Prestige 645R

ADSL Router

User's Guide

Version 2.50

September 2002

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 patents' 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. ZyNOS is a registered trademark of ZyXEL Communications Corporation.

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.

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.

Note

Certifications

For more information about certifications please refer to www.zyxel.com.

Customer Support

When contacting your Customer Support Representative, please have the following information ready:

- Product model and serial number.
- Loopback Test information.
- Warranty Information.
- Date you received your Product.
- Brief description of the problem and the steps you took to solve it.

METHOD LOCATION	E-MAIL SUPPORT/ SALES	TELEPHONE/FAX	WEB SITE/ FTP SITE	REGULAR MAIL
WORLDWIDE	support@zyxel.com.tw support@europe.zyxel.com sales@zyxel.com.tw	+886-3-578-3942 +886-3-578-2439	www.zyxel.com www.europe.zyxel.com ftp.europe.zyxel.com	ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, HsinChu, Taiwan 300, R.O.C.
NORTH AMERICA	support@zyxel.com sales@zyxel.com	+1-714-632-0882 800-255-4101 +1-714-632-0858	www.zyxel.com ftp.zyxel.com	ZyXEL Communications Inc., 1650 Miraloma Avenue, Placentia, CA 92870, U.S.A.
SCANDINAVIA	support@zyxel.dk sales@zyxel.dk	+45-3955-0700 +45-3955-0707	www.zyxel.dk ftp.zyxel.dk	ZyXEL Communications A/S, Columbusvej 5, 2860 Soeborg, Denmark.
GERMANY	support@zyxel.de sales@zyxel.de	+49-2405-6909-0 +49-2405-6909-99	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A4 D-52146 Wuerselen, Germany

Table of Contents

List of Figures

List Of Tables

Preface

About Your ADSL Internet Access Router

Congratulations on your purchase of the Prestige 645R ADSL Internet Access Router.

The Prestige 645R is an ADSL router used for Internet/LAN access via an ADSL line. We will refer to the Prestige 645R router as the P645R or simply the Prestige from now on.

The P645R can run upstream maximum transmission rates of 800 Kbps and downstream maximum transmission rates of 8Mbps. The actual rate depends on the type of ADSL service subscribed to, the copper category of your telephone wire and the distance from the central office. See the following sections for more background information on DSL and ADSL.

The P645R's 10/100M LAN interface enables fast data transfer of 10Mbps or 100Mbps in either half-duplex or full-duplex mode depending on your Ethernet network.

Your Prestige is easy to install and to configure. All functions of the Prestige are software configurable via the SMT (System Management Terminal) interface.

About This User's Guide

This user's guide covers all aspects of the Prestige 645R's operations and shows you how to get the best out of the multiple advanced features of your ADSL Internet Access Router using the SMT. It is designed to guide you through the correct configuration of your Prestige 645R for various applications.

Related Documentation

➢ Supporting Disk

More detailed information and examples can be found in our included disk (as well as on the zyxel.com web site). This disk contains information on configuring your Prestige for Internet Access, general and advanced FAQs, Application Notes, Troubleshooting, a reference for CI Commands and bundled software.

➢ Read Me First

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

➢ ZyXEL Glossary and Web Site

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

Syntax Conventions

- "Type" means for you to type one or more characters and press the carriage return. "Select" or "Choose" means for you to select one from the predefined choices.
- The SMT menu titles and labels are in **Bold Times New Roman** font. Predefined field choices are in **Bold Arial** font. Command and arrow keys are enclosed in square brackets. [ENTER] means the Enter, or carriage return key; [ESC] means the Escape key and [SPACE BAR] means the Space Bar.
- For brevity's sake, we will use "e.g." as a shorthand for "for instance", and "i.e." as a shorthand for "that is" or "in other words" throughout this manual

What Is ADSL?

About ADSL

Asymmetric Digital Subscriber Line (ADSL) technology provides high-speed data access across regular phone lines (copper wires) by making use of previously unused frequency bandwidth above the voice band. By placing the ADSL signal above the frequency of voice signals, ADSL service is able to coexist on the same line with your telephone service. ADSL is asymmetric in the sense that it provides a higher downstream data rate transfer (up to 8Mbps), than in the upstream transfer (up to 832 Kbps). Asymmetric operation is ideal for typical home and small office use where files and information are downloaded more frequently than uploaded.

Advantages of ADSL

1. ADSL provides a private (unlike cable telephone and modem services where the line is shared), dedicated and secure channel of communications between you and your service provider.
2. Because your line is dedicated (not shared), transmission speeds are not affected by other users. With cable modems, transmission speeds drop significantly as more users go on-line because the line is shared.
3. ADSL is "always on" (connected). This means that there is no time wasted dialing up the service several times a day and waiting to be connected; ADSL is on standby, ready for use whenever you need it.

Part I:

Getting Started

This part covers Getting to Know Your Prestige, Hardware Indtallation and Setup and Internet Access.

Chapter 1
Getting to Know Your Prestige

This chapter describes the key features and applications of your ADSL Internet Access Router.

1.1 Prestige 645R ADSL Internet Access Router

Your Prestige integrates a high-speed 10/100Mbps auto-negotiating LAN interface and a high-speed ADSL port into a single package. The Prestige is ideal for high-speed Internet browsing and making LAN-to-LAN connections to remote networks.

1.2 Features of the Prestige 645R

Your Prestige is packed with a number of features that give it the flexibility to provide a complete networking solution for almost any user.

Ease of Installation

Your Prestige is designed for quick, intuitive and easy installation. Physically, its compact size and lightness make it easy to position anywhere in your busy office.

High Speed Internet Access

The P645R ADSL router can support downstream transmission rates of up to 8Mbps and upstream transmission rates of 800 Kbps.

10/100Mbps Fast Ethernet LAN Interface

The P645R's 10/100M LAN interface enables fast data transfers of 10Mbps or 100Mbps in either half-duplex or full-duplex mode depending on your Ethernet network. Auto-sensing enables you to use either a crossover Ethernet cable or a straight-through Ethernet cable to connect your device to either a computer or external hub. In other words these ports automatically adjust according to the type of cable so that either straight-through Ethernet cable or crossover Ethernet cable may be used.

Protocols Supported

- TCP/IP (Transmission Control Protocol/Internet Protocol) network layer protocol.
- PPP (Point-to-Point Protocol) link layer protocol.
- Novel IPX (Internetwork Packet eXchange) network layer protocol.
- Transparent bridging for unsupported network layer protocols.
- DHCP Client, Server and Relay
- RIP I and RIP II

IP Policy Routing

IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator.

Call Scheduling

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

Networking Compatibility

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

Multiplexing

The Prestige 645R supports VC-based and LLC-based multiplexing.

Encapsulation

The Prestige 645R supports PPP (RFC 2364 - PPP over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM and MAC encapsulated routing (ENET ENCAP) as well as PPP over Ethernet (RFC 2516).

NAT/SUA for single-IP-address Internet Access

The Prestige's SUA (Single User Account) feature allows multiple user Internet access for the cost of a single IP account. SUA supports popular Internet applications, such as MS traceroute, CuSeeMe, IRC, RealAudio, VDOLive, Quake, and PPTP. No configuration is needed to support these applications.

Full Network Management

- SNMP (Simple Network Management Protocol) support.
- SMT (System Management Terminal) through a telnet connection.

PAP and CHAP Security

The Prestige supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure since the password is scrambled prior to transmission. However, PAP is readily available on more platforms.

Filters

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

Reset Button

The Prestige comes with a reset button built into the rear panel. Use this button to restore the factory default password to 1234, IP address to 192.168.1.1, subnet mask to 255.255.255.0 and DHCP server enabled with a pool of 32 IP addressed starting at 192.168.1.33.

1.3 Applications for the Prestige 645R

1.3.1 Internet Access

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

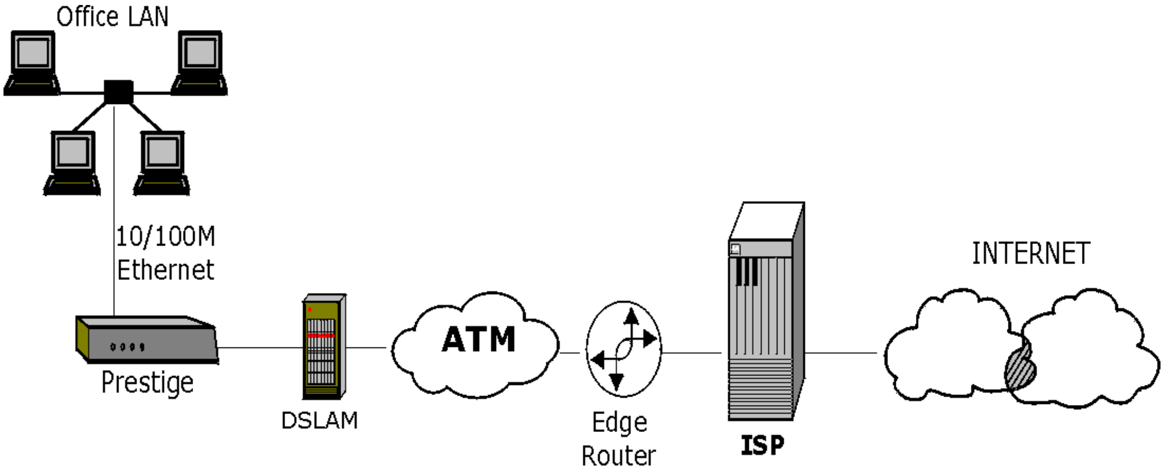


Figure 1-1 Internet Access Application

Internet Single User Account

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

1.3.2 LAN to LAN Application

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

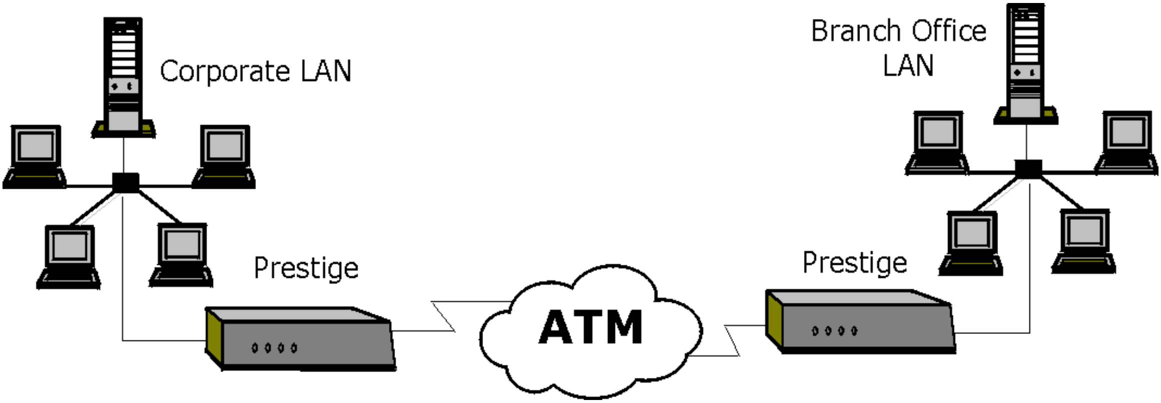


Figure 1-2 LAN-to-LAN Application

Chapter 2
Hardware Installation & Initial Setup

This chapter describes the physical features and cable connections of the Prestige and how to access and use the SMT interface for configuration.

2.1 Front Panel LEDs of the P645R

The LED indicators on the front panel indicate the operational status of the Prestige 645R. The table below the diagram describes the LED functions:

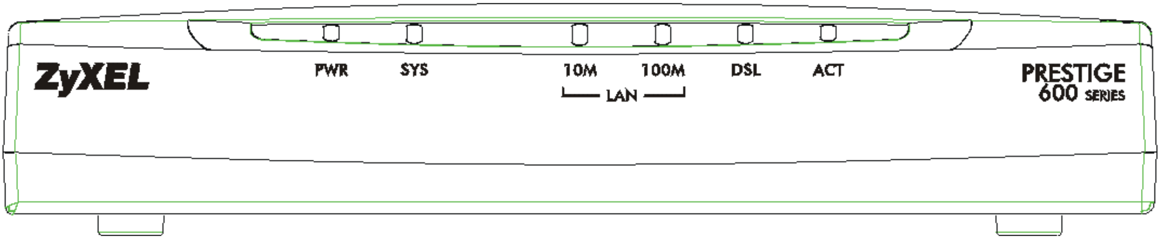


Figure 2-1 Prestige 645R Front Panel

Table 2-1 Front Panel LED Description

LED NAME	DESCRIPTION
PWR	The PWR (power) LED is on when power is applied to the Prestige.
SYS	A steady on SYS (system) LED indicates the Prestige is on and functioning properly while an off SYS LED indicates the system is not ready or has a malfunction. The SYS LED blinks when the system is rebooting.
LAN 10M	A steady light indicates a 10Mb Ethernet connection. The LED blinks when data is being sent/received.
LAN 100M	A steady light indicates a 100Mb Ethernet connection. The LED blinks when data is being sent/received.
DSL	The ADSL LED is on when the Prestige is connected successfully to a DSLAM. The LED blinks during ADSL line initialization. The LED is off when the link is down.
ACT	The ACT LED blinks during data transfer via the ADSL line. The LED is off when no data is being transferred on the ADSL line.

2.2 Prestige 645R Rear Panel and Connections

The following figure shows the rear panel connectors of your Prestige.

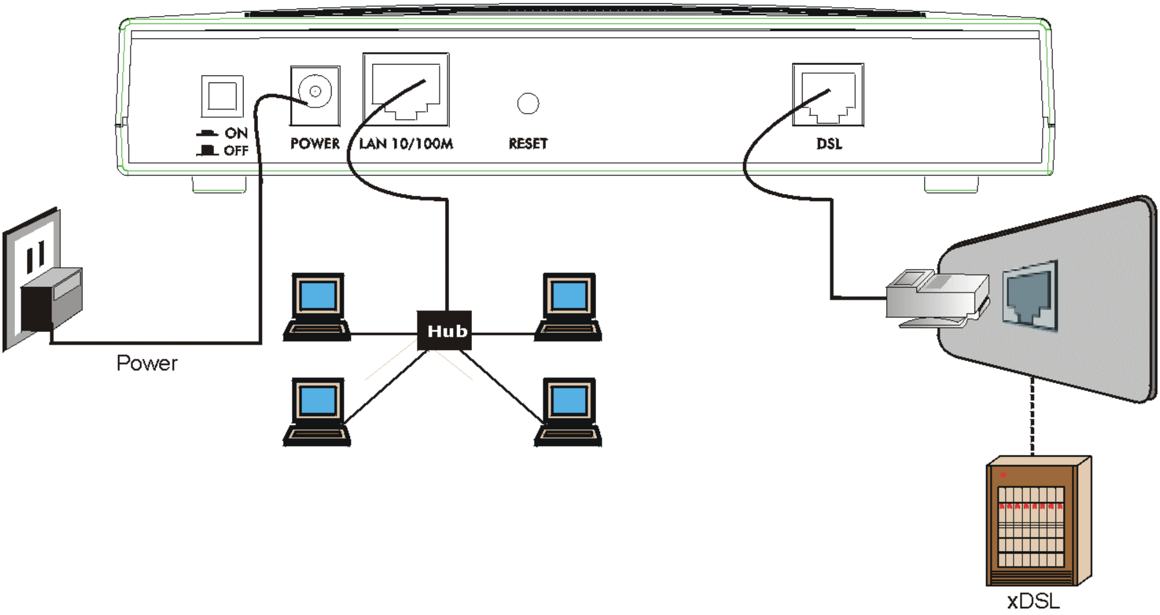


Figure 2-2 Prestige 645R Rear Panel Connections

2.2.1 Using the Reset Button

The reset button restores the default IP address of 192.168.1.1 and subnet mask of 255.255.255.0, as well as the default SMT password of **1234**. The DHCP server will also be reset to server mode with a pool of 32 IP addressed starting at 192.168.1.33.

In order to prevent accidental use of the reset button, it only works as follows. To use the reset button, turn off the Prestige and insert a small pointed object (like a pen) into the reset hole to push the reset button. Next, turn on your Prestige and keep the reset button pressed for one minute.

2.2.2 Making the Connections

Step 1. Connecting the ADSL line

Connect the RJ-11 DSL port on the Prestige to the POTS splitter using the included ADSL cable (telephone wire). Connect the micro filter(s) (optional– see

Figure 2-4 Connecting the Microfilter) between the wall jack and your telephone(s). The micro filters act as low pass filters (voice transmission takes place in the 0 to 4KHz bandwidth).

Step 2. Connecting a computer to the Prestige 10/100M LAN port

Be careful not to plug a RJ-11 connector into the RJ-45 port.

Ethernet 10Base-T/100Base-T networks use Shielded Twisted Pair (STP) cable with RJ-45 connectors that look like a bigger telephone plug with 8 pins. The auto-sensing Ethernet LAN port enables you to use either a crossover Ethernet cable or a straight-through Ethernet cable to connect your device to either a computer or external hub. In other words these ports automatically adjust according to the type of cable so that either straight-through Ethernet cable or crossover Ethernet cable may be used.

Step 3. Connecting the power adapter to your Prestige

Make sure that you use a P/N DV-121AACS (rated 12VAC 1.0A) or equivalent power supply.

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

2.3 Additional Installation Requirements

In addition to the contents of your package your computer must have a properly installed and enabled Ethernet 10Base-T/100Base-T NIC.

2.4 Connecting the POTS Splitter

You may purchase an optional POTS splitter for use with the Full Rate (G.dmt and ANSI T1.413) standards. One major difference between ADSL and dial-up modems is the need for a telephone splitter. This device keeps the telephone and ADSL signals separated, giving the capability to provide simultaneous Internet access and telephone service on the same line. Splitters also eliminate the destructive interference conditions caused by telephone sets. The telephone splitter has to be installed on the line at the point of entry to the residence.

Noise generated from a telephone in the same frequency range as the ADSL signal can be disruptive to the ADSL signal. In addition the impedance of a telephone when off-hook may be so low that it essentially shunts the strength of the ADSL signal. When a POTS splitter is installed at the entry point where the line comes into the home, it will filter the telephone signals before combining the ADSL and telephone signals transmitted and received. The issues of noise and impedance are eliminated with a single POTS splitter installation.

A telephone splitter can be installed as shown in the following figure.

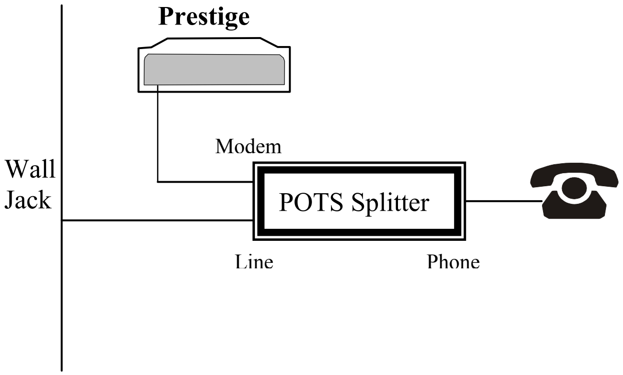


Figure 2-3 Connecting a POTS Splitter

Step 1. Connect the side labeled “Phone” to your telephone.

Step 2. Connect the side labeled “Modem” to your Prestige.

Step 3. Connect the side labeled “Line” to the telephone wall jack.

2.5 Telephone Microfilters

You may also opt to purchase telephone microfilters. Telephone voice transmissions take place in the lower frequency range, 0 - 4KHz, while ADSL transmissions take place in the higher bandwidth range, above 4KHz. ZyXEL provides a microfilter that acts as a low-pass filter for your telephone to ensure that ADSL transmissions do not interfere with your telephone voice transmissions.

Step 1. Connect a phone cable from the wall jack to the single jack end of the Y- Connector.

Step 2. Connect a cable from the double jack end of the Y-Connector to the “wall side” of the microfilter.

Step 3. Connect another cable from the double jack end of the Y-Connector to the Prestige.

Step 4. Connect the “phone side” of the microfilter to your telephone as shown in the following figure.

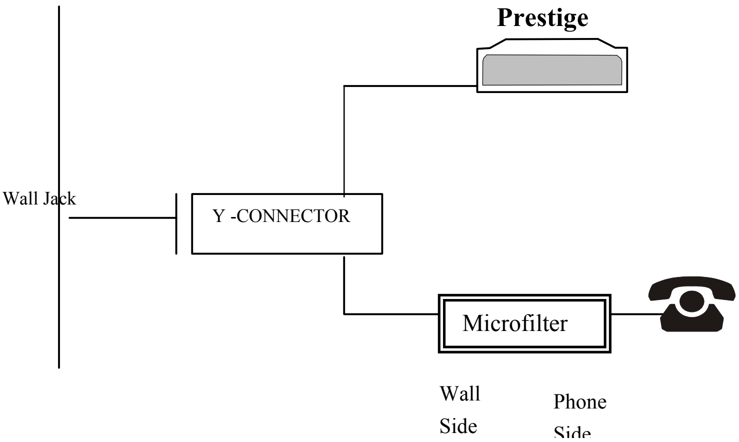


Figure 2-4 Connecting the Microfilter

2.6 Turning On Your Prestige

At this point, you should have connected the ADSL line, the Ethernet port and the power port to the appropriate devices or lines. You can now turn on the Prestige by pushing the power button on. Refer to the Read Me First for instructions on setting up your computer. The following procedure details how to telnet into your Prestige.

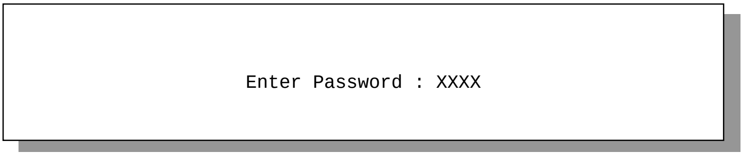
Step 1. In Windows, click **Start** (usually in the bottom left corner), **Run** and then type "telnet 192.168.1.1" (the default IP address) and click **OK**. The Prestige should already be on when you turn on your computer, see the Read Me First for details.

Step 2. Entering the password

The login screen appears prompting you to enter the password, as shown below.

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

Please note that if there is no activity for longer than 5 minutes after you log in, your Prestige will automatically log you out. You will have to telnet into the Prestige again.



```
Enter Password : XXXX
```

Figure 2-5 Login Screen

2.7 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 following table.

Table 2-2 Main Menu Commands

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

2.7.1 SMT Menu Overview

The following figure shows the titles and layout of the various SMT menu screens of your Prestige.

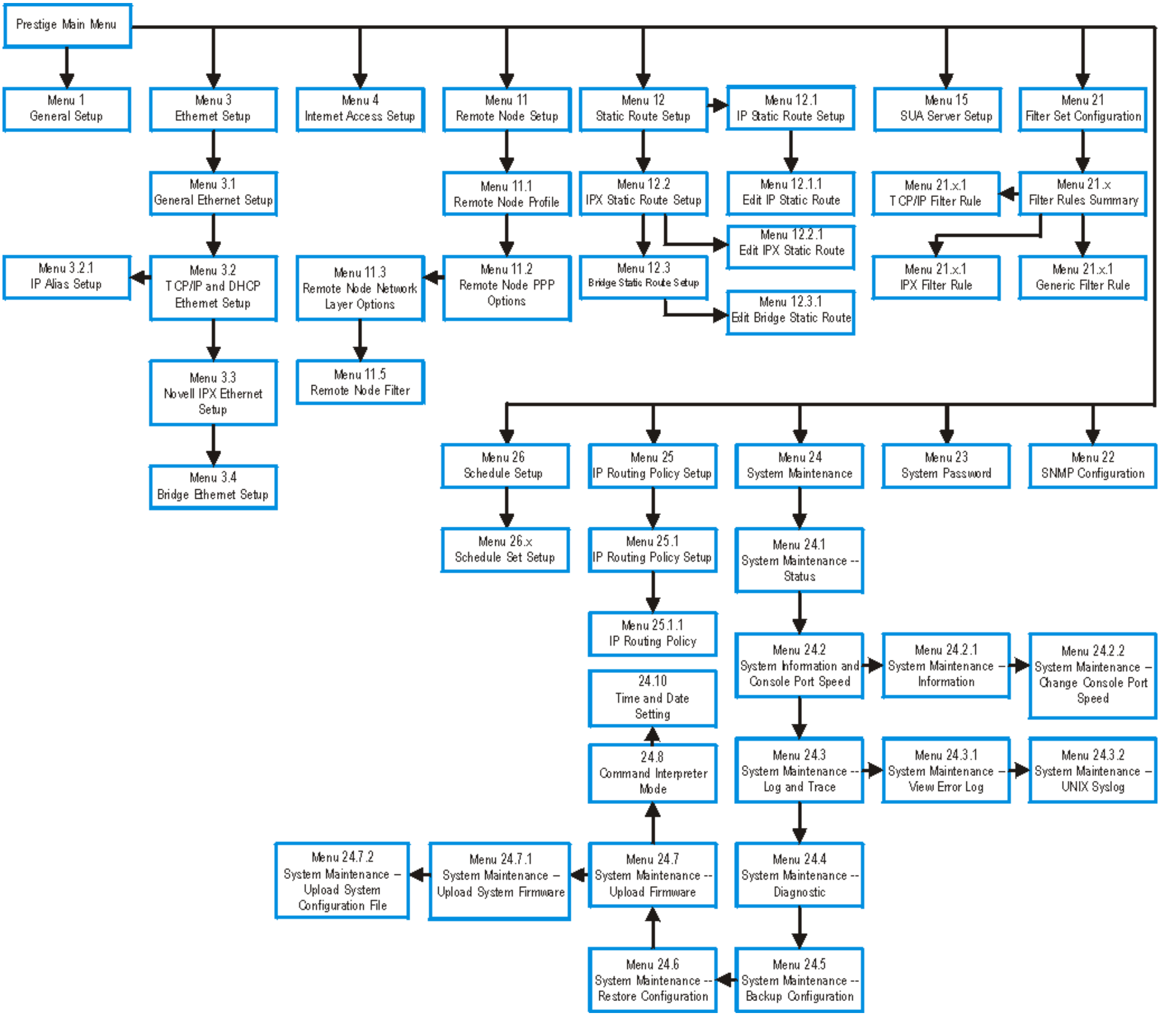
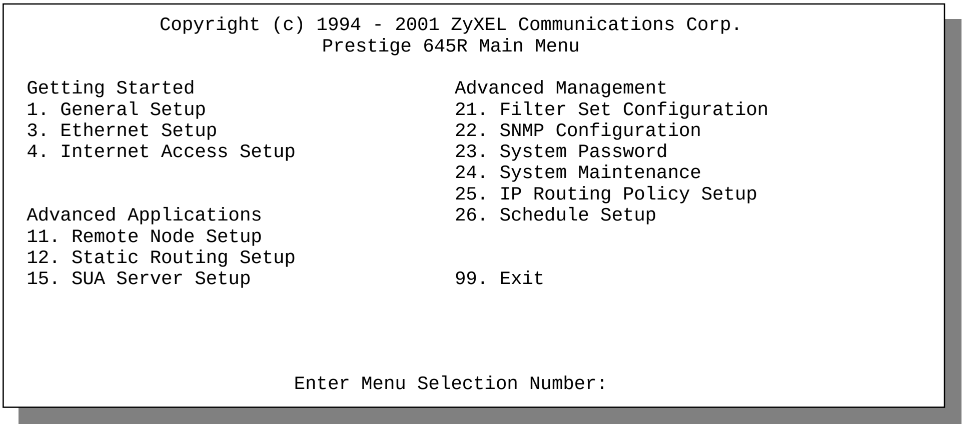


Figure 2-6 SMT Menu Overview

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



```
              Copyright (c) 1994 - 2001 ZyXEL Communications Corp.
                             Prestige 645R Main Menu

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




                         Enter Menu Selection Number:
```

Figure 2-7 SMT Main Menu

2.7.2 System Management Terminal Interface Summary

Table 2-3 Main Menu Summary

#	MENU TITLE	DESCRIPTION
1	General Setup	Use this menu to set up general information.
3	Ethernet Setup	Use this menu to set up your LAN connection.
4	Internet Access Setup	This menu provides convenient set up for an Internet connection.
11	Remote Node Setup	Use this menu to configure the Remote Node(s) for LAN-to-LAN connection(s), including the Internet.
12	Static Routing Setup	Use this menu to set up static routes.
15	SUA Server Setup	Use this menu to specify inside servers when SUA is enabled.
21	Filter Set Configuration	Use this menu to set up filters to provide security, etc.
22	SNMP Configuration	Use this menu to set up SNMP related parameters.
23	System Password	Use this menu to change your password.
24	System Maintenance	This menu provides diagnostic, file transfer, time setting and other tools for maintaining your Prestige.
25	IP Routing Policy Setup	Use this menu to configure routing policies.

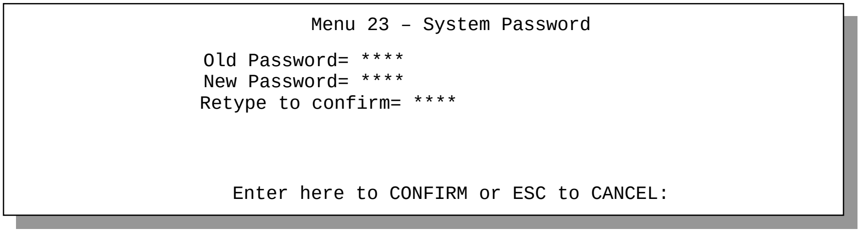
#	MENU TITLE	DESCRIPTION
26	Schedule Setup	Use this menu to configure times for calls to remote nodes.
99	Exit	Use this to exit the SMT and return to a blank screen.

2.8 Changing the System Password

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

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

When the **Menu 23 System Password** appears, type your system password (1234 is the default when shipped) and press [ENTER].



```
                           Menu 23 – System Password

                  Old Password= ****
                  New Password= ****
                 Retype to confirm= ****



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

Figure 2-8 Menu 23.1 - System Password

Step 2. Enter your new system password. You can use up to 30 alphanumeric characters. Do not use spaces, but dashes "-" and underscores "_" are accepted. Then press [ENTER].

Step 3. Re-type your new system password for confirmation and press [ENTER].

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

If you forget your password, use the reset button to restore the default password of 1234. This will allow you to enter the SMT. Then use the above instructions to set a new password.

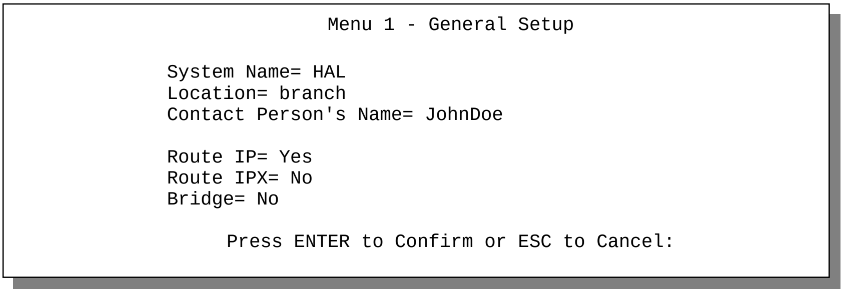
2.9 General Setup

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 below. Fill in the required fields marked [?] and turn on the individual protocols for your applications, as explained in the following table.



