Prestige 642R Series

ADSL Router

User's Guide

Version 2.50

(September 2000)

ZyXEL

TOTAL INTERNET ACCESS SOLUTION

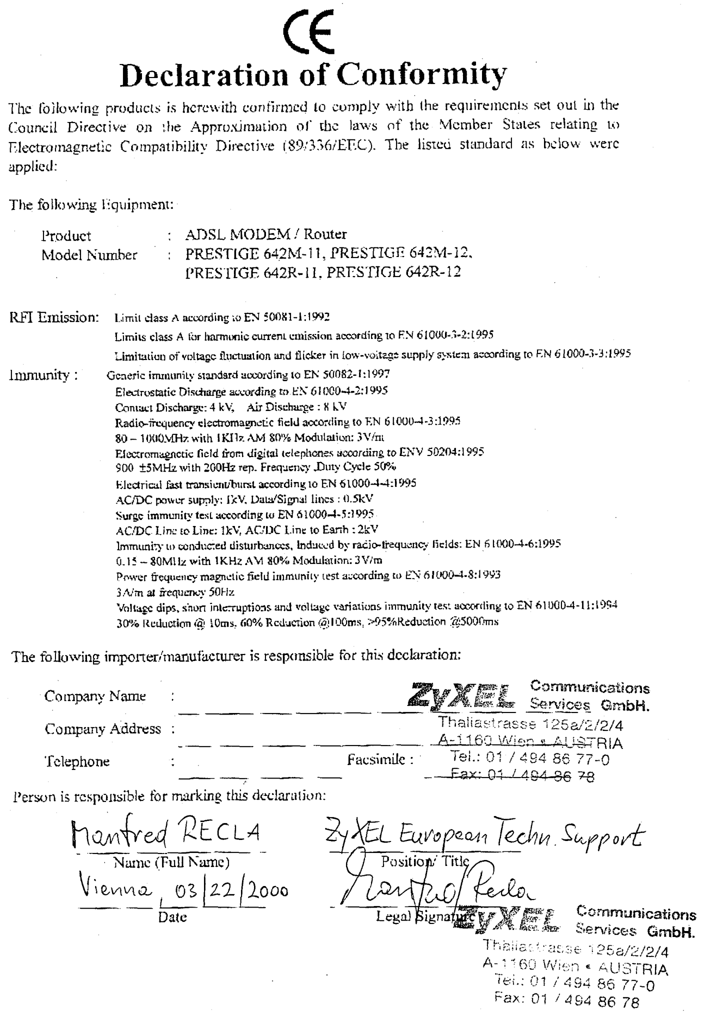
Copyright

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's 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.



CE

Declaration of Conformity

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

The following Equipment:

Product : ADSL MODEM / Router
Model Number : PRESTIGE 642M-11, PRESTIGE 642M-12, PRESTIGE 642R-11, PRESTIGE 642R-12

RFI Emission: Limit class A according to EN 50081-1:1992
Limits class A for harmonic current emission according to EN 61000-3-2:1995
Limitation of voltage fluctuation and flicker in low-voltage supply system according to EN 61000-3-3:1995

Immunity : Generic immunity standard according to EN 50082-1:1997
Electrostatic Discharge according to EN 61000-4-2:1995
Contact Discharge: 4 kV, Air Discharge : 8 kV
Radio-frequency electromagnetic field according to EN 61000-4-3:1995
80 – 1000MHz with 1KHz AM 80% Modulation: 3V/m
Electromagnetic field from digital telephones according to ENV 50204:1995
900 ±5MHz with 200Hz rep. Frequency Duty Cycle 50%
Electrical fast transient/burst according to EN 61000-4-4:1995
AC/DC power supply: 1kV, Data/Signal lines : 0.5kV
Surge immunity test according to EN 61000-4-5:1995
AC/DC Line to Line: 1kV, AC/DC Line to Earth : 2kV
Immunity to conducted disturbances, Induced by radio-frequency fields: EN 61000-4-6:1995
0.15 – 80MHz with 1KHz AM 80% Modulation: 3V/m
Power frequency magnetic field immunity test according to EN 61000-4-8:1993
3A/m at frequency 50Hz
Voltage dips, short interruptions and voltage variations immunity test according to EN 61000-4-11:1994
30% Reduction @ 10ms, 60% Reduction @100ms, >95%Reduction @5000ms

The following importer/manufacturer is responsible for this declaration:

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

Person is responsible for marking this declaration:

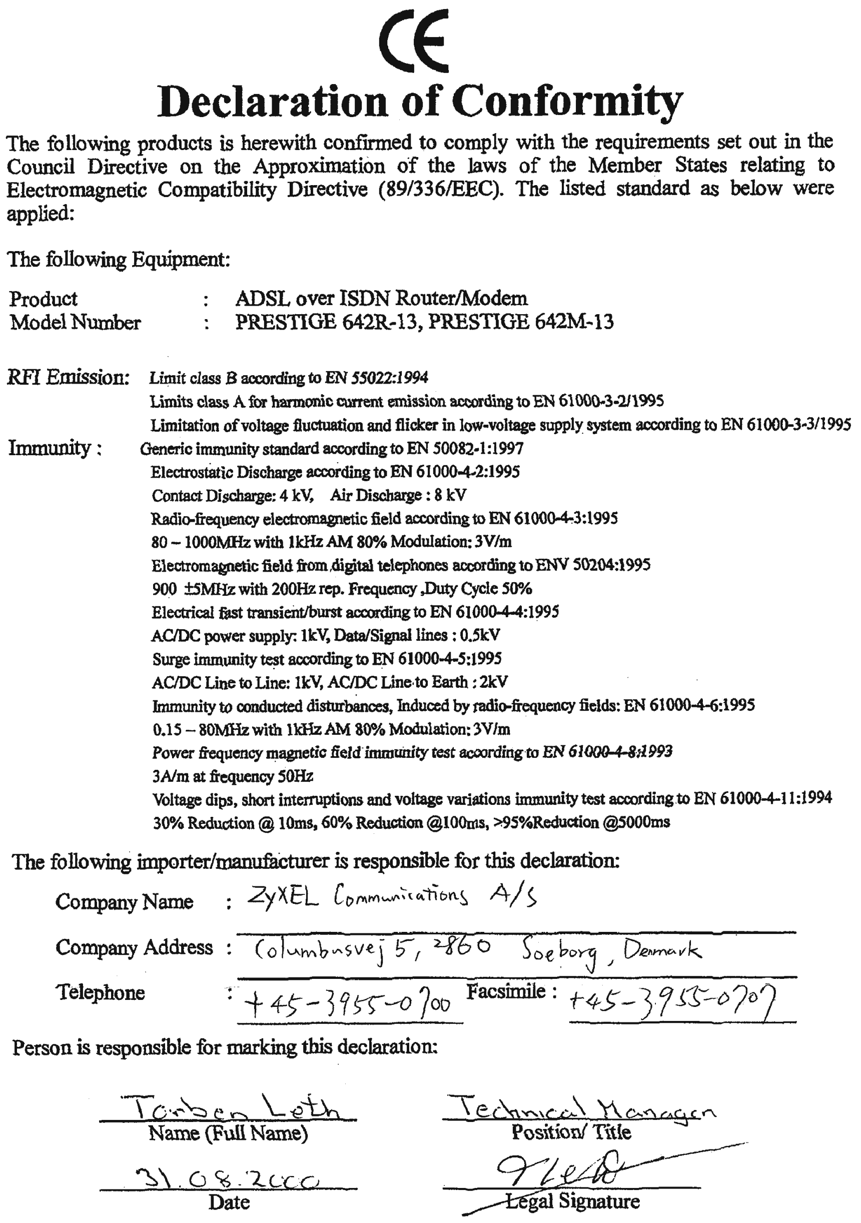
Manfred RECLA
Name (Full Name)

ZyXEL European Techn. Support
Position/ Title

Vienna, 03/22/2000
Date

Legal Signature

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



CE

Declaration of Conformity

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

The following Equipment:

Product	:	ADSL over ISDN Router/Modem
Model Number	:	PRESTIGE 642R-13, PRESTIGE 642M-13

RFI Emission: *Limit class B according to EN 55022:1994*
Limits class A for harmonic current emission according to EN 61000-3-2/1995
Limitation of voltage fluctuation and flicker in low-voltage supply system according to EN 61000-3-3/1995

Immunity : Generic immunity standard according to EN 50082-1:1997
Electrostatic Discharge according to EN 61000-4-2:1995
Contact Discharge: 4 kV, Air Discharge : 8 kV
Radio-frequency electromagnetic field according to EN 61000-4-3:1995
80 – 1000MHz with 1kHz AM 80% Modulation: 3V/m
Electromagnetic field from digital telephones according to ENV 50204:1995
900 ±5MHz with 200Hz rep. Frequency ,Duty Cycle 50%
Electrical fast transient/burst according to EN 61000-4-4:1995
AC/DC power supply: 1kV, Data/Signal lines : 0.5kV
Surge immunity test according to EN 61000-4-5:1995
AC/DC Line to Line: 1kV, AC/DC Line to Earth : 2kV
Immunity to conducted disturbances, Induced by radio-frequency fields: EN 61000-4-6:1995
0.15 – 80MHz with 1kHz AM 80% Modulation: 3V/m
Power frequency magnetic field immunity test according to EN 61000-4-8:1993
3A/m at frequency 50Hz
Voltage dips, short interruptions and voltage variations immunity test according to EN 61000-4-11:1994
30% Reduction @ 10ms, 60% Reduction @100ms, >95%Reduction @5000ms

The following importer/manufacturer is responsible for this declaration:

Company Name : ZyXEL Communications A/S

Company Address : Columbusvej 5, 2860 Soeborg, Denmark

Telephone : +45-3955-0700 Facsimile : +45-3955-0707

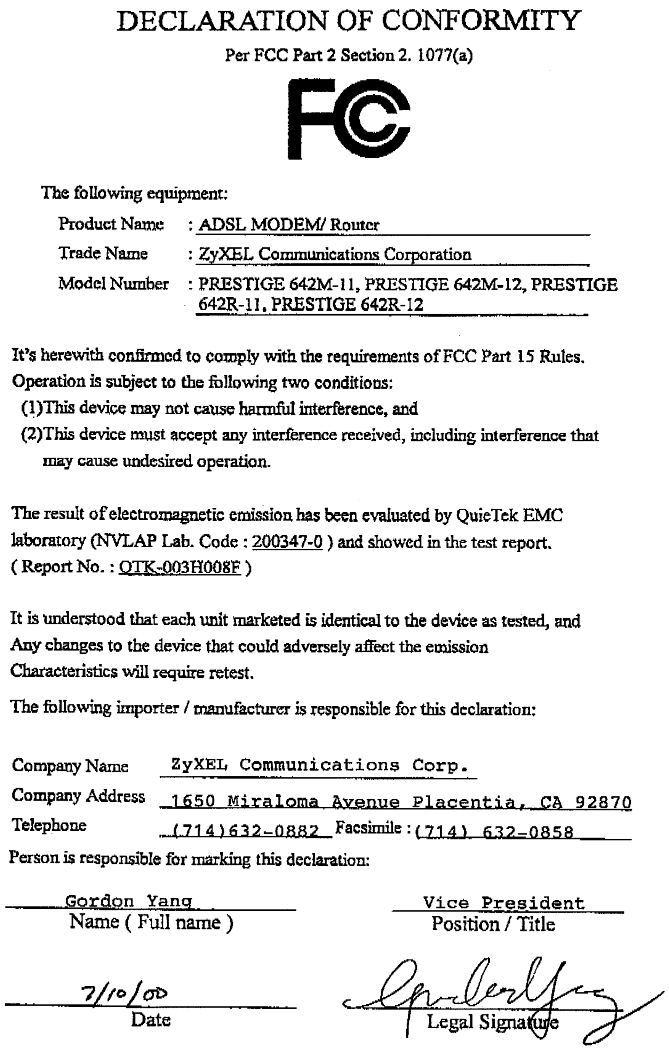
Person is responsible for marking this declaration:

Torben Leth
Name (Full Name)

Technical Manager
Position/ Title

31.08.2000
Date

Legal Signature



DECLARATION OF CONFORMITY

Per FCC Part 2 Section 2. 1077(a)

The following equipment:

Product Name : ADSL MODEM/ Router

Trade Name : ZyXEL Communications Corporation

Model Number : PRESTIGE 642M-11, PRESTIGE 642M-12, PRESTIGE 642R-11, PRESTIGE 642R-12

It's herewith confirmed to comply with the requirements of FCC Part 15 Rules.
Operation is subject to the following two conditions:
(1)This device may not cause harmful interference, and
(2)This device must accept any interference received, including interference that may cause undesired operation.

The result of electromagnetic emission has been evaluated by QuieTek EMC laboratory (NVLAP Lab. Code : 200347-0) and showed in the test report.
(Report No. : QTK-003H008F)

It is understood that each unit marketed is identical to the device as tested, and Any changes to the device that could adversely affect the emission Characteristics will require retest.

