developed in the late 1980s as a way for multiple users on a system to “chat” over the network. Today IRC is a very popular way to “talk” in real time with other people on the Internet. However, IRC is also one avenue hackers use to get information from you about your system and your company. Moreover, IRC sessions are prone to numerous attacks that while not dangerous can cause your system to crash. |
| **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. |
| **Jack Type** | Different types of jacks (RJ-11, RJ45 or RJ-48) can be used for an ISDN line. The RJ-11 is the most common in the world and is most often used for analog phones, modems and fax machines. RJ-48 and RJ-45 are essentially the same, as they both have the same 8-pin configuration. An RJ-11 jack can fit into an RJ-45/RJ-48 connector, however, an RJ-45/RJ-48 cannot fit into an RJ-11 connector. |
| **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. |
| **LEC** | Local Exchange Carrier. The local phone companies – either a Regional Bell Operating Company (RBOC) or an independent phone company (e.g., GTE) – that provide local transmission services. |
| **LED** | Light Emitting Diode. LEDs are visual indicators that relay information about the status of specific MI1951 functions to the user by lighting up, turning off or blinking. LEDs are usually found on the front panel of the physical device. Examples include Status, Power and System LEDS. |
| **MAC** | On a local area network (LAN) or other network, the MAC (Media Access Control) address is a 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. |
| **Megahertz (MHz)** | One million cycles per second. A unit of measure for frequency. |
| **Modulation** | Any of several techniques for combining user information with a transmitter's carrier signal. |
| **Multicast** | A medium access control (MAC) address that has the group bit set. A multicast MAC service data unit (MSDU) is one with a multicast destination address. A multicast MAC protocol data unit (MPDU) or control frame is one with a multicast receiver address. |
| **Multiplexor** | Multiplexors or MUXs, as they are often called, are devices that combine signals from various sources such as PBX (Private Branch Exchange), asynchronous terminals or a bridge connected to a WAN. A multiplexor transmits these signals as a single data stream over a digital line. Multiplexors, among other tasks, conserve bandwidth. |
| **Name Resolution** | The allocation of an IP address to a host name. See also 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 on 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 computer to connect to and communicate with a LAN. |
| **Network** | Any time you connect two or more computers together, allowing them to share resources, you have a computer network. Connect two 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. |
| **PAC** | The PPTP Access Concentrator (PAC) is the box that calls/answers the phone call and relays the PPP frames to the PNS (PPTP Network Server). A PAC must have IP and dial-up capability. |
| **Packet** | A basic message unit for communication across a network. A packet usually includes routing information, data and (sometimes) error detection information. |
| **Packet Filter** | A filter that scans packets and decides whether to let them through or not. |
| **PAP** | Password Authentication Protocol 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. |
| **PBX** | A Private Branch Exchange is a subscriber-owned telecommunications exchange that usually includes access to the public switched network. It may also be a private telephone switchboard that provides on-premises dial service and may provide connections to local and trunked communications networks. |
| **Penetration** | Gaining access to computers or networks by bypassing security programs and passwords. |
| **Personal Communication Systems** | COMPUTERS networks in the U.S. provide narrowband digital communications in the 900 MHz band for paging and broadband digital communications in the 1,900 MHz band for cellular telephone service. In the U.S., COMPUTERS 1,900 is the same as Global System for Mobile Communications (GSM) 1,900. |
| **Personal Digital Communication** | PDC is used only in Japan and is rapidly being replaced with CDMA to alleviate overcrowding of PDC bandwidth. |
| **Ping Attack** | An attack that slows down the network until it is unusable. The attacker sends a "ping" command to the network repeatedly to slow it down. See also Denial of Service. |
| **Point of** | The physical point where the phone company ends its responsibility with the wiring of |

| | |
|---|---|
| **Demarcation** | the phone line. |
| **POP** | Post Office Protocol. This is a common protocol used for sending, receiving, and delivering mail messages. |
| **Port** | An Internet port refers to a number that is part of a URL, appearing after a colon (:), directly following 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. |
| **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. |
| **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. |
| **PPPoE** | PPPoE (Point-to-Point Protocol over Ethernet) relies on two widely accepted standards: PPP and Ethernet. PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as a single DSL line, wireless device or cable modem. All the users over the Ethernet share a common connection, so the Ethernet principles supporting multiple users in a LAN combine with the principles of PPP, which apply to serial connections. From authentication, accounting and secure access to configuration management, PPPoE supports a broad range of existing applications and services. |
| **PPTP** | Point-to-Point Tunneling Protocol. |
| **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. |
| **Protocol Filters** | Use Protocol Filters to decide whether or not to allow passage of a data packet and/or to make a call. Protocol filters act on IP/IPX packets and can serve as a limited |