```
                              Menu 1 - General Setup

                 System Name= HAL
                 Location= branch
                 Contact Person's Name= JohnDoe

                 Route IP= Yes
                 Route IPX= No
                 Bridge= No

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

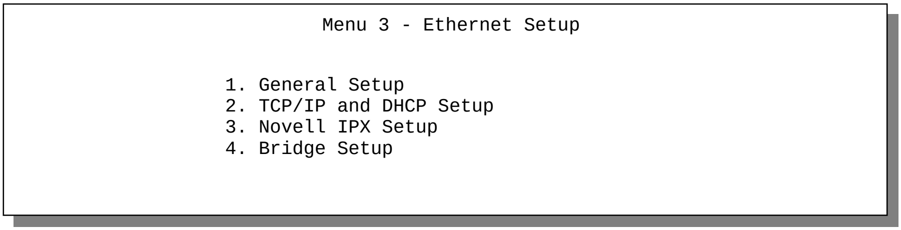
Figure 2-9 Menu 1 – General Setup

Table 2-4 General Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
System Name	Choose a descriptive name for identification purposes. This name can be up to 30 alphanumeric characters long. Spaces are not allowed, but dashes "-" and underscores "_" are accepted.	HAL
Location (optional)	Enter the geographic location (up to 31 characters) of your Prestige.	branch
Contact Person's Name (optional)	Enter the name (up to 30 characters) of the person in charge of this Prestige.	JohnDoe
Protocols:	Press the [SPACE-BAR] to select **Yes** or **No** to turn the individual routing protocols on or off.	
Route IP	Set this field to **Yes** to enable IP routing. You must enable IP routing for Internet access.	**Yes**
Route IPX	Set this field to **Yes** to enable IPX routing.	**No**
Bridge	Turn on/off bridging for protocols not supported (e.g., SNA) or not turned on in the previous Route fields.	**No**

2.10 Ethernet Setup

This section describes how to configure the Ethernet using **Menu 3 – Ethernet Setup**. From the main menu, enter 3 to open menu 3.

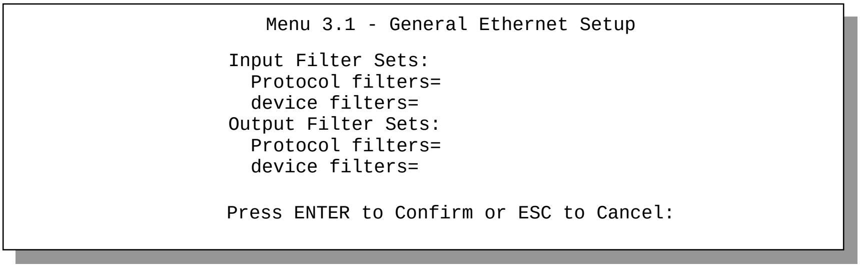


```
                          Menu 3 - Ethernet Setup


                 1. General Setup
                 2. TCP/IP and DHCP Setup
                 3. Novell IPX Setup
                 4. Bridge Setup
```

Figure 2-10 Menu 3 - Ethernet Setup

2.10.1 General Ethernet Setup

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



```
                     Menu 3.1 - General Ethernet Setup
                 Input Filter Sets:
                   Protocol filters=
                   device filters=
                 Output Filter Sets:
                   Protocol filters=
                   device filters=

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

Figure 2-11 Menu 3.1 - General Ethernet Setup

If you need to define filters, please read the chapter on configuring filters first, then return to this menu to define the filter sets.

The factory configured filters in SMT menu 21.3 are designed to block incoming telnet from the WAN (DSL) port. Do not configure SMT menu 3.1 filter rules to block all telnet from the Ethernet. This would block the telnet connection from your computer to the Prestige.

2.11 Protocol Dependent Ethernet Setup

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

- For TCP/IP Ethernet setup refer to the *Internet Access* chapter.
- For Novell IPX Ethernet setup refer to the *IPX Configuration* chapter.
- For bridging Ethernet setup refer to the *Bridging Setup* Chapter.

Chapter 3
Internet Access

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

3.1 Factory Ethernet Defaults

The Ethernet 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 to3.4 TCP/IP Ethernet Setup and DHCP 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.

3.2 TCP/IP Parameters

3.2.1 IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, the machines on a LAN also share one common network number.

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

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 (ignoring the trailing zero) and you must enable the Single User Account feature of the Prestige. The Internet Assigned Number Authority (IANA) has reserved this block of addresses specifically for private use; please do *not* use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first 3 numbers specify the network number while the last number identifies an individual computer on that network.

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

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

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

3.2.3 RIP Setup

RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The **RIP Direction** field controls the sending and receiving of RIP packets. When set to both, the Prestige will broadcast its routing table periodically and incorporate the RIP information that it receives; 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** send 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**.

3.2.4 IP Multicast

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

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

The P645R supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the P645R queries all directly connected networks to gather group membership. After that, the P645R periodically updates this information. IP Multicasting can be enabled/disabled on the P645R LAN and/or WAN interfaces using menus 3.2 (LAN) and 11.3 (WAN). Select **None** to disable IP Multicasting on these interfaces.

3.2.5 IP Alias

IP Alias allows you to partition a physical network into different logical networks over the same Ethernet interface. The P645R supports three logical LAN interfaces via its single physical Ethernet interface with the P645R itself as the gateway for each LAN network.

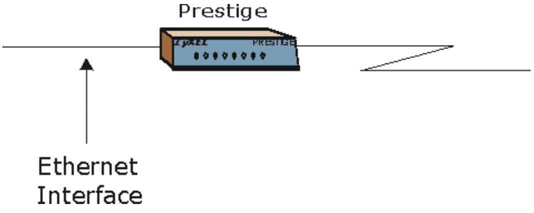


Figure 3-1 Physical Network

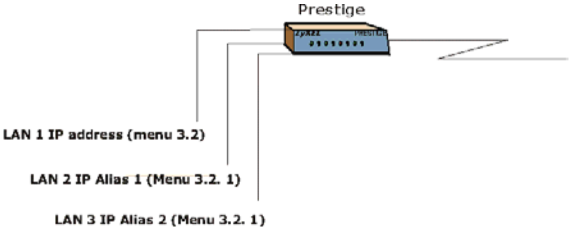

Prestige
LAN 1 IP address (menu 3.2)
LAN 2 IP Alias 1 (Menu 3.2. 1)
LAN 3 IP Alias 2 (Menu 3.2. 1)

Figure 3-2 Partitioned Logical Networks

3.2.6 DHCP Configuration

DHCP (Dynamic Host Configuration Protocol) allows the individual clients (computers) to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The Prestige has built-in DHCP server capability, enabled by default, which means it can assign IP addresses, an IP default gateway and DNS servers to Windows 98, Windows 2000 and other systems that support the DHCP client. The Prestige can also act as a surrogate DHCP server where it relays IP address assignment from the actual DHCP server to the clients.

IP Pool Setup

The Prestige is pre-configured with a pool of 32 IP addresses ranging from 192.168.1.33 to 192.168.1.64 for the client machines. This leaves 31 IP addresses, 192.168.1.2 to 192.168.1.32 (excluding the Prestige itself which has a default IP of 192.168.1.1) for other server machines, 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. The DNS server addresses that you enter in the DHCP setup are passed to the client machines along with the assigned IP address and subnet mask.

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

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

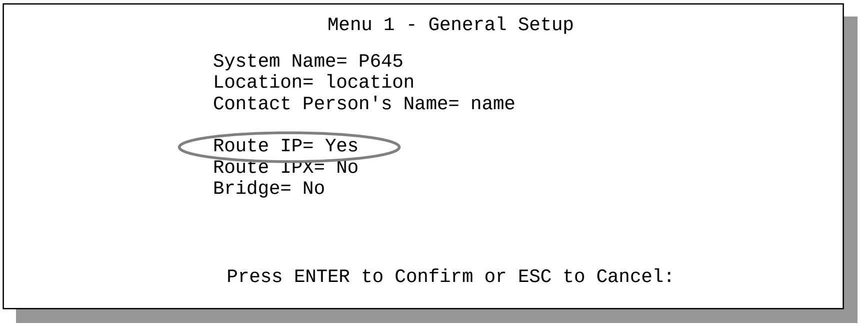
If the **Primary** and **Secondary DNS Server** fields in **DHCP Setup** are not specified, i.e., left as 0.0.0.0, the Prestige tells the DHCP clients that it itself is the DNS server. When a computer sends a DNS query to the Prestige, the Prestige forwards the query to the real DNS server learned through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

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

3.3 Route IP Setup

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

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



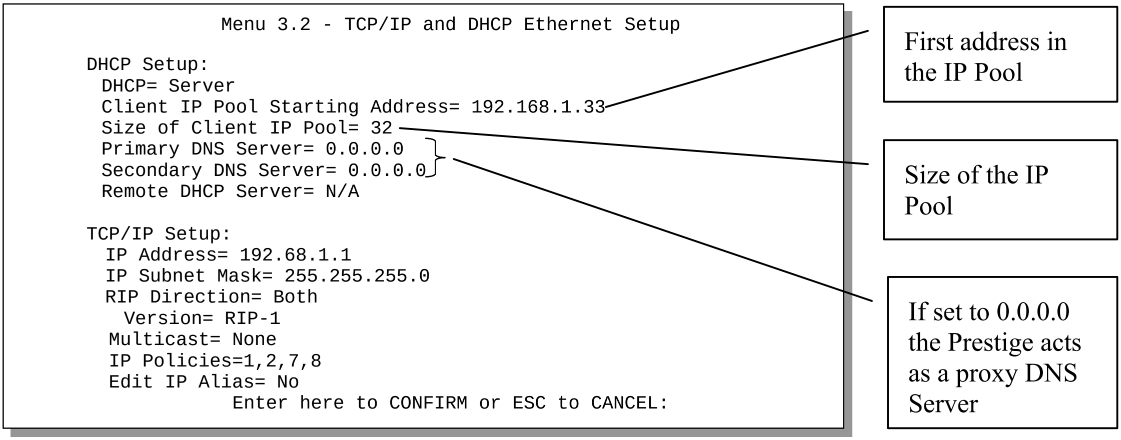
```
                        Menu 1 - General Setup

                System Name= P645
                Location= location
                Contact Person's Name= name

                Route IP= Yes
                Route IPX= No
                Bridge= No



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

Figure 3-3 Menu 1 – General Setup

3.4 TCP/IP Ethernet Setup and DHCP

You will now use menu 3.2 to configure your Prestige for TCP/IP.

To edit menu 3.2, enter 3 in the main menu to open **Menu 3 - Ethernet Setup**. In menu 3, select 2 and press [ENTER]. The screen now displays **Menu 3.2 - TCP/IP and DHCP Ethernet Setup**, as shown next



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

       DHCP Setup:
        DHCP= Server
        Client IP Pool Starting Address= 192.168.1.33
        Size of Client IP Pool= 32
        Primary DNS Server= 0.0.0.0
        Secondary DNS Server= 0.0.0.0
        Remote DHCP Server= N/A

       TCP/IP Setup:
         IP Address= 192.68.1.1
         IP Subnet Mask= 255.255.255.0
         RIP Direction= Both
           Version= RIP-1
         Multicast= None
         IP Policies=1,2,7,8
         Edit IP Alias= No
                   Enter here to CONFIRM or ESC to CANCEL:
```

First address in the IP Pool

Size of the IP Pool

If set to 0.0.0.0 the Prestige acts as a proxy DNS Server

Figure 3-4 Menu 3.2 – TCP/IP and DHCP Ethernet Setup

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

Table 3-1 DHCP Ethernet Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
DHCP Setup		
DHCP=	If it is set to **Server**, your Prestige can assign IP addresses, an IP default gateway and DNS servers to Windows 98, Windows 2000 and other systems that support the DHCP client. If set to **None**, the DHCP server will be disabled. If set to **Relay,** the Prestige acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the **Remote DHCP Server** in this case. When DHCP is used, the following items need to be set:	**Server** (default)
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.	192.168.1.33
Size of Client IP Pool	This field specifies the size, or count, of the IP address pool.	32
Primary DNS Server Secondary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.	
Remote DHCP Server	If **Relay** is selected in the **DHCP=** field above, then enter the IP address of the actual, remote DHCP server here.	

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

Table 3-2 TCP/IP Ethernet Setup Menu Fields

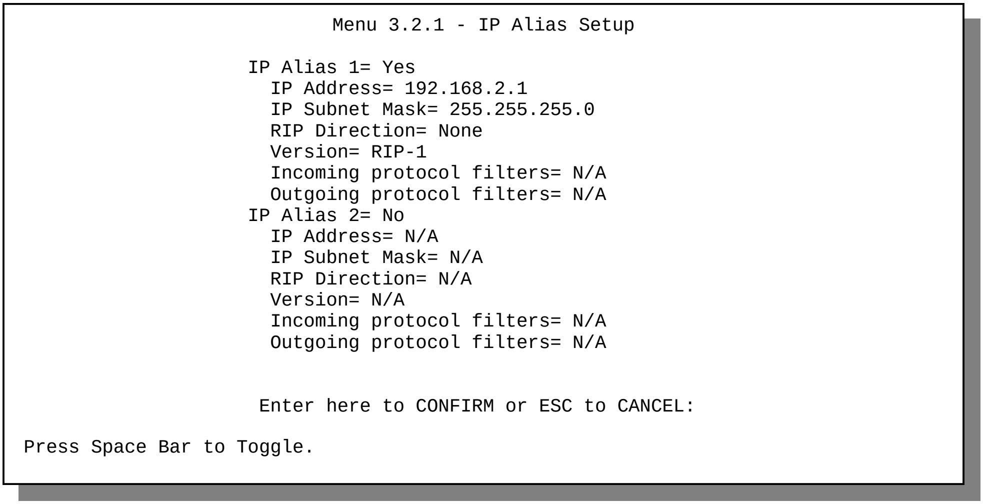
FIELD	DESCRIPTION	EXAMPLE
TCP/IP Setup		
IP Address	Enter the (LAN) IP address of your Prestige in dotted decimal notation	192.168.1.1 (default)
IP Subnet Mask	Your Prestige will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Prestige	255.255.255.0
RIP Direction	Press the [SPACE BAR] to select the RIP direction from **Both**, **In Only**, **Out Only** or **None**.	**Both** (default)
Version	Press the [SPACE BAR] to select the RIP version from **RIP-1**, **RIP-2B** or **RIP-2M**.	**RIP-1** (default)

FIELD	DESCRIPTION	EXAMPLE
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The P645R supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). Press the [SPACE BAR] to enable IP Multicasting or select **None** (default) to disable it.	**None** (default)
IP Policies	You can apply up to four IP Policy sets (from twelve) by entering their numbers separated by commas. None are applied by default.	1,2,7,8
Edit IP alias	The P645R supports three logical LAN interfaces via its single physical Ethernet interface with the P645R itself as the gateway for each LAN network. Press the [SPACE BAR] to select **Yes**, then press [ENTER] to display menu 3.2.1	**No**
When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm…] to save your configuration, or press [ESC] at any time to cancel.		

3.4.1 IP Alias Setup

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

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



```
                             Menu 3.2.1 - IP Alias Setup

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


                       Enter here to CONFIRM or ESC to CANCEL:

Press Space Bar to Toggle.
```

Figure 3-5 Menu 3.2.1 — IP Alias Setup

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

Table 3-3 IP Alias Setup Menu Fields

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

3.5 LANs & WANs

A LAN (Local Area Network) is a computer network limited to the immediate area, usually the same building or floor of a building. A WAN (Wide Area Network), on the other hand is an outside connection to another network or the Internet.

3.5.1 LANs, WANs and the Prestige

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

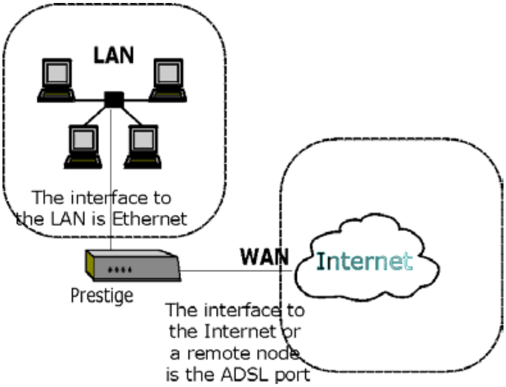

LAN
The interface to the LAN is Ethernet
WAN
Internet
Prestige
The interface to the Internet or a remote node is the ADSL port

Figure 3-6 LAN & WAN IPs

3.6 VPI & VCI

Be sure to use the Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) numbers supplied by your telephone company. The valid range for the VPI is 1 to 255 and for the VCI is 32 to 65535 (1 to 32 is reserved for local management of ATM traffic). Please see Appendix VPI and VCI for more information.

3.7 Multiplexing

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

3.7.1 VC-based multiplexing

In this case, by prior mutual agreement, each protocol is assigned to a specific virtual circuit; for example, VC1 carries IP, 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.

3.7.2 LLC-based multiplexing

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

3.8 Encapsulation

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

3.8.1 ENET ENCAP

The MAC Encapsulated Routing Link Protocol (**ENET ENCAP**) is only implemented with the IP network protocol. IP packets are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment i.e., it encapsulates routed Ethernet frames into bridged ATM cells. **ENET ENCAP** requires that you specify a gateway IP address in the **Ethernet Encapsulation Gateway** field in menu 4 and in the **Rem IP Addr** field in menu 11.1. You can get this information from your ISP.

3.8.2 PPP

Please refer to RFC 2364 for more information on PPP over ATM Adaptation Layer 5 (AAL5). Refer to RFC 1661 for more information on PPP.

3.8.3 RFC 1483

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

3.9 IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed. The ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled no matter whether you have a dynamic or static IP. However the encapsulation method assigned influences your choices for IP Address and ENET ENCAP Gateway.

3.9.1 Using PPP Encapsulation

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

3.9.2 Using RFC 1483 Encapsulation

In this case the IP Address Assignment *must* be static with the same requirements for the IP Address and ENET ENCAP Gateway fields as stated above (in 3.9.1).

3.9.3 Using ENET ENCAP Encapsulation

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

3.10 Internet Access Configuration

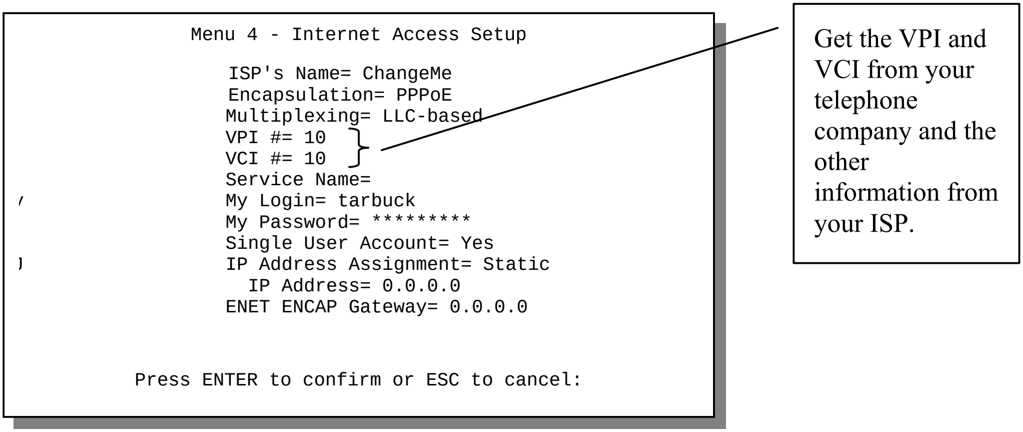
Menu 4 allows you to enter the Internet Access information in one screen. Menu 4 is actually a simplified setup for one of the remote nodes that you can access in menu 11. Before you configure your Prestige for Internet access, you need to collect your Internet account information from your ISP and telephone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

Use the following table to record your Internet Account Information. Note that if you are using PPP encapsulation, then the only ISP information you need is a login name and password. You only need to know the Ethernet Encapsulation Gateway IP address if you are using ENET ENCAP encapsulation.

Table 3-4 Internet Account Information

Internet Account Information	Write your account information here
Telephone Company Information	
VPI (Virtual Path Identifier)	—
VCI (Virtual Channel Identifier)	—
ISP Information	
IP Address of the ISP's Gateway (Optional)	—
Login Name	—
Password for ISP authentication	—
Type of Multiplexing	—
Type of Encapsulation	—
Ethernet Encapsulation Gateway	—

From the main menu, enter 4 to go to **Menu 4 - Internet Access Setup**, as shown next. The following table contains instructions on how to configure your Prestige for Internet access.



```
                Menu 4 - Internet Access Setup

                   ISP's Name= ChangeMe
                   Encapsulation= PPPoE
                   Multiplexing= LLC-based
                   VPI #= 10
                   VCI #= 10
                   Service Name=
                   My Login= tarbuck
                   My Password= *********
                   Single User Account= Yes
                   IP Address Assignment= Static
                     IP Address= 0.0.0.0
                   ENET ENCAP Gateway= 0.0.0.0



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

Get the VPI and VCI from your telephone company and the other information from your ISP.

Figure 3-7 Internet Access Setup

Table 3-5 Internet Access Setup Menu Fields

FIELD	DESCRIPTION	EXAMPLE
ISP's Name	Enter the name of your Internet Service Provider, e.g., MyISP. This information is for identification purposes only.	MyISP
Encapsulation	Press the [SPACE BAR] to select the method of encapsulation used by your ISP. The choices are PPP, RFC 1483, PPPoE or ENET ENCAP. Please see section 3.9 for related information.	**PPP**
Multiplexing	Press the [SPACE BAR] to select the method of multiplexing used by your ISP - either VC-based or LLC-based.	**VC-based**
VPI #	Enter the Virtual Path Identifier (VPI) that the telephone company gives you.	10
VCI #	Enter the Virtual Channel Identifier (VCI) that the telephone company gives you.	10
Service Name	Only available when PPPoE encapsulation is used. Enter the name of your PPPoE service provider. This is the same as PPPoE Service Name in menu 11.1.	
My Login	Enter the login name that your ISP gives you.	tarbuck
My Password	Enter the password associated with the login name above.	***
Single User Account	Press the [SPACE BAR] to enable or disable SUA. Please see the following section for a more detailed discussion on	**No**

FIELD	DESCRIPTION	EXAMPLE
Single User Account	Press the [SPACE BAR] to enable or disable SUA. Please see the following section for a more detailed discussion on the Single User Account feature.	**No**
IP Address Assignment	Press the [SPACE BAR] to select **Static** or **Dynamic** address assignment. Please see section 3.9 for related information.	**Dynamic**
IP Address	Enter the IP address supplied by your ISP if applicable.	
ENET ENCAP Gateway	Enter the gateway IP address supplied by your ISP if applicable.	

At this point, if all your settings are correct your Prestige should connect automatically to the Internet.

3.11 Single User Account

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

The Single User Account (SUA) feature allows you to have the same benefits as having multiple legal addresses, but only pay for one IP address, thus saving significantly on the subscription fees. (Check with your ISP before you enable this feature). SUA supports popular Internet applications such as MS traceroute, CuSeeMe, IRC, RealAudio, VDOLive, Quake and PPTP with no extra configuration needed.

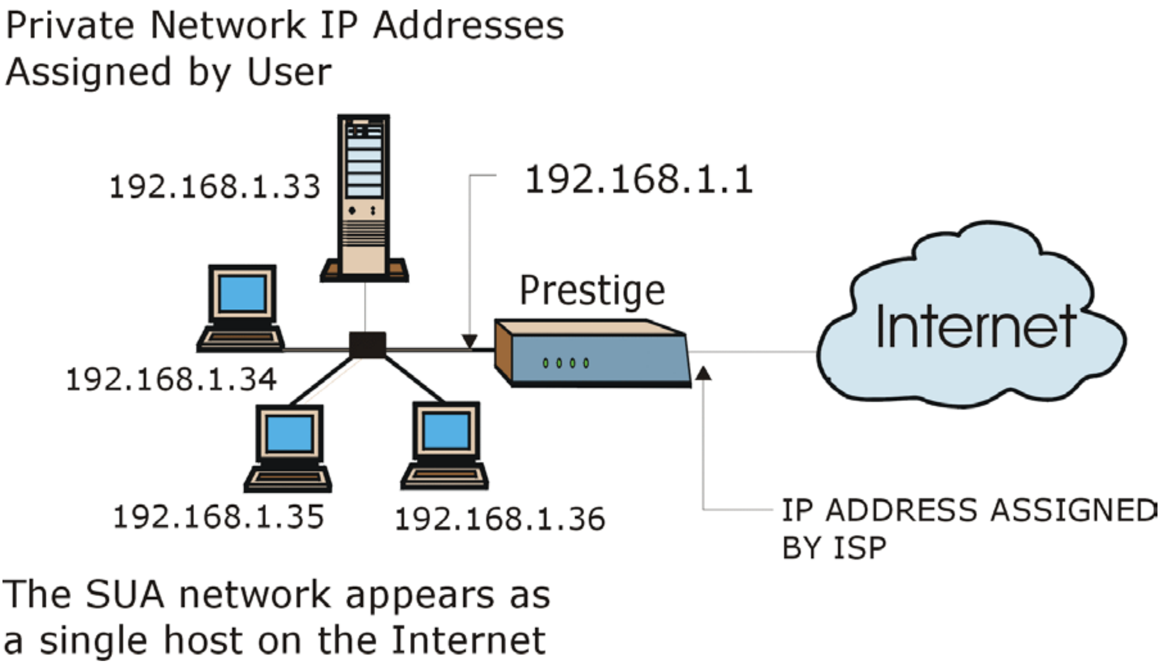


Figure 3-8 Single User Account Topology

The IP address for the SUA can be either fixed or dynamically assigned by the ISP. In addition, you can designate servers; for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any server, SUA offers the additional benefit of firewall protection. If no server is defined, all incoming inquiries will be filtered out by your Prestige, thus preventing intruders from probing your network. Your Prestige accomplishes this address sharing by translating the internal LAN IP addresses to a single address that is globally unique on the Internet. For more information on IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT).*

3.11.1 Advantages of SUA

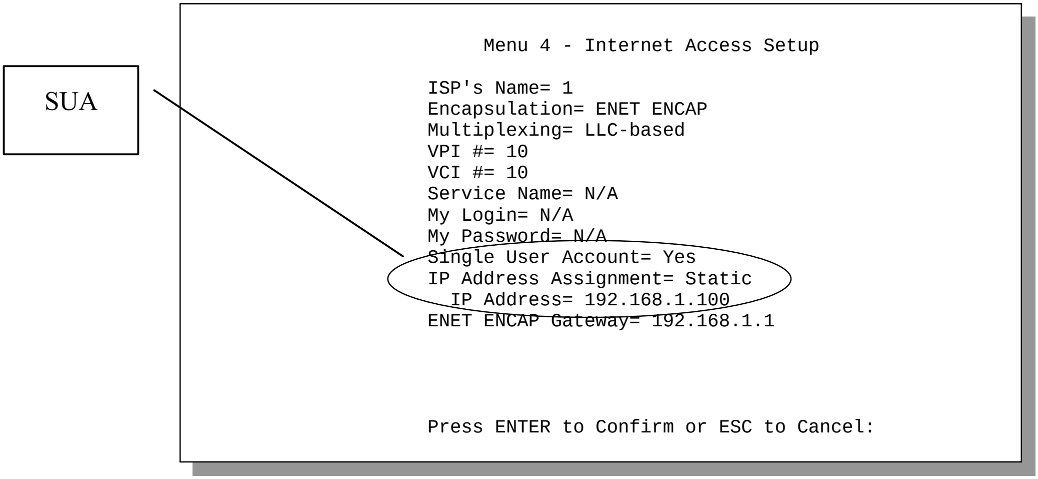
In summary:

- SUA is a cost-effective solution for small offices to access the Internet or other remote TCP/IP networks.
- SUA supports servers to be accessible to the outside world.
- SUA can provide firewall protection if you do not specify a server. All incoming inquiries will be filtered out by your Prestige.

- UDP and TCP packets can be routed. In addition, partial ICMP, including echo and traceroute, is supported.

3.11.2 Single User Account Configuration

The steps for configuring your Prestige for Single User Account are identical to the conventional Internet access with the exception that you need to fill in two extra fields in **Menu 4 - Internet Access Setup**, as shown below.



```
                    Menu 4 - Internet Access Setup

          ISP's Name= 1
          Encapsulation= ENET ENCAP
          Multiplexing= LLC-based
          VPI #= 10
          VCI #= 10
          Service Name= N/A
          My Login= N/A
          My Password= N/A
          Single User Account= Yes
          IP Address Assignment= Static
            IP Address= 192.168.1.100
          ENET ENCAP Gateway= 192.168.1.1




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

Figure 3-9 Menu 4 – Internet Access Setup for Single User Account

To enable the SUA feature in menu 4, move the cursor to the **Single User Account** field and select **Yes** (or **No** to disable SUA). Then follow the instructions on how to configure the SUA fields.

Table 3-6 Single User Account Menu Fields

FIELD	DESCRIPTION
Single User Account	Use the [SPACE BAR] to select **Yes** to enable SUA or **No** to disable it.
IP Address Assignment	Use the [SPACE BAR] to select **Static** or **Dynamic**.
IP Address	With **Dynamic** in the **IP Address Assignment** field, this field will be **N/A**; otherwise, enter the static IP address here.
Press [ENTER] at the message [Press ENTER to Confirm ...] to save your configuration, or press [ESC] at any time to cancel.	

3.12 Multiple Servers behind SUA

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

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

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

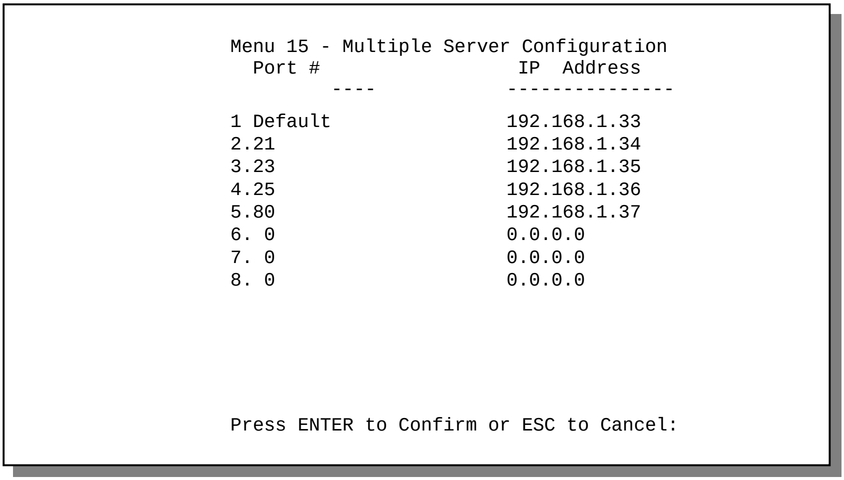
In addition to the servers for specific services, SUA supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default server is not defined, the service request is simply discarded.

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

3.12.1 Configuring a Server behind SUA

Follow the steps below to configure a server behind SUA:

1. Enter 15 in the main menu to go to **Menu 15 - Multiple Server Configuration**.
2. Enter an index number in menu 15 to go to **Menu 15.1 - SUA Server Configuration**.
3. Enter the service port number in the **Port #** field and the inside IP address of the server in the **IP Address** field.
4. 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 - Multiple Server Configuration
  Port #                  IP  Address
         ----           ---------------

1 Default               192.168.1.33
2.21                    192.168.1.34
3.23                    192.168.1.35
4.25                    192.168.1.36
5.80                    192.168.1.37
6. 0                    0.0.0.0
7. 0                    0.0.0.0
8. 0                    0.0.0.0




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

Figure 3-10 Multiple Server Configuration

The most often used port numbers are:

Table 3-7 Services vs. Port number

SERVICES	PORT NUMBER
FTP (File Transfer Protocol)	21
Telnet	23
SMTP (Simple Mail Transfer Protocol)	25
DNS(Domain Name System)	53
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
PPTP (Point-to-Point Tunneling Protocol)	1723

Part II:

Advanced Applications

This part describes Remote Node Configuration, Remote Node TCP/IP Configuration, IPX Configuration and Bridging Setup.

Chapter 4
Remote Node Configuration

This chapter is about parameters that are protocol independent. The protocol-dependent configuration will be covered in subsequent chapters.

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 one of the remote nodes.

4.1 Remote Node Setup

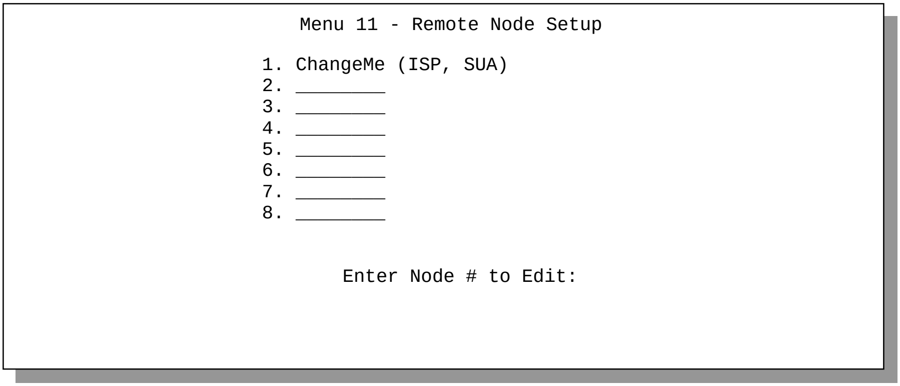
This section describes the protocol-independent parameters for a remote node.

4.1.1 Remote Node Profile

To configure a remote node, follow these steps:

Step 1. In the main menu, enter 11 to open menu **11 - Remote Node Setup**.

Step 2. When menu 11 appears, as shown below, enter the number of the remote node that you wish to configure.