The following importer / manufacturer is responsible for this declaration:

Company Name ZyXEL Communications Corp.

Company Address 1650 Miraloma Avenue Placentia, CA 92870

Telephone (714)632-0882 Facsimile : (714) 632-0858

Person is responsible for marking this declaration:

Gordon Yang
Name (Full name)

Vice President
Position / Title

7/10/00
Date

Legal Signature

Federal Communications Commission (FCC) Interference Statement

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

- ♦ This device may not cause harmful interference.
- ♦ This device must accept any interference received, including interference that may cause undesired operations.

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

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

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

Notice 1

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

Notice 2

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

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

Note

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

To obtain the services of this warranty, contact ZyXEL's Service Center; refer to the separate Warranty Card for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid (USA and territories only). If the customer desires some other return destination beyond the U.S. borders, the customer shall bear the cost of the return shipment. This warranty gives you specific legal rights, and you may also have other rights that vary from state to state.

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

Customer Support

If you have questions about your ZyXEL product(s) or desire assistance, please contact ZyXEL Communications Corporation offices worldwide, in any one of the following ways. Our ftp sites are also available for software and ROM upgrades.

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

Table of Contents

List of Figures

List Of Tables

Preface

About Your ADSL Internet Access Router

Congratulations on your purchase of the Prestige 642R Series ADSL Internet Access Router.

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

The Prestige 642R is an ADSL router used for Internet/LAN access via an ADSL line. We will refer to the Prestige 642R Series as the Prestige 642R, P642 or simply the Prestige from now on.

The P642 can run maximum upstream transmission rates of 640Kbps and maximum downstream transmission rates of 8Mbps. The actual rate depends on the copper category of your telephone wire, distance from the central office and the type of ADSL service subscribed to. See the sections below for more background information on DSL and ADSL.

The P642's 10/100M auto-negotiating LAN interface enables fast data transfer of either 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 or the Prestige Network Commander (PNC).

About This User's Guide

This user's guide covers all aspects of the Prestige 642R 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 642R for various applications.

Related Documentation

➢ Supporting CD
The contents of this disk are:

1. PNC Software
2. Support Notes include:
   a. Configuring your P642 for Internet Access
   b. General FAQ
   c. Advanced FAQ
   d. Applications Notes
   e. Troubleshooting
   f. Reference CI Command
3. On-line Manual
4. Utility
5. Firmware/ROM File – this refers to the ZyNOS firmware and the router configuration file.

This information may also be viewed at our website (http://www.zyxel.com/). The website FAQs and Notes are periodically updated as new information becomes available.

➢ Read Me First

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

➢ Packing List Card

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

Syntax Conventions

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

Structure of this Manual

This manual is structured as follows:

Part 0: This part contains a Copyright Statement, a Declaration of Conformity, an FCC Interference Statement, a Warranty Description, Customer Support Contact Information, a Table of Contents, a List of Figures, a List of Tables, a Preface and notes on (A)DSL.

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

Part II: Advanced Applications (Chapters 4-7) describe the advanced applications of your Prestige, such as Remote Node Configuration, IPX Configuration and Bridging.

Part III: Advanced Management (Chapter 8 - 12) provides information on Prestige Filtering, SNMP, System Maintenance and Troubleshooting as well as some Appendices and a Glossary.

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

What is DSL?

DSL (Digital Subscriber Line) enhances the data capacity of the existing twisted-pair wire that runs between the local telephone company switching offices and most homes and offices. While the wire itself can handle higher frequencies, the telephone switching equipment is designed to cut off signals above 4,000 Hz to filter noise off the voice line, but now everybody is searching for ways to get more bandwidth to improve access to the Web - hence DSL technologies.

There are actually seven types of DSL service, ranging in speeds from 16 Kbits/sec to 52 Mbits/sec. The services are either symmetrical (traffic flows at the same speed in both directions), or asymmetrical (the downstream capacity is higher than the upstream capacity). Asymmetrical services (ADSL) are suitable for Internet users because more information is usually downloaded than uploaded. For example, a simple button click in a web browser can start an extended download that includes graphics and text.

As data rates increase, the carrying distance decreases. That means that users who are beyond a certain distance from the telephone company's central office may not be able to obtain the higher speeds.

A DSL connection is a point-to-point dedicated circuit, meaning that the link is always up and there is no dialing required.

What is ADSL?

It is an asymmetrical technology, meaning that the downstream data rate is much higher than the upstream data rate. As mentioned, this works well for a typical Internet session in which more information is downloaded, e.g., from Web servers, than is uploaded. ADSL operates in a frequency range that is above the frequency range of voice services, so the two systems can operate over the same cable. What are the advantages of ADSL from the point of view of the Network Service Provider (NSP) and the end user?

Advantages to the Network Service Provider (NSP)

1. ADSL enables telephone companies (telcos) to use the world's nearly 750 million existing copper wires to deliver affordable high-speed remote access to the Internet, corporate networks and on-line services over ordinary phone lines.
2. ADSL enables new applications that require real-time, interactive multimedia and broadcast-quality video. Such applications include collaborative computing, video conferencing, distance learning and video-on-demand.
3. The industry is rapidly converging on standards that will enable interoperability and ultimately make a mass market possible.
4. ADSL empowers service providers to provide either a guaranteed sustained or adaptive rate, or best effort service similar to analog modems.
   - Nearly 300 times faster than 24.4 Kbps modems
   - Over 100 times faster than 56 Kbps modems
   - 70 times faster than 128 Kbps ISDN
5. Both residential and business properties around the world are already running out of spare lines on existing installed telephone cables. ADSL provides service providers with the capability to use one line to provide new data services while maintaining the telephone service on the same line, thus leveraging the existing infrastructure.

6. ADSL provides telcos with the ability to offer a private, secure channel of communications between the consumer and the service provider.
7. Data travels along the customers own line, unlike cable telephone and modem services where the line is shared with others
8. Because it is one customer's dedicated line, transmission speeds are not affected by other users going on-line. With cable modems, transmission speeds drop significantly as more users go on-line
9. ADSL is "always on" and connected, just like a standard telephone. There is no time wasted dialing up the service several times a day and waiting to be connected; ADSL is on standby, waiting ready for use whenever your customer is ready.
10. Every major service provider has conducted trials and proven that the technology works. Today, service providers are rolling out ADSL services worldwide, with widespread deployment expected. In support of this market, a large number of major equipment vendors are shipping second and third-generation products offering higher performance and lower costs.
11. ADSL-based networks are well suited for carrying ATM traffic, thus guaranteeing ADSL technology for decades to come.
12. ADSL provides the communication bridge into the next century without adding new infrastructure, costly outside plant additions and reinvestment.

Advantages to the End User

1. ADSL transforms plain old telephone lines into a high speed conduit for data, information, entertainment and more. And while it is doing that, you can use your telephone for normal conversations at the same time. This provides enormous advantages whether at home or at work.
2. ADSL provides affordable high-speed remote access to the Internet, corporate networks and on-line services over ordinary phone lines.
   - Nearly 300 times faster than 24.4 Kbps modems
   - Over 100 times faster than 56 Kbps modems
   - 70 times faster than 128 Kbps ISDN

For example, if there were no constraints of the Internet backbone or if fast servers were located in every telephone central office, an ADSL modem could download the entire Encyclopedia Britannica to a user's laptop in 16.6 minutes, compared to 6.4 days using a typical modem speed of 14,400 bps.

3. ADSL enables the use of real-time, interactive multimedia and broadcast-quality video for such new services as collaborative computing, video conferencing, distance learning and video-on-demand.
4. ADSL gives you the ability to have both voice and data services in use simultaneously and all over one phone line. Both residential and business properties around the world are already running out of spare lines on existing installed telephone cables so effectively doubling your capacity in this way is a real benefit.
5. ADSL provides a private, secure channel of communications between you and the service provider.
6. Your data travels along you own line, unlike cable telephone and modem services where the line is shared with others.
7. Because it is your own dedicated line, transmission speeds are not affected by other users going on-line. With cable modems, transmission speeds drop significantly as more users go on-line.

8. ADSL is "always on" and connected, just like your telephone. 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 are.

Part I:

Getting Started

Chapters 1-3 are structured as a step-by-step guide to help you connect, install and set up your Prestige to operate on your network and to access the Internet. Described are Key Features and Applications, Hardware Installation, Initial Setup and Internet Access.

Chapter 1
Getting to Know Your ADSL Internet Access Router

This chapter describes the key features and applications of the Prestige 642.

1.1 Prestige 642R Series ADSL Internet Access Router

Your Prestige integrates a high-speed 10/100Mbps auto-negotiating LAN interface and one 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 642R

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

- **High Speed Internet Access**

The P642 ADSL router can support downstream transmission rates of up to 8Mbps and upstream transmission rates of 640Kbps. The P642 also supports rate management; rate management allows ADSL subscribers to select an Internet access speed that best suits their needs and budgets.

- **PPPoE Support (RFC2516)**

PPPoE (Point-to-Point Protocol over Ethernet) emulates a Dial-Up connection. It allows your ISP to use their existing network configuration with newer broadband technologies such as ADSL. The PPPoE driver on the Prestige is transparent to the PCs on the LAN, which see only Ethernet and are not aware of PPPoE thus saving you from having to manage PPPoE clients on individual PCs.

- **Transmission Rate Standards**
  - Supports Multi-Mode standard (ANSI T1.413, Issue 2; G.dmt(G.992.1); G.lite(G992.2)) [1].
  - Full-Rate (ANSI T1.413, Issue 2; G.dmt(G.992.1)) with line rate support of up to 8Mbps downstream and 1024kbps upstream.
  - G.lite (G.992.2) with line rate support of up to 1.5Mbps downstream and 512Kbps upstream.

- **IP Alias**

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

[1] Depends on firmware release version.

- **IP Multicast**

Traditionally, IP packets are transmitted in two ways: unicast or broadcast. Multicast is a third way to deliver IP packets to a group of hosts. IGMP (Internet Group Management Protocol) is the protocol used to support multicast groups. The latest version is version 2 (see RFC2236). Both versions 1 and 2 are supported by the Prestige

- **IP Policy Routing (IPPR)**

Traditionally, routing is based on the destination address only and the router takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator.

- **10/100M Fast Ethernet LAN Interface**

The P642's 10/100M auto-negotiating LAN interface enables fast data transfer of either 10Mbps or 100Mbps in either half-duplex or full-duplex mode depending on your Ethernet network.

- **Protocols Supported**
  - TCP/IP (Transmission Control Protocol/Internet Protocol) network layer protocol.
  - PPP (Point-to-Point Protocol) link layer protocol.
  - SUA™ (Single User Account) and NAT (Network Address Translation).

- **Multiple Protocol Support**
  - Novel IPX (Internetwork Packet eXchange) network layer protocol.
  - Transparently bridging for unsupported network layer protocols.

- **DHCP Support**

DHCP (Dynamic Host Configuration Protocol) allows the individual clients (computers) to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The Prestige has the built-in DHCP **Server** enabled by default. DHCP **Relay** allows the Prestige to act as a surrogate DHCP server where it relays IP address assignment from the actual DHCP server to its clients.

- **Multiple PVC (Permanent Virtual Circuits) Support**

Your Prestige supports up to 8 PVC’s.

- **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 642R Series supports VC-based and LLC-based multiplexing.

- **Encapsulation**

The Prestige 642R Series supports PPP (RFC 2364 - PPP over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM, MAC encapsulated routing 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.
    - ♦ Accessing SMT (System Management Terminal) through a Telnet connection
    - ♦ Windows-based PNC (Prestige Network Commander)

- **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 allows added network security and management.

- **Ease of Installation**

Your Prestige is designed for quick, intuitive and easy installation.

- **Housing**

Your Prestige's all new compact, ventilated housing minimizes space requirements making it easy to position anywhere in your busy office.

1.3 Applications for the Prestige 642R

1.3.1 Internet Access

The Prestige is the ideal high-speed Internet access solution. Your Prestige supports the TCP/IP protocol, which the Internet uses exclusively. It is compatible with all major ADSL DSLAM (Digital Subscriber Line Access Multiplexer) providers. A DSLAM is a rack of ADSL line cards with data multiplexed into a backbone network interface/connection (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 below.