| | |
|---|---|
| | firewall. |
| **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. |
| **Radio Frequency (RF)** | A generic term for radio-based technology. |
| **Range** | A linear measure of the distance that a transmitter can send a signal. |
| **ras** | This is the name of the firmware on the ZyXEL device.  Renaming may be necessary when uploading new firmware to the device. |
| **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 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. |
| **Rom-0** | This is the name of the configuration file on your ZyXEL device.  Renaming may be necessary when uploading a new configuration file to your ZyXEL device. |

| | |
|---|---|
| **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. |
| **Server** | A computer, or a software package, that provides a specific kind of service to client software running on other computers. |
| **Server** | A computer, or a software package, that provides a specific kind of service to client software running on other computers. |
| **Service Set IDentifier (SSID)** | The SSID indicates the identity of an ESS or IBSS. |
| **SMT** | System Management Terminal. The SMT is a menu-based interface that you use to configure your device. |
| **SNMP** | Simple 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. |
| **Splitter** | In telephony, a splitter, sometimes called a “plain old telephone service splitter" is a device that divides a telephone signal into two or more signals, each carrying a selected frequency range, and can also reassemble signals from multiple signal sources into a single signal |
| **Spoofing** | To forge something, such as an IP address. IP spoofing is a common way for hackers to hide their location and identity |
| **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. |
| **Static Routing** | Static routes tell routing information that a networking device cannot learn automatically through other means. The need for static routing can arise in cases where RIP is disabled on the LAN or a remote network is beyond the one that is directly connected to a remote node. |
| **Station (STA)** | Any device that contains an IEEE 802.11 conformant medium access control (MAC) and physical layer (PHY) interface to the wireless medium (WM). |
| **STP** | Shielded Twisted-Pair cable consists of copper-core wires surrounded by an insulator. Two wires are twisted together to form a pair; the pair form a balanced circuit.  The twisting prevents interference problems, STP 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 commonly used Ethernet cable. |
| **SUA** | Single User Account. Your system's SUA feature allows multiple user Internet access for the cost of a single ISP account. See also NAT. |
| **Subnet Mask** | The subnet mask specifies the network number portion of an IP address. Your device will compute the subnet mask automatically based on the IP Address that you entered. You do not need to change the sutomatically computer subnet mask unless you are instructed to do so. |
| **Syslog** | An abbreviated form of System Log. Using the UNIX syslog facility, a device records (logs) phone calls or creates a CDR (Call Detail Record). Syslog is an administrative tool that assists in accounting and is configurable via the SMT. |
| **TCP** | Transmission Control Protocol is a connection-oriented transport service that ensures the reliability of message delivery. It verifies that messages and data were received. |
| **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, display screen and some simple circuitry. |
| **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 Emulation 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). |
| **Twisted Pair** | Two insulated wires, usually copper, twisted together and often bound into a common sheath to form multi-pair cables. In ISDN, the cables are the basic path between a subscriber's terminal or telephone and the PBX or the central office. |
| **UDP** | User Datagram Protocol. DP is a connectionless transport service that dispenses with the reliability services provided by TCP. UDP gives applications a direct interface with the Internet Protocol (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. Usually used on workstations and |

| | |
|---|---|
| | servers. |
| **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. A URL is basically a pointer to the location of an object. |
| **VC-based Multiplexing** | By prior mutual agreement, each protocol is assigned to a specific virtual circuit, eg., VCI carries IP, VC2 carries IPX, etc. VC-based multiplexing may be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical. |
| **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. |
| **Wired Equivalent Privacy (WEP)** | The optional cryptographic confidentiality algorithm specified by IEEE 802.11 used to provide data confidentiality that is subjectively equivalent to the confidentiality of a wired local area network (LAN) medium that does not employ cryptographic techniques to enhance privacy. |
| **Wireless Local Area Network (WLAN)** | A flexible data communications system implemented as an extension to, or as an alternative for a wired LAN. Using radio frequency (RF) technology, wireless LANs transmit and receive data over the air, minimizing the need for wired connections. |
| **Wireless Medium (WM)** | The medium used to implement the transfer of protocol data units (PDUs) between peer physical layer (PHY) entities of a wireless local area network (LAN). |
| **WWW** | World Wide Web. Frequently used (incorrectly) when referring to "The Internet". WWW has two major definitions. One, the whole constellation of resources that can be accessed using Gopher, FTP, HTTP, telnet, USENET, WAIS and other tools. Two, the universe of hypertext servers (HTTP servers). |
| **ZyNOS** | ZyXEL Network Operating System is the firmware used in many ZyXEL products. |

# Index