```
                    Menu 11 - Remote Node Setup

                1. ChangeMe (ISP, SUA)
                2. ________
                3. ________
                4. ________
                5. ________
                6. ________
                7. ________
                8. ________


                    Enter Node # to Edit:
```

Figure 4-1 Menu 11 – Remote Node Setup

When **Menu 11.1 - Remote Node Profile** appears fill in the fields to define this remote profile. Descriptions and information about configuring the fields is given in the table that follows.

4.1.2 Encapsulation & Multiplexing Scenarios

For Internet Access you should use the encapsulation and multiplexing methods used by your ISP. For a LAN-to-LAN application, e.g., branch office and corporate headquarters, prior mutual agreement on methods used is necessary because there is no mechanism to automatically determine encapsulation/multiplexing. Selection of which encapsulation and multiplexing methods to use depends on how many VCs you have and how many different network protocols you need. The extra overhead that **PPPoE** and **ENET ENCAP** encapsulation entails makes it a poor choice in a LAN-to-LAN application. Here are some examples of more suitable combinations in such an application.

Scene 1. One VC, Multiple Protocols

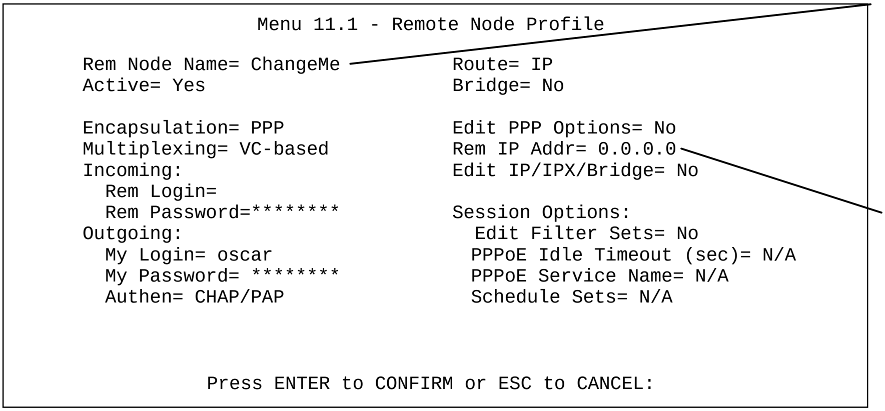
PPP (RFC 2364) encapsulation with **VC-based** multiplexing is the best combination because the extra protocol identifying headers that **LLC-based** multiplexing uses are unneeded. The **PPP** protocol already contains this information.

Scene 2. One VC, One Protocol (IP)

Selecting **RFC-1483** encapsulation with VC-based multiplexing requires the least amount of overhead (0 octets). However, if there is a potential need for multiple protocol support in the future, it may be safer to select **PPP** encapsulation instead of **RFC-1483**, so you don't need to reconfigure when the time comes.

Scene 3. Multiple VCs

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



```
                      Menu 11.1 - Remote Node Profile

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

       Encapsulation= PPP                Edit PPP Options= No
       Multiplexing= VC-based            Rem IP Addr= 0.0.0.0
       Incoming:                         Edit IP/IPX/Bridge= No
         Rem Login=
         Rem Password=********           Session Options:
       Outgoing:                           Edit Filter Sets= No
         My Login= oscar                  PPPoE Idle Timeout (sec)= N/A
         My Password= ********            PPPoE Service Name= N/A
         Authen= CHAP/PAP                 Schedule Sets= N/A



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

Enter a unique name, up to eight characters, for the remote node.

Use 0.0.0.0 to connect to your ISP or enter the IP address of the remote gateway here.

Figure 4-2 Menu 11.1 Remote Node Profile

Table 4-1 Remote Node Profile Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Rem Node Name	This is a required field [?]. Enter a descriptive name for the remote node, for example, “Changeme”. This field can be up to eight characters. This name must be unique from any other remote node name.	Changeme
Active	Press the [SPACE BAR] to select either **Yes** or **No**. Inactive nodes are displayed with a minus sign (-) at the beginning of the name in menu 11.	**No**

FIELD		DESCRIPTION	EXAMPLE
Encapsulation=		**PPP** refers to RFC 2364, "PPP Encapsulation over ATM Adaptation Layer 5". If **RFC 1483** ("Multiprotocol Encapsulation over ATM Adaptation Layer 5") or **ENET ENCAP** are selected, then the **Rem Login**, **Rem Password**, **My Login**, **My Password**, **Edit PPP Options** and **Authen** fields will not be applicable (N/A). Moreover, **ENET ENCAP** encapsulation does not apply for IPX routing.	**PPP**
Multiplexing=		Press the [SPACE BAR] to select either **VC-based or** **LLC-based** multiplexing.	**LLC-based**
Incoming:	Rem Login Name	Enter the login name that this remote node will use when it calls your Prestige. The login name in this field combined with the Rem Node Password will be used to authenticate this node.	bucket
Incoming:	Rem Password	Enter the password used when this remote node calls your Prestige.	***
Outgoing:	My Login	Enter the login name for your Prestige when it calls this remote node.	oscar
Outgoing:	My Password	Enter the password for your Prestige when it calls this remote node.	***
Outgoing:	Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are: **CHAP/PAP** - Your Prestige will accept either CHAP or PAP when requested by this remote node. **CHAP** - accept CHAP only. **PAP** - accept PAP only.	**CHAP/PAP**
Route		This field determines the protocols that your Prestige will route. Options are **IP**, **IPX**, **IP+!PX** and **None**; although with **ENET ENCAP** the only available protocol is **IP**.	**IP**
Bridge		Bridging is used for protocols that are not supported by the Prestige, e.g., SNA, or are not turned on in the previous Route field. Select **Yes** to enable and **No** to disable. When bridging is enabled, your Prestige will forward any packet that it does not route to this remote node; otherwise, the packets are discarded.	**No** (default)

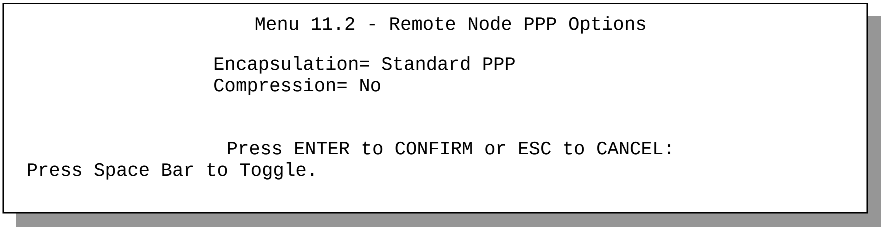
FIELD	DESCRIPTION	EXAMPLE
Edit PPP Options	Only available when using PPPoE or PPP. To edit the PPP options for this remote node, move the cursor to this field, use the [SPACE BAR] to select **Yes** and press [ENTER]. This will bring you to **Menu 11.2 - Remote Node PPP Options**. For more information on configuring PPP options, see the section *Editing PPP Options*.	**No** (default)
Rem IP Addr	Enter the IP address of the remote gateway or leave this field set to 0.0.0.0 for connecting to your ISP.	0.0.0.0
Edit IP/IPX/Bridge	Press the [SPACE BAR] to select **Yes** and press [ENTER] to go to **Menu 11.3 - Remote Node Network Layer Options** menu.	**No**
Session Options: Edit Filter Sets	Use the [SPACE BAR] to select **Yes** in this field and press [ENTER] to open menu 11.5 to edit the filter sets. See the Remote Node Filter section for more details.	**No** (default)
PPPoE Idle Timeout (sec)	This value specifies the number of idle seconds that elapse before the Prestige automatically disconnects the PPPoE session.	N/A
PPPoE Service Name	Only available when PPPoE encapsulation is used. Enter the name of your PPPoE service provider. This is the same as **Service Name** in menu 4.	N/A
Schedule Sets	Only available when using PPPoE. You can select up to four schedule sets here and configure them in menu 26. For more details, please see the *Call Scheduling* chapter.	N/A
Once you have completed filling in **Menu 11.1 – Remote Node Profile**, press [ENTER] at the message [Press ENTER to Confirm…] to save your configuration, or press [ESC] at any time to cancel.		

4.1.3 Outgoing Authentication Protocol

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

4.1.4 Editing PPP Options

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



```
                      Menu 11.2 - Remote Node PPP Options

                  Encapsulation= Standard PPP
                  Compression= No


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

Figure 4-3 Menu 11.2 - Remote Node PPP Options

The following table describes the Remote Node PPP Options Menu, and contains instructions on how to configure the PPP options fields.

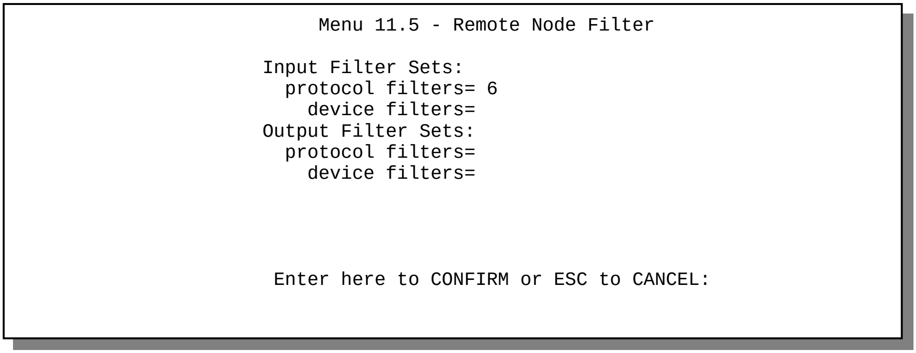
Table 4-2 Remote Node PPP Options Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Encapsulation	Select **CISCO PPP** only when this remote node is a Cisco machine; otherwise, select the **Standard PPP.**	**Standard PPP**
Compression	Turn on/off Stac Compression. The default for this field is **Off**.	**Off** (Default)
Once you have completed filling in **Menu 11.2 – Remote Node PPP Options**, press [ENTER] at the message [Press ENTER to Confirm…] to save your configuration, or press [ESC] at any time to cancel.		

4.1.5 Remote Node Filter

Use **Menu 11.5 – Remote Node Filter** to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the Prestige. You can specify up to four filter sets separated by commas, e.g., 1, 5, 9, 12, in each filter field. The Prestige comes with default filter number 6 applied. This filter blocks FTP, Telnet, TFTP and HTTP from coming in from the WAN.

Note that spaces are accepted in this field. For more information on defining the filters, see the section on Filter Configuration.



```
                        Menu 11.5 - Remote Node Filter

                   Input Filter Sets:
                     protocol filters= 6
                       device filters=
                   Output Filter Sets:
                     protocol filters=
                       device filters=





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

Figure 4-4 Menu 11.5 – Remote Node Filter

Chapter 5
Remote Node TCP/IP Configuration

This chapter shows you how to configure the TCP/IP parameters of a remote node.

A typical LAN-to-LAN application is to use your Prestige to connect a branch office to the headquarters, as depicted in the following diagram.

5.1 LAN-to-LAN Application

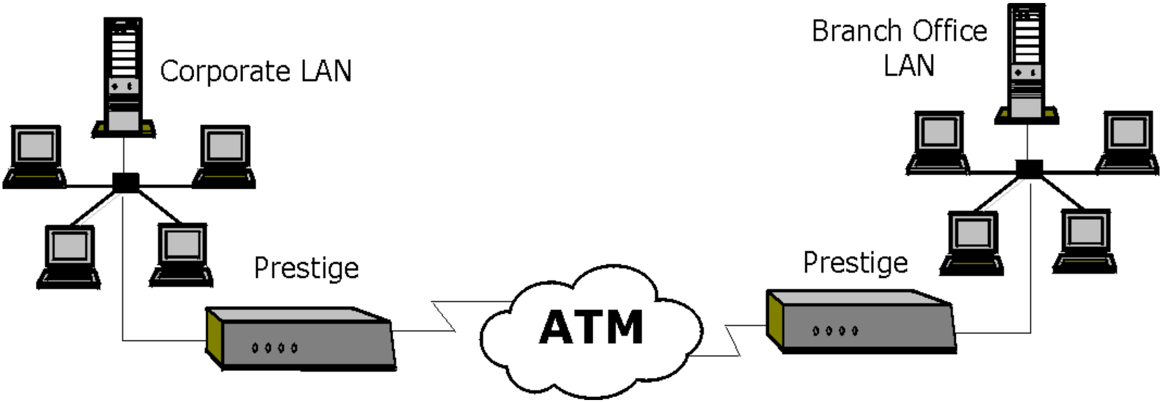


Figure 5-1 TCP/IP LAN-to-LAN Application

For the branch office, you need to configure a remote node in order to dial out to the headquarters. Additionally, you may also need to define static routes if some services reside beyond the immediate remote LAN.

5.1.1 Editing TCP/IP Options

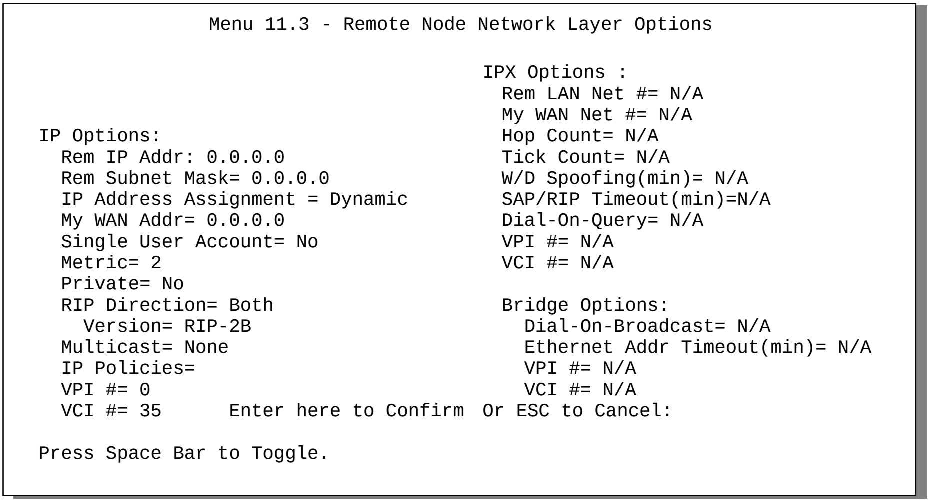
Follow the steps below to edit **Menu 11.3 - Remote Node Network Layer Options** shown next.

In menu 11.1, move the cursor to the **Edit IP/IPX/Bridge**, then press the [SPACE BAR] to select **Yes**. Press [ENTER] to open **Menu 11.3 - Network Layer Options**.

There are two versions of menu 11.3 for the Prestige, depending on whether you chose **VC-based** or **LLC-based** multiplexing in menu 11.1.

VC-Based Multiplexing

Remember that for **VC-based** multiplexing, by prior mutual agreement, a protocol is assigned a specific virtual circuit, e.g., VC1 will carry IP, VC2 will carry IPX etc.



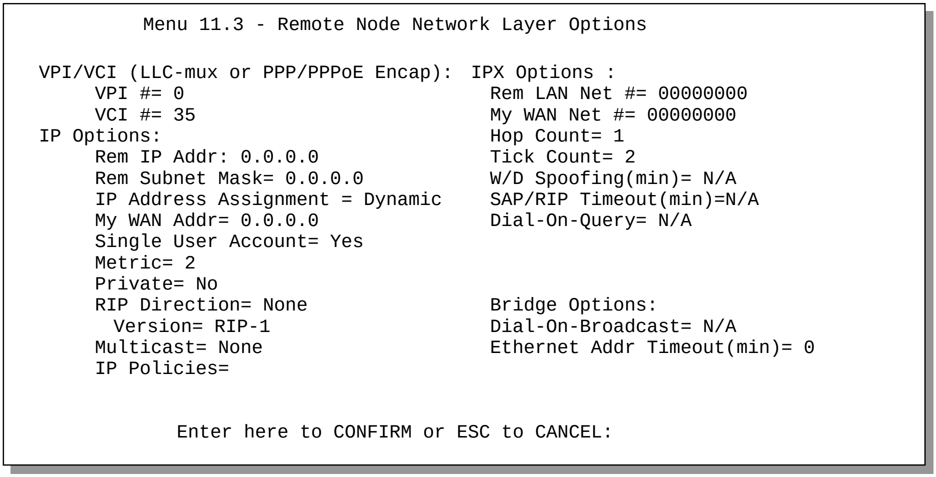
```
                  Menu 11.3 - Remote Node Network Layer Options

                                           IPX Options :
                                             Rem LAN Net #= N/A
                                             My WAN Net #= N/A
   IP Options:                               Hop Count= N/A
     Rem IP Addr: 0.0.0.0                    Tick Count= N/A
     Rem Subnet Mask= 0.0.0.0                W/D Spoofing(min)= N/A
     IP Address Assignment = Dynamic         SAP/RIP Timeout(min)=N/A
     My WAN Addr= 0.0.0.0                    Dial-On-Query= N/A
     Single User Account= No                 VPI #= N/A
     Metric= 2                               VCI #= N/A
     Private= No
     RIP Direction= Both                     Bridge Options:
       Version= RIP-2B                         Dial-On-Broadcast= N/A
     Multicast= None                           Ethernet Addr Timeout(min)= N/A
     IP Policies=                              VPI #= N/A
     VPI #= 0                                  VCI #= N/A
     VCI #= 35      Enter here to Confirm  Or ESC to Cancel:

   Press Space Bar to Toggle.
```

Figure 5-2 Menu 11.3 for VC-based multiplexing with RFC 1483 and ENET ENCAP

In this case, separate VPI and VCI numbers must be specified for each protocol.

LLC-based multiplexing

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



```
         Menu 11.3 - Remote Node Network Layer Options

VPI/VCI (LLC-mux or PPP/PPPoE Encap):  IPX Options :
     VPI #= 0                           Rem LAN Net #= 00000000
     VCI #= 35                          My WAN Net #= 00000000
IP Options:                             Hop Count= 1
     Rem IP Addr: 0.0.0.0               Tick Count= 2
     Rem Subnet Mask= 0.0.0.0           W/D Spoofing(min)= N/A
     IP Address Assignment = Dynamic    SAP/RIP Timeout(min)=N/A
     My WAN Addr= 0.0.0.0               Dial-On-Query= N/A
     Single User Account= Yes
     Metric= 2
     Private= No
     RIP Direction= None                Bridge Options:
       Version= RIP-1                   Dial-On-Broadcast= N/A
     Multicast= None                    Ethernet Addr Timeout(min)= 0
     IP Policies=


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

Figure 5-3 Menu 11.3 for LLC-based multiplexing

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

The following diagram explains the Sample IP Addresses to help you understand the **My Wan Addr** field in menu 11.3. Refer to the section on Internet access for a brief review of what a WAN IP is. **My WAN Addr** indicates the local Prestige WAN IP while **Rem IP Address** indicates the peer WAN IP.

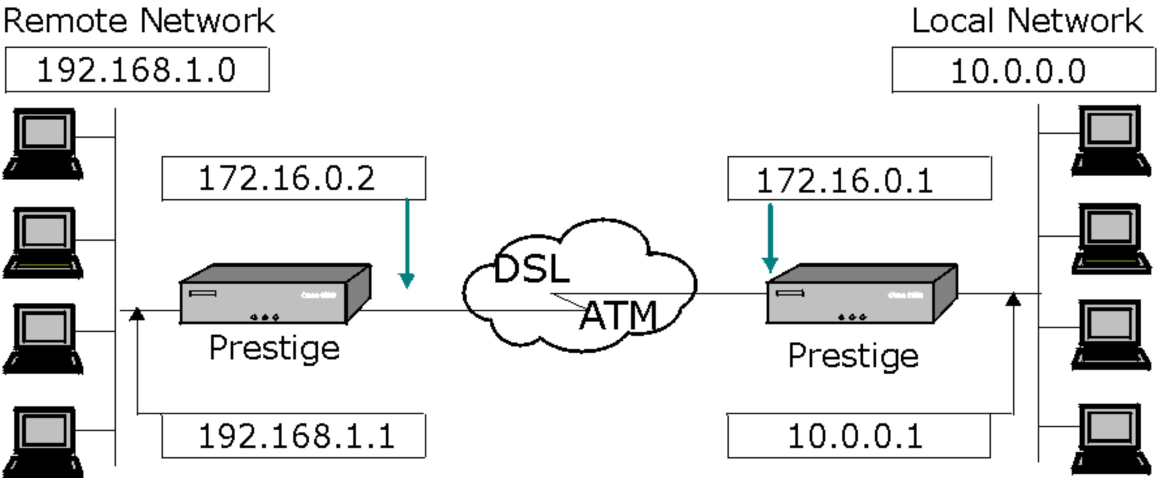
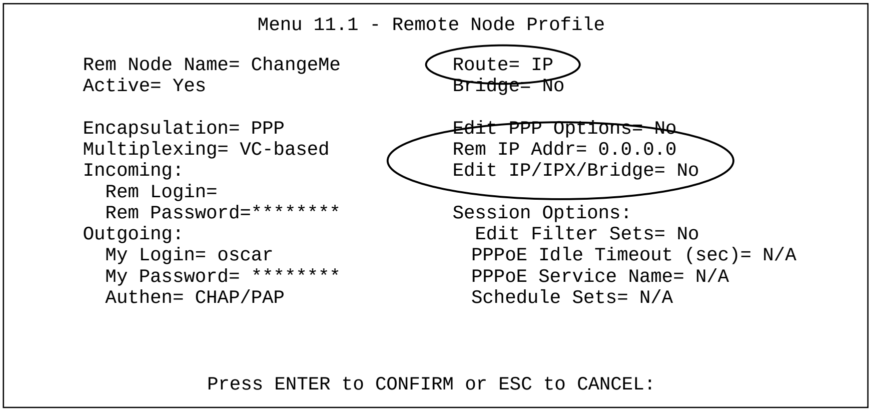


Figure 5-4 Sample IP Addresses for a TCPI/IP LAN-to-LAN Connection

To configure the TCP/IP parameters of a remote node, first configure the fields in **Menu 11.1 – Remote Node Profile**, as shown in the next table. For more details on the IP Option fields, refer to the section on Internet access.



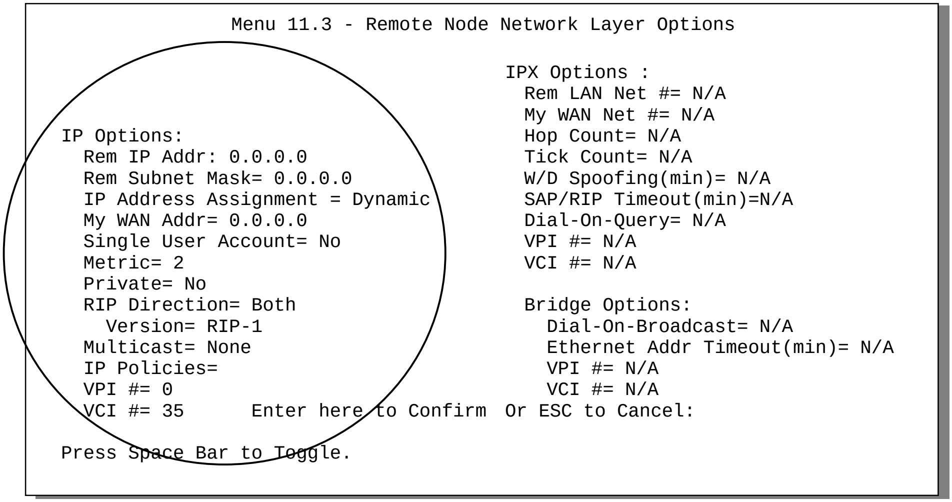
```
                      Menu 11.1 - Remote Node Profile

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

     Encapsulation= PPP               Edit PPP Options= No
     Multiplexing= VC-based           Rem IP Addr= 0.0.0.0
     Incoming:                        Edit IP/IPX/Bridge= No
       Rem Login=
       Rem Password=********          Session Options:
     Outgoing:                          Edit Filter Sets= No
       My Login= oscar                  PPPoE Idle Timeout (sec)= N/A
       My Password= ********            PPPoE Service Name= N/A
       Authen= CHAP/PAP                 Schedule Sets= N/A



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

Figure 5-5 Menu 11.1 Remote Node Profile

Table 5-1 TCP/IP related fields in Remote Node Profile

FIELD	DESCRIPTION	EXAMPLE
Route	Make sure **IP** is among the protocols in the **Route** field in **Menu 11.1 - Remote Node Profile**. Options are **IP**, **IPX**, **IP+IPX** and **None**; although with **ENET ENCAP** the only available protocol is **IP**.	**IP**
Rem IP Address	Enter the IP address of the remote gateway in **Menu 11.1 - Remote Node Profile**. You must fill in either the remote Prestige WAN IP address or the remote Prestige LAN IP address. This depends on the remote router's WAN IP i.e., for the (remote) Prestige, the **My WAN Addr** settings in **Menu 11.3 – Remote Node Network Layer Options**). For example (*see Figure 5-4*), if the remote WAN IP is set to 172.16.0.2 (the remote router's WAN IP), then you should enter 172.16.0.2 in the **Rem IP Address** field. If the remote WAN IP is 0.0.0.0, then enter 192.168.1.1(the remote router's LAN IP) in the **Rem IP Address** field).	0.0.0.0
Edit IP/IPX/Bridge	Press the [SPACE BAR] to select **Yes** in this field and then press [ENTER] to go to **Menu 11.3 - Remote Node Network Layer Options**.	**No**

The following table shows the TCP/IP related fields in **Menu 11.3 - Remote Node Network Layer Options**.



```
                 Menu 11.3 - Remote Node Network Layer Options

                                         IPX Options :
                                           Rem LAN Net #= N/A
                                           My WAN Net #= N/A
  IP Options:                              Hop Count= N/A
    Rem IP Addr: 0.0.0.0                   Tick Count= N/A
    Rem Subnet Mask= 0.0.0.0               W/D Spoofing(min)= N/A
    IP Address Assignment = Dynamic        SAP/RIP Timeout(min)=N/A
    My WAN Addr= 0.0.0.0                   Dial-On-Query= N/A
    Single User Account= No                VPI #= N/A
    Metric= 2                              VCI #= N/A
    Private= No
    RIP Direction= Both                    Bridge Options:
      Version= RIP-1                         Dial-On-Broadcast= N/A
    Multicast= None                          Ethernet Addr Timeout(min)= N/A
    IP Policies=                             VPI #= N/A
    VPI #= 0                                 VCI #= N/A
    VCI #= 35      Enter here to Confirm  Or ESC to Cancel:

  Press Space Bar to Toggle.
```

Figure 5-6 Menu 11.3 for VC-based multiplexing with RFC 1483 and ENET ENCAP

Table 5-2 TCP/IP Remote Node Configuration

FIELD	DESCRIPTION	EXAMPLE
Rem IP Address	This will show the IP address you entered for this remote node in the previous menu.	172.16.0.2
Rem IP Subnet Mask	Enter the subnet mask for the remote network.	255.255.255.0
IP Address Assignment	Press the [SPACE BAR] to select **Static** for a fixed IP address given by an ISP or **Dynamic** for the IP address to be assigned automatically by a server each time the remote node logs on.	**Dynamic**
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. Note that this is the address assigned to your local Prestige WAN, not the remote router. If the remote router is a Prestige, then this entry determines the local Prestige **Rem IP Address** in menu 11.1 (*see Table 5-1*).	
Single User Account	Use the [SPACE BAR] to select either **Yes** or **No**. Set this field to **Yes** to enable the Single User Account feature for your Prestige. See the section on Internet access for more information on the	**No**

FIELD	DESCRIPTION	EXAMPLE
Single User Account	Use the [SPACE BAR] to select either **Yes** or **No**. Set this field to **Yes** to enable the Single User Account feature for your Prestige. See the section on Internet access for more information on the Single User Account feature.	**No**
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.	2
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.	**No**
RIP Direction	Press the [SPACE BAR] to select the **RIP direction** from **Both**/**In Only**/**Out Only** or **None**.	**Both** (default)
Version=	Press the [SPACE BAR] to select the RIP version from **RIP-1/RIP-2B/RIP-2M.**	**RIP-1** (default)
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The P645R supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). Press the [SPACE BAR] to enable IP Multicasting or select **None** (default) to disable it.	**None** (default)
IP Policies	You can apply up to four IP Policy sets (from twelve) by entering their numbers separated by commas.	3,4,5,6
VPI (VC –based ENET ENCAP and RFC 1483)	Enter the Virtual Path Identifier (VPI) number that your telephone company supplies.	0
VCI (VC –based ENET ENCAP and RFC 1483)	Enter the Virtual Channel Identifier (VCI) number that your telephone company supplies.	35
Once you have completed filling in the Network Layer Options Menu, press [ENTER] to return to menu 11. Press [ENTER] at the message [Press ENTER to Confirm...] to save your configuration, or press [ESC] at any time to cancel.		

5.1.2 Static Route Setup

Static routes tell the Prestige routing information that it cannot learn automatically through other means. This can arise in cases where RIP is disabled on the LAN or a remote network is beyond the one that is directly connected to a remote node. Each remote node specifies only the network to which the gateway is directly connected, and the Prestige has no knowledge of the networks beyond.