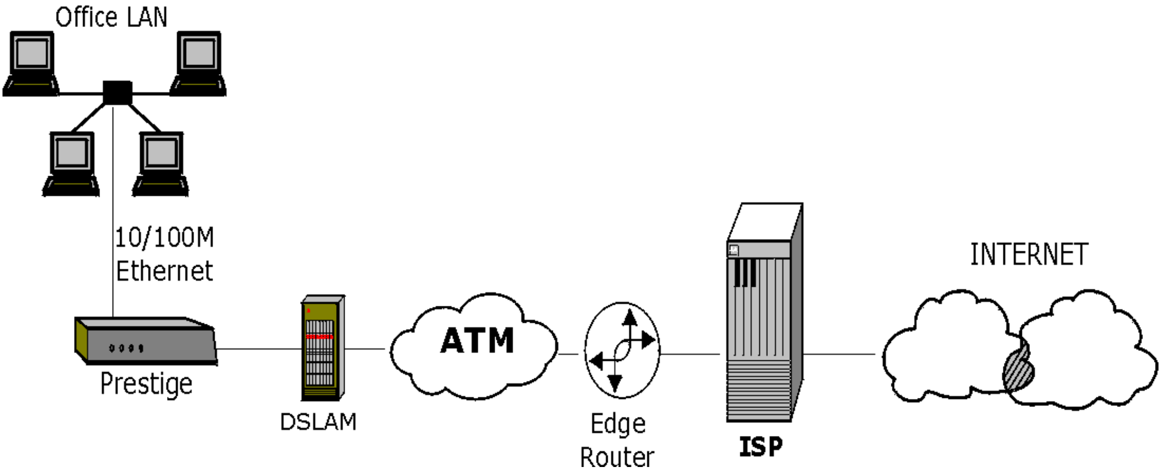


Figure 1-1 Internet Access Application

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 over the ADSL line. A typical LAN-to-LAN application for your Prestige is shown as follows.

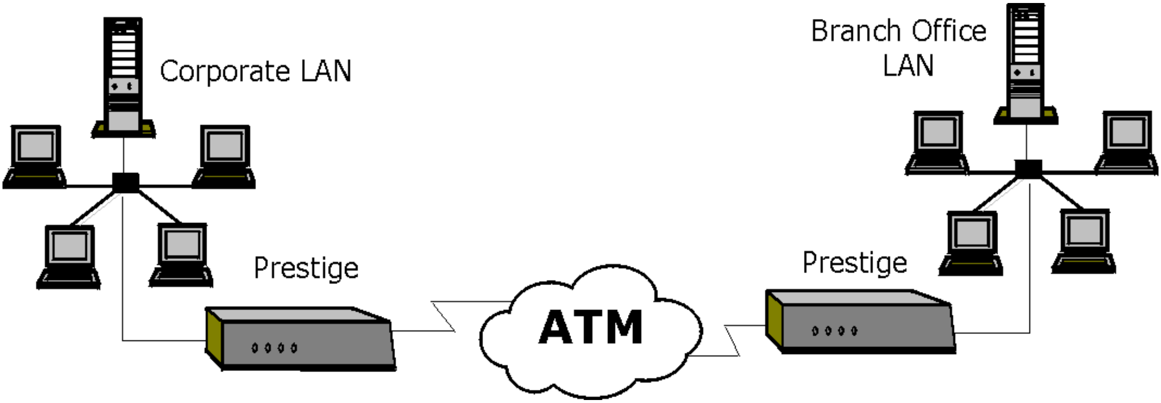


Figure 1-2 LAN-to-LAN Application

Chapter 2
Hardware Installation & Initial Setup

This chapter describes the physical features of the Prestige and how to make the cable connections.

2.1 Front Panel LEDs of the P642R

The LED indicators on the front panel indicate the operational status of the Prestige 642. The table below the diagram describes the LED functions:

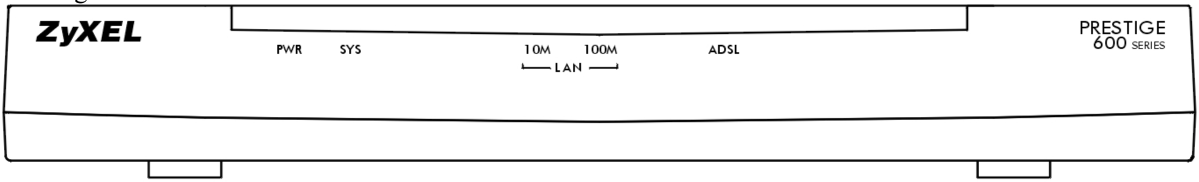


Figure 2-1 Prestige 642R Series Front Panel.

Table 2-1 Front Panel LED 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 system is rebooting when the SYS LED is blinking.
LAN 10M	A steady light indicates a 10Mb Ethernet connection. The LED will blink when data is being sent/received.
LAN 100M	A steady light indicates a 100Mb Ethernet connection. The LED will blink when data is being sent/received.
ADSL	The ADSL LED is on when the Prestige is connected successfully to a DSLAM. The LED blinks when data is being sent/received. The LED is off when the link is down.

2.2 Rear Panel and Connections of the Prestige 642R

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

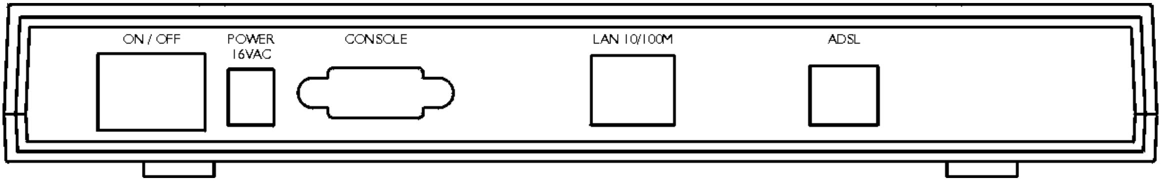


Figure 2-2 Prestige 642R Series Rear Panel

Step 1: *Connecting the ADSL Line*

Connect the Prestige directly to the wall jack using the included ADSL cable. Connect a microfilter(s) (see Figure 2-4 Connecting a 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 Workstation to the Prestige 10/100M LAN 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. Use the crossover cable (red tag) to connect your Prestige 642 to a computer directly. Use a straight-through-Ethernet cable (white tag) to connect to an external hub, then connect one end of the straight-through-Ethernet cable (white tag) from the hub to the NIC on the workstation.

Step 3. *Connecting the Power Adapter to your Prestige*

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

Please note that the Power Switch is not available in all P642 models.

Step 4. *Connecting the Console Port*

For the initial configuration of your Prestige, you need to use terminal emulator software on a workstation and connect it to the Prestige through the console port. Connect the 9-pin end of the console cable (9-pin to 25-pin console cable supplied) to the console port of the Prestige and the 25-pin end to a serial port (COM1, COM2 or other COM port) of your workstation. You can use an extension RS-232 cable if the enclosed one is too short.

2.3 Additional Installation Requirements

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

- A computer with an Ethernet 10Base-T/100Base-T NIC (Network Interface Card).
- A computer equipped with communications software (for example, Hyper Terminal in Win95) configured to the following parameters:
  - VT100 terminal emulation.
  - 9600 Baud rate.
  - Parity set to None, 8 Data bits, 1 Stop bit.

- Flow Control set to None

After the Prestige has been successfully connected to your network, you can make future changes to the configuration via Telnet.

2.4 Connecting a POTS Splitter

This is for the P642's following the Full Rate (G.dmt) standard only. 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 them 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 purchase of a POTS splitter is optional.

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 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 is easy to install as shown in the following figure.

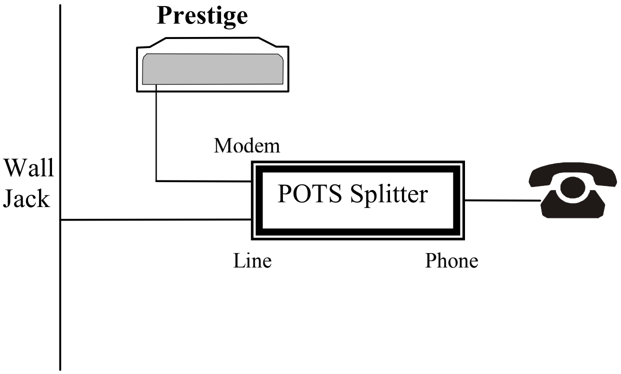


Figure 2-3 Connecting a POTS Splitter

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

Telephone voice transmissions take place in the lower frequency range, 0 - 4KHz, while ADSL transmissions take place in the higher bandwidth range, above 4KHz. A microfilter acts as a low-pass filter, for your telephone, to ensure that ADSL transmissions do not interfere with your telephone voice transmissions. . The purchase of a telephone microfilter is optional.

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

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

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

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

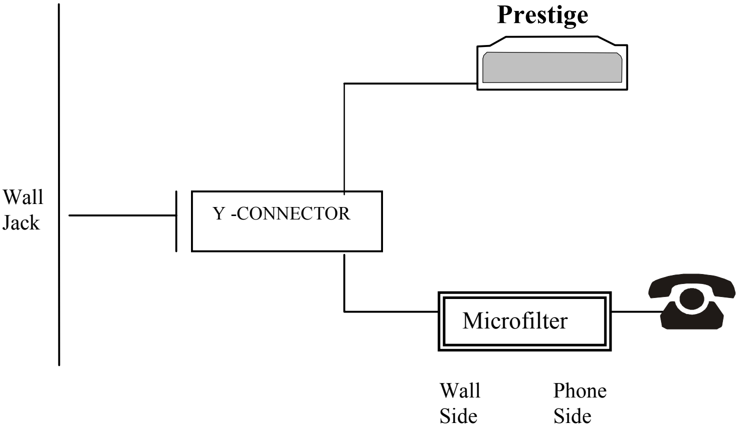


Figure 2-4 Connecting a Microfilter

2.6 Special Note for P642 ISDN Users

Please note that section 2.4 "**Connecting a POTS Splitter**" and sections 2.5 "**Telephone Microfilters**" of the P642 User's Guide do **not** apply for P642 ISDN users.

The following is an example installation for the P642 with ISDN.

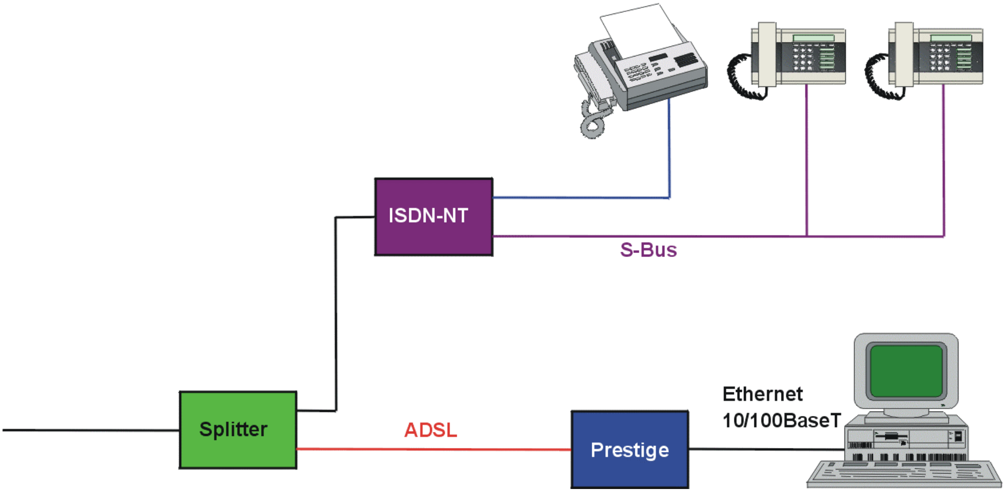


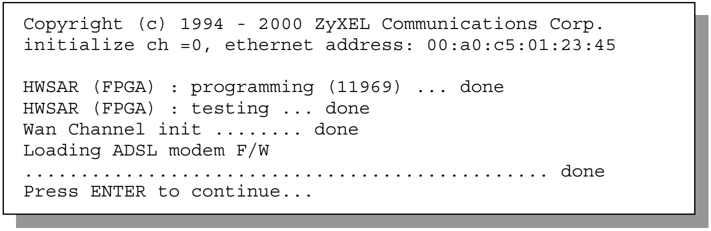
Figure 2-5 P642 with ISDN

2.7 Power Up Your Prestige

At this point, you should have connected the console port, the ADSL line, the Ethernet port and the power port to the appropriate devices or lines. You can now apply power to the Prestige.