For instance, the Prestige knows about network N2 in the following diagram through remote node Router 1. However, the Prestige is unable to route a packet to network N3 because it doesn't know that there is a route through remote node Router 1 (via Router 2). The static routes are for you to tell the Prestige about the networks beyond the remote nodes.

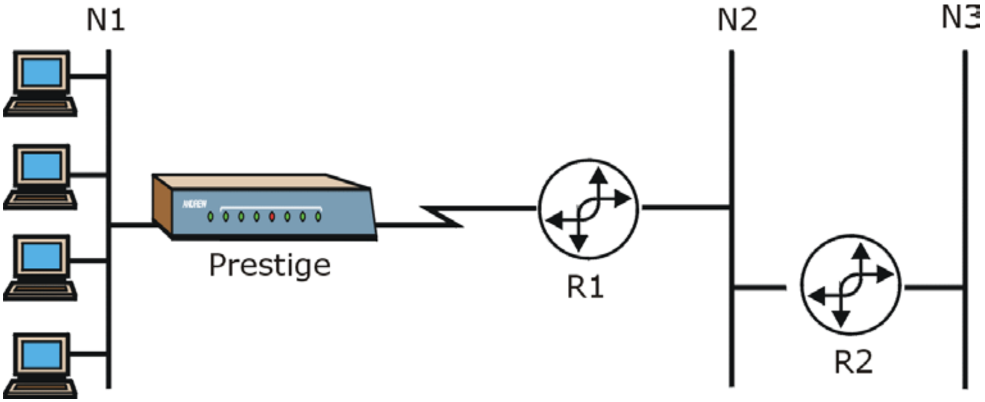
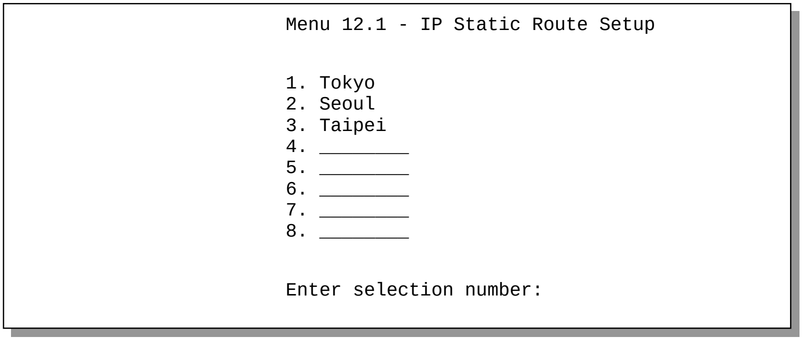


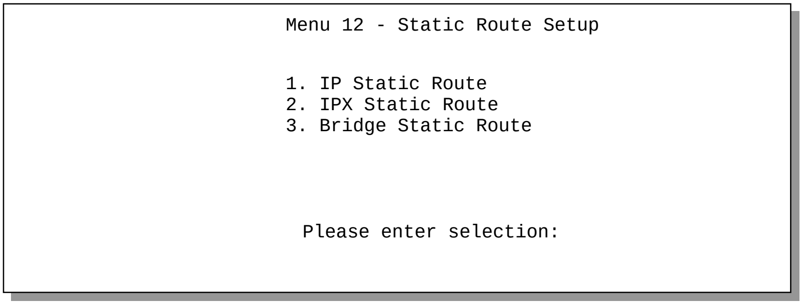
Figure 5-7 Example of Static Routing Topology



```
                        Menu 12.1 - IP Static Route Setup


                        1. Tokyo
                        2. Seoul
                        3. Taipei
                        4. ________
                        5. ________
                        6. ________
                        7. ________
                        8. ________


                        Enter selection number:
```

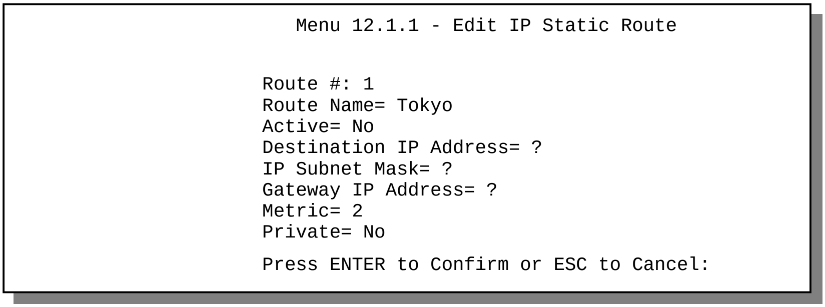
Figure 5-8 Menu 12 Static Route Setup

Menu 12 Static Route Setup is shown above. This section describes how to configure an IP static route. See the following chapters for IPX configuration and bridging setup. To configure an IP static route, enter 1 in menu 12 to go to **Menu 12.1 – IP Static Route Setup**, as shown next. From menu 12.1, enter the index number of the static route you wish to edit to open **Menu 12.1.1 - Edit IP Static Route.**



```
                        Menu 12 - Static Route Setup


                        1. IP Static Route
                        2. IPX Static Route
                        3. Bridge Static Route




                          Please enter selection:
```

Figure 5-9 Menu 12.1 - IP Static Route Setup



```
                    Menu 12.1.1 - Edit IP Static Route


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

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

Figure 5-10 Menu 12.1.1 - Edit IP Static Route

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

Table 5-3 Edit IP Static Route Menu Fields

FIELD	DESCRIPTION
Route Name	Enter a descriptive name for this route. This is for identification purposes only.
Active	Use the [SPACE BAR] to select **Yes** to activate or **No** to 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 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 WAN, the gateway must be the IP address of one of the remote nodes.
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.
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 broadcasts. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.
Once you have completed filling in the Edit IP Static Route, press [ENTER] to return to menu 12.1. Press [ENTER] at the message [Press ENTER to Confirm...] to save your configuration, or press [ESC] at any time to cancel.	

Chapter 6
IPX Configuration

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

6.1 IPX Network Environment

Novell bundles the protocol stack, the server software and routing functionality in their NetWare server products, so a NetWare server is not only a file or print server, it is also a router.

6.1.1 Network and Node Number

Every IPX machine has a network number and a node number, together they form the complete address of the machine. The IPX network number is a 32-bit quantity and is usually expressed in 8 hexadecimal digits, e.g., 0893A8CF. The host number is a 48-bit quantity and usually is taken from the MAC (Media Access Control) address of the Ethernet hardware, so you don't have to explicitly configure the node number.

An IPX client obtains its network number from a server that has the network numbers statically configured. If there are multiple servers on a network, only one server needs to have the network numbers configured and all other stations (clients and servers) can obtain the network numbers from it. The server with configured network numbers is called a seed router.

If you have a NetWare server on the same LAN as the Prestige 645R, we recommend that you set up a NetWare server as a seed router. Even though the Prestige 645R is capable of functioning as a seed router, a NetWare server offers a much more extensive facility for network management.

6.1.2 Frame Types

IPX can run on top of four different frame types on the Ethernet. These frame types are 802.2, 802.3, Ethernet II (DIX) and SNAP (Sub-Network Access Protocol). Each frame type is a separate logical network, even though they exist on one physical cable (see the following diagram).

Although there are four frame types available on the Ethernet, you should configure as few frame types as possible on your NetWare server and use automatic frame detection on the clients to simplify management and to reduce network overhead.

6.1.3 External Network Number

Each of the four logical networks (based on frame type) has its own external network number.

6.1.4 Internal Network Number

In addition to the external network numbers, each NetWare server has its own internal network number that is a virtual network to which the server is attached. It is important to remember that every network number must be unique for that entire internetwork, either internal or external.

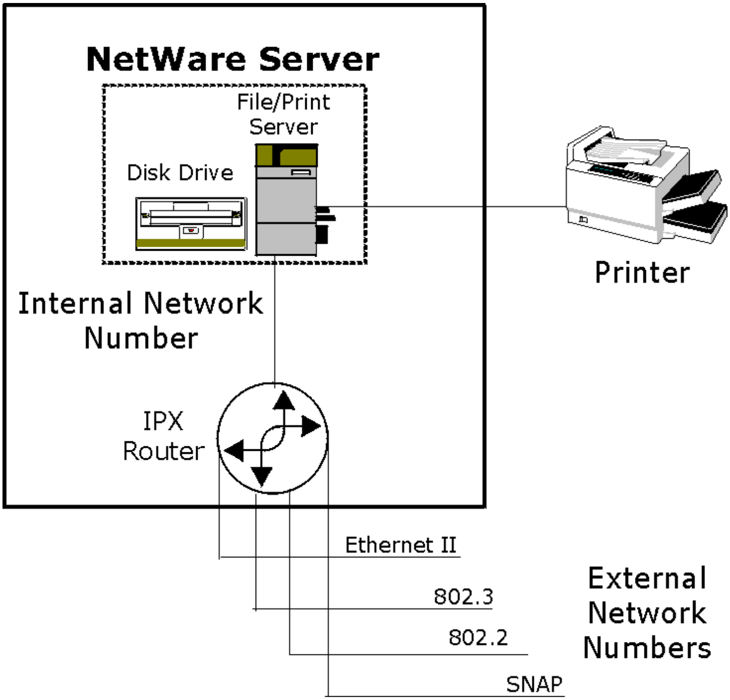


Figure 6-1 NetWare Server

6.2 Prestige in an IPX Environment

There are two scenarios in which your Prestige 645R is deployed, depending on whether there is a NetWare server on the LAN, as depicted in the following diagram.

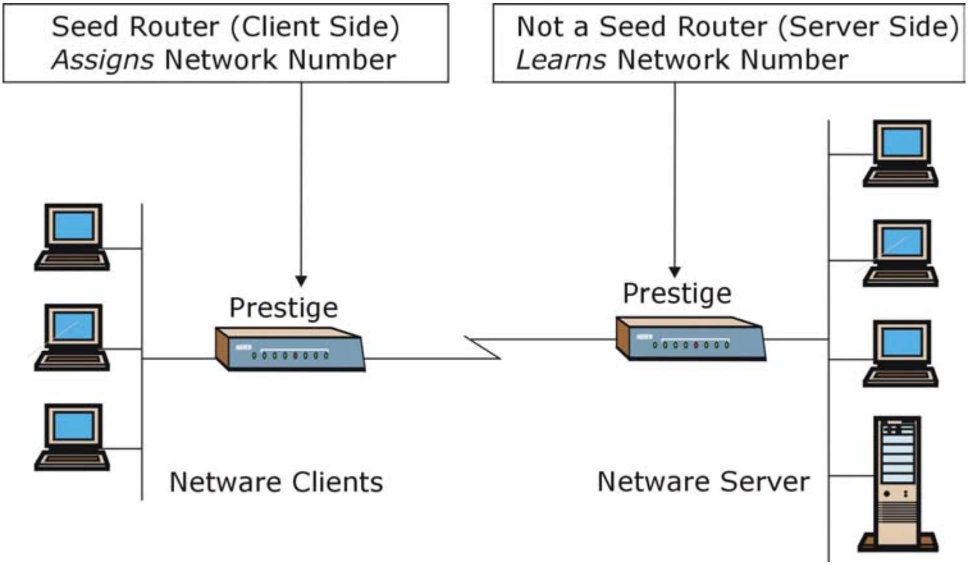


Figure 6-2 Prestige 645R in an IPX Environment

6.2.1 Prestige 645R on LAN with Server

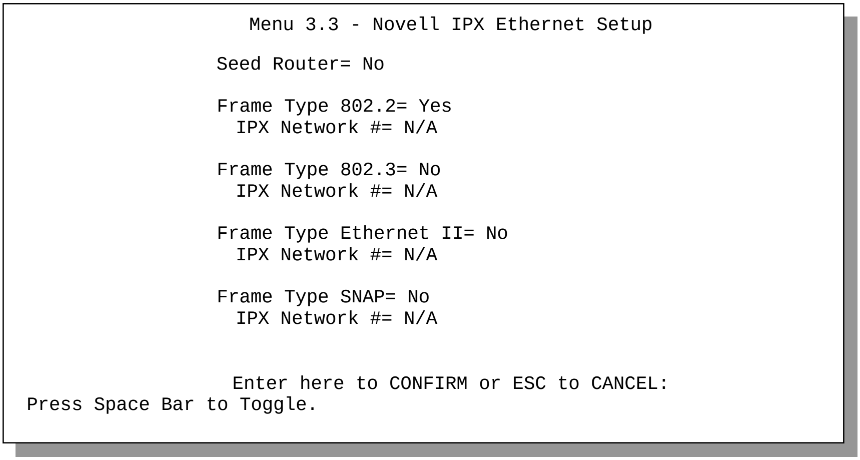
If your Prestige is on a LAN with a seed router, you do not need to configure the LAN network numbers. Your Prestige will learn the network number from the seed router and add the routes to its routing table.

6.2.2 Prestige 645R on LAN without Server

Each IPX network must have a seed router. If you only have NetWare clients on your network, then you must configure the Prestige as a seed router and set up unique network numbers for each frame type enabled using the Ethernet Setup Menu.

6.3 IPX Ethernet Setup

From **Menu 3 - Ethernet Setup**, enter 3 to go to **Menu 3.3 - Novell IPX Ethernet Setup** as shown in the figure below.



```
                     Menu 3.3 - Novell IPX Ethernet Setup

                  Seed Router= No

                  Frame Type 802.2= Yes
                    IPX Network #= N/A

                  Frame Type 802.3= No
                    IPX Network #= N/A

                  Frame Type Ethernet II= No
                    IPX Network #= N/A

                  Frame Type SNAP= No
                    IPX Network #= N/A


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

Figure 6-3 Menu 3.3 - Novell IPX Ethernet Setup

The following table describes the Novell IPX Ethernet Setup Menu.

Table 6-1 Novell IPX Ethernet Setup Fields

FIELD	DESCRIPTION	EXAMPLE
Seed Router	Select **Yes** or **No** to determine if your Prestige 645R is to act as a seed router.	**No**
Frame Type	Enable/Disable the individual frame type. Remember to enable only the ones that are actually used on your network. **802.2, 802.3, Ethernet II and SNAP**	**No**
IPX Network #	If your Prestige 645R is a seed router, enter a unique network number for each frame type enabled.	N/A
Press [ENTER] at the message [Press ENTER to Confirm ...] to save your configuration, or press [ESC] at any time to cancel.		

6.4 LAN-to-LAN Application with Novell IPX

A typical LAN-to-LAN application is to use your Prestige 645R to call from a branch office to the corporate headquarters to enable the stations in the branch office to access the NetWare servers at the headquarters, as depicted in the figure below.

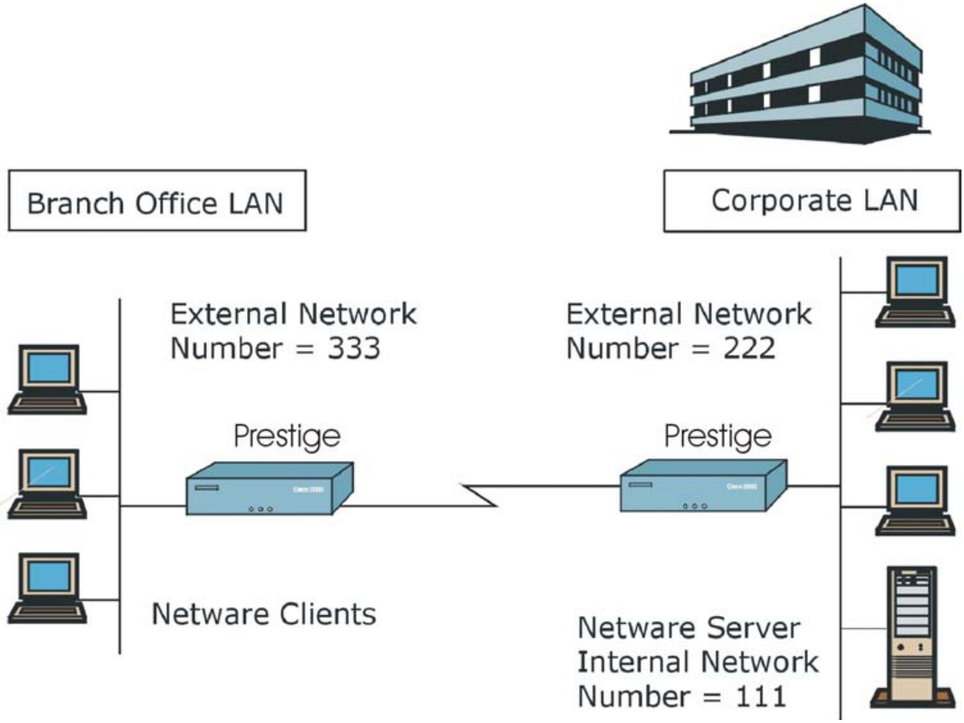

Branch Office LAN
Corporate LAN
External Network Number = 333
External Network Number = 222
Prestige
Prestige
Netware Clients
Netware Server Internal Network Number = 111

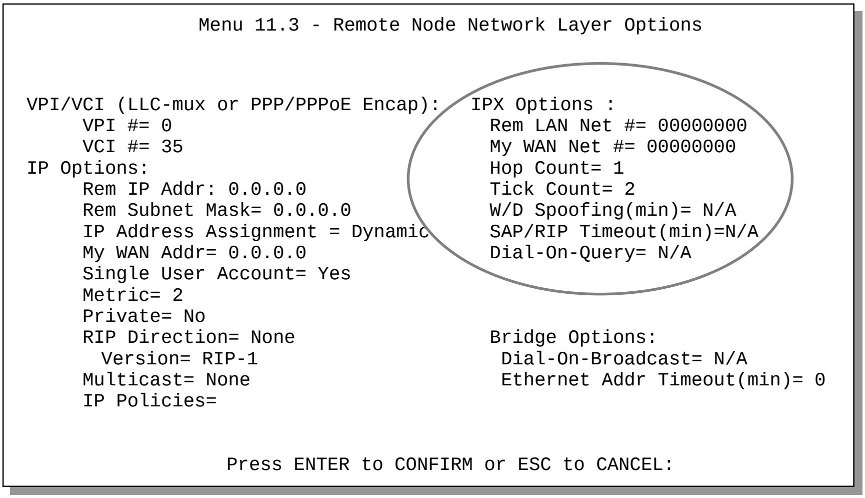
Figure 6-4 LAN-to-LAN Application with Novell IPX

6.4.1 IPX Remote Node Setup

Follow the procedure in *Chapter 5* to configure the protocol-independent parameters in **Menu 11.1 - Remote Node Profile**. For the IPX-specific parameters in **Menu 11.3 - Remote Node Network Layer Options** follow the instructions below.

Step 1. In menu 11.1, make sure **IPX** is among the protocols in the **Route** field. (The **Route** field should display **Route** = **IPX** or **Route** = **IP + IPX**.)

Step 2. Move the cursor to the **Edit IP/IPX/Bridge** field, then press the space bar to select **Yes** and press [ENTER] to open **Menu 11.3 - Network Layer Options**.



```
                  Menu 11.3 - Remote Node Network Layer Options


  VPI/VCI (LLC-mux or PPP/PPPoE Encap):   IPX Options :
       VPI #= 0                             Rem LAN Net #= 00000000
       VCI #= 35                            My WAN Net #= 00000000
  IP Options:                               Hop Count= 1
       Rem IP Addr: 0.0.0.0                 Tick Count= 2
       Rem Subnet Mask= 0.0.0.0             W/D Spoofing(min)= N/A
       IP Address Assignment = Dynamic      SAP/RIP Timeout(min)=N/A
       My WAN Addr= 0.0.0.0                 Dial-On-Query= N/A
       Single User Account= Yes
       Metric= 2
       Private= No
       RIP Direction= None                  Bridge Options:
         Version= RIP-1                      Dial-On-Broadcast= N/A
       Multicast= None                       Ethernet Addr Timeout(min)= 0
       IP Policies=


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

Figure 6-5 Menu 11.3 - Remote Node Novell IPX Options

The table below describes the IPX-specific parameters of the remote node setup.

Table 6-2 Remote Node Novell IPX Options

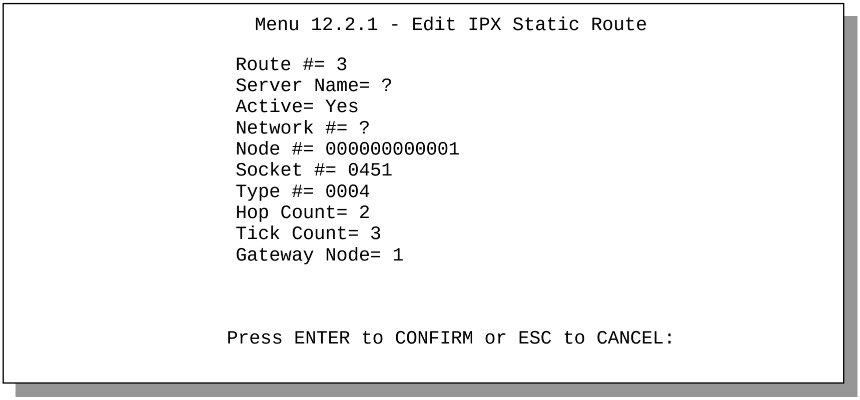
FIELD	DESCRIPTION	EXAMPLE
Rem LAN Net #	In this field, enter the internal network number of the NetWare server on the remote LAN.	00000000
My WAN Net #	In this field, enter the network number of the WAN link. If you leave this field as 00000000, your Prestige will determine automatically the network number through negotiation with the PPP peer.	00000000 (default)
Hop Count	This field indicates the number of intermediate networks that must be passed through to reach the remote node.	1 (default)
Tick Count	This field indicates the time-ticks required to reach the remote node.	2 (default)
W/D	This field is for the P645R on the server side. Your Prestige 645R	

FIELD	DESCRIPTION	EXAMPLE
W/D Spoofing(min)	This field is for the P645R on the server side. Your Prestige 645R can spoof a response to a server's watchdog request after the connection is dropped. In this field, type in the time (number of minutes) that you want your Prestige 645R to spoof the watchdog response.	
SAP/RIP Timeout (min)	This field indicates the amount of time that you want your Prestige to maintain the SAP and RIP entries learned from this remote node in its internal tables after the connection has been dropped. If this information is retained, then your Prestige will not have to get the SAP information when the line is brought back up. Enter the time (number of minutes) in this field.	
Dial - On - Query	This field is necessary for your Prestige on the client side. When set to **Yes**, any Get Service SAP or RIP broadcasts will trigger your Prestige to make a call to that remote mode.	**No**
Once you have completed filling in the Network Layer Options Menu, press [ENTER] to return to menu 11.1. Then press [ENTER] at the message [Press ENTER to Confirm] to save your configuration, press [ESC] to cancel.		

6.4.2 IPX Static Route Setup

Similar to IP, IPX static routes tell the Prestige 645R how to reach servers beyond a remote node before a connection to that remote node is established.

From menu 12, select 2 to bring up **Menu 12.2 IPX Static Route Setup**, then select one of the IPX Static Routes to open **Menu 12.2.1 - Edit IPX Static Route**, as shown next.



```
                      Menu 12.2.1 - Edit IPX Static Route

                    Route #= 3
                    Server Name= ?
                    Active= Yes
                    Network #= ?
                    Node #= 000000000001
                    Socket #= 0451
                    Type #= 0004
                    Hop Count= 2
                    Tick Count= 3
                    Gateway Node= 1



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

Figure 6-6 Menu 12.2.1 - Edit IPX Static Route

The following table contains the instructions on how to configure the Edit IP Static Route Menu.

Table 6-3 Edit IPX Static Route Menu Fields

FIELD	DESCRIPTION
Route #	The number of this static route that you chose in menu 12.2.
Server Name	In this field, enter the name of the server. This must be the *exact* name configured in the NetWare server**.**
Active	Use the [SPACE BAR] to select **Yes** to activate or **No** to deactivate this IPX static route.
Network #	This field contains the internal network number of the remote server that you wish to access. [00000000] or [FFFFFFFF] are reserved.
Node #	This field contains the address of the node on which the server resides. If you are using a Novell IPX implementation, this value is [000000000001].
Socket #	This field contains the socket number on which the server will receive service requests. The default for this field is hex [0451].
Type #	This field identifies the type of service the server provides. The default for this field is hex [0004].
Gateway Node	In this field, enter the number of the remote node that is the gateway for this static route.
Hop Count and Tick Count	These two fields have the same meaning as those in the Ethernet setup.

Once you have completed filling in the menu, press [ENTER] at the message [Press ENTER to Confirm…] to save your configuration, or press [ESC] to cancel.

Chapter 7
Bridging Setup

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

7.1 Bridging in General

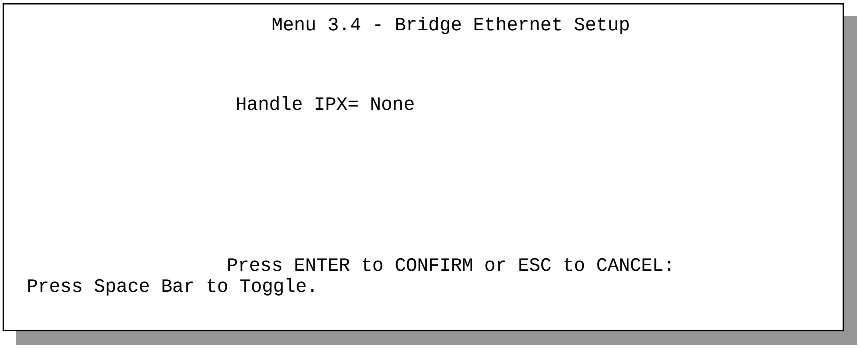
Bridging bases the forwarding decision on the MAC (Media Access Control), or hardware address, while routing does it on the network layer (IP or IPX) address. Bridging allows the Prestige 645R to transport packets of network layer protocols that the Prestige 645R does not route, e.g., SNA, from one network to another. The caveat is that, compared to routing, bridging generates more traffic for the same network layer protocol and it also demands more CPU cycles and memory.

For efficiency reasons, do *not* turn on bridging unless you need to support protocols other than IP and IPX on your network. For IP and IPX, enable the respective routing if you need it; do not bridge what the Prestige 645R can route.

7.2 Bridge Ethernet Setup

Basically, all non-local packets are bridged to the WAN; however, your Prestige 645R applies special handling for certain IPX packets to reduce the number of calls, depending on the setting of the **Handle IPX** field.

From **Menu 3 - Ethernet Setup**, enter 4 to bring up **Menu 3.4 - Bridge Ethernet Setup** as shown next.



```
                             Menu 3.4 - Bridge Ethernet Setup



                         Handle IPX= None








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

Figure 7-1 Menu 3.4 - Bridge Ethernet Setup

The following table describes how to configure the **Handle IPX** field in menu 3.4.

Table 7-1 Bridge Ethernet Setup Menu - Handle IPX Field Configuration

HANDLE IPX FIELD OPTIONS	DESCRIPTION
None	When there is no IPX traffic on the LAN or when you do not want to apply any special handling for IPX.
Client	When there are only client computers on the LAN. RIP and SAP (Service Advertising Protocol) response packets will not trigger calls.
Server	When there are only IPX servers on the LAN. No RIP or SAP packets will trigger calls. In addition, during the time when the line is down, your Prestige 645R will reply to watchdog messages from the servers on behalf of remote clients. The period of time that your Prestige 645R will do this is linked to the Ethernet Address Timeout parameter in each remote node (see Remote Node Configuration). When a remote Ethernet address is aged out, there is no need to maintain its connection to the IPX server.

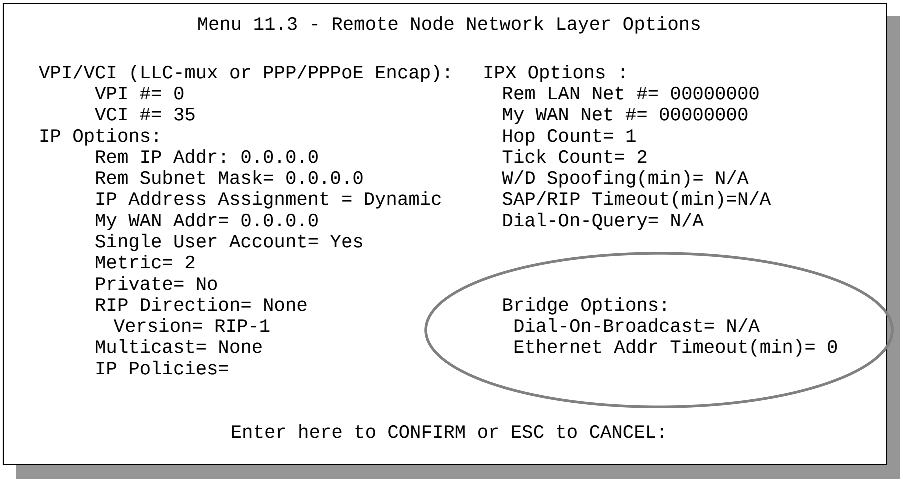
7.2.1 Remote Node Bridging Setup

Follow the procedure in *Chapter 5* to configure the protocol-independent parameters in **Menu 11.1 - Remote Node Profile**. For bridging-specific parameters, you need to configure **Menu 11.3 - Remote Node Network Layer Options**.

To set up **Menu 11.3 - Remote Node Network Layer Options** follow these steps:

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

Step 2. Move the cursor to the **Edit IP/IPX/Bridge** field, then press the [SPACE BAR] to select **Yes** and press [ENTER] to open **Menu 11.3 - Network Layer Options**.



```
                 Menu 11.3 - Remote Node Network Layer Options

   VPI/VCI (LLC-mux or PPP/PPPoE Encap):   IPX Options :
        VPI #= 0                             Rem LAN Net #= 00000000
        VCI #= 35                            My WAN Net #= 00000000
   IP Options:                               Hop Count= 1
        Rem IP Addr: 0.0.0.0                 Tick Count= 2
        Rem Subnet Mask= 0.0.0.0             W/D Spoofing(min)= N/A
        IP Address Assignment = Dynamic      SAP/RIP Timeout(min)=N/A
        My WAN Addr= 0.0.0.0                 Dial-On-Query= N/A
        Single User Account= Yes
        Metric= 2
        Private= No
        RIP Direction= None                  Bridge Options:
          Version= RIP-1                      Dial-On-Broadcast= N/A
        Multicast= None                       Ethernet Addr Timeout(min)= 0
        IP Policies=


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

Figure 7-2 Menu 11.3 - Remote Node Bridging Options

The following table describes the bridging-specific parameters in **Menu 11.1 - Remote Node Profile** and **Menu 11.3 - Remote Node Network Layer Options** menus.

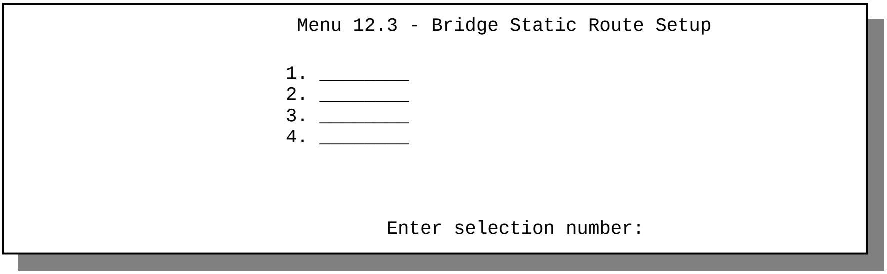
Table 7-2 P645R Remote Node Network Layers Menu Bridge Options

FIELD	DESCRIPTION
Bridge (menu 11.1)	Make sure this field is set to **Yes**.
Edit IP/IPX/Bridge (menu 11.1)	Press the [SPACE BAR] to change it to **Yes** and press [ENTER] to go to **Menu 11.3 –Remote Node Network Layer Options**.
Dial-On-Broadcast (menu 11.3)	This field is necessary for your Prestige on the caller side LAN. When set to **Yes**, any broadcasts coming from the LAN will trigger your Presige to make a call to this remote node. If it is set to **No**, your Prestige will not make the outgoing call.
Ethernet Addr Timeout (min) (menu 11.3)	In this field, enter the time (number of minutes) that you wish your Prestige 645R to retain the Ethernet Addr information in its internal tables while the line is down. If this information is retained, your Prestige 645R will not have to recompile the tables when the line is brought back up.

Once you have completed filling in the Network Layer Options Menu, press [ENTER] to return to menu 11.1. Then press [ENTER] at the message [Press ENTER to Confirm…] to save your configuration, or press [ESC] to cancel.

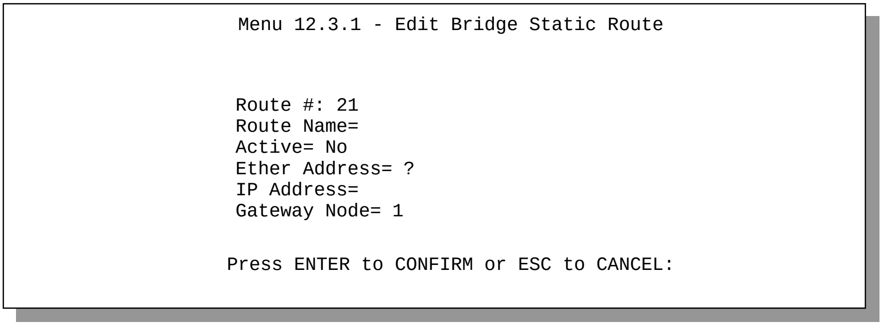
7.3 Bridge Static Route Setup

Similar to network layer static routes, a bridging static route tells the Prestige 645R about the route to a node before a connection is established. You configure bridge static routes in menu 12.3.1, by pressing 3 in menu 12 and then selecting one of the bridge static routes as shown below.



```
                    Menu 12.3 - Bridge Static Route Setup

                   1. ________
                   2. ________
                   3. ________
                   4. ________



                          Enter selection number:
```

Figure 7-3 Menu 12.3 - Bridge Static Route Setup



```
                    Menu 12.3.1 - Edit Bridge Static Route



                    Route #: 21
                    Route Name=
                    Active= No
                    Ether Address= ?
                    IP Address=
                    Gateway Node= 1


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

Figure 7-4 Menu 12.3.1 - Edit Bridge Static Route

The following table describes the Bridge Static Route Menu.

Table 7-3 Bridge Static Route Menu Fields

FIELD	DESCRIPTION
Route Name	Enter a name for the bridge static route for identification purposes.
Active	Use the [SPACE BAR] to select **Yes** to activate or **No** to deactivate the static route.
Ether Address	Enter the MAC address of the destination machine that you wish to bridge the packets to.
IP Address	If available, enter the IP address of the destination machine that you wish to bridge the packets to.
Gateway Node	Enter the number of the remote node that is the gateway of this static route.
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.	

Part III:

Advanced Management

Advanced Management provides information on Filter Configuration, SNMP Configuration, System Maintenance, Firmware and Configuration and Firmware File Maintenance, IP Policy Routing, Call Scheduling and Troubleshooting. Also included are Appendices, a Glossary and the Index.

Chapter 8
Filter Configuration

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

8.1 About Filtering

Your Prestige uses filters to decide whether or not to allow passage of a packet. Data filters are divided into incoming and outgoing filters, depending on the direction of the packet relative to a port. These filters are further subdivided into device and protocol filters, which are discussed later. 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 **PPPoE** encapsulation. Outgoing packets must undergo data filtering before they encounter call filtering as shown in the following figure.

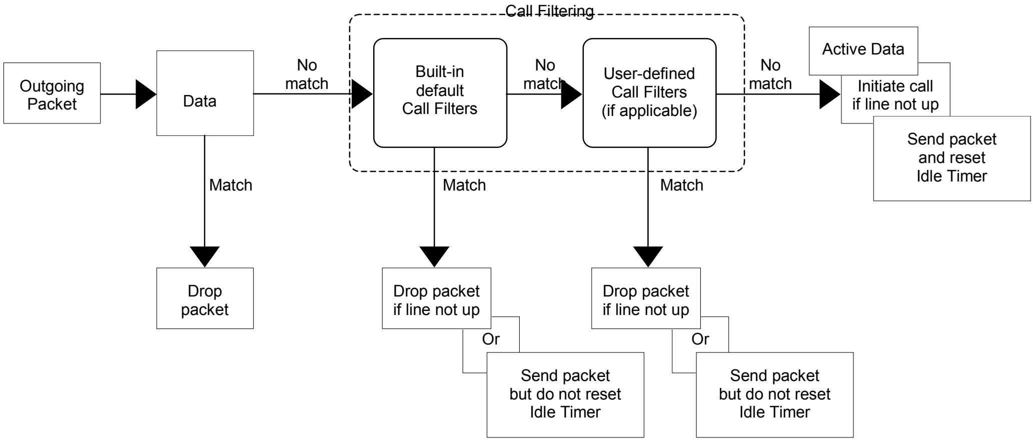

Call Filtering
Outgoing Packet
Data
No match
Built-in default Call Filters
No match
User-defined Call Filters (if applicable)
No match
Active Data
Initiate call if line not up
Send packet and reset Idle Timer
Match
Match
Match
Drop packet
Drop packet if line not up
Or
Send packet but do not reset Idle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

Figure 8-1 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.

The following sections describe how to configure filter sets.

The Filter Structure of the Prestige

A filter set consists of one or more filter rules. Usually, you would group related rules, 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.

Six 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 and section *8.4* also has example.

The factory configured filters in SMT menu 21.3 are designed to block incoming telnet from the WAN (DSL) port. Do not configure SMT menu 3.1 filter rules to block all telnet from the Ethernet. This would block the telnet connection from your computer to the Prestige.

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

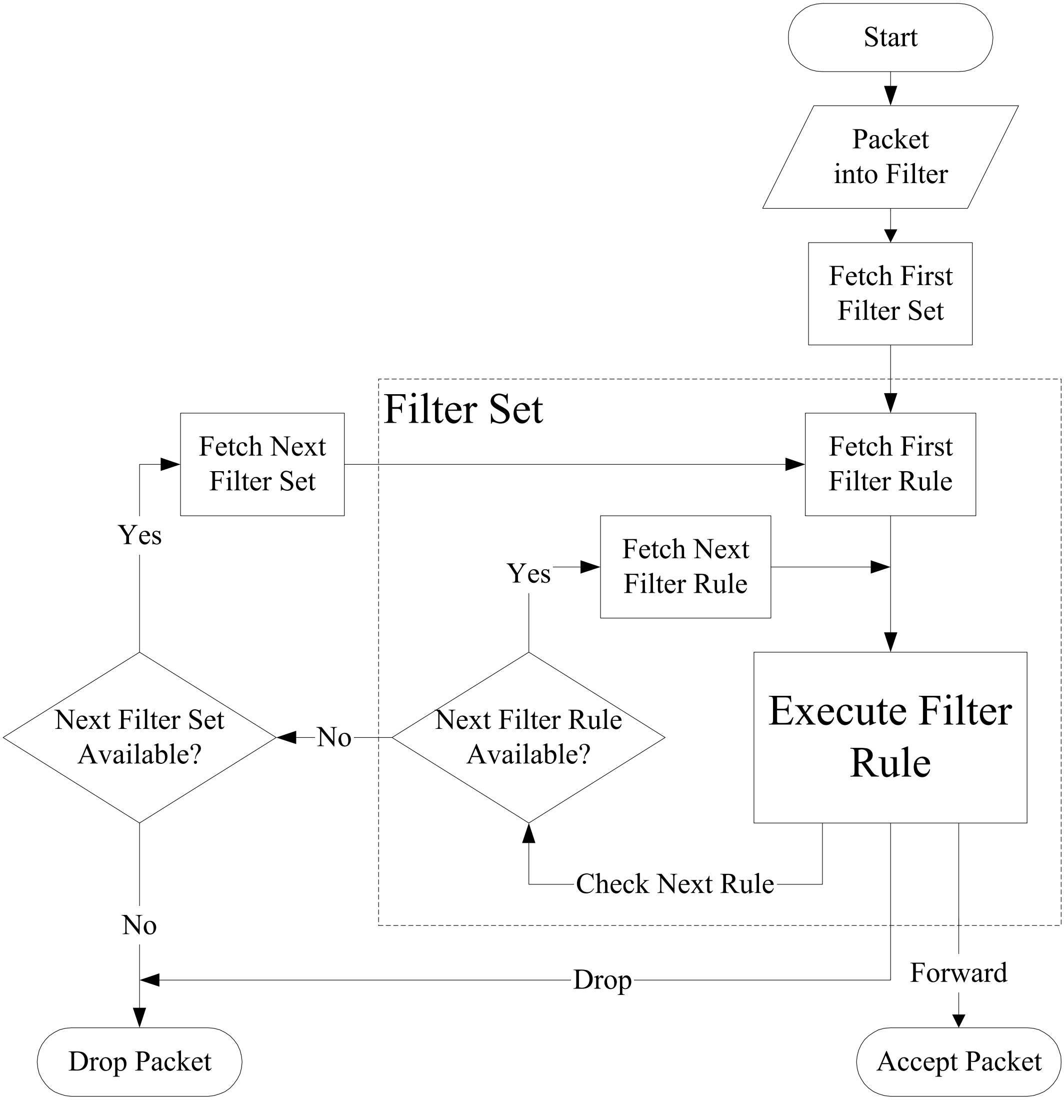


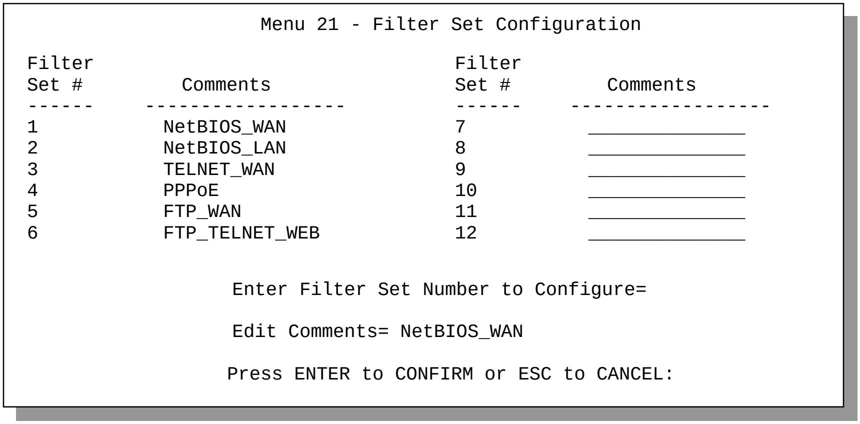
Figure 8-2 Filter Rule Process

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.

8.2 Configuring a Filter Set

To configure a filter set, follow this procedure:

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



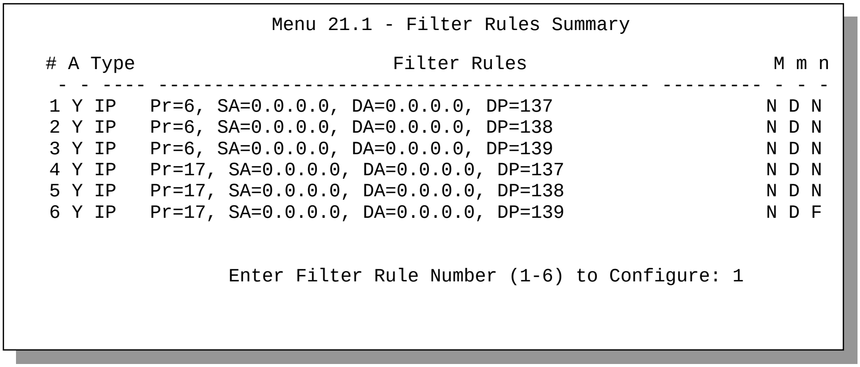
```
                    Menu 21 - Filter Set Configuration

Filter                                Filter
Set #         Comments                Set #         Comments
------     ------------------         ------     ------------------
1            NetBIOS_WAN              7            ______________
2            NetBIOS_LAN              8            ______________
3            TELNET_WAN               9            ______________
4            PPPoE                    10           ______________
5            FTP_WAN                  11           ______________
6            FTP_TELNET_WEB           12           ______________


                  Enter Filter Set Number to Configure=

                  Edit Comments= NetBIOS_WAN

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

Figure 8-3 Menu 21 - Filter Set Configuration

Step 2. Enter the index of the filter set you wish to configure (no. 1-12) and press [ENTER]**.**

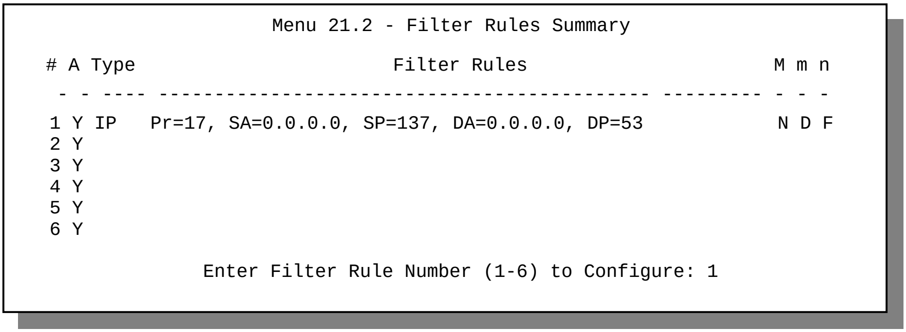
Step 3. Enter a descriptive name or comment in the Edit Comments field and press [ENTER].

Step 4. Press [ENTER] at the message: [Press ENTER to confirm] to open **Menu 21.1 - Filter Rules Summary**.



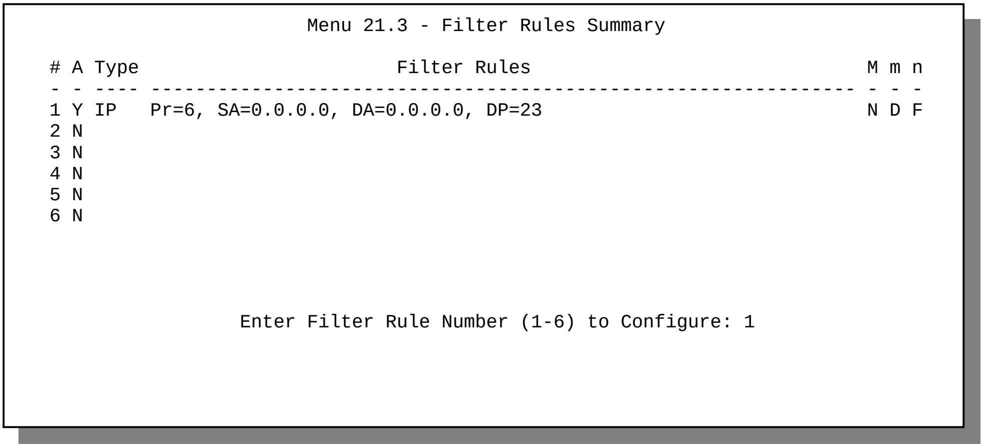
```
                       Menu 21.1 - Filter Rules Summary

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


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

Figure 8-4 NetBIOS_WAN Filter Rules Summary



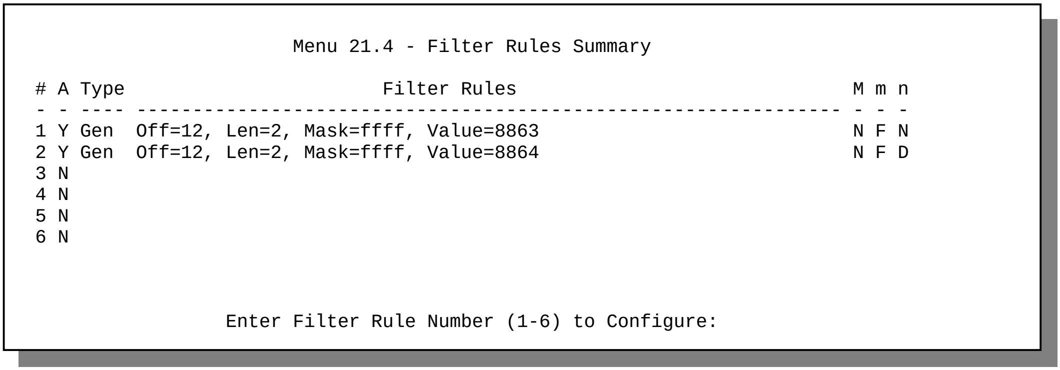
```
                       Menu 21.2 - Filter Rules Summary

   # 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: 1
```

Figure 8-5 NetBIOS _LAN Filter Rules Summary



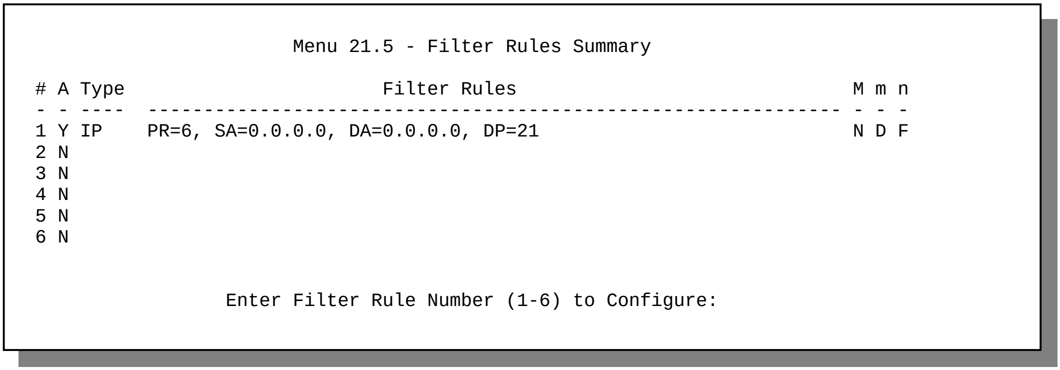
```
                         Menu 21.3 - Filter Rules Summary

    # 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 F
    2 N
    3 N
    4 N
    5 N
    6 N



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

Figure 8-6 Telnet Filter Rules Summary



```
                       Menu 21.4 - Filter Rules Summary

# A Type                       Filter Rules                              M m n
- - ---- --------------------------------------------------------------- - - -
1 Y Gen  Off=12, Len=2, Mask=ffff, Value=8863                            N F N
2 Y Gen  Off=12, Len=2, Mask=ffff, Value=8864                            N F D
3 N
4 N
5 N
6 N



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

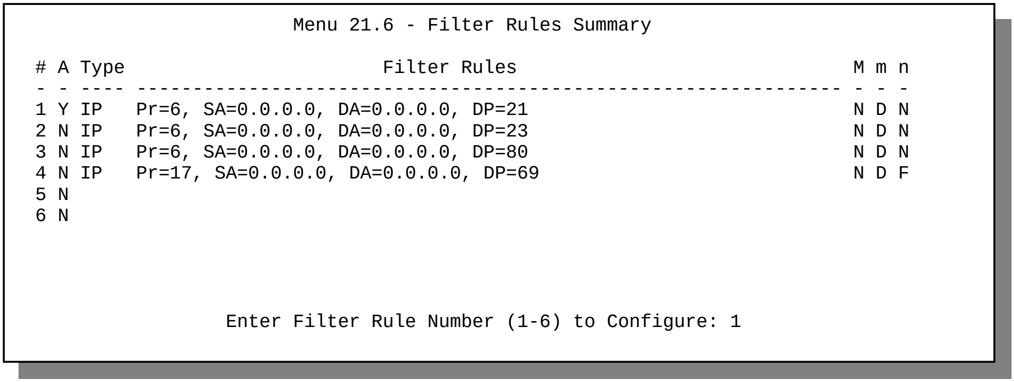
Figure 8-7 PPPoE Filter Rules Summary



```
                       Menu 21.5 - Filter Rules Summary

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


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

Figure 8-8 FTP _WAN Filter Rules Summary

In filter rule 6, FTP_TELNET_WEB, the WEB means that HTTP and TFTP traffic are blocked.



```
                       Menu 21.6 - Filter Rules Summary

# A Type                       Filter Rules                              M m n
- - ---- --------------------------------------------------------------- - - -
1 Y IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=21                             N D N
2 N IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=23                             N D N
3 N IP   Pr=6, SA=0.0.0.0, DA=0.0.0.0, DP=80                             N D N
4 N IP   Pr=17, SA=0.0.0.0, DA=0.0.0.0, DP=69                            N D F
5 N
6 N



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

Figure 8-9 FTP_TELNET_WEB Filter Rules Summary

8.2.1 Filter Rules Summary Menu

This screen shows a summary of the existing rules in an example filter set. The following tables contain a brief description of the abbreviations used in menu 21.1.

Table 8-1 Abbreviations Used in the Filter Rules Summary Menu

ABBREVIATIONS	DESCRIPTION	DISPLAY
#	Refers to the filter rule number (1-6).	
A	Shows whether the rule is active or not.	[Y] means the filter rule is active. [N] means the filter rule is inactive.
Type	Refers to the type of filter rule.	[GEN] = Generic. [IP] = TCP/IP.
Filter Rules	The filter rule parameters will be displayed here (see below).	
M	Refers to **More**. **More** in a set behaves like a logical AND i.e., the set is only matched if ALL rules in it are matched. [Y] means an action can not yet be taken as there are more rules to	[Y] means there are more rules to check. [N] means there are no more rules to check.

ABBREVIATIONS	DESCRIPTION	DISPLAY
M	Refers to **More**. **More** in a set behaves like a logical AND i.e., the set is only matched if ALL rules in it are matched. [Y] means an action can not yet be taken as there are more rules to check, which are concatenated with the present rule to form a rule chain. When the rule chain is complete an action can be taken. [N] means you can now specify an action to be taken i.e., forward the packet, drop the packet or check the next rule. For the latter, the next rule is independent of the rule just checked. If More is **Yes**, then **Action Matched** and **Action Not Matched** will be **N/A**.	[Y] means there are more rules to check. [N] means there are no more rules to check.
M	Refers to **Action Matched**. [F] means to forward the packet immediately and skip checking the remaining rules.	[F] means to forward the packet. [D] means to drop the packet. [N] means check the next rule.
N	Refers to **Action Not Matched.** [F] means to forward the packet immediately and skip checking the remaining rules.	[F] means to forward the packet. [D] means to drop the packet. [N] means check the next rule.

The protocol dependent filter rules abbreviations are listed as follows:

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

Table 8-2 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

- Abbreviations Used If Filter Type Is IPX

Table 8-3 Abbreviations Used If Filter Type Is IPX

ABBREVIATION	DESCRIPTION
PT	IPX Packet Type
SS	Source Socket
DS	Destination Socket

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

Table 8-4 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.

8.3 Configuring a Filter Rule

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

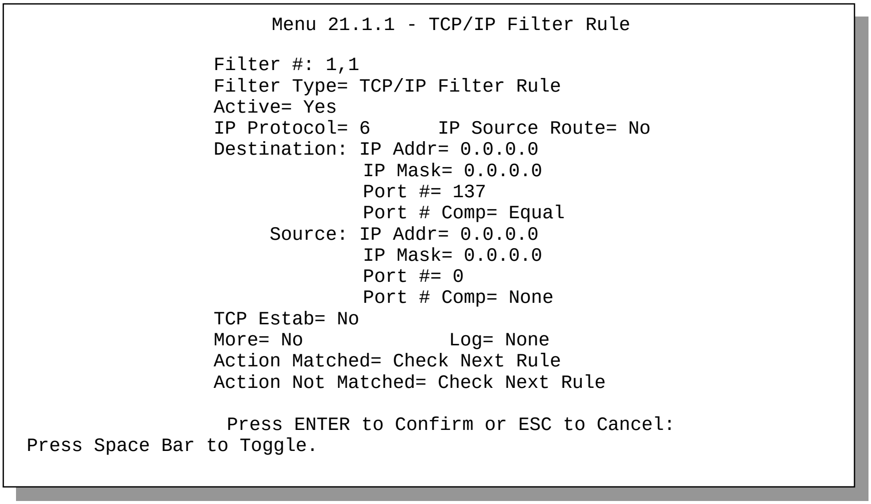
There are three types of filter rules: **TCP/IP**, **IPX** and **Generic**. Depending on the type of rule, the parameters below the type will be different. Use the [SPACE BAR] to select the type of rule that you wish to create in the **Filter Type** field and press [ENTER] to open the respective menu.

To speed up filtering, all rules in a filter set must be of the same class, 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 filters field or vice versa, the Prestige will warn you and will not allow you to save.

8.3.1 TCP/IP Filter Rule

This section shows you how to configure a TCP/IP filter rule. TCP/IP rules allow you to base the rule on the fields in the IP and the upper layer protocol, 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 #= 0
                              Port # Comp= None
                 TCP Estab= No
                 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 8-10 Menu 21.1.1 - TCP/IP Filter Rule

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

Table 8-5 TCP/IP Filter Rule Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Active	Use **Yes** to activate and **No** to deactivate the filter rule.	**Yes**
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	6
IP Source Route	IP source route is an optional header that dictates the route an IP packet takes from its source to its destination. If **Yes**, the rule applies to any packet with an IP source route. The majority of IP packets do not have source route.	**No**

FIELD	DESCRIPTION	EXAMPLE
Destination: IP Addr	Enter the destination IP Address of the packet you wish to filter. This field is a don't-care if it is 0.0.0.0.	0.0.0.0
Destination: IP Mask	Enter the IP subnet mask to apply to the Destination: IP Addr.	255.255.255.1
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 a don't-care if it is 0.	1378
Destination: Port # Comp	Select the comparison (either **None**, **Less**, **Greater**, **Equal** or **Not Equal**) to apply to the destination port in the packet against the value given in Destination: Port #.	**Greater**
Source: IP Addr	Enter the source IP Address of the packet you wish to filter. This field is a don't-care if it is 0.0.0.0.	0.0.0.0
Source: IP Mask	Enter the IP subnet mask to apply to the Source: IP Addr.	
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 a don't-care if it is 0.	0
Source: Port # Comp	Select the comparison to apply to the source port in the packet against the value given in Source: Port #. Choose from **None, Less, Greater, Equal** and **Not Equal**.	**None**
TCP Estab	This field is applicable only when IP Protocol field is 6, TCP. If **Yes**, the rule matches only established TCP connections; otherwise the rule matches all TCP packets.	**No**
More	If **Yes**, a matching packet is passed to the next filter rule before an action is taken; else the packet is disposed of according to the action fields. If More is **Yes**, then Action Matched and Action Not Matched will be **N/A**.	**No**
Log	Select the logging option from the following: **None** – No packets will be logged. **Action Matched** - Only packets that match the rule parameters will be logged. **Action Not Matched** - Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.	**None**
Action Matched	Select the action for a matching packet. Choices are **Check Next Rule**, **Forward** and **Drop**.	**Check Next Rule**

FIELD	DESCRIPTION	EXAMPLE
Action Not Matched	Select the action for a packet not matching the rule. Choices are: **Check Next Rule**, **Forward** and **Drop**.	**Drop**
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 in **Menu 21.1 - Filter Rules Summary**.		

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

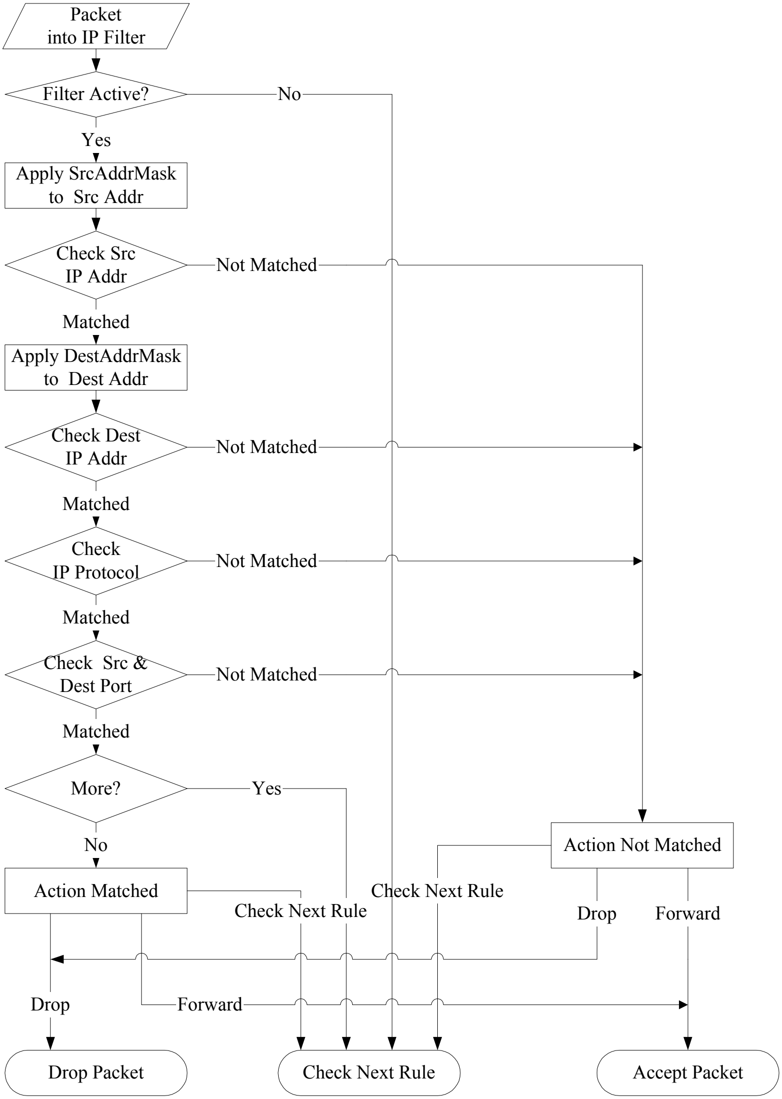


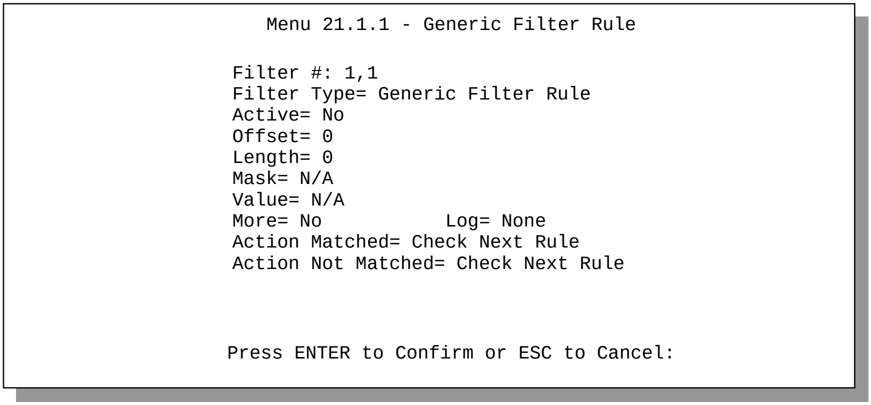
Figure 8-11 Executing an IP Filter

8.3.2 Generic Filter Rule

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

For generic rules, the Prestige treats a packet as a byte stream as opposed to an IP 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 and press [ENTER] to open **Menu 21.1.1 - Generic Filter Rule**, as shown next.