Step 1. Initial Screen

When you power up your Prestige, it performs several internal tests as well as line initialization. After the initialization, the Prestige asks you to press [ENTER] to continue, as shown.



```
Copyright (c) 1994 - 2000 ZyXEL Communications Corp.
initialize ch =0, ethernet address: 00:a0:c5:01:23:45

HWSAR (FPGA) : programming (11969) ... done
HWSAR (FPGA) : testing ... done
Wan Channel init ........ done
Loading ADSL modem F/W
............................................... done
Press ENTER to continue...
```

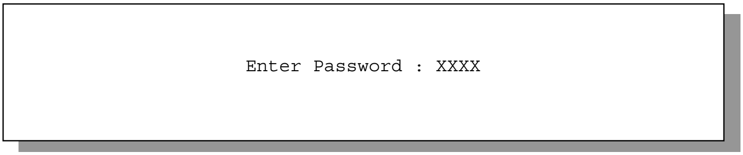
Figure 2-6 Power-On Display

Step 2. Entering Password

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

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

Please note that if there is no activity for longer than 5 minutes after you log in, your Prestige will automatically log you out and will display a blank screen. If you see a blank screen, press [ENTER] to bring up the login screen again.



```
Enter Password : XXXX
```

Figure 2-7 Login Screen

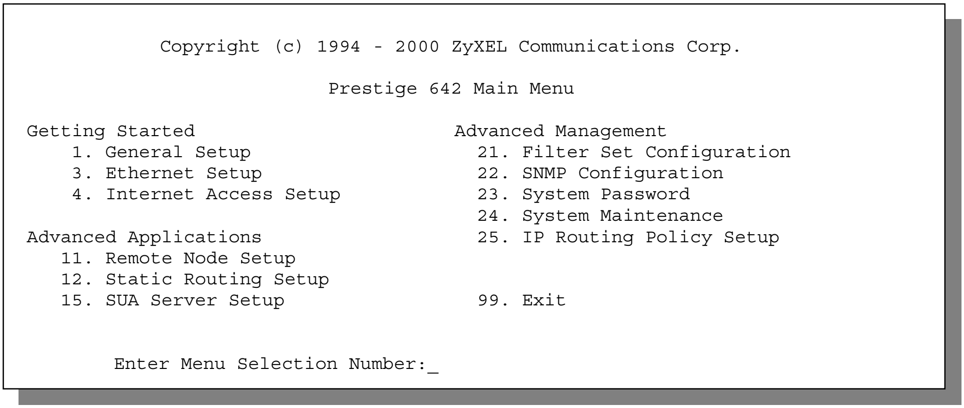
2.8 Navigating the SMT Interface

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

Table 2-2 Main Menu Commands

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

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



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

                            Prestige 642 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
 Advanced Applications                    25. IP Routing Policy Setup
    11. Remote Node Setup
    12. Static Routing Setup
    15. SUA Server Setup                  99. Exit


         Enter Menu Selection Number:_
```

Figure 2-8 SMT Main Menu

The SMT Menu continually improves and changes with new firmware upgrades. Check the release notes at www.zyxel.com to find the most recent upgrades and information.

2.8.1 System Management Terminal Interface Summary

Table 2-3 Main Menu Summary

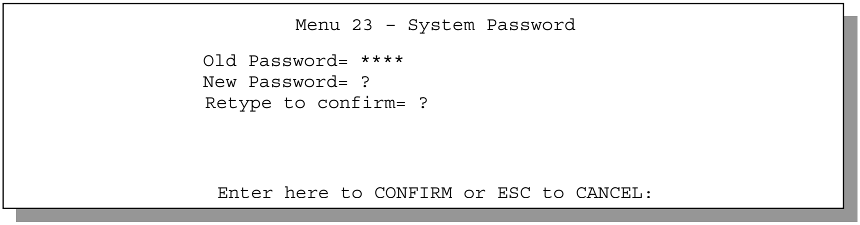
#	Menu Title	Description
1	General Setup	Use this menu to set up your general information.
3	Ethernet Setup	Use this menu to set up your LAN connection.
4	Internet Access Setup	A quick and easy way to set up an Internet connection.
11	Remote Node Setup	Use this menu to set up the Remote Node for LAN-to-LAN connection, including Internet connection.
12	Static Routing Setup	Use this menu to set up static routes.
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.

#	Menu Title	Description
24	System Maintenance	This menu provides system status, diagnostics, software upload, etc.
25	IP Routing Policy Setup	Use this menu to configure your IP routing policy.
99	Exit	Use this to exit from SMT and return to a blank screen.

2.9 Changing the System Password

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

Step 1. Enter 23 in the **Main Menu** to open **Menu 23 - System Password** as shown below. When this appears, type in your existing system password, i.e., 1234, and press [ENTER].



```
                     Menu 23 - System Password

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



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

Figure 2-9 Menu 23.1 - System Password

Step 2. Enter your new system password (up to 30 characters), and 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.

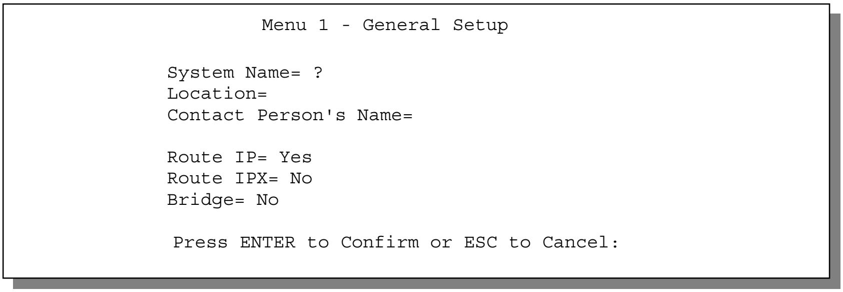
2.10 General Setup

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= ?
          Location=
          Contact Person's Name=

          Route IP= Yes
          Route IPX= No
          Bridge= No

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

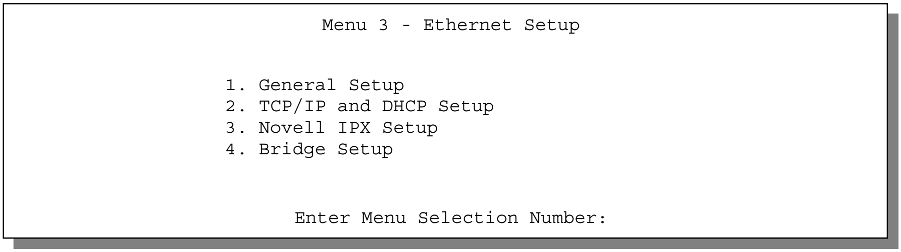
Figure 2-10 Menu 1 - General Setup

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.	P642
Location (optional)	Enter the geographic location (up to 31 characters) of your Prestige.	MyHouse
Contact Person's Name (optional)	Enter the name (up to 30 characters) of the person in charge of this Prestige.	JohnDoe
Protocols:	Press [SPACE BAR] to toggle routing on or off for the individual protocols.	
Route IP	Set this field to **Yes** to enable IP routing. You must enable IP routing for Internet access.	**Yes/No**
Route IPX	Set this field **Yes** to enable IPX routing.	**Yes/No**
Bridge	Turn on/off bridging for protocols not supported (e.g., SNA) or not turned on in the previous Route fields.	**Yes/No**

2.11 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.

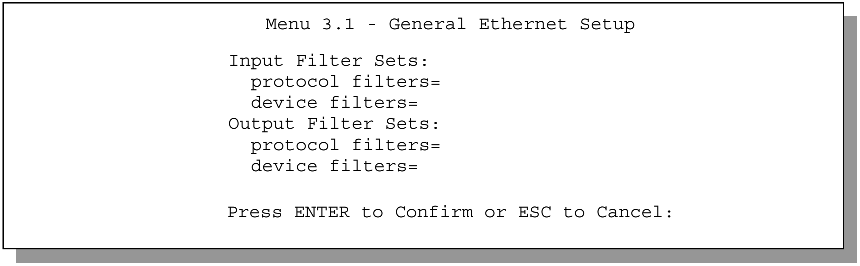


```
                          Menu 3 - Ethernet Setup


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



                        Enter Menu Selection Number:
```

Figure 2-11 Menu 3 - Ethernet Setup

2.11.1 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 2-12 Menu 3.1 - General Ethernet Setup

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

2.12 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 *Chapter 3 - Internet Access Application*.
- For Novell IPX Ethernet setup refer to *Chapter 6 - IPX Configuration*.
- For bridging Ethernet setup refer to *Chapter 7 - Bridging Setup.*

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 to section 3.4 **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 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.

3.2.1 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:

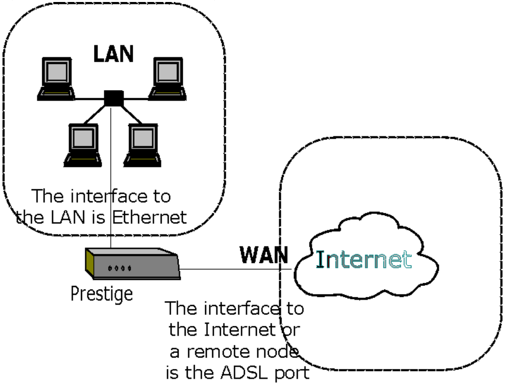

LAN
The interface to the LAN is Ethernet
WAN
Internet
Prestige
The interface to the Internet or a remote node is the ADSL port

Figure 3-1 LAN & WAN IPs

3.3 TCP/IP Parameters

3.3.1 IP Address and Subnet Mask

Like houses on a street that share a common street name, the machines on a LAN share one common network number.

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

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

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

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

Note: 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.*

3.3.3 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 a unusual network topology. Both **RIP-2B** and **RIP-2M** sends the routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on non-router machines since they generally do not listen to the RIP multicast address and so will not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting as well.

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

3.3.4 DHCP Configuration

DHCP (Dynamic Host Configuration Protocol) allows the individual clients (workstations) to obtain the TCP/IP configuration at start-up from a centralized DHCP server. The Prestige has built-in DHCP server capability, enabled by default, which means it can assign IP addresses, an IP default gateway and DNS servers to Windows 95, Windows NT 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 starting from 192.168.1.33 to 192.168.1.64 for the client machines. This leaves 31 IP addresses, 192.168.1.2 to 192.168.1.32 (excluding the Prestige itself which has a default IP of 192.168.1.1) for other server machines, 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 does give 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 workstation 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 workstation.

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 workstations and the workstations can query the DNS server directly without the Prestige's intervention.

3.4 IP Multicast

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

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

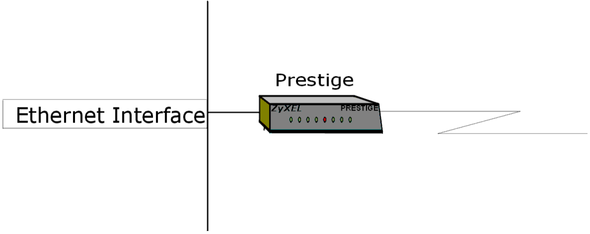
The Prestige supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). At start up, the Prestige queries all directly connected networks to gather group membership. After that, the Prestige periodically updates this information. IP Multicasting can be enabled/disabled on the Prestige LAN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

3.5 IP Policies

Traditionally, routing is based on the destination address *only* and the router takes the shortest path to forward a packet. IP Policy Routing (IPPR) provides a mechanism to override the default routing behavior and alter the packet forwarding based on the policy defined by the network administrator. Policy-based routing is applied to incoming packets on a per interface basis, prior to the normal routing. Create policies using SMT Menu 25 (*see the IP Policy Routing chapter in Part 3*) and apply them on the Prestige LAN and/or WAN interfaces using menus 3.2 (LAN) and 11.3 (WAN).

3.6 IP Alias

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



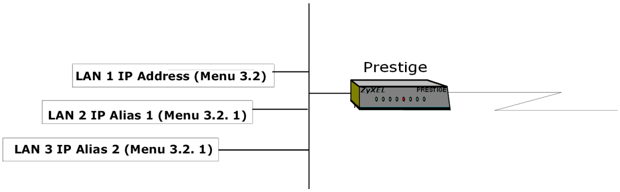
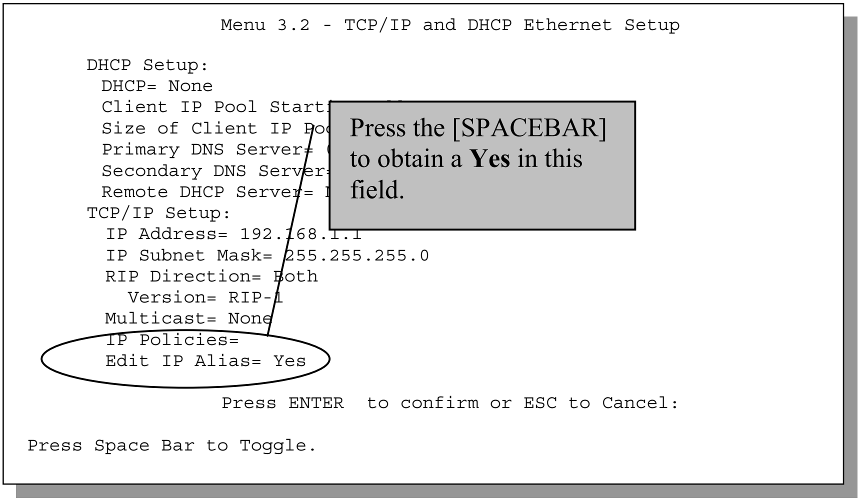

Prestige
LAN 1 IP Address (Menu 3.2)
LAN 2 IP Alias 1 (Menu 3.2. 1)
LAN 3 IP Alias 2 (Menu 3.2. 1)
ZyXEL
PRESTIGE

Figure 3-2 Physical Network ➔ Figure 3-3 Partitioned Logical Networks

Use menu 3.2.1 to configure IP Alias on your Prestige.