```
                    Menu 21.1.1 - Generic Filter Rule

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



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

Figure 8-12 Menu 21.1.1 - Generic Filter Rule

The following table describes the fields in the generic filter rule menu.

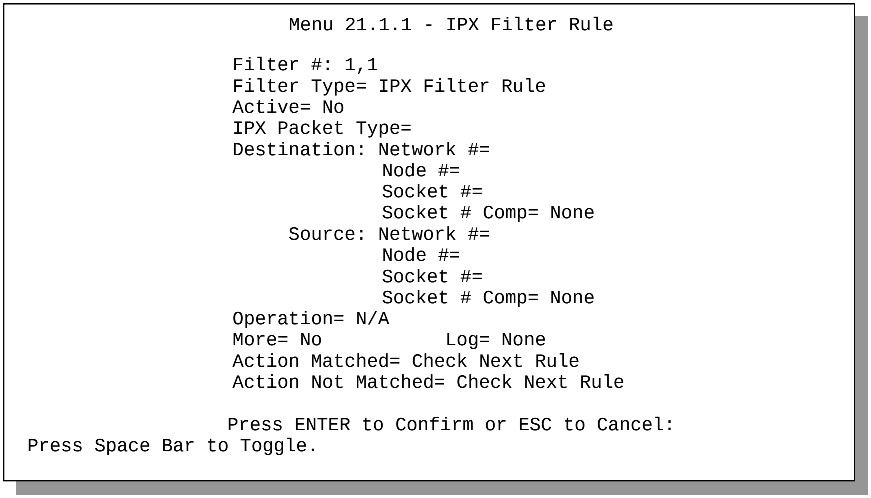
Table 8-6 Generic Filter Rule Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Filter #	This is the filter set, filter rule co-ordinates, i.e., 1,1 refers to the first filter set and the first filter rule of that set.	1,1
Filter Type	Use the [SPACE BAR] to select a rule type from **Generic Filter Rule**, **TCP/IP Filter Rule** and **IPX Filter Rule**. Parameters displayed below each type will be different.	**Generic Filter Rule**
Active	Select **Yes** to turn on the filter rule or **No** to turn the filter rule off.	**Yes**
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; otherwise the packet is disposed of according to the action fields. If More is **Yes**, then Action Matched and Action Not Matched will be **N/A**.	**Yes**
Log	Select the logging option from the following: **None** – No packets will be logged. **Action Matched** - Only packets that match the rule parameters will be logged. **Action Not Matched** - Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.	**None**
Action Matched	Select the action for a matching packet: **Check Next Rule**, **Forward** or **Drop**.	**Forward**
Action Not Matched	Select the action for a packet not matching the rule: **Check Next Rule**, **Forward or Drop**.	**Drop**
Once you have completed filling in **Menu 21.1.1 - Generic Filter Rule**, press [ENTER] at the message [Press ENTER to Confirm] to save your configuration, or press [ESC] to cancel. This data will now be displayed on **Menu 21.1 - Filter Rules Summary**.		

8.3.3 Novell IPX Filter Rule

This section shows you how to configure an IPX filter rule. IPX filters allow you to base the rules on the fields in the IPX headers.

To configure an IPX rule, select **IPX Filter Rule** from the **Filter Type** field and press [ENTER] to open **Menu 21.1.1 IPX Filter Rule**, as shown in the figure below.



```
                         Menu 21.1.1 - IPX Filter Rule

                    Filter #: 1,1
                    Filter Type= IPX Filter Rule
                    Active= No
                    IPX Packet Type=
                    Destination: Network #=
                                 Node #=
                                 Socket #=
                                 Socket # Comp= None
                         Source: Network #=
                                 Node #=
                                 Socket #=
                                 Socket # Comp= None
                    Operation= 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 8-13 Menu 21.1.1 - IPX Filter Rule

The following table describes the IPX Filter Rule.

Table 8-7 IPX Filter Rule Menu Fields

FIELD	DESCRIPTION
IPX Packet Type	Enter the IPX packet type (1-byte in hexadecimal) you wish to filter. The popular types are (in hexadecimal): 01 - RIP 04 - SAP 05 - SPX (Sequenced Packet eXchange) 11 - NCP (NetWare Core Protocol) 14 - Novell NetBIOS

FIELD	DESCRIPTION
Destination/Source Network #	Enter the destination/source network numbers (4-byte in hexadecimal) of the packet that you wish to filter.
Destination/Source Node #	Enter the destination/source node number (6-byte in hexadecimal) of the packet you wish to filter.
Destination/Source Socket #	Enter the destination/source socket number (2-byte in hexadecimal) of the packets that you wish to filter.
Destination/Source Socket # Comp	Select the comparison you wish to apply to the destination/source socket in the packet against that specified above. Choose from **Equal**, **Not Equal**, **Less**, **Greater** or **None**.
Operation	This field is applicable only if one of the Socket # fields is 0452 or 0453 indicating SAP and RIP packets. There are seven options for this field that specify the type of the packet. ● **None** ● **RIP Request** ● **RIP Response** ● **SAP Request** ● **SAP Response** ● **SAP Get Nearest Server Request** ● **SAP Get Nearest Server Response**
Once you have completed filling in **Menu 21.1.1 - IPX 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**.	

8.4 Example Filter

Let's look at a TELNET_WAN filter that block s outside users from telnetting into the Prestige. Please see the supporting CD that came with your Prestige for more example filters. This filter is designed.

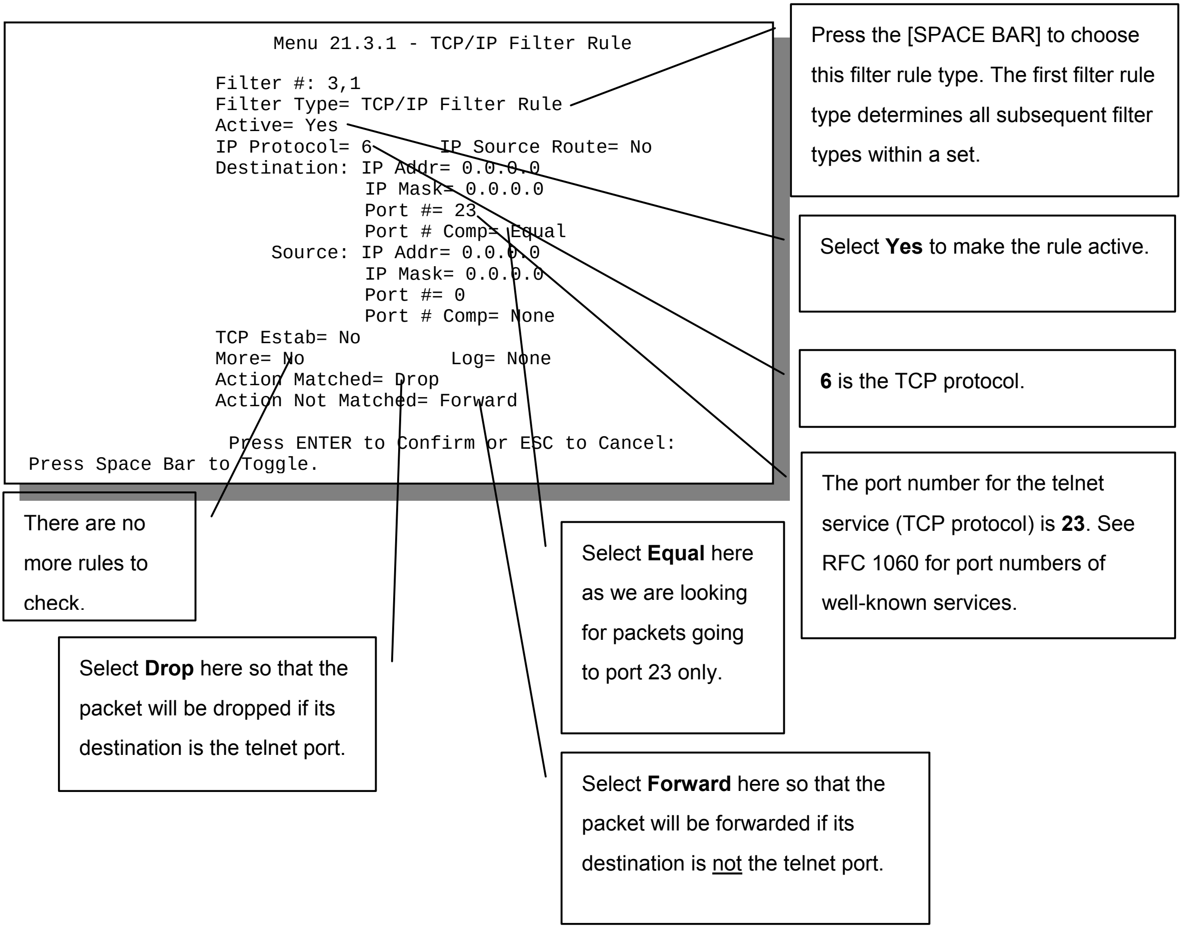
Step 1. Enter 21 from the main menu to open **Menu 21 - Filter Set Configuration**.

Step 2. Enter the index of the filter set you wish to configure (for example, 3) and press [ENTER].

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

Step 4. Press [ENTER] at the message: [Press ENTER to confirm] to open **Menu 21.3 - Filter Rules Summary**.

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



```
                      Menu 21.3.1 - TCP/IP Filter Rule

                 Filter #: 3,1
                 Filter Type= TCP/IP Filter Rule
                 Active= Yes
                 IP Protocol= 6      IP Source Route= No
                 Destination: IP Addr= 0.0.0.0
                              IP Mask= 0.0.0.0
                              Port #= 23
                              Port # Comp= Equal
                      Source: IP Addr= 0.0.0.0
                              IP Mask= 0.0.0.0
                              Port #= 0
                              Port # Comp= None
                 TCP Estab= No
                 More= No              Log= None
                 Action Matched= Drop
                 Action Not Matched= Forward

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

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

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

6 is the TCP protocol.

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

There are no more rules to check.

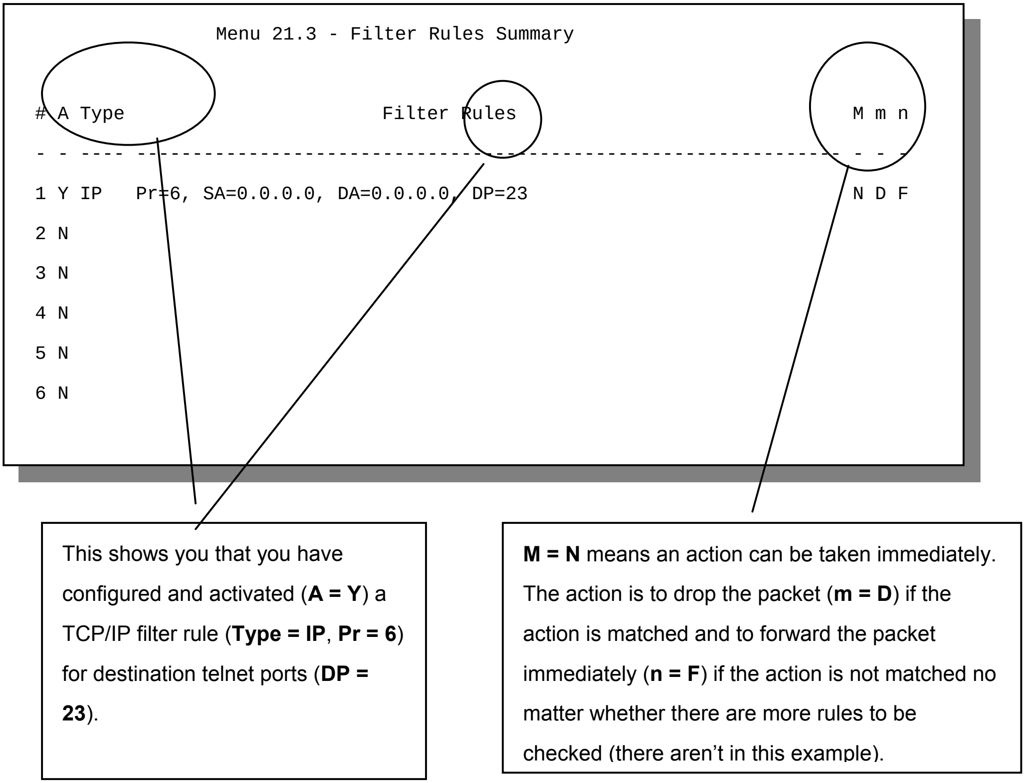
Select **Equal** here as we are looking for packets going to port 23 only.

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

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

Figure 8-14 Example Filter – Menu 21.3.1

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



```
                   Menu 21.3 - 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
```

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

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

Figure 8-15 Example Filter Rules Summary – Menu 21.3

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

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

Step 2. Select a remote node number and press [ENTER].

Step 3. Go to the **Edit Filter Sets** field, press the [SPACE BAR] to select **Yes** and press [ENTER].

This brings you to menu 11.5. Apply the TELNET_WAN filter set (filter set 3) as shown later.

8.5 Filter Types and SUA

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

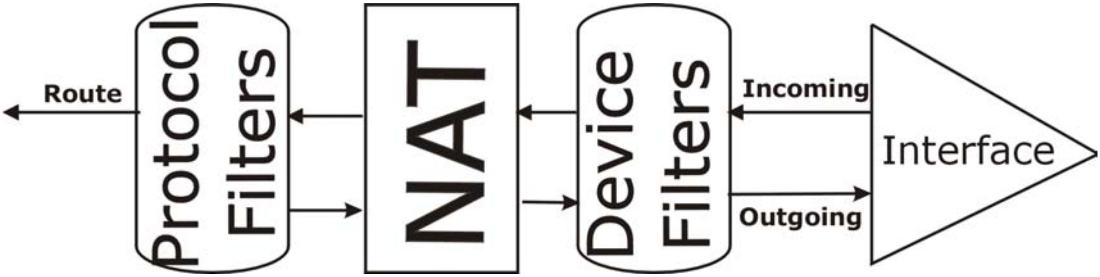


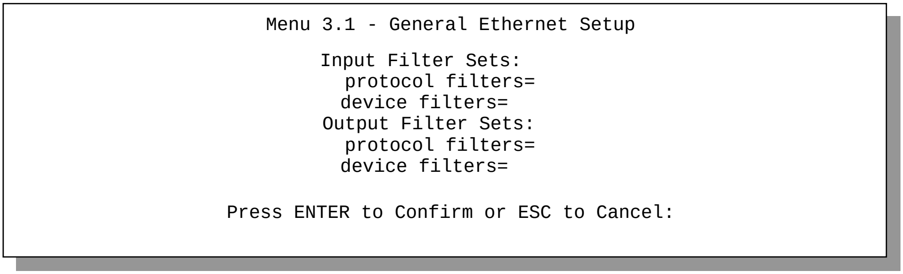
Figure 8-16 Protocol and Device Filter Sets

8.6 Applying a Filter and Factory Defaults

This section shows you where to apply the filter(s) after you design it (them). Six sets of factory default filter rules have been configured in menu 21 to prevent NetBIOS traffic from triggering calls, prevent incoming telnetting, forward PPPoE packets, and prevent incoming FTP and HTTP.

8.6.1 Ethernet traffic

You seldom need to filter Ethernet traffic; however, the filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to menu 3.1 (shown below) and enter the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by entering their numbers separated by commas, for example, 2, 4, 7, 9. The Prestige does not have any of the default filters applied to the Ethernet port when it is shipped.

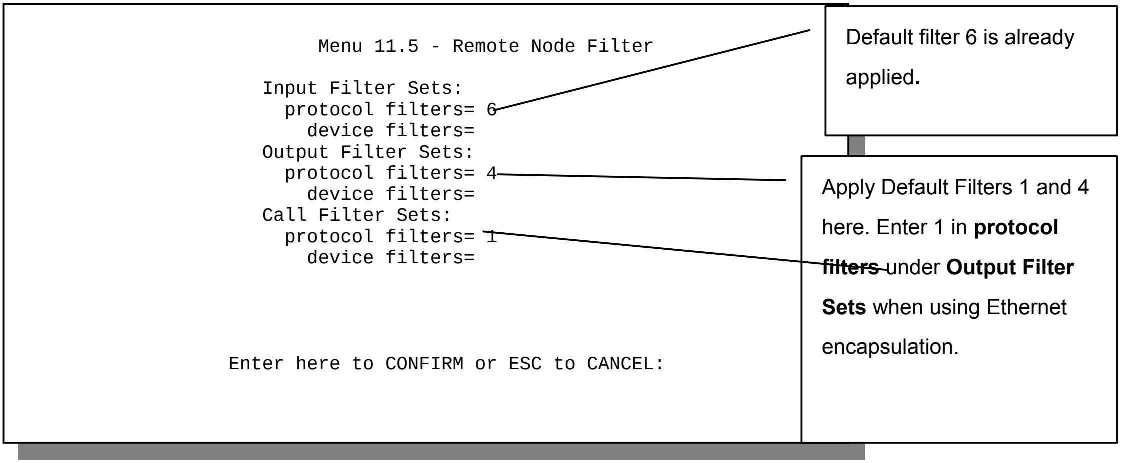


```
                 Menu 3.1 - General Ethernet Setup

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

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

Figure 8-17 Filtering Ethernet traffic

8.6.2 Remote Node Filters

Go to Menu 11.5 (shown below – note that call filter sets are only present for PPPoE encapsulation) and enter the number(s) of the filter set(s) as appropriate. You can cascade up to four filter sets by entering their numbers separated by commas. The factory default filter set, NetBIOS_WAN, can be applied in Menu 11.5 to block local NetBIOS traffic from triggering calls to the ISP (when you are using **PPPoE** encapsulation only). Enter “1” in the **protocol filters** field under **Call Filter Sets** when using PPPoE encapsulation and in **protocol filters** under **Output Filter Sets – protocol filters** when using Ethernet encapsulation**.** The factory default filter set “6”, FTP_TELNET_WEB, is inserted in the **protocol filters** field under **Input Filter Sets** in menu 11.5 to block FTP, Telnet, HTTP and TFTP traffic from coming into the WAN port. Filter set “4”, PPPoE, blocks PPP connections from the WAN Port. Apply them as shown in the following figure.



```
                    Menu 11.5 - Remote Node Filter

               Input Filter Sets:
                 protocol filters= 6
                   device filters=
               Output Filter Sets:
                 protocol filters= 4
                   device filters=
               Call Filter Sets:
                 protocol filters= 1
                   device filters=



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

Default filter 6 is already applied**.**

Apply Default Filters 1 and 4 here. Enter 1 in **protocol filters** under **Output Filter Sets** when using Ethernet encapsulation.

Figure 8-18 Filtering Remote Node Traffic (PPPoE Encapsulation)

Chapter 9
SNMP Configuration

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

SNMP is only available if TCP/IP is configured.

9.1 About SNMP

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

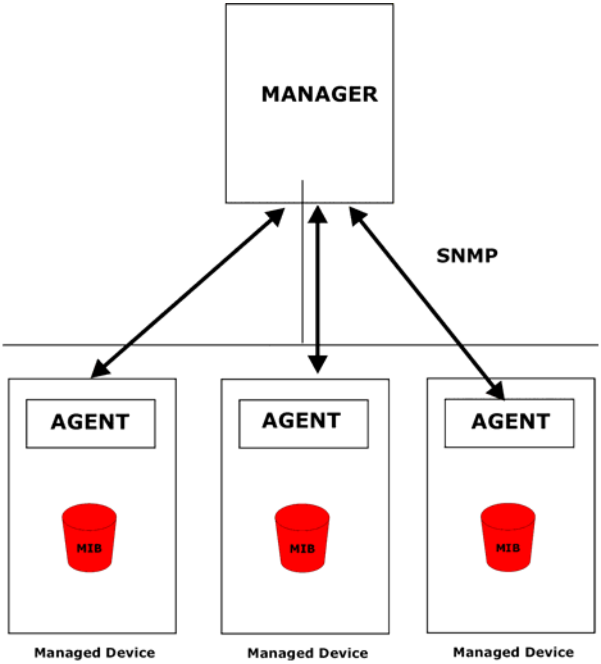


Figure 9-1 SNMP Management Model

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. The manager issues a request and the agent returns responses using the following protocol operations:

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

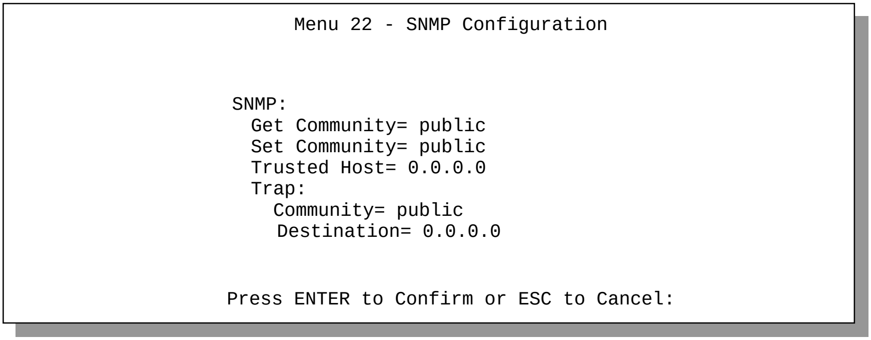
9.2 Supported MIBs

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).

9.3 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 9-2 Menu 22 — SNMP Configuration

The following table describes the SNMP configuration parameters.

Table 9-1 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.		

9.4 SNMP Traps

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

Table 9-2 SNMP Traps

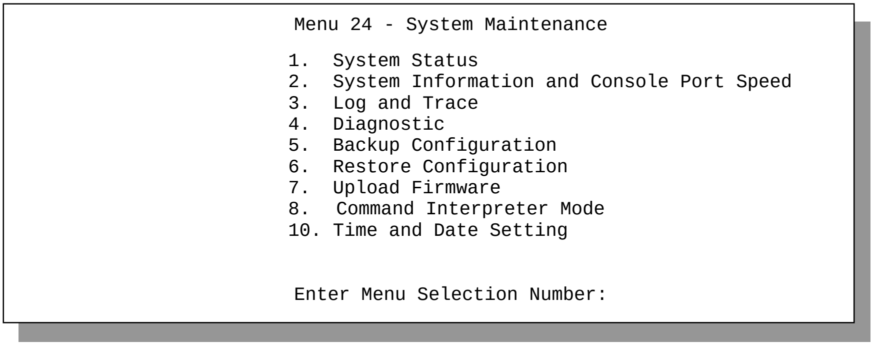
TRAP #	TRAP NAME	DESCRIPTION
1	coldStart (*defined in RFC-1215*)	A trap is sent after booting (power on).
2	warmStart (*defined in RFC-1215*)	A trap is sent after booting (software reboot).
3	linkUp (*defined in RFC-1215*)	A trap is sent with the port number.
4	authenticationFailure (*defined in RFC-1215*)	A trap is sent to the manager when receiving any SNMP get or set requirements with wrong community (password).
5	whyReboot (*defined in ZYXEL-MIB*)	A trap is sent with the reason of restart before rebooting when the system is going to restart (warmstart).
5a	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.).
5b	For fatal error :	A trap is sent with the message of the fatal code if the system reboots because of fatal errors.
6	linkDown (*defined in RFC-1215*)	A trap is sent with the port number when any of the links are down. See the following table.

Chapter 10
System Maintenance

This chapter covers the diagnostic tools that help you to maintain your Prestige.

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

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



```
                         Menu 24 - System Maintenance

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


                         Enter Menu Selection Number:
```

Figure 10-1 Menu 24 - System Maintenance

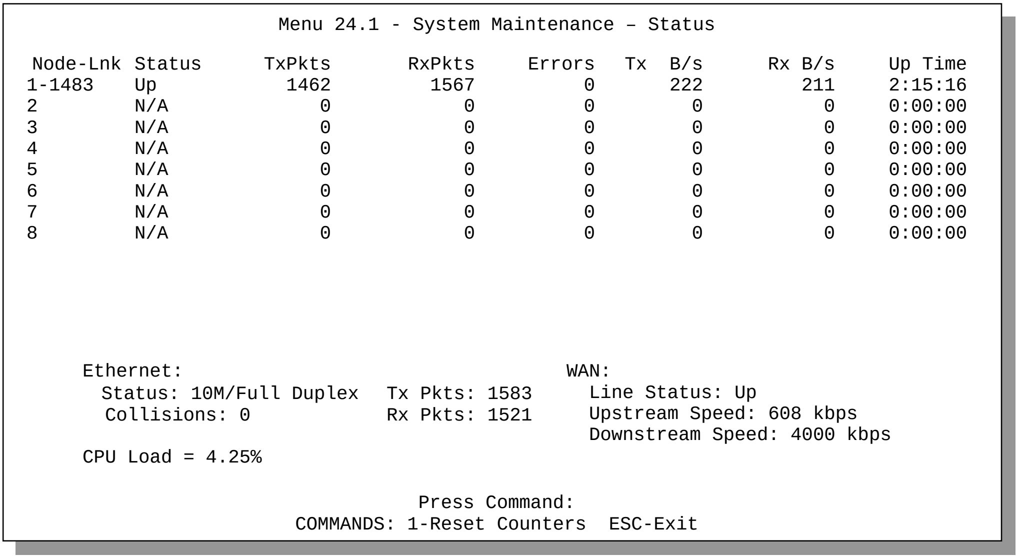
10.1 System Status

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

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

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

Please note that displaying this screen degrades system performance.



```
                        Menu 24.1 - System Maintenance – Status

  Node-Lnk Status      TxPkts       RxPkts     Errors   Tx  B/s      Rx B/s     Up Time
 1-1483   Up            1462         1567          0       222         211     2:15:16
 2        N/A              0            0          0         0           0     0:00:00
 3        N/A              0            0          0         0           0     0:00:00
 4        N/A              0            0          0         0           0     0:00:00
 5        N/A              0            0          0         0           0     0:00:00
 6        N/A              0            0          0         0           0     0:00:00
 7        N/A              0            0          0         0           0     0:00:00
 8        N/A              0            0          0         0           0     0:00:00




       Ethernet:                                          WAN:
         Status: 10M/Full Duplex   Tx Pkts: 1583            Line Status: Up
         Collisions: 0             Rx Pkts: 1521            Upstream Speed: 608 kbps
                                                            Downstream Speed: 4000 kbps
       CPU Load = 4.25%

                                    Press Command:
                         COMMANDS: 1-Reset Counters  ESC-Exit
```

Figure 10-2 Menu 24.1 - System Maintenance – Status

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

Table 10-1 System Maintenance - Status Menu Fields

FIELD	DESCRIPTION
Node-Lnk	This is the remote node index number and link type. Link types are: **PPP, ENET, 1483** and **PPPoE**.
Status	Shows the status of the remote node.
TxPkts	The number of packets transmitted to this remote node.
RxPkts	The number of packets received from this remote node.
Errors	The number of error packets on this connection.
Tx B/s	Shows the transmission rate in bytes per second.
Rx B/s	Shows the receiving rate in bytes per second.
Up Time	Time this channel has been connected to the remote node.
Ethernet	
Status	Shows the current status of the LAN.

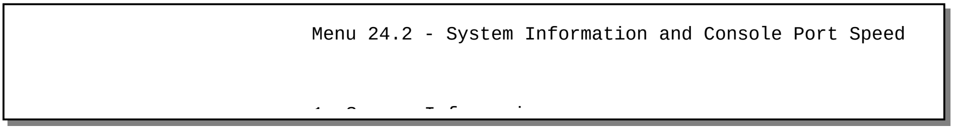
FIELD	DESCRIPTION
Tx Pkts	The number of transmitted packets to the LAN.
Rx Pkts	The number of received packets from the LAN.
Collision	Number of collisions.
WAN	
Line Status	Shows the current status of the ADSL line which can be **Up, Down, Wait for Init** or **Initializing**.
Upstream Speed	Shows the ADSL line upstream speed.
Downstream Speed	Shows the ADSL line downstream speed
CPU Load	Specifies the percentage of CPU utilization.
Press Command	
1 - Reset Counters	Press 1 to reset all the above statistics to 0.
ESC - Exit	Press [ESC] to go back to menu 24.

10.2 System Information and Console Port speed

System information list important data about your Prestige and its firmware.

Console port speed is included for use by qualified technical support personnel, do not configure it.

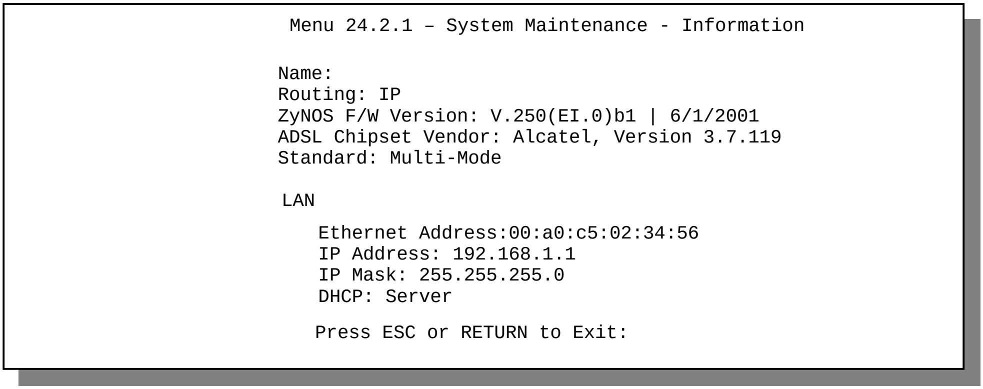
Menu 24.2 System Information and Console Port Speed is as follows.



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

Figure 10-3 System Information and Console Port Speed

Press 1 to display the next screen, **Menu 24.2.1 - System Maintenance - Information.**



```
                         Menu 24.2.1 – System Maintenance - Information

                        Name:
                        Routing: IP
                        ZyNOS F/W Version: V.250(EI.0)b1 | 6/1/2001
                        ADSL Chipset Vendor: Alcatel, Version 3.7.119
                        Standard: Multi-Mode

                        LAN

                           Ethernet Address:00:a0:c5:02:34:56
                           IP Address: 192.168.1.1
                           IP Mask: 255.255.255.0
                           DHCP: Server

                           Press ESC or RETURN to Exit:
```

Figure 10-4 System Maintenance - Information

Table 10-2 Fields in System Maintenance - Information

FIELD	DESCRIPTION
Name	Displays the system name of your Prestige. This information can be modified in **Menu 1 - General Setup**.
Routing	Refers to the routing protocol used.
ZyNOS F/W Version	Refers to the ZyNOS (ZyXEL Network Operating System) firmware version and date created. ZyNOS is a registered trademark of ZyXEL Communications Corporation.
ADSL Chipset Vendor	Displays the vendor of the ADSL chipset and ADSL modem software version.
Version	Refers to the ANSI Version.
Standard	Refers to the ADSL standard in use. Full rate G.dmt and ANSI T1.413 allow rates up to 8 Mbps downstream and 832 Kbps upstream and require the use of a telephone splitter. The reduced rate G.Lite provides up to 1.536 Mbps downstream and 512 Kbps upstream and does not require a telephone splitter. Multi-Mode allows the standard to be negotiated automatically.
Ethernet Address	Refers to the Ethernet MAC (Media Access Control) of your Prestige.
IP Address	This is the IP address of the Prestige in dotted decimal notation.
IP Mask	This shows the subnet mask of the Prestige.
DHCP	This field shows the DHCP setting (**None, Relay** or **Server**) of the Prestige.