3.6.1 IP Alias Setup

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

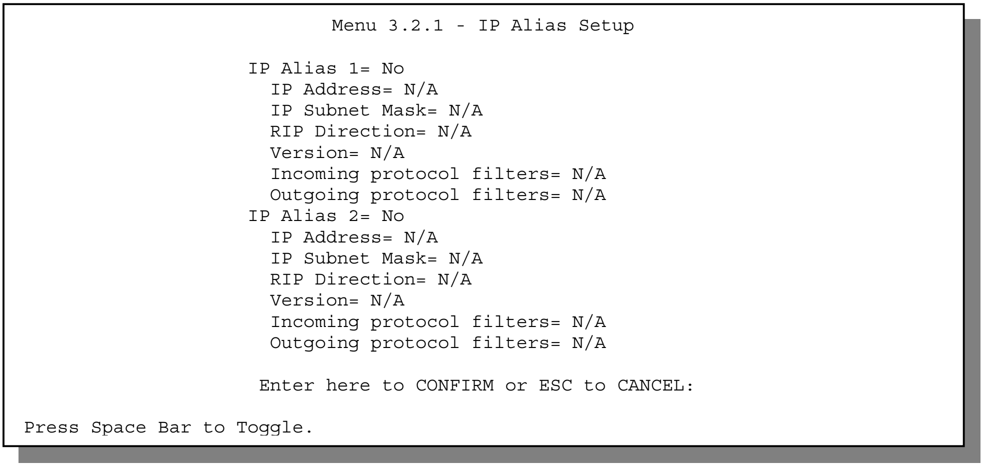


```
                   Menu 3.2 - TCP/IP and DHCP Ethernet Setup

       DHCP Setup:
        DHCP= None
        Client IP Pool Start
        Size of Client IP Poo
        Primary DNS Server= (
        Secondary DNS Server=
        Remote DHCP Server= N
       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=
         Edit IP Alias= Yes

                   Press ENTER  to confirm or ESC to Cancel:

  Press Space Bar to Toggle.
```

Press the [SPACEBAR] to obtain a **Yes** in this field.

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

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



```
                       Menu 3.2.1 - IP Alias Setup

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

                  Enter here to CONFIRM or ESC to CANCEL:

Press Space Bar to Toggle.
```

Figure 3-5 Menu 3.2.1 - IP Alias Setup

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

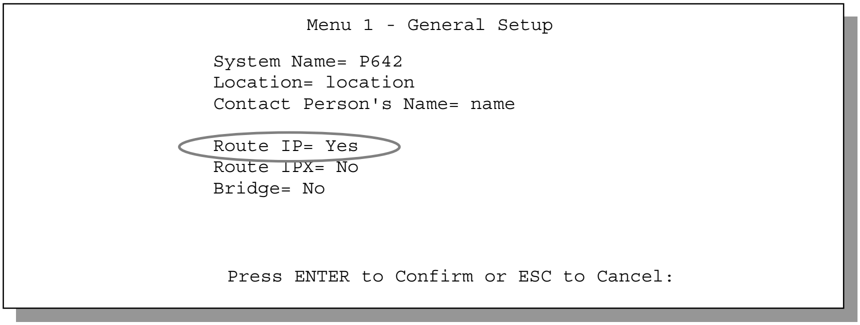
Table 3-1 IP Alias Setup Menu Fields

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 from **None, Both/In Only/Out Only.**	**None**
Version	Press the space bar to select the RIP version from **RIP-1/RIP-2B/RIP-2M.**	**RIP-1**
Incoming Protocol Filters	Enter the filter set(s) you wish to apply to the incoming traffic between this node and the Prestige.	
Outgoing Protocol Filters	Enter the filter set(s) you wish to apply to the outgoing traffic between this node and the Prestige.	
When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm…] to save your configuration, or press [ESC] at any time to cancel.		

3.7 Route IP Setup

The first step is to enable the 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.



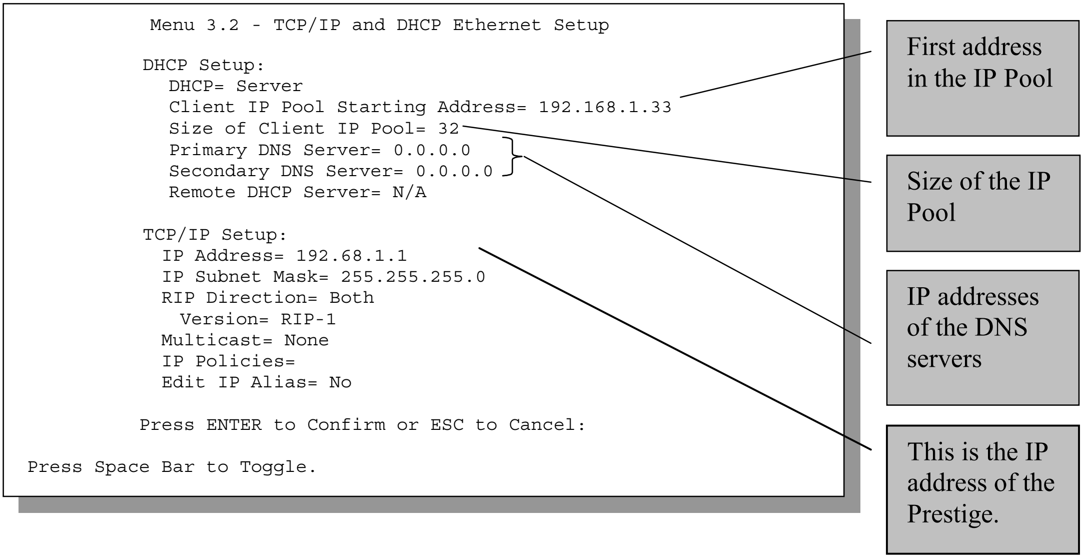
```
                        Menu 1 - General Setup

                System Name= P642
                Location= location
                Contact Person's Name= name

                Route IP= Yes
                Route IPX= No
                Bridge= No



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

Figure 3-6 Menu 1 - General Setup

3.8 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 from the **Main Menu** to open the **Menu 3 - Ethernet Setup**. When Menu 3 appears, select the submenu option **TCP/IP and DHCP Setup** 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=
             Edit IP Alias= No

            Press ENTER to Confirm or ESC to Cancel:

  Press Space Bar to Toggle.
```

First address in the IP Pool

Size of the IP Pool

IP addresses of the DNS servers

This is the IP address of the Prestige.

Figure 3-7 Menu 3.2 - TCP/IP and DHCP Ethernet Setup

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

Table 3-2 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 95, Windows NT and other systems that support the DHCP client. If set to **None**, the DHCP server will be disabled. If set to **Relay,** the Prestige acts as a surrogate DHCP server and relays DHCP requests and responses between the remote server and the clients. Enter the IP address of the actual, remote DHCP server in the **Remote DHCP Server** in this case. When DHCP is used, the following items need to be set:	**None** **Server** (default) **Relay**
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 3-3 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/RIP-2M**.	**RIP-1** (default)
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The Prestige supports both IGMP version 1 (**IGMP-v1**) and **IGMP-v2**. Press the	**IGMP-v1** **IGMP-v2** **None**

	space bar to enable IP Multicasting or select **None** to disable it.	
IP Policies	Create policies using SMT Menu 25 (*see the IP Policy Routing chapter in Part 3*) and apply them on the Prestige LAN interface here. You can apply up to four IP Policy sets (from twelve) by entering their numbers here separated by commas, e.g., 2, 4, 7, 9.	
Edit IP Alias	The Prestige supports three logical LAN interfaces via its single physical Ethernet interface with the Prestige itself as the gateway for each LAN network. Press the [SPACEBAR] to toggle **No** to **Yes**, then press [ENTER] to bring you to menu 3.2.1	**Yes** **No** (default)
When you have completed this menu, press [ENTER] at the prompt [Press ENTER to Confirm…] to save your configuration, or press [ESC] at any time to cancel.		

The following terminology may seem a little overwhelming at first to new users of broadband technology. Relax! This information should be either pre-configured on your Prestige or supplied by your ISP or telephone company. Think of them as the equivalent of “telephone numbers” on traditional dial-up PSTN and ISDN modems and routers.

3.9 VPI & VCI

Be sure to use the correct Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) numbers supplied by the telephone company. The valid range for the VPI is 1 to 255 and for the VCI is 32 to 65535 (1 to 31 is reserved for local management of ATM traffic). Please see the Appendices for more information.

3.10 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.

3.10.1 VC-based multiplexing

In this case, by prior mutual agreement, each protocol is assigned to a specific virtual circuit, e.g., 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.

3.10.2 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, e.g., if charging heavily depends on the number of simultaneous VCs.

3.11 Encapsulation

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

3.11.1 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.

3.11.2 PPP over Ethernet

PPPoE provides access control and billing functionality in a manner similar to dial-up services using PPP. The Prestige bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your PC to an ATM PVC (Permanent Virtual Circuit) which connects to a xDSL Access Concentrator where the PPP session terminates. One PVC can support any number of PPP sessions from your LAN. For more information on PPPoE, see the Appendices.

3.11.3 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.

3.11.4 RFC 1483

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

3.12 IP Address Assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However the encapsulation method assigned influences your choices for IP Address and ENET ENCAP Gateway.

3.12.1 Using PPP or PPPoE Encapsulation

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

3.12.2 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.

3.12.3 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.

3.13 Internet Access Configuration

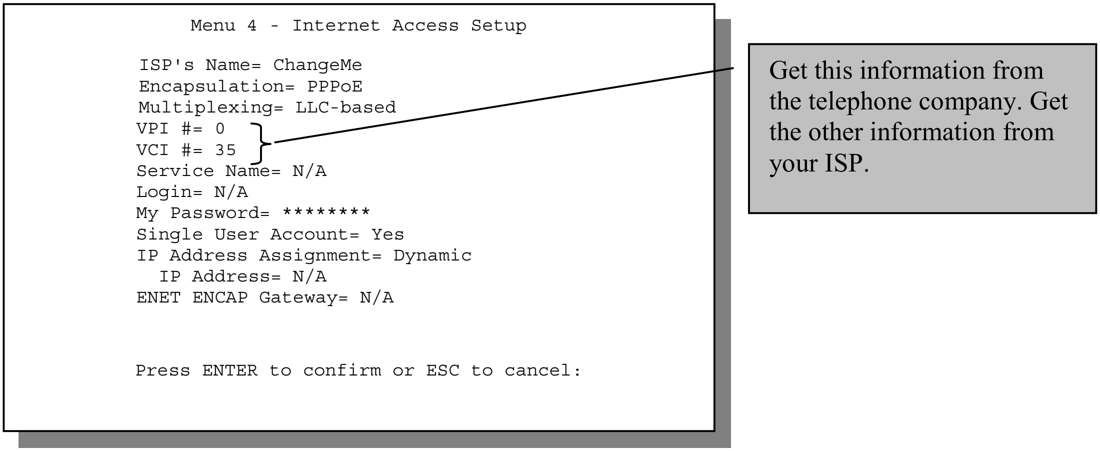
Menu 4 allows you to enter the Internet Access information in one screen. Menu 4 is actually a simplified setup for one of the remote nodes that you can access in Menu 11. Before you configure your Prestige for Internet access, you need to collect your Internet account information from your ISP and telephone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

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

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 displayed below. 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 #= 0
            VCI #= 35
            Service Name= N/A
            Login= N/A
            My Password= ********
            Single User Account= Yes
            IP Address Assignment= Dynamic
              IP Address= N/A
            ENET ENCAP Gateway= N/A



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

Get this information from the telephone company. Get the other information from your ISP.

Figure 3-8 Internet Access Setup

Table 3-5 Internet Access Setup Menu Fields

Field	Description	Options/E.G.
ISP's Name	Enter the name of your Internet Service Provider, e.g., myISP. This information is for identification purposes only.	**e.g., MyISP**
Encapsulation	Press [SPACE BAR] to select the method of encapsulation used by your ISP.	**PPPoE, PPP, RFC 1483 or ENET ENCAP.**
Multiplexing	Press [SPACE BAR] to select the method of multiplexing used by your ISP - either **VC-based** or **LLC-based**.	**VC-based LLC-based**
Service Name	This is valid only when you have chosen **PPPoE** encapsulation. If you are using **PPPoE** encapsulation, then type the name of your PPPoE service here.	**poellc**
VPI #	Enter the Virtual Path Identifier (VPI) that the telephone company gives you.	**e.g., 0**
VCI #	Enter the Virtual Channel Identifier (VCI) that the telephone company gives you.	**e.g., 35**
My Login	Enter the login name that your ISP gives you. If you are using **PPPoE** encapsulation, then this field must be of the form user@domain where domain identifies your ISP.	**e.g., tarbuck**
My Password	Enter the password associated with the login name above.	***
Single User Account	Press [SPACE BAR] to enable or disable SUA. Please see the following section for a more detailed discussion on the Single User Account feature.	**Yes/No**
IP Address Assignment	Press [SPACE BAR] to select **Static** or **Dynamic** address assignment.	**Static / Dynamic**
IP Address	Enter the IP address supplied by your ISP if applicable.	**e.g., 192.168.1.1**
ENET ENCAP Gateway	Enter the gateway IP address supplied by your ISP if applicable.	**e.g., 192.168.1.100**
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.		