10.3 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.

10.3.1 Viewing Error Log

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

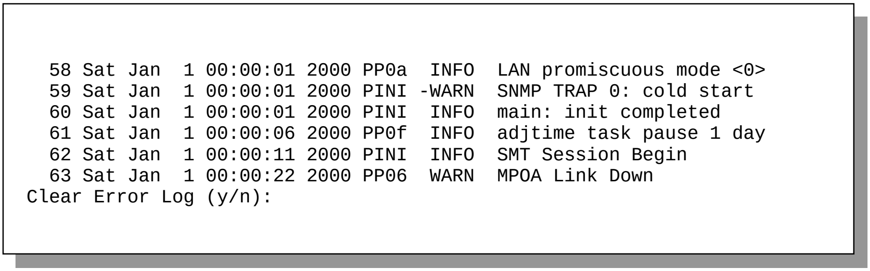
Step 1. Enter 24 from the main menu to open **Menu 24 - System Maintenance**.

Step 2. From menu 24, enter 3 to open **Menu 24.3 - System Maintenance - Log and Trace**.

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

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

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

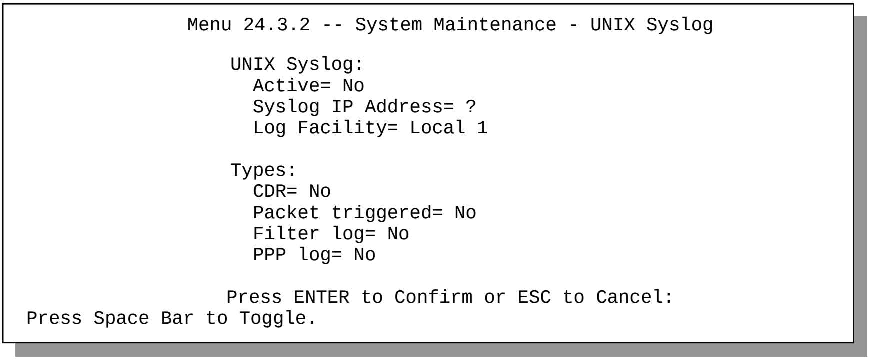


```
  58 Sat Jan  1 00:00:01 2000 PP0a  INFO  LAN promiscuous mode <0>
  59 Sat Jan  1 00:00:01 2000 PINI -WARN  SNMP TRAP 0: cold start
  60 Sat Jan  1 00:00:01 2000 PINI  INFO  main: init completed
  61 Sat Jan  1 00:00:06 2000 PP0f  INFO  adjtime task pause 1 day
  62 Sat Jan  1 00:00:11 2000 PINI  INFO  SMT Session Begin
  63 Sat Jan  1 00:00:22 2000 PP06  WARN  MPOA Link Down
Clear Error Log (y/n):
```

Figure 10-5 Examples of Error and Information Messages

10.3.2 Syslog

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



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

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

                    Types:
                      CDR= No
                      Packet triggered= No
                      Filter log= No
                      PPP log= No

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

Figure 10-6 Menu 24.3.2 - System Maintenance - Syslog and Accounting

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

Table 10-3 System Maintenance Menu Syslog Parameters

PARAMETER	DESCRIPTION
UNIX Syslog:	
Active	Use the [SPACE BAR] to turn on or off syslog.
Syslog IP Address	Enter the IP Address of the server that will log the CDR (Call Detail Record) and system messages i.e., the syslog server.
Log Facility	Use the [SPACE BAR] to select from the 7 different Local options. The log facility allows you to log the message in 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 Filter** field set to **Yes** are logged when this field is set to **Yes.**
PPP log	PPP events are logged when this field is set to **Yes.**

Your Prestige sends four types of syslog messages. Some examples 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 Communications Corp.: 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 Communications Corp.: board 0 line 0 channel 0, call
1, C02 OutCall Connected 64000 40002
```

```
Jul 19 11:20:06 192.168.102.2 ZyXEL Communications Corp.: 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 Communications Corp.: Packet Trigger: Protocol=1,
Data=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a6b6c6d6e6
f7071727374
```

```
Jul 19 11:28:56 192.168.102.2 ZyXEL Communications Corp.: Packet Trigger: Protocol=1,
Data=4500002c1b0140001f06b50ec0a86614ca849a7b0427001700195b3e00000000600220008cd4000002040
5b4

Jul 19 11:29:06 192.168.102.2 ZyXEL Communications Corp.: 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

```
Jul 19 14:43:55 192.168.102.2 ZyXEL Communications Corp.: IP[Src=202.132.154.123
Dst=255.255.255.255 UDP spo=0208  dpo=0208]}S03>R01mF

Jul 19 14:44:00 192.168.102.2 ZyXEL Communications Corp.: IP[Src=192.168.102.20
Dst=202.132.154.1 UDP spo=05d4  dpo=0035]}S03>R01mF

Jul 19 14:44:04 192.168.102.2 ZyXEL Communications Corp.: IP[Src=192.168.102.20
Dst=202.132.154.1 UDP spo=05d4  dpo=0035]}S03>R01mF
```

4. PPP log

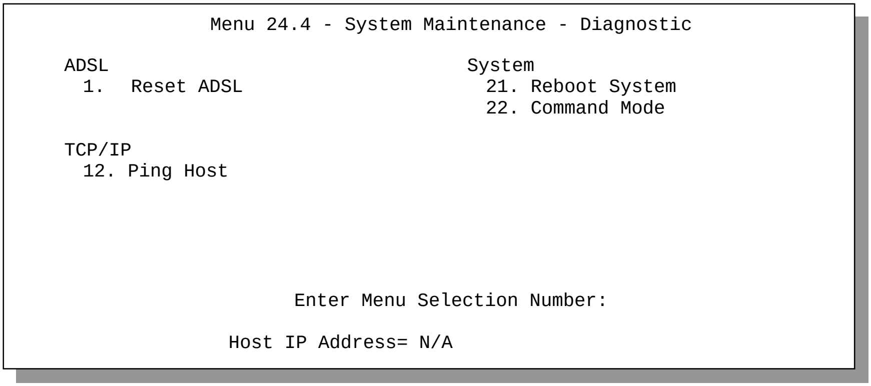
PPP Log Message Format

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 Communications Corp.: ppp:LCP Closing

Jul 19 11:42:49 192.168.102.2 ZyXEL Communications Corp.: ppp:IPCP Closing

Jul 19 11:42:54 192.168.102.2 ZyXEL Communications Corp.: ppp:CCP Closing
```

10.4 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.



```
                  Menu 24.4 - System Maintenance - Diagnostic

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


     TCP/IP
      12. Ping Host






                         Enter Menu Selection Number:

                    Host IP Address= N/A
```

Figure 10-7 Menu 24.4 - System Maintenance - Diagnostic

Follow the procedure below to get to Diagnostic

Step 1. From the main menu, enter 24 to open **Menu 24 - System Maintenance**.

Step 2. From this menu, enter 4 to open **Menu 24.4 - System Maintenance - Diagnostic**.

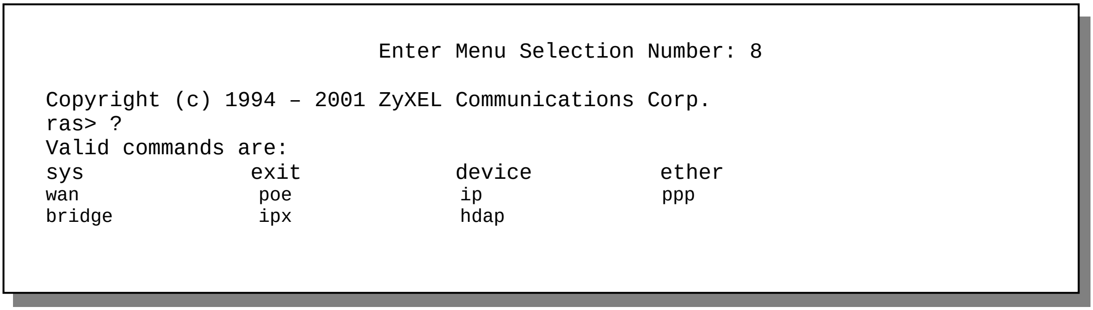
The following table describes the diagnostic tests available in menu 24.4 for your Prestige and the connections.

Table 10-4 System Maintenance Menu Diagnostic

FIELD	DESCRIPTION
Reset ADSL	This command re-initializes the ADSL link to the telephone company.
Ping Host	This diagnostic test pings the host, which determines the functionality of the TCP/IP protocol on both systems and the links in between.
Reboot System	This option reboots the Prestige.
Command Mode	This option allows you to enter the command mode. This mode allows you to diagnose and test your Prestige using a specified set of commands.

10.5 Command Interpreter Mode

The Command Interpreter (CI) is a part of the main system firmware. The CI provides much of the same functionality as the SMT, while adding some low-level setup and diagnostic functions. The CI can be entered from the SMT by selecting menu 24.8. Access is by Telnet. For more detailed information on CI commands see the Support Notes on the Supporting CD. Enter 8 from **Menu 24 - System Maintenance**. A list of valid commands can be found by typing `help` or `?` at the command prompt. Type “exit” to return to the SMT main menu when finished.



```
                          Enter Menu Selection Number: 8

Copyright (c) 1994 – 2001 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys             exit            device          ether
wan             poe             ip              ppp
bridge          ipx             hdap
```

Figure 10-8 Command mode

Chapter 11
Configuration and Firmware File Maintenance

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

11.1 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.

Table 11-1 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.

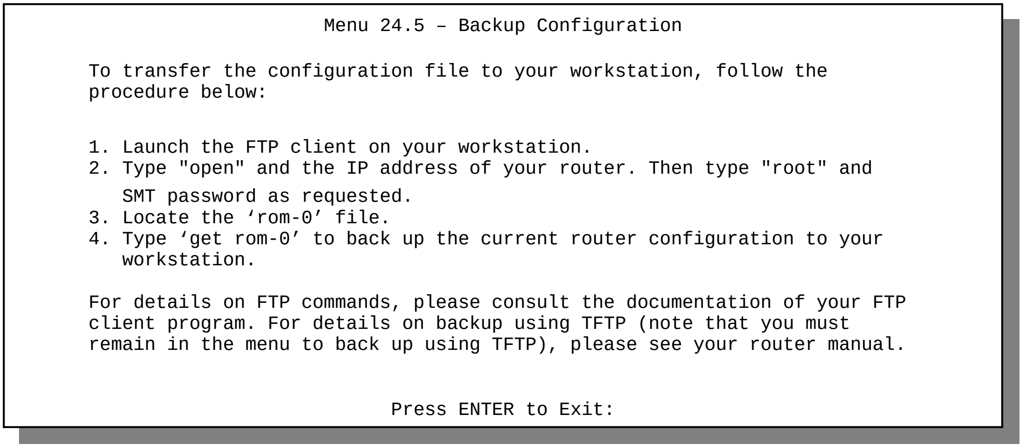
11.2 Backup Configuration

Option 5 from **Menu 24 - System Maintenance** allows you to backup the current Prestige configuration to your computer. Backup is highly recommended once your Prestige is functioning properly. FTP is the preferred method, although TFTP can also be used.

Please note that the 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.

11.2.1 Backup Configuration Using FTP

Enter 5 in **Menu 24 - System Maintenance** to get the following screen.



```
                          Menu 24.5 – 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 the menu to back up using TFTP), please see your router manual.


                                Press ENTER to Exit:
```

Figure 11-1 Menu 24.5 — Backup Configuration

11.2.2 Using the FTP command from the DOS Prompt

Step 1. Launch the FTP client on your computer.

Step 2. Enter “open” and the IP address of your Prestige.

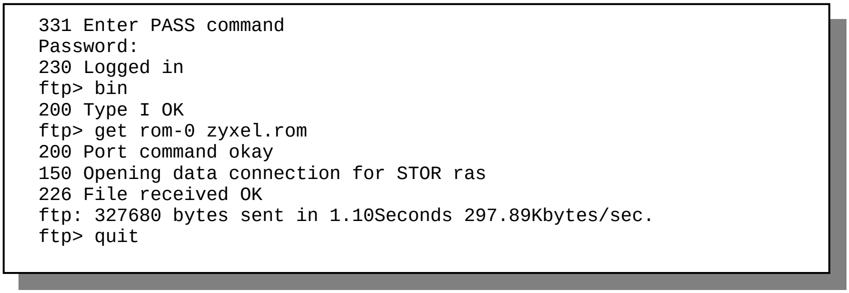
Step 3. Press [ENTER] when prompted for a username.

Step 4. Enter “root” and your SMT 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.



```
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: 327680 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

Figure 11-2 FTP Session Example

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

Table 11-2 General Commands for GUI-based FTP Clients

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

FTP over WAN will not work if you have applied a filter in menu 11.5 (WAN) to block Telnet service.

11.2.3 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.

11.2.4 Example: TFTP Command

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.

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

Table 11-3 General Commands for Third Party TFTP Clients

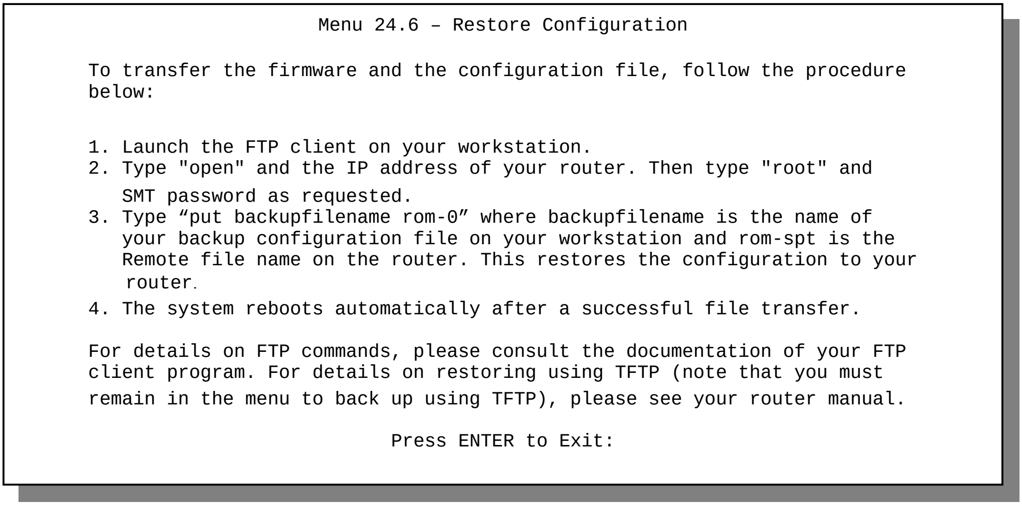
COMMAND	DESCRIPTION
Host	Enter the IP address of the Prestige. 192.168.1.1 is the Prestige’s default IP address when shipped.

COMMAND	DESCRIPTION
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.

TFTP over WAN will not work if you have applied a filter in menu 11.5 (WAN) to block Telnet service.

11.3 Restore Configuration

Menu 24.6 -- System Maintenance - Restore Configuration allows you to restore the configuration via FTP or TFTP to your Prestige. The preferred method is FTP. Note that this function erases the current configuration before restoring the previous backup configuration; please do not attempt to restore unless you have a backup configuration stored on disk. To restore configuration using FTP or TFTP is the same as uploading the configuration file, please refer to the following sections on FTP and TFTP file transfer for more details. The Prestige restarts automatically after the file transfer is complete.



```
                          Menu 24.6 – Restore Configuration

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


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

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

                                Press ENTER to Exit:
```

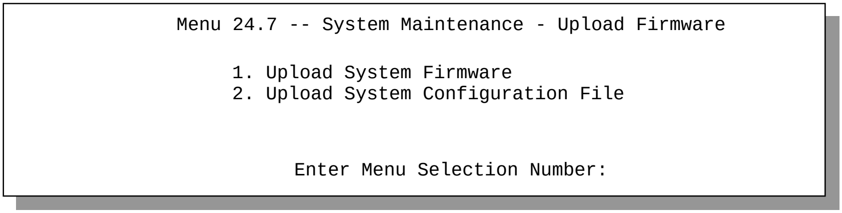
Figure 11-3 Menu 24.6 — Restore Configuration

11.4 Uploading Firmware and Configuration Files

Menu 24.7 - System Maintenance - Upload Firmware allows you to upgrade the firmware and the configuration file.

WARNING!

PLEASE WAIT A FEW MINUTES FOR THE PRESTIGE TO RESTART AFTER FIRMWARE OR CONFIGURATION FILE UPLOAD. INTERRUPTING THE UPLOAD PROCESS MAY PERMANENTLY DAMAGE YOUR PRESTIGE.



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

                    1. Upload System Firmware
                    2. Upload System Configuration File



                          Enter Menu Selection Number:
```

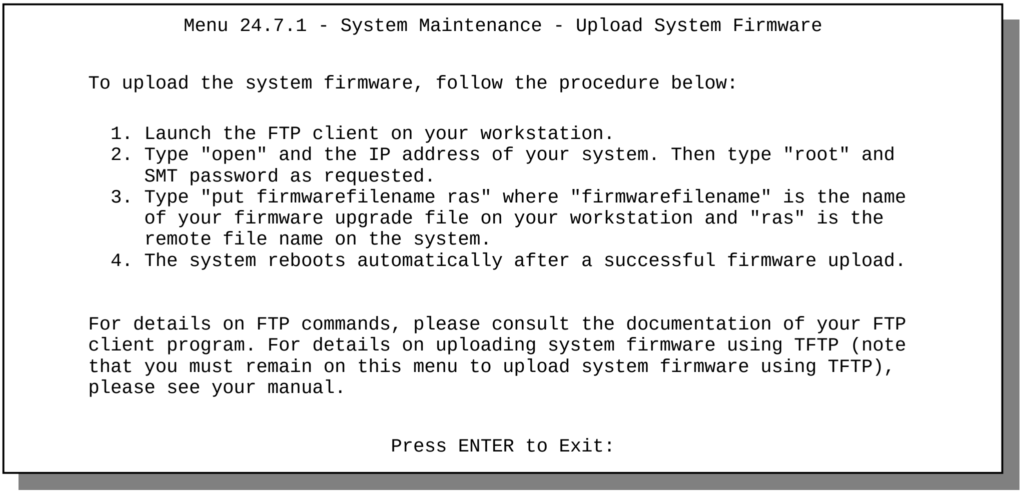
Figure 11-5 Menu 24.7 — System Maintenance — Upload Firmware

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

11.4.1 Firmware 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.

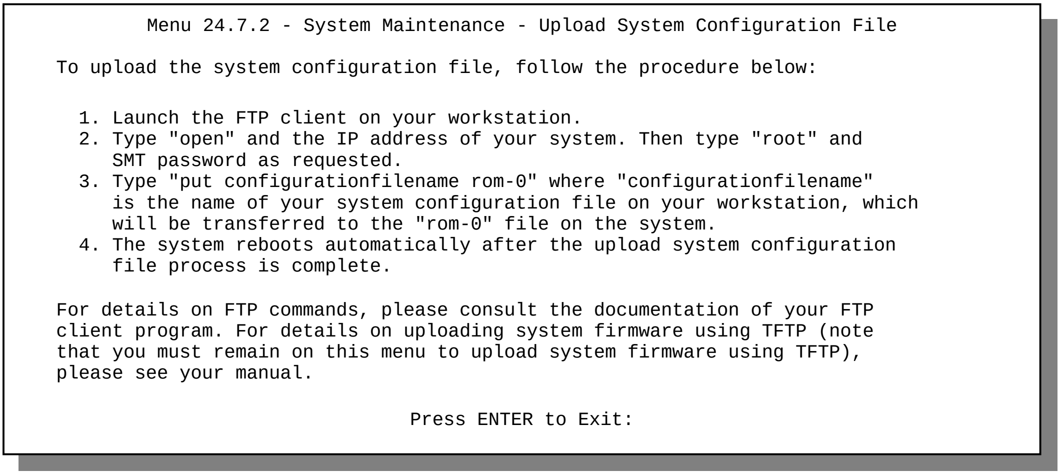


```
                Menu 24.7.1 - System Maintenance - Upload System Firmware


       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 11-6 Menu 24.7.1 — Upload System Firmware

11.4.2 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 11-7 Menu 24.7.2 — System Maintenance

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

11.4.3 Using the FTP command from the DOS Prompt Example

Step 1. Launch the FTP client on your computer.

Step 2. Enter “open” and the IP address of your Prestige.

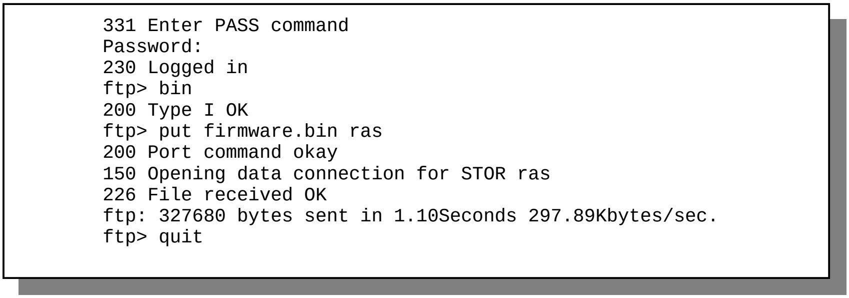
Step 3. Press [ENTER] when prompted for a username.

Step 4. Enter “root” and your SMT 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, e.g., 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.



```
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: 327680 bytes sent in 1.10Seconds 297.89Kbytes/sec.
ftp> quit
```

Figure 11-8 FTP Session Example

More commands that you may find in third party FTP clients, are listed earlier in this chapter.

FTP over WAN will not work if you have applied a filter in menu 11.5 (WAN) to block Telnet service.

11.4.4 TFTP File Upload

The Prestige also 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 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 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 firmware is “ras” and 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, “put” the other way around, and “binary” to set binary transfer mode.

11.4.5 Example: TFTP Command

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.

TFTP over WAN will not work if you have applied a filter in menu 11.5 (WAN) to block Telnet service.

Chapter 12
IP Policy Routing

This chapter covers setting and applying policies used for IP routing.

12.1 Introduction

Traditionally, routing is based on the destination address only and the P645R takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing.

12.2 Benefits

- Source-Based Routing – Network administrators can use policy-based routing to direct traffic from different users through different connections.
- Quality of Service (QoS) – Organizations can differentiate traffic by setting the precedence or TOS (Type of Service) values in the IP header at the periphery of the network to enable the backbone to prioritize traffic.
- Cost Savings – IPPR allows organizations to distribute interactive traffic on high-bandwidth, high-cost paths while using low-cost paths for batch traffic.
- Load Sharing – Network administrators can use IPPR to distribute traffic among multiple paths.

12.3 Routing Policy

Individual routing policies are used as part of the overall IPPR process. A policy defines the matching criteria and the action to take when a packet meets the criteria. The action is taken only when all the criteria are met. The criteria includes the source address and port, IP protocol (ICMP, UDP, TCP, etc.), destination address and port, TOS and precedence (fields in the IP header) and length. The inclusion of length criterion is to differentiate between interactive and bulk traffic. Interactive applications, telnet for example, tend to have short packets, while bulk traffic, file transfer for example, tends to have large packets.

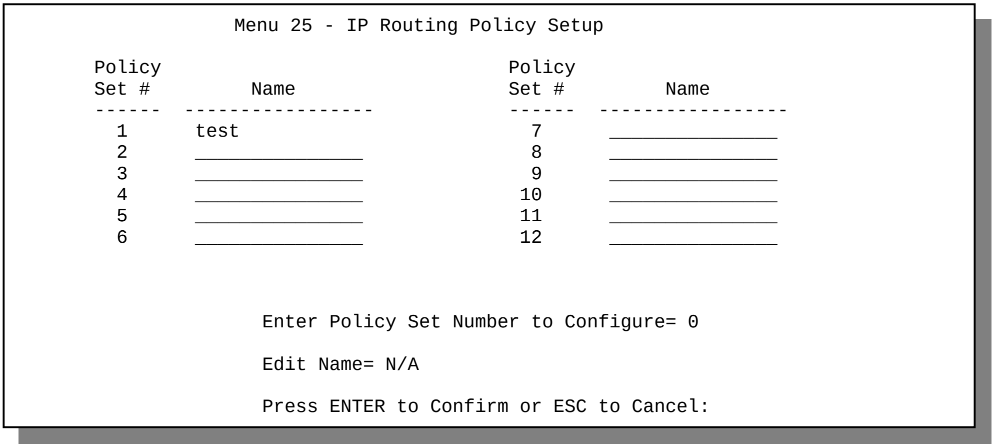
The actions that can be taken include:

- routing the packet to a different gateway (and hence the outgoing interface).
- setting the TOS and precedence fields in the IP header.

IPPR follows the existing packet filtering facility of RAS in style and in implementation. The policies are divided into sets, where related policies are grouped together. A user defines the policies before applying them to an interface or a remote node, in the same fashion as the filters. There are 12 policy sets with six policies in each set.

12.4 IP Routing Policy Setup

Menu 25 shows all the policies defined.



```
                    Menu 25 - IP Routing Policy Setup

        Policy                                Policy
        Set #         Name                    Set #         Name
        ------  -----------------             ------  -----------------
          1      test                           7      _______________
          2      _______________                8      _______________
          3      _______________                9      _______________
          4      _______________               10      _______________
          5      _______________               11      _______________
          6      _______________               12      _______________


                       Enter Policy Set Number to Configure= 0

                       Edit Name= N/A

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

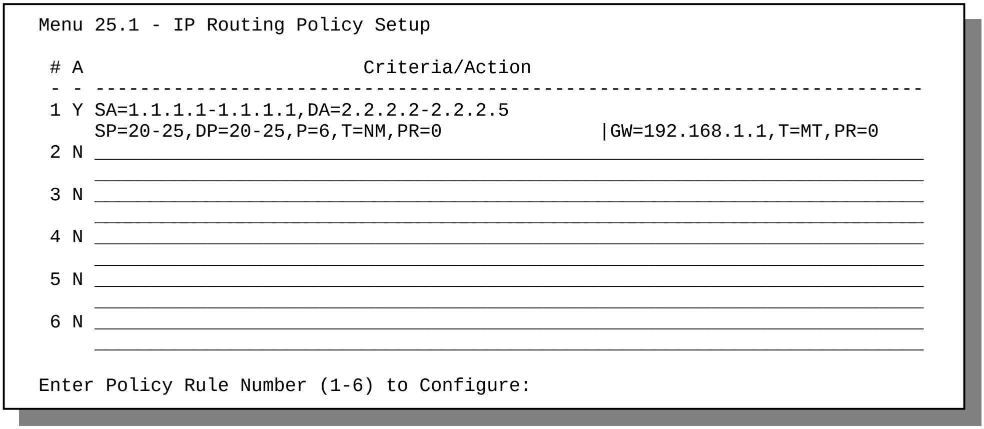
Figure 12-1 IP Routing Policy Setup

To setup a routing policy, perform the following procedures:

Step 1. Type 25 in the main menu to open **Menu 25 – IP Routing Policy Setup.**

Step 2. Type the index of the policy set you want to configure to open **Menu 25.1 – IP Routing Policy Setup**.

Menu 25.1 shows the summary of a policy set, including the criteria and the action of a single policy, and whether a policy is active or not. Each policy contains two lines. The former part is the criteria of the incoming packet and the latter is the action. Between these two parts, separator "|" means the action is taken on criteria matched and separator "=" means the action is taken on criteria not matched.



```
Menu 25.1 - IP Routing Policy Setup

 # A                         Criteria/Action
 - - -------------------------------------------------------------------------
 1 Y SA=1.1.1.1-1.1.1.1,DA=2.2.2.2-2.2.2.5
     SP=20-25,DP=20-25,P=6,T=NM,PR=0              |GW=192.168.1.1,T=MT,PR=0
 2 N ___________________________________________________________________________
     ___________________________________________________________________________
 3 N ___________________________________________________________________________
     ___________________________________________________________________________
 4 N ___________________________________________________________________________
     ___________________________________________________________________________
 5 N ___________________________________________________________________________
     ___________________________________________________________________________
 6 N ___________________________________________________________________________
     ___________________________________________________________________________

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

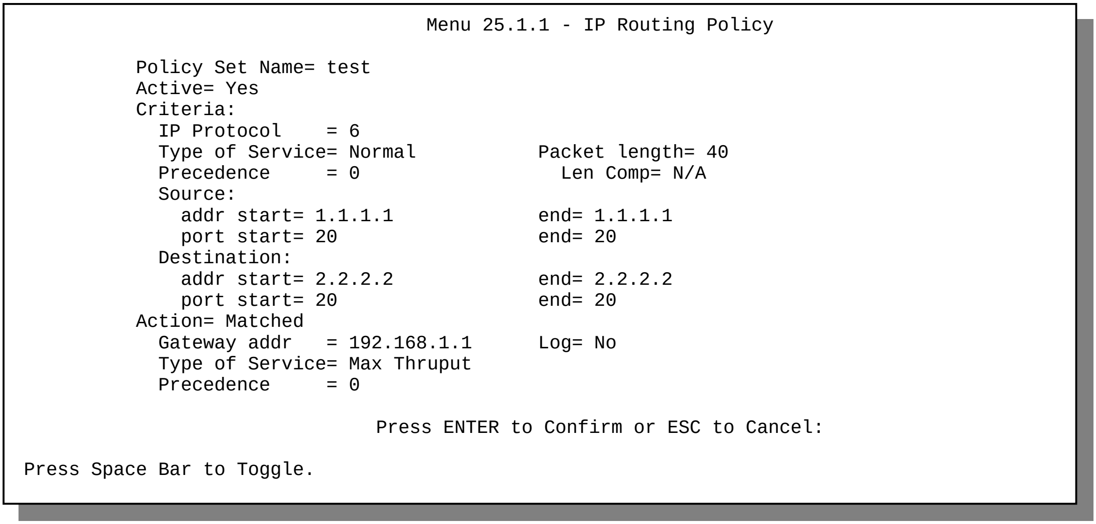
Figure 12-2 Menu 25.1 – Sample IP Routing Policy Setup

Table 12-1 IP Routing Policy Setup

ABBREVIATION	MEANING
Criterion SA	Source IP Address
SP	Source Port
DA	Destination IP Address

	DP	Destination Port
	P	IP layer 4 protocol number (TCP=6, UDP=17…)
	T	Type of service of incoming packet
	PR	Precedence of incoming packet
Action	GW	Gateway IP address
	T	Outgoing Type of service
	P	Outgoing Precedence
Service	NM	Normal
	MD	Minimum Delay
	MT	Maximum Throughput
	MR	Maximum Reliability
	MC	Minimum Cost

Type a number from 1 to 6 to display **Menu 25.1.1 – IP Routing Policy** (see the next figure). This menu allows you to configure a policy rule.



```
                              Menu 25.1.1 - IP Routing Policy

          Policy Set Name= test
          Active= Yes
          Criteria:
            IP Protocol    = 6
            Type of Service= Normal           Packet length= 40
            Precedence     = 0                  Len Comp= N/A
            Source:
              addr start= 1.1.1.1             end= 1.1.1.1
              port start= 20                  end= 20
            Destination:
              addr start= 2.2.2.2             end= 2.2.2.2
              port start= 20                  end= 20
          Action= Matched
            Gateway addr   = 192.168.1.1      Log= No
            Type of Service= Max Thruput
            Precedence     = 0

                               Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 12-3 IP Routing Policy

Table 12-2 IP Routing Policy

FIELD	DESCRIPTION
Policy Set Name	This is the policy set name assigned in **Menu 25 – IP Routing Policy Setup**.
Active	Press [SPACE BAR] to select **Yes** to activate the policy.
Criteria:	
IP Protocol	IP layer 4 protocol, e.g., **UDP**, **TCP**, **ICMP**, etc.
Type of Service	Prioritize incoming network traffic by choosing from **Don't Care**, **Normal**, **Min Delay**, **Max Thruput** or **Max Reliable**.
Precedence	Precedence value of the incoming packet. Values are 0 to 7 or **Don't Care**.
Packet Length	Type the length of incoming packets (in bytes). The operators in the **Len Comp** (next field) apply to packets of this length.
Len Comp	Press [SPACE BAR] to choose from **Equal**, **Not Equal**, **Less**, **Greater**, **Less or Equal** or **Greater or Equal**.
Source:	
addr start / end	Source IP address range from start to end.
port start / end	Source port number range from start to end; applicable only for TCP/UDP.
Destination:	
addr start / end	Destination IP address range from start to end.
port start / end	Destination port number range from start to end; applicable only for TCP/UDP.
Action	Specifies whether action should be taken on criteria **Matched** or **Not Matched**.
Gateway addr	Defines the outgoing gateway address. The gateway must be on the same subnet as the P645R if it is on the LAN, otherwise, the gateway must be the IP address of a remote node. The default gateway is specified as 0.0.0.0.
Type of Service	Set the new TOS value of the outgoing packet. Prioritize incoming network traffic by choosing **No Change**, **Normal**, **Min Delay**, **Max Thruput**, **Max Reliable** or **Min Cost**.
Precedence	Set the new outgoing packet precedence value. Values are 0 to 7 or **No Change**.
Log	Press [SPACE BAR] to select **Yes** to make an entry in the system log when a policy is executed.

FIELD	DESCRIPTION
When you have completed this menu, press [ENTER] at the prompt “Press [ENTER] to confirm or [ESC] to cancel” to save your configuration or press [ESC] to cancel and go back to the previous screen.	

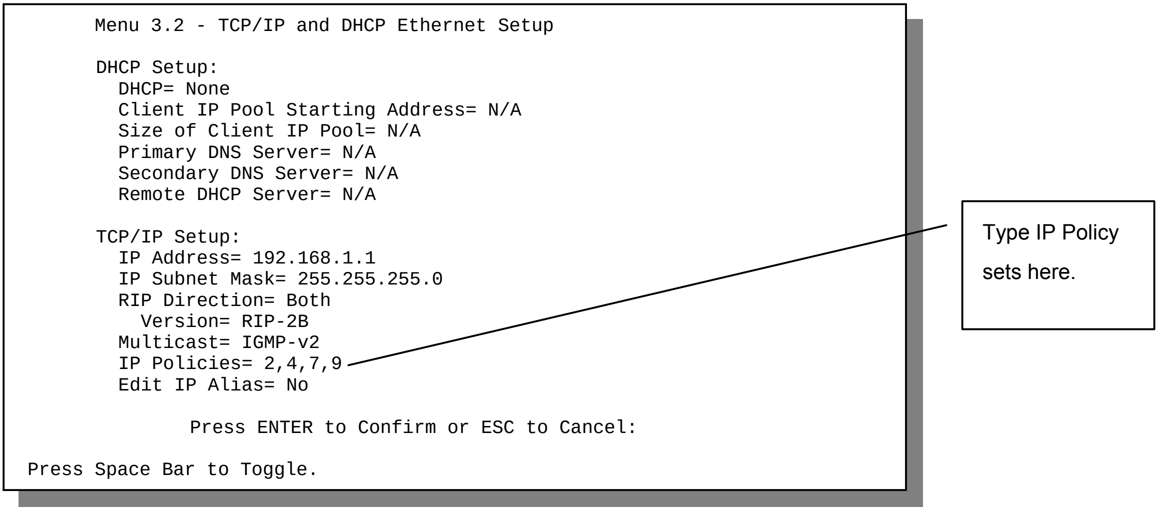
12.5 Applying an IP Policy

This section shows you where to apply the IP policies after you design them.

12.5.1 Ethernet IP Policies

From **Menu 3 – Ethernet Setup**, type 2 to go to **Menu 3.2 – TCP/IP and DHCP Ethernet Setup**.

You can choose up to four IP policy sets (from 12) by typing their numbers separated by commas, e.g., 2, 4, 7, 9.

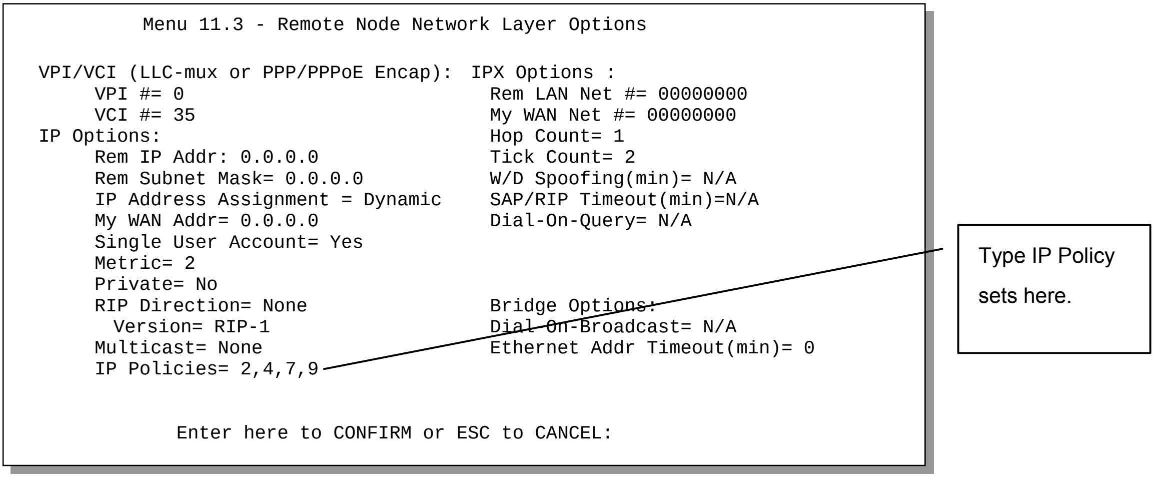


```
      Menu 3.2 - TCP/IP and DHCP Ethernet Setup

      DHCP Setup:
        DHCP= None
        Client IP Pool Starting Address= N/A
        Size of Client IP Pool= N/A
        Primary DNS Server= N/A
        Secondary DNS Server= N/A
        Remote DHCP Server= N/A

      TCP/IP Setup:
        IP Address= 192.168.1.1
        IP Subnet Mask= 255.255.255.0
        RIP Direction= Both
          Version= RIP-2B
        Multicast= IGMP-v2
        IP Policies= 2,4,7,9
        Edit IP Alias= No

              Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Type IP Policy sets here.

Figure 12-4 Menu 3.2 – TCP/IP and DHCP Ethernet Setup

Go to menu 11.3 (shown next) and type the number(s) of the IP Routing Policy set(s) as appropriate. You can cascade up to four policy sets by typing their numbers separated by commas.



```
            Menu 11.3 - Remote Node Network Layer Options

   VPI/VCI (LLC-mux or PPP/PPPoE Encap):  IPX Options :
        VPI #= 0                            Rem LAN Net #= 00000000
        VCI #= 35                           My WAN Net #= 00000000
   IP Options:                              Hop Count= 1
        Rem IP Addr: 0.0.0.0                Tick Count= 2
        Rem Subnet Mask= 0.0.0.0            W/D Spoofing(min)= N/A
        IP Address Assignment = Dynamic     SAP/RIP Timeout(min)=N/A
        My WAN Addr= 0.0.0.0                Dial-On-Query= N/A
        Single User Account= Yes
        Metric= 2
        Private= No
        RIP Direction= None                 Bridge Options:
          Version= RIP-1                    Dial-On-Broadcast= N/A
        Multicast= None                     Ethernet Addr Timeout(min)= 0
        IP Policies= 2,4,7,9


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

Type IP Policy sets here.

Figure 12-5 Menu 11.3 – Remote Node Network Layer Options

12.6 IP Policy Routing Example

If a network has both Internet and remote node connections, you can route Web packets to the Internet using one policy and route FTP packets to a remote network using another policy. See the next figure.

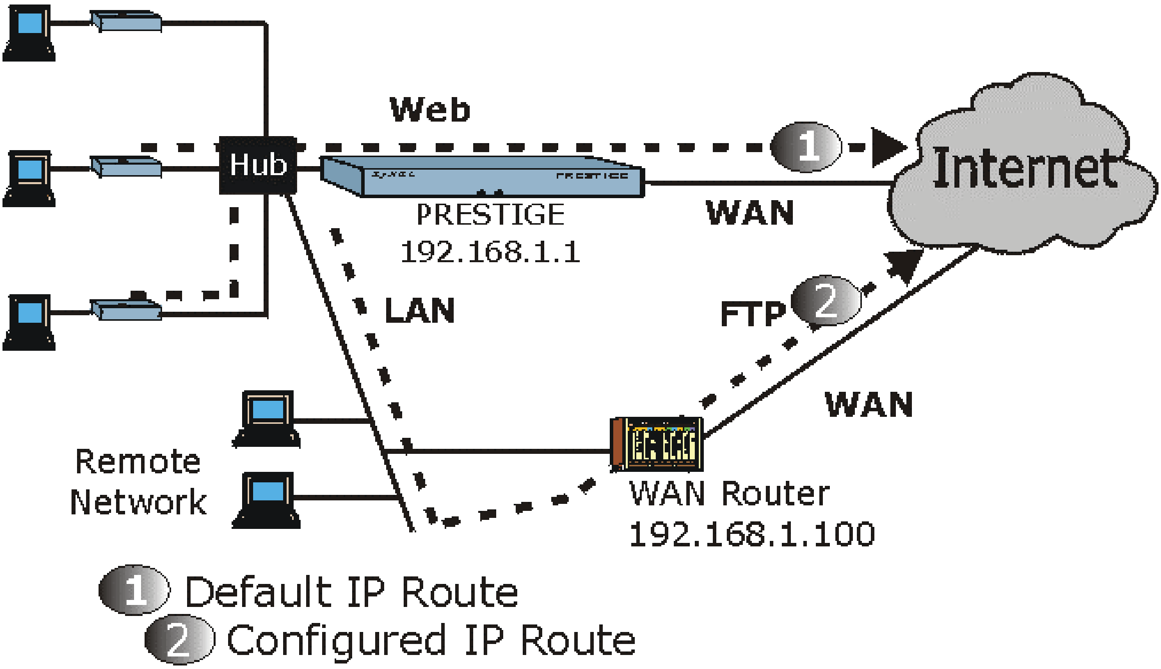
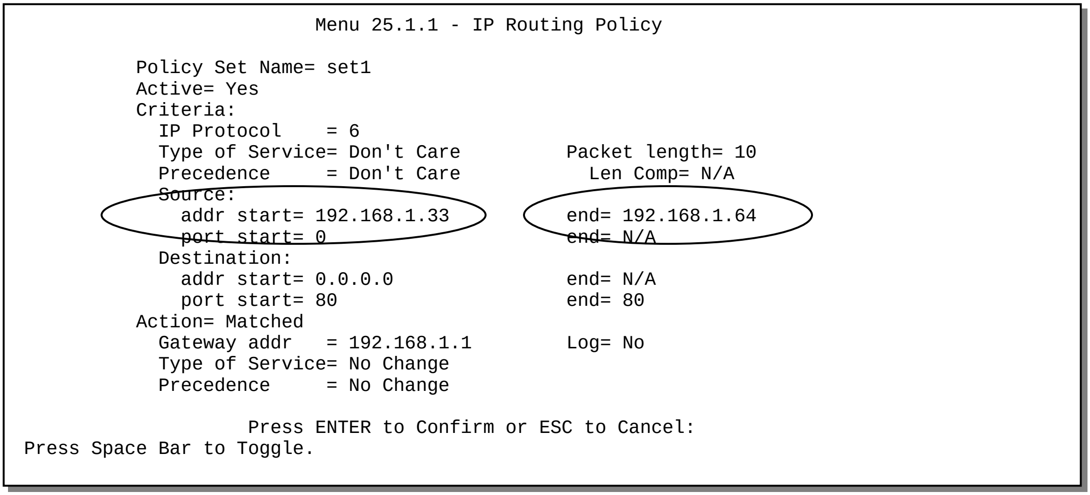


Figure 12-6 Example of IP Policy Routing

To force Web packets coming from clients with IP addresses of 192.168.1.33 to 192.168.1.64 to be routed to the Internet via the WAN port of the P645R, follow the steps as shown next.

Step 1. Create a routing policy set in menu 25.

Step 2. Create a rule for this set in **Menu 25.1.1 - IP Routing Policy** as shown next.



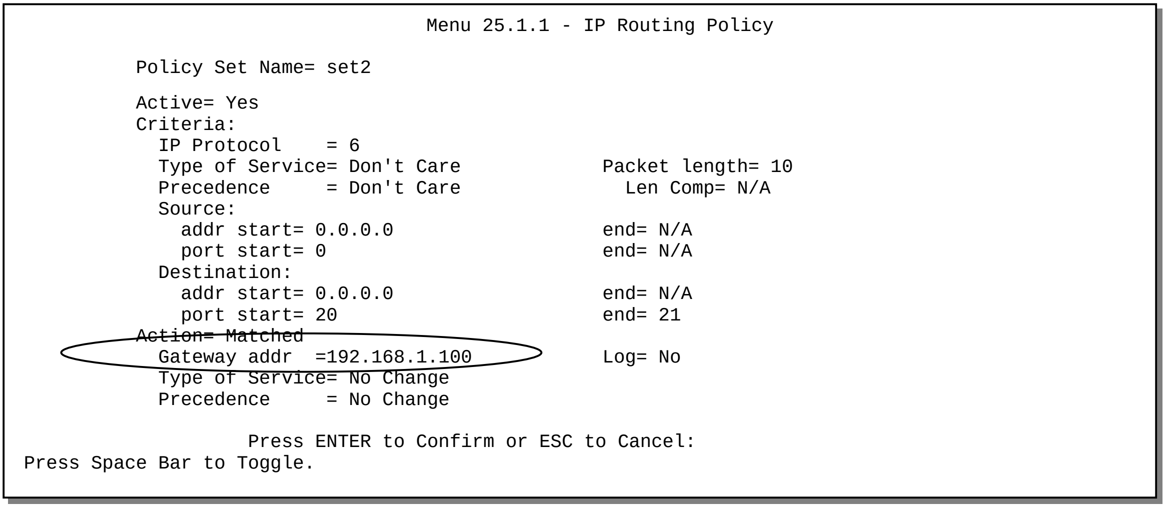
```
                           Menu 25.1.1 - IP Routing Policy

          Policy Set Name= set1
          Active= Yes
          Criteria:
            IP Protocol    = 6
            Type of Service= Don't Care         Packet length= 10
            Precedence     = Don't Care           Len Comp= N/A
            Source:
              addr start= 192.168.1.33          end= 192.168.1.64
              port start= 0                     end= N/A
            Destination:
              addr start= 0.0.0.0               end= N/A
              port start= 80                    end= 80
          Action= Matched
            Gateway addr   = 192.168.1.1        Log= No
            Type of Service= No Change
            Precedence     = No Change

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

Figure 12-7 IP Routing Policy Example

Step 3. Check **Menu 25.1 - IP Routing Policy Setup** to see if the rule is added correctly.

Step 4. Create another policy set in menu 25.

Step 5. Create a rule in menu 25.1.1 for this set to route packets from any host (IP=0.0.0.0 means any host) with protocol TCP and port FTP access through another gateway (192.168.1.100).

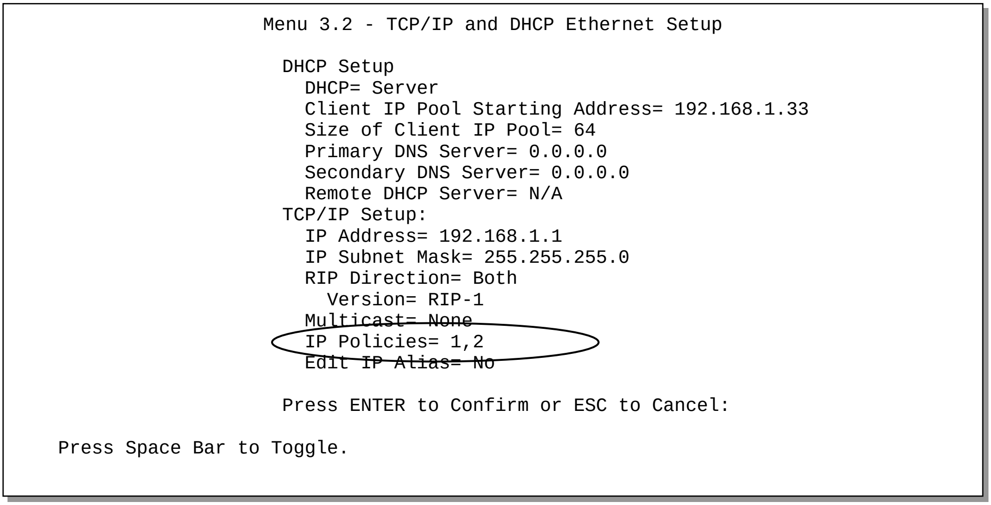


```
                                  Menu 25.1.1 - IP Routing Policy

          Policy Set Name= set2

          Active= Yes
          Criteria:
            IP Protocol    = 6
            Type of Service= Don't Care            Packet length= 10
            Precedence     = Don't Care              Len Comp= N/A
            Source:
              addr start= 0.0.0.0                  end= N/A
              port start= 0                        end= N/A
            Destination:
              addr start= 0.0.0.0                  end= N/A
              port start= 20                       end= 21
          Action= Matched
            Gateway addr  =192.168.1.100           Log= No
            Type of Service= No Change
            Precedence     = No Change

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

Figure 12-8 IP Routing Policy

Step 6. Check **Menu 25.1 - IP Routing Policy Setup** to see if the rule is added correctly.

Step 7. Apply both policy sets in menu 3.2 as shown next.



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

                         DHCP Setup
                           DHCP= Server
                           Client IP Pool Starting Address= 192.168.1.33
                           Size of Client IP Pool= 64
                           Primary DNS Server= 0.0.0.0
                           Secondary DNS Server= 0.0.0.0
                           Remote DHCP Server= N/A
                         TCP/IP Setup:
                           IP Address= 192.168.1.1
                           IP Subnet Mask= 255.255.255.0
                           RIP Direction= Both
                             Version= RIP-1
                           Multicast= None
                           IP Policies= 1,2
                           Edit IP Alias= No

                         Press ENTER to Confirm or ESC to Cancel:

     Press Space Bar to Toggle.
```

Figure 12-9 Applying IP Policies

Chapter 13
Call Scheduling

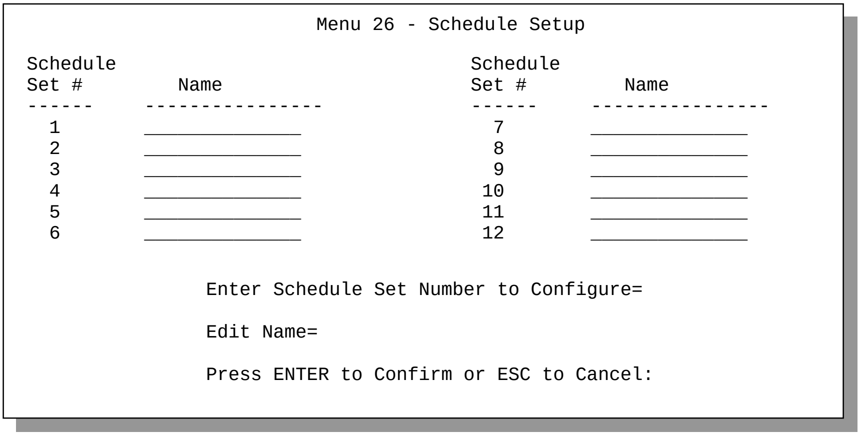
This chapter shows you how to set up call time periods for remote nodes.

13.1 Introduction

The call scheduling feature allows the P645R 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**.

13.2 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 13-1 Schedule Setup

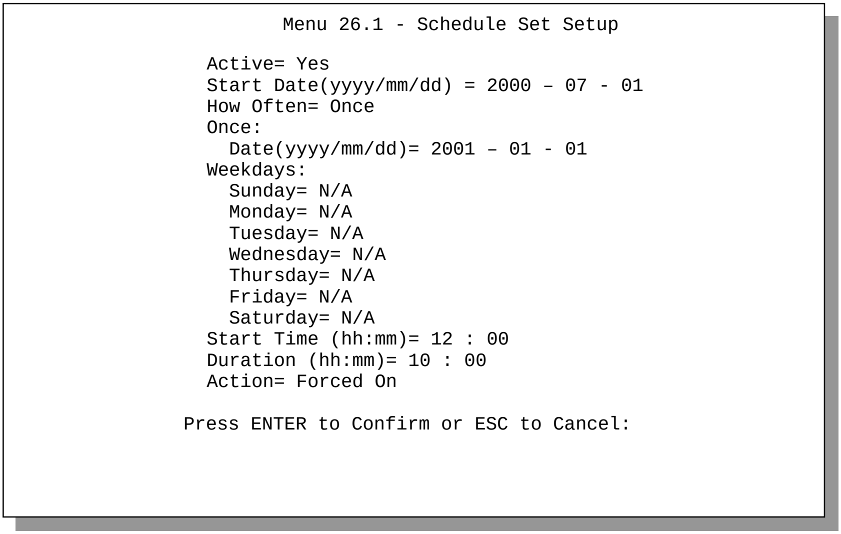
Lower numbered sets take precedence over higher numbered sets thereby avoiding scheduling conflicts. For example, if sets 1, 2, 3 and 4 are applied in the remote node then set 1 will take precedence over sets 2, 3 and 4 as the P645R, by default, applies the lowest numbered set first. Set 2 will take 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, enter the set number and press the [SPACE BAR] in the Edit Name **field.**

13.3 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 13-2 Schedule Set Setup

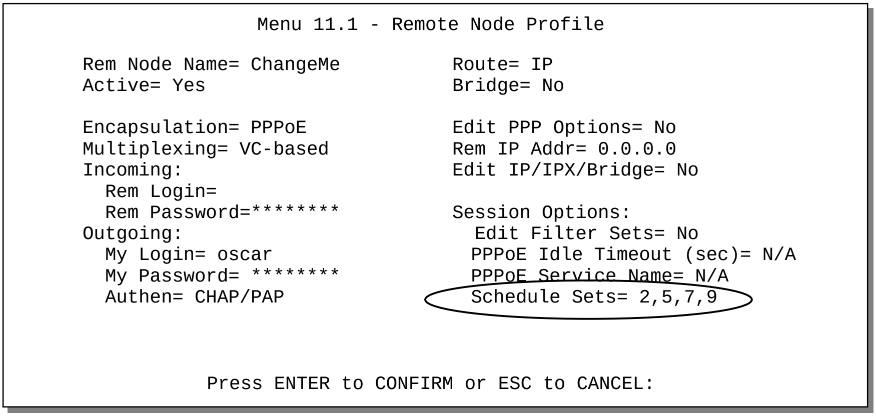
If a connection has already been established, your P645R will not drop it. Once the connection is dropped manually or it times out (the time configured in the **Duration** field expires), then that remote node can't be triggered again until the next configured start time.

Table 13-1 Schedule Set Setup Fields

FIELD	DESCRIPTION	EXAMPLE
Active	Choose **Yes** to activate and **No** to deactivate the schedule set.	**Yes** (default)
Start Date	Enter the start date that you wish the set to take effect in year -month-day format. Valid dates are from the present to February 5, 2036.	2000 – 07 – 01
How Often	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** (default)
Once: Date	If you select **Once** in the **How Often** field above, enter the date the set should activate in year-month-day format. If you select **Weekly** in the **How Often** field above, this field is **N/A**.	2001 – 01 – 01
Weekday: Day	If you select **Weekly** in the **How Often** field above, then choose the day(s) the set should activate (and recur). Individual **Day** parameters are active when their fields read **Yes** and inactive when their fields read **No** or **N/A**.	**N/A** (default)
Start Time	Enter the start time that you wish the schedule set to take effect in hour : minute format.	12 : 00
Duration	Enter the maximum duration allowed in hour : minute format for this scheduled connection.	10 : 00
Action	Choose an action. Choices are: **Forced On** means that the connection is maintained whether or not there is a demand call on the line and will persist for the time period specified in the **Duration** field. **Forced Down** means that the connection is blocked whether or not there is a demand call on the line. **Enable Dial-On-Demand** means that this schedule permits a demand call on the line. **Disable Dial-On-Demand** means that this schedule prevents a demand call on the line.	**Forced On**

13.4 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                      Bridge= No

       Encapsulation= PPPoE             Edit PPP Options= No
       Multiplexing= VC-based           Rem IP Addr= 0.0.0.0
       Incoming:                        Edit IP/IPX/Bridge= No
         Rem Login=
         Rem Password=********          Session Options:
       Outgoing:                          Edit Filter Sets= No
         My Login= oscar                  PPPoE Idle Timeout (sec)= N/A
         My Password= ********            PPPoE Service Name= N/A
         Authen= CHAP/PAP                 Schedule Sets= 2,5,7,9



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

Figure 13-3 Applying Schedule Sets to a Remote Node Example (PPPoE Encapsulation)

Chapter 14
Troubleshooting

This chapter covers problems you may run into and possible remedies. After each problem description, some instructions are provided to help you diagnose and solve the problem.

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 turn on the Prestige	Make sure that you have the correct AC adapter and that is plugged in and connected to the Prestige. If the error persists, you may have a hardware problem. In this case you should contact your vendor.

14.2 Problems Telnetting into the Prestige

Table 14-2 Troubleshooting Telnet

PROBLEM	CORRECTIVE ACTION
Can't access the Prestige through telnet.	Check the LAN port and the other Ethernet connections.
	Check your computer's IP address, it should be in the same subnet as the Prestige.
	Use the reset button as follows to restore the IP address to 192.168.1.1, subnet mask to 255.255.255.0, DHCP server to active with addresses starting at 192.168.1.33 and the password to 1234. Turn the Prestige off. Use a pointed object to push the RESET button while you turn the Prestige back on. Keep the RESET button pressed for one minute.

	Make sure your computer is set to get a dynamic IP address; or if you want to use a static IP address on your computer, make sure that it is on the same subnet as the Prestige.

14.3 Problems With the WAN Interface

Table 14-3 Troubleshooting the ADSL connection

PROBLEM	CORRECTIVE ACTION
Initialization of the ADSL connection failed.	Check the cable connections between the ADSL port and the wall jack. The DSL LED on the front panel of the Prestige should be on.
	Check that your VPI, VCI, type of encapsulation and type of multiplexing settings are the same as what you collected from your telephone company and ISP.
	Restart the Prestige. If you still have problems, you may need to verify your VPI, VCI, type of encapsulation and type of multiplexing settings with the telephone company and ISP.

14.4 Problems With the LAN Interface

Table 14-4 Troubleshooting the LAN Interface

PROBLEM	CORRECTIVE ACTION
Can’t ping any station on the LAN	Check the Ethernet LEDs on the front panel. A LAN LED should be on if the port is connected to a computer or hub. If they are off, check the cable connections between your Prestige and the computer or hub.
	Verify that the IP addresses of the Prestige and the computers are on the same subnet.

14.5 Problems Connecting to a Remote Node or ISP

Table 14-5 Troubleshooting a Connection to a Remote Node or ISP

PROBLEM	CORRECTIVE ACTION
Can’t connect to a remote node or ISP	Check menu 4 to verify that the **My Login** and **My Password** fields have the proper entries.
	In menu 11.1, verify your login name and password for the remote node.
	If these steps fail, you may need to verify your login and password with your ISP.

Appendix A
Virtual Circuit Topology

ATM is a connection-oriented technology, meaning that it sets up virtual circuits over which end systems communicate. The terminology for virtual circuits is as follows:

● **Virtual Channel**	Logical connections between ATM switches
● **Virtual Path**	A bundle of virtual channels
● **Virtual Circuit**	A series of virtual paths between end points in a network

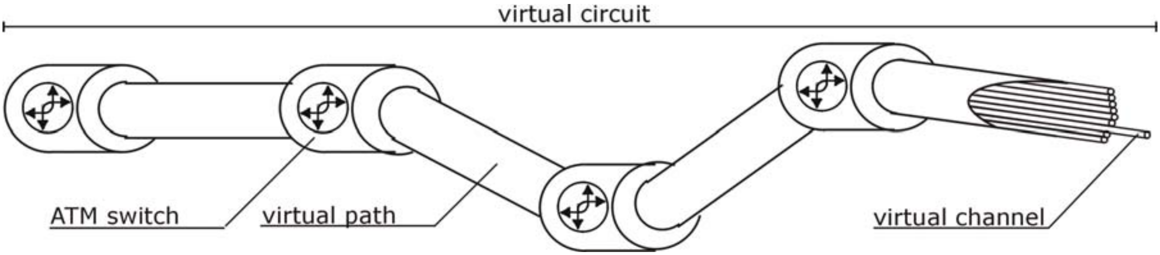


Diagram 1 Virtual Circuit Topology

Think of a virtual path as a cable that contains a bundle of wires. The cable connects two points and wires within the cable provide individual circuits between the two points. In an ATM cell header, a VPI (Virtual Path Identifier) identifies a link formed by a virtual path; a VCI (Virtual Channel Identifier) identifies a channel within a virtual path.

The VPI and VCI identify a virtual path, that is, termination points between ATM switches. A series of virtual paths make up a virtual circuit.

Your service provider should supply you with VPI/VCI numbers.

Appendix B
Power Adapter Specifications

NORTH AMERICAN PLUG STANDARDS	
AC Power Adapter Model	DV-121AACS
Input Power	AC120Volts/60Hz/23W
Output Power	AC12Volts/1.0A
Power Consumption	10 W
Safety Standards	UL, CUL (UL 1310, CSA C22.2 No.223)
EUROPEAN PLUG STANDARDS	
AC Power Adapter Model	DV-121AACUP-5716
Input Power	AC230Volts/50Hz/19W
Output Power	AC12Volts/1.0A
Power Consumption	10 W
Safety Standards	TUV, CE (EN 61558)
CHINESE PLUG STANDARDS	
AC Power Adapter Model	DV-121AACCP-5720
Input Power	AC220Volts/50Hz/18W
Output Power	AC12Volts/1.0A
Power Consumption	10 W
Safety Standards	CCEE (GB8898)

Index