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

3.14 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).

The IP address for the SUA can be either fixed or dynamically assigned by the ISP. In addition, you can designate servers, e.g., a web server and a Telnet server, on your local network and make them accessible to the outside world. If you do not define any 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).*

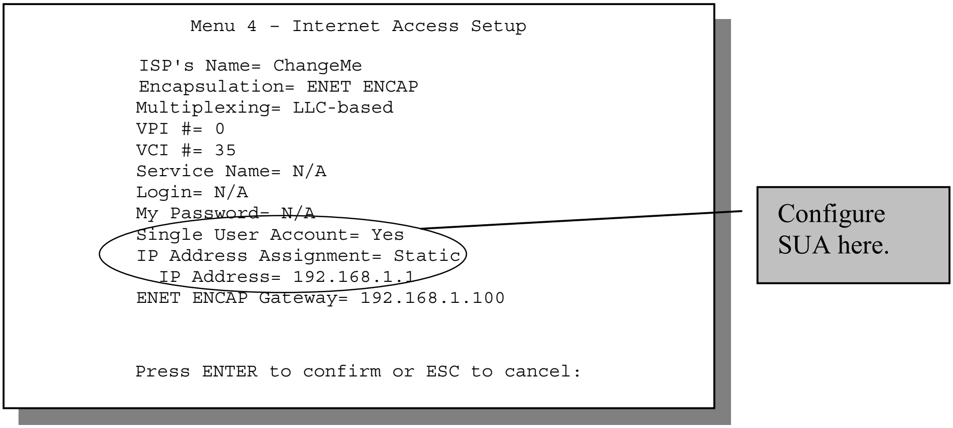
3.14.1 Advantages of SUA

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.

3.14.2 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= ChangeMe
    Encapsulation= ENET ENCAP
    Multiplexing= LLC-based
    VPI #= 0
    VCI #= 35
    Service Name= N/A
    Login= N/A
    My Password= N/A
    Single User Account= Yes
    IP Address Assignment= Static
      IP Address= 192.168.1.1
    ENET ENCAP Gateway= 192.168.1.100


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

Configure SUA here.

.

Figure 3-9 Menu 4 - Internet Access Setup and 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	Select **Yes** to enable SUA.
IP Address Assignment	Press [SPACE BAR] to toggle between Dynamic and Static. If you have a static IP Address, enter it in dotted decimal notation into the IP Address field. If you have a dynamic IP Address, the IP Address field will be N/A.
IP Address	Enter your IP Address here in dotted decimal notation if you have a static IP. If you have a dynamic IP address then the field becomes N/A.
Press [ENTER] at the message [Press ENTER to confirm...] to save your configuration, or press [ESC] at any time to cancel.	

3.15 Multiple Servers behind SUA

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

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

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

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

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

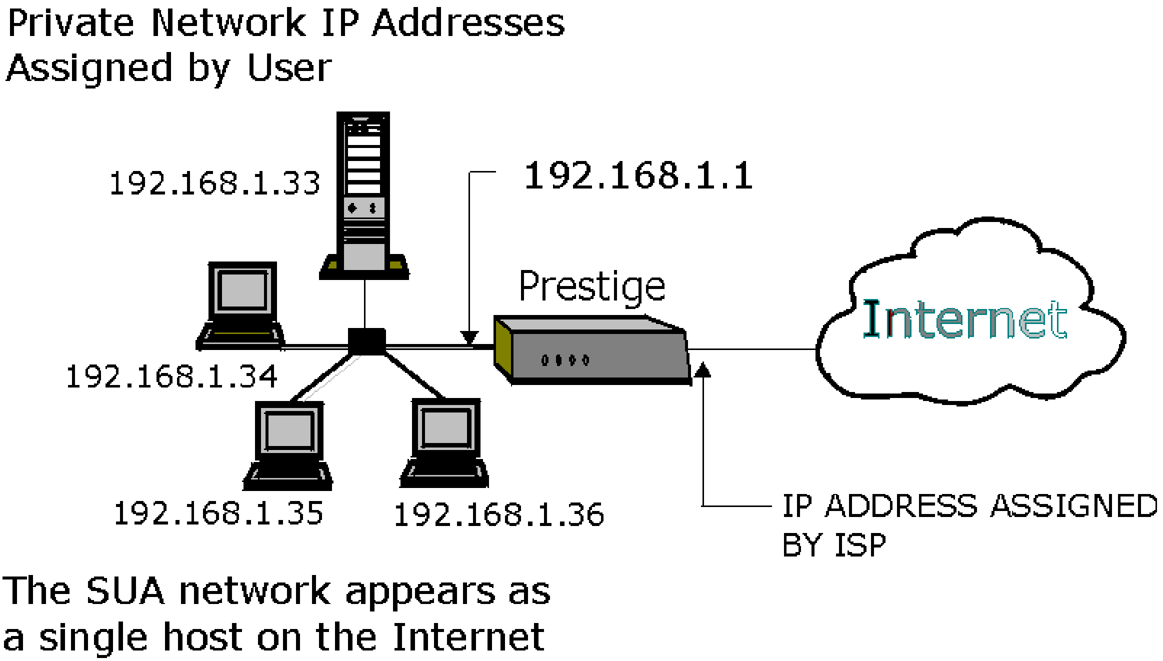


Figure 3-10 Single User Account Topology

3.15.1 Configuring a Server behind SUA

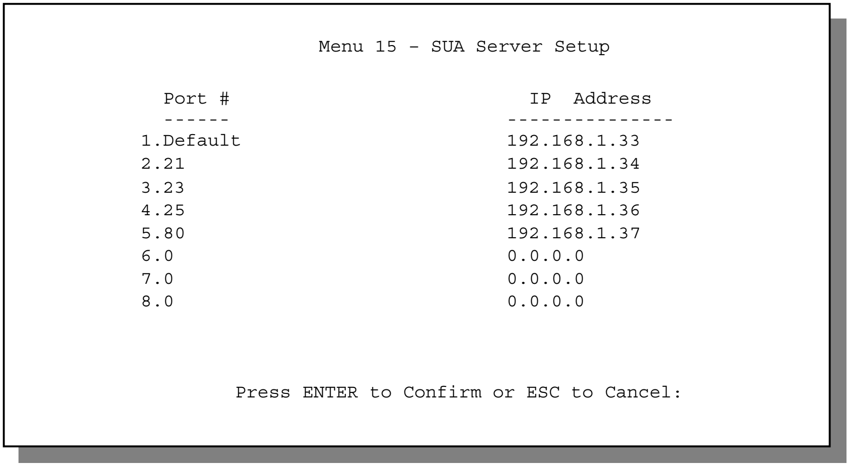
Follow the steps below to configure a server behind SUA:

1. Enter 15 in the main menu to go to **Menu 15 - SUA Server Setup**.
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.

Figure 3-11 Multiple Server Configuration

The most often used port numbers are:



```
                          Menu 15 - SUA Server Setup

            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:
```

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

Advanced Applications (Chapters 4 to 7) describes the advanced applications of your Prestige. Described are Remote Node Setup, Remote Node TCP/IP Configuration, IPX Configuration and Bridging Setup.

Chapter 4
Remote Node Configuration

In this chapter, we discuss the parameters that are protocol independent. The protocol-dependent configurations are 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

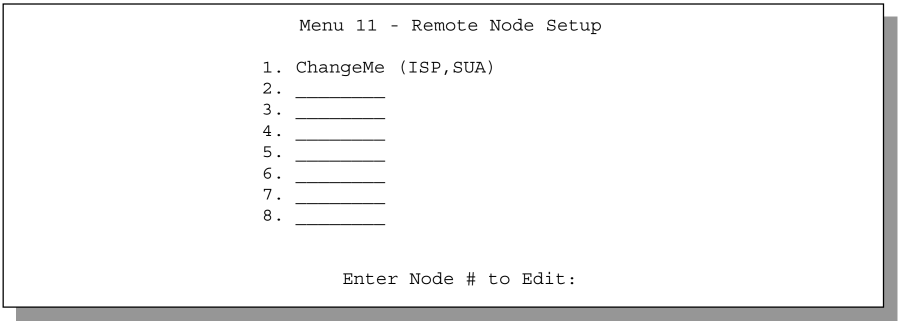
This section describes the protocol-independent parameters for a remote node.

4.1.1 Remote Node Profile

To configure a remote node, follow these steps:

Step 1. From the **Main Menu**, select menu option **11 - Remote Node Setup.**

Step 2. When **Menu 11** appears, as shown in the following figure, 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

4.1.2 Encapsulation and Multiplexing Scenarios

For Internet access you should use the encapsulation and multiplexing methods used by your ISP. For LAN-to-LAN applications, e.g., branch office and corporate headquarters, prior mutual agreement on methods used is necessary because there is no mechanism to automatically determine encapsulation or 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 PPP over Ethernet (**PPPoE**) and **ENET ENCAP** encapsulation entail makes them a poor choice in a LAN-to-LAN application. Here are some examples of more suitable combinations in such an application.

Scenario 1. One VC, Multiple Protocols

PPP (RFC-2364) encapsulation with **VC-based** multiplexing is the best combination because the extra protocol identifying headers that **LLC-based** multiplexing uses is not needed. The **PPP** protocol already contains this information.

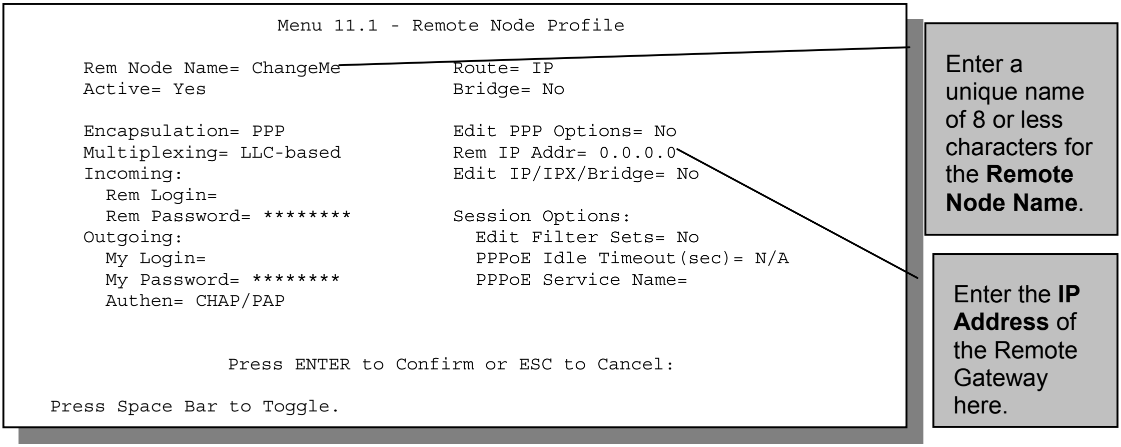
Scenario 2. One VC, One Protocol (IP)

Select **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 do not need to reconfigure either machine when the time comes.

Scenario 3. Multiple VCs

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

When **Menu 11.1** – **Remote Node Profile** appears fill in the fields as described in the following table to define this remote profile. The Remote Node Profile Menu Fields table shows you how to configure the Remote Node Menu.



```
                        Menu 11.1 - Remote Node Profile

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

       Encapsulation= PPP               Edit PPP Options= No
       Multiplexing= LLC-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=                        PPPoE Idle Timeout(sec)= N/A
         My Password= ********            PPPoE Service Name=
         Authen= CHAP/PAP


                    Press ENTER to Confirm or ESC to Cancel:

    Press Space Bar to Toggle.
```

Enter a unique name of 8 or less characters for the **Remote Node Name**.

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	OPTIONS
Rem Node Name	This is a required field. Enter a descriptive name for the remote node, for example, Corp. This field can be up to eight characters. This name must be unique from any other remote node name or remote dial-in user name.	
Active	Press [space bar] to toggle between **Yes** and **No**. Inactive nodes are displayed with a minus sign (–) at the beginning of the name in **Menu 11**.	**Yes** or **No**
Encapsulation	**PPP** refers to RFC-2364 (PPP Encapsulation over ATM Adaptation Layer 5). If **RFC-1483** (Multiprotocol Encapsulation over ATM Adaptation Layer 5) of **ENET ENCAP** are selected, then the **Rem Login**, **Rem Password**, **My Login**, **My Password**, **Edit PPP Options** and **Authen** fields is not applicable (**N/A**). Moreover, **ENET ENCAP** encapsulaton does not apply for IPX routing.	**PPP** **RFC-1483** **ENET ENCAP**

Multiplexing	Press [space bar] to select the multiplexing method.	**VC-based** **LLC-based**
Incoming: Rem Login	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 Password will be used to authenticate this node.	
Rem Password	Enter the password used when this remote node calls your Prestige.	
Outgoing: My Login	Enter the login name assigned by your ISP when the Prestige calls this remote node.	
My Password	Enter the password assigned by your ISP when the Prestige calls this remote node.	
Authen	This field sets the authentication protocol used for outgoing calls. Options for this field are:	
	● **CHAP/PAP** – Your Prestige will accept either CHAP or PAP when requested by this remote node.	**CHAP/PAP**
	● **CHAP** – accept CHAP (Challenge Handshake Authentication Protocol) only.	**CHAP**
	● **PAP** – accept PAP (Password Authentication Protocol) only.	**PAP**
Route	This field determines the protocol that your Prestige will route.	**IP / IPX / IP+IPX / None**
Bridge	Bridging is used for protocols that the Prestige does not route, e.g., SNA, or not turned on in the previous Route field. When bridging is enabled, your Prestige will forward any packet that it does not route to this remote node; otherwise, the packets are discarded. Press the [space bar] to toggle between the options.	**Yes** or **No**
Edit PPP Options	To edit the PPP options for this remote node, move the cursor to this field. Use [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*	Press [space bar] to toggle **Yes** then press [Enter]

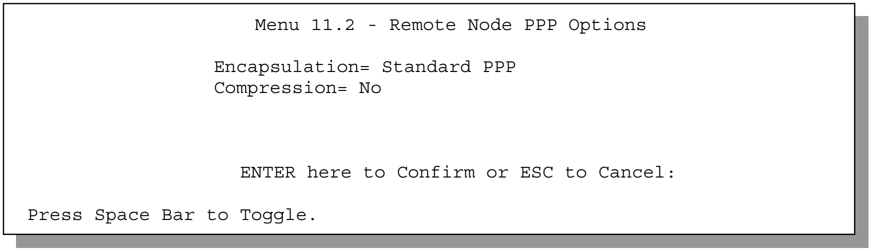
	Options.	
Rem IP Addr	Enter the IP address of the remote gateway.	
Edit IP/IPX/Bridge	Press [space bar] to select **Yes** and press [Enter] to go to **Menu 11.3 – Remote Node Network Layer Options**.	**Yes** or **No**
Session Options: Edit Filter Sets	Press [space bar] to select **Yes** and press [Enter] to open Menu 11.5 to edit the filter sets. See the Remote Node Filter section for more details.	**Yes** or **No**
PPPoE Idle Timeout (sec)	This value specifies the number of idle seconds that elapse before the Prestige automatically disconnects the PPPoE session.	**100** (default)
PPPoE Service Name	This is valid only when you have chosen PPPoE encapsulation. If you are using PPPoE encapsulation, then type the name of your PPPoE service here.	
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

Generally speaking, you should employ the strongest authentication protocol possible, for obvious reasons. However, some vendor's implementation includes specific authentication protocol in the user profile. It will disconnect if the negotiated protocol is different from that in the user profile, even when the negotiated protocol is stronger than specified. If you encounter the 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 [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



                    ENTER here 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.

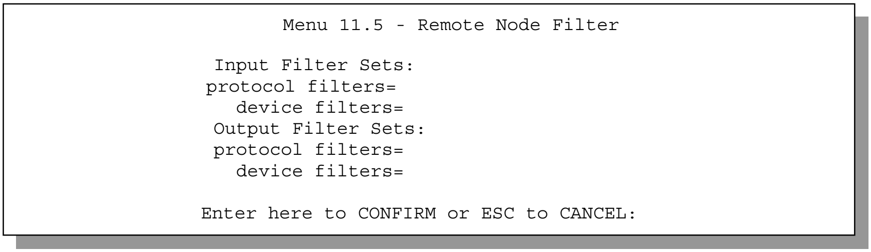
Table 4-2 Remote Node PPP Options Menu Fields

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

4.1.5 Remote Node Filter

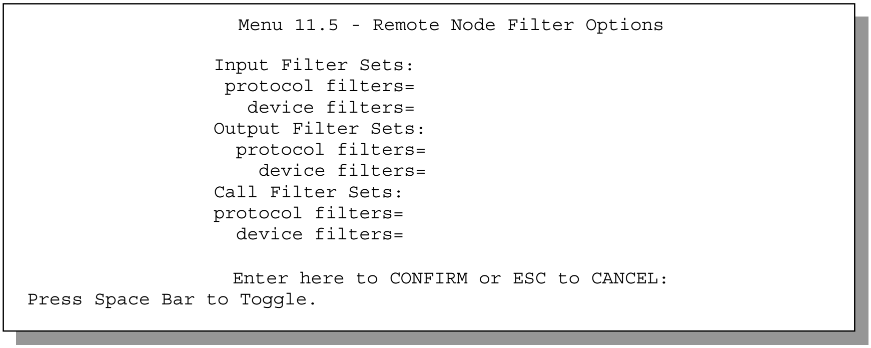
In **Menu 11.1 – Remote Node Profile** make sure the **Edit Filter Sets** field displays **Yes** by toggling the [spacebar]. Press [ENTER] to access **Menu 11.5 – Remote Node Filter**.

Use **Menu 11.5 – Remote Node Filter** to specify the filter set(s) to apply to the incoming and outgoing traffic between this remote node and the Prestige. You can specify up to 4 filter sets separated by commas, eg. 1, 5, 9, 12 in each filter field. For more information on defining the filters, see the **Filter Configuration** chapter. Note that there are two versions of this menu depending on whether you use PPPoE encapsulation or not. When using PPPoE encapsulation, you can also specify remote nodes called filter sets.



```
                       Menu 11.5 - Remote Node Filter

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

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

Figure 4-4 Menu 11.5 - Remote Node Filter



```
                   Menu 11.5 - Remote Node Filter Options

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

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

Figure 4-5 Remote Node Filter (PPPoE Encapsulation)

Chapter 5
Remote Node TCP/IP Configuration

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

5.1 LAN-to-LAN Application

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.

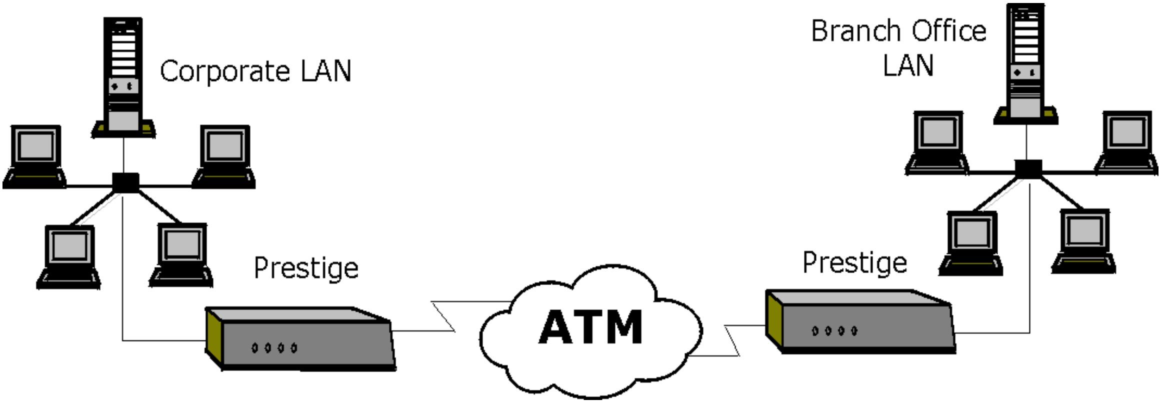


Figure 5-1 TCP/IP LAN-to-LAN Application

For the branch office, you need to configure a remote node in order to dial out to 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

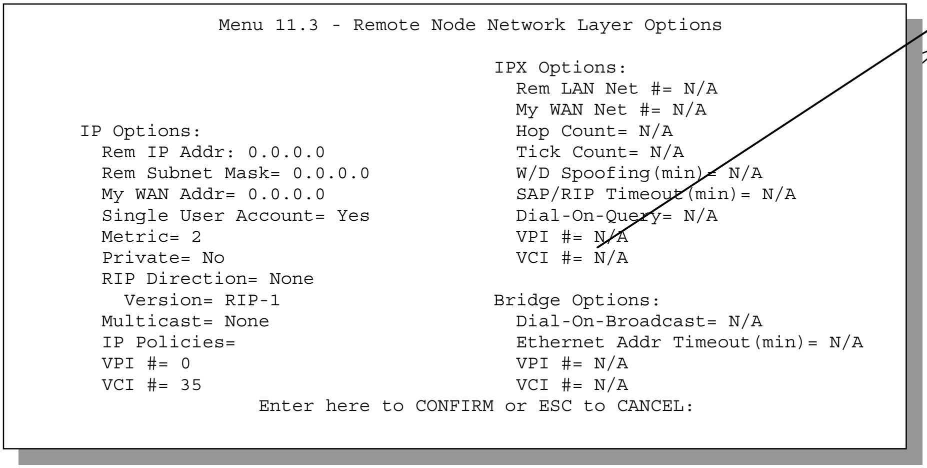
Follow the steps below to edit **Menu 11.3 – Remote Node Network Layer Options**.

In **Menu 11.1**, move the cursor to the **Edit IP/IPX/Bridge**, then press [space bar] to toggle and set the value to **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. However, note that for PPP or PPPoE encapsulation, we just need 1 VC no matter what protocol (IP/IPX/Bridge) is being carried.



```
                   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
         My WAN Addr= 0.0.0.0             SAP/RIP Timeout(min)= N/A
         Single User Account= Yes         Dial-On-Query= N/A
         Metric= 2                        VPI #= N/A
         Private= No                      VCI #= N/A
         RIP Direction= None
           Version= RIP-1                Bridge Options:
         Multicast= None                   Dial-On-Broadcast= N/A
         IP Policies=                      Ethernet Addr Timeout(min)= N/A
         VPI #= 0                          VPI #= N/A
         VCI #= 35                         VCI #= N/A
                       Enter here to CONFIRM or ESC to CANCEL:
```

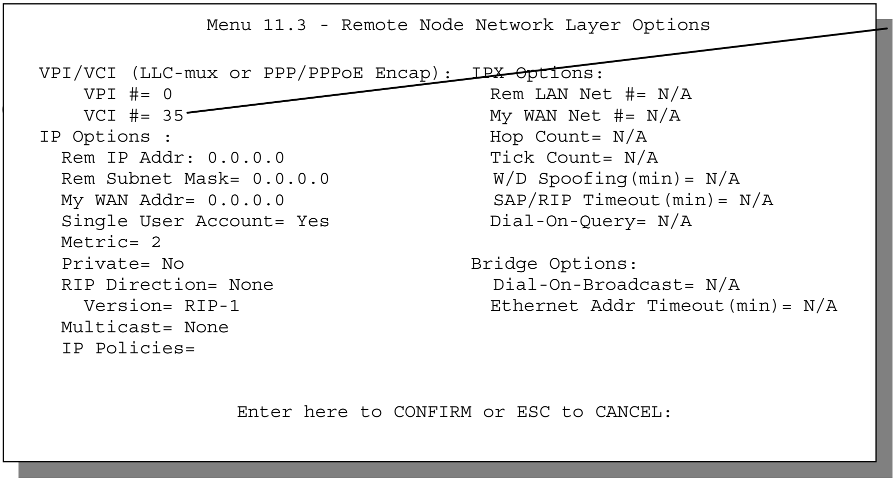
Separate VPI and VCI numbers must be specified for each protocol when using VC-based multiplexing as there must be a distinct PVC for each

Figure 5-2 Menu 11.3 for VC-based Multiplexing

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

LLC-based Multiplexing

For **LLC-based** multiplexing, one VC may carry 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 #= N/A
    VCI #= 35                           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
  My WAN Addr= 0.0.0.0                  SAP/RIP Timeout(min)= N/A
  Single User Account= Yes              Dial-On-Query= N/A
  Metric= 2
  Private= No                          Bridge Options:
  RIP Direction= None                   Dial-On-Broadcast= N/A
    Version= RIP-1                      Ethernet Addr Timeout(min)= N/A
  Multicast= None
  IP Policies=


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

Only one set of VPI and VCI numbers need be specified as for **LLC-based** multiplexing or when using **PPP** or **PPPoE** encapsulation. One VC may carry different protocols.

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 0 to 255 and for the VCI is 32 to 65535 (1 to 31 is reserved for local management of ATM traffic).

The following diagram explains the sample IP addresses to help you understand the field of **My Wan Addr** in **Menu 11.3**. Refer to the following figure for a brief review of what a WAN IP is. **My WAN Addr** indicates the local Prestige WAN IP while **Rem IP Addr** indicates the peer WAN IP.

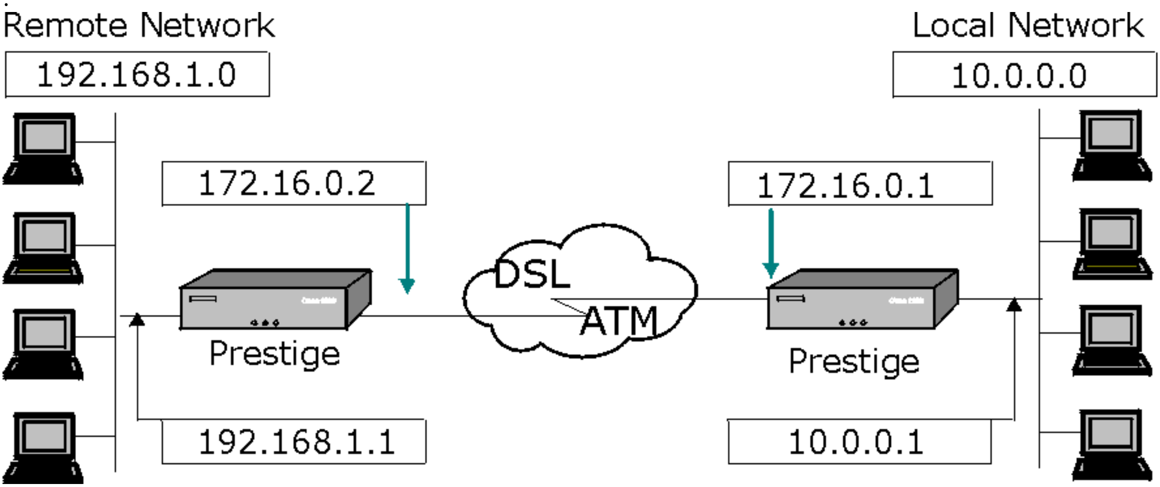


Figure 5-4 Sample IP Addresses for a TCPI/IP LAN-to-LAN Connection

To configure the TCP/IP parameters of a remote node, first configure the three fields in **Menu 11.1 – Remote Node Profile**, as shown in the table below.

Table 5-1 TCP/IP-Related Fields in Remote Node Profile

FIELD	DESCRIPTION	OPTION S
Route	Make sure IP is among the protocols in the **Route** field in **Menu 11.1** – **Remote Node Profile**.	**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**. For example (see previous *Figure*), 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 Addr** 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 Addr** field.	
Edit IP	Press [space bar] to toggle this field to **Yes** and then press [Enter] to go to **Menu 11.3** – **Remote Node Network Layer Options** menu.	**Yes** or **No**

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

Table 5-2 TCP/IP Remote Node Configuration

FIELD	DESCRIPTION	OPTIONS
VPI VCI	Enter the Virtual Path Identifier (VPI) number that your telephone company supplies. Enter the Virtual Channel Identifier (VCI) number that your telephone company supplies.	
Rem IP Adress	This will show the IP address you entered for this remote node in the previous menu.	
Rem IP Subnet Mask	Enter the subnet mask for the remote network.	
My Wan Address	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**: 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 Addr** in **Menu 11.1**.	
Single User Account	Set this field to **Yes** to enable the Single User Account feature for your Prestige. Use the [space bar] to toggle between **Yes** and **No**. See ***Chapter 3 – Internet Access Application*** for more information on the Single User Account feature.	**Yes** or **No**
Metric	Metric represents the “cost” of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.	**1** to **15**
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.	**Yes** or **No**
RIP Direction	Press [space bar] to select from **Both**, **In Only**, **Out Only** or **None**.	**Both**, **In Only**, **Out Only** or **None**

FIELD	DESCRIPTION	OPTIONS
Version	Press [space bar] to select the RIP version from **RIP-1/ RIP-2B/RIP-2M.**	**RIP-1**, **RIP-2B** or **RIP-2M**
Multicast	Sets IGMP to version 1, version 2, or disables IGMP. IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The Prestige supports both IGMP version 1 (IGMP-v1) and version 2 (IGMP-v2). Press [space bar] to enable IP Multicasting or select None to disable it.	**IGMP-v1/** **IGMP-v2/** **None** (default)
IP Policies	Create policies using SMT Menu 25 (see the **IP Routing Policy Chapter** in Part 3) and apply them on the Prestige LAN interface here. You can apply up to four IP Policy sets (from twelve) by entering their numbers separated by commas.	e.g., **3**, **4**, **5**, **6**
Once you have completed filling in the Remote Node Network Layer Options Menu, press [Enter] to return to **Menu 11**. Press [Enter] at the message [Press ENTER to Confirm…] to save your configuration or press [Esc] at any time to cancel.		

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

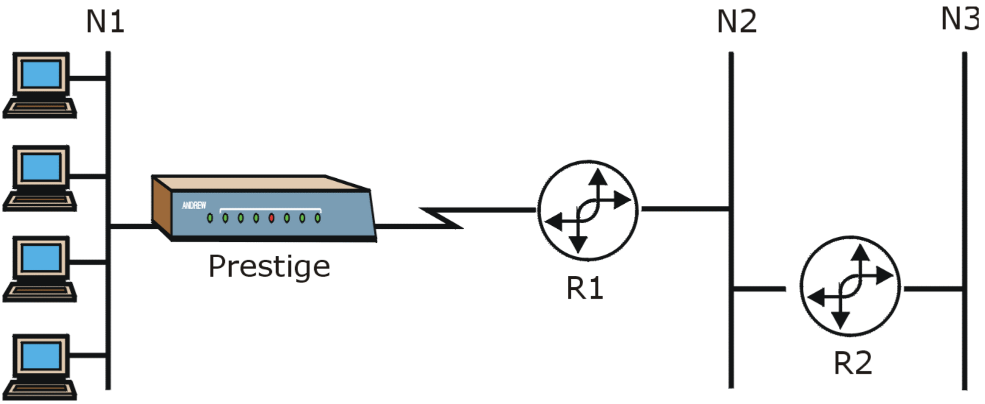
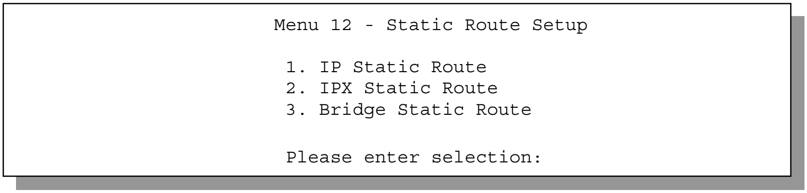


Figure 5-5 Sample Static Routing Topology

To configure an IP static route, use **Menu 12.1 - Static Route Setup**. Follow the procedure below.

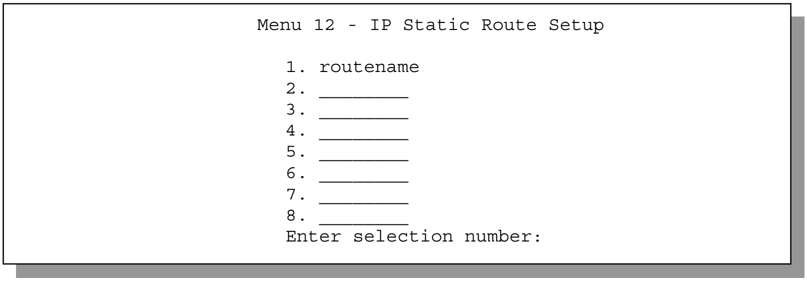
Step 1. Enter **12** from the **Main Menu** to bring up the following screen.



```
                    Menu 12 - Static Route Setup

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

                     Please enter selection:
```

Figure 5-6 Menu 12 - Static Route Setup

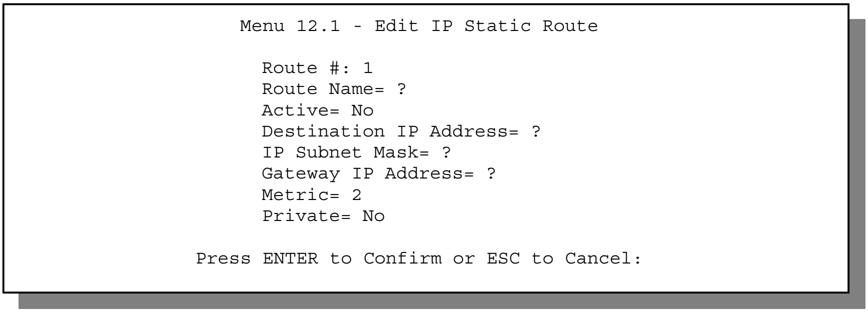
Step 2. From **Menu 12**, enter **1** to bring up the next screen.



```
                  Menu 12 - IP Static Route Setup

                     1. routename
                     2. ________
                     3. ________
                     4. ________
                     5. ________
                     6. ________
                     7. ________
                     8. ________
                     Enter selection number:
```

Figure 5-7 Menu 12.1 - IP Static Route Setup

Step 3. From **Menu 12.1**, enter the index number of one of the static routes that you want to configure.



```
                    Menu 12.1 - Edit IP Static Route

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

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

Figure 5-8 Edit IP Static Route

The following table describes the fields for **Menu 12.1 - Edit IP Static Route Setup**.

Table 5-3 Edit IP Static Route Menu Fields

FIELD	DESCRIPTION
Route #	This is the index number of the static route that you chose in Menu 12.1.
Route Name	Enter a descriptive name for this route. This is for identification purpose only.
Active	This field allows you to activate/deactivate this static route.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the subnet mask for this destination. Follow the discussion on IP subnet mask in Chapter 3.
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	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.

FIELD	DESCRIPTION
Private	This parameter determines if the Prestige will include the route to this remote node in its RIP broadcasts. If set to **Yes**, this route is kept private and is not included in RIP broadcast. If **No**, the route to this remote node will be propagated to other hosts through RIP broadcasts.
Once you have completed filling in this menu, press [Enter] at the message [Press ENTER to Confirm...] to save your configuration, or press [Esc] to cancel.	

Chapter 6
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 do not 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 need 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, we recommend that you set up a NetWare server as a seed router. Even though the Prestige is capable 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 network (see the following diagram).

Even though 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.

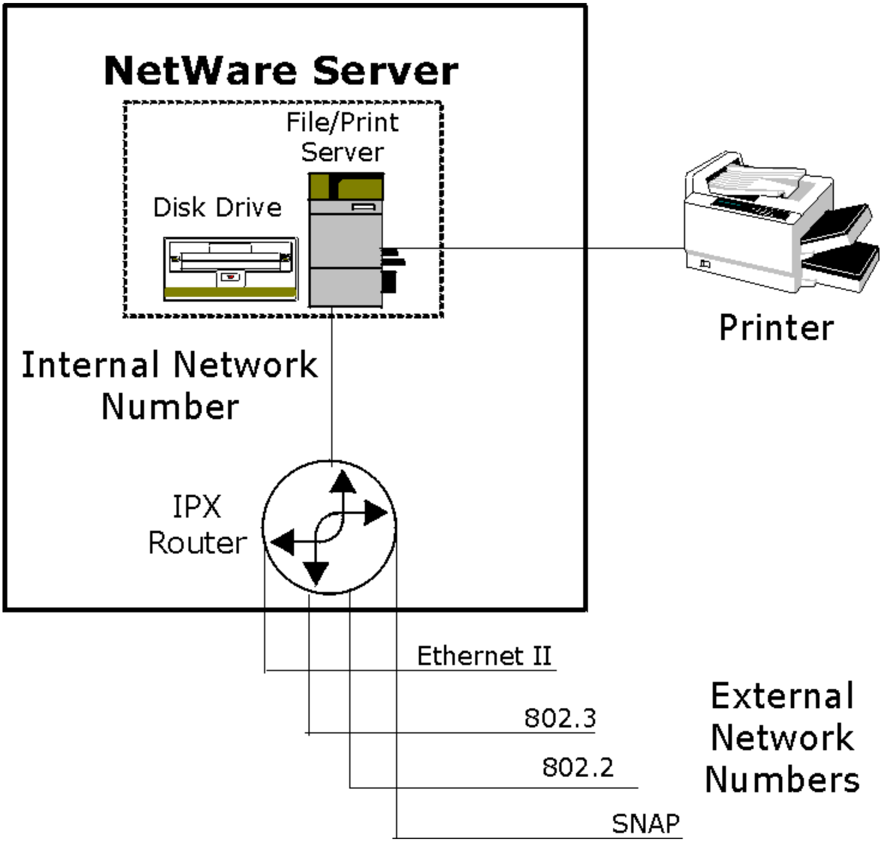


Figure 6-1 NetWare Network Numbers

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.

6.2 Prestige 642R in an IPX Environment

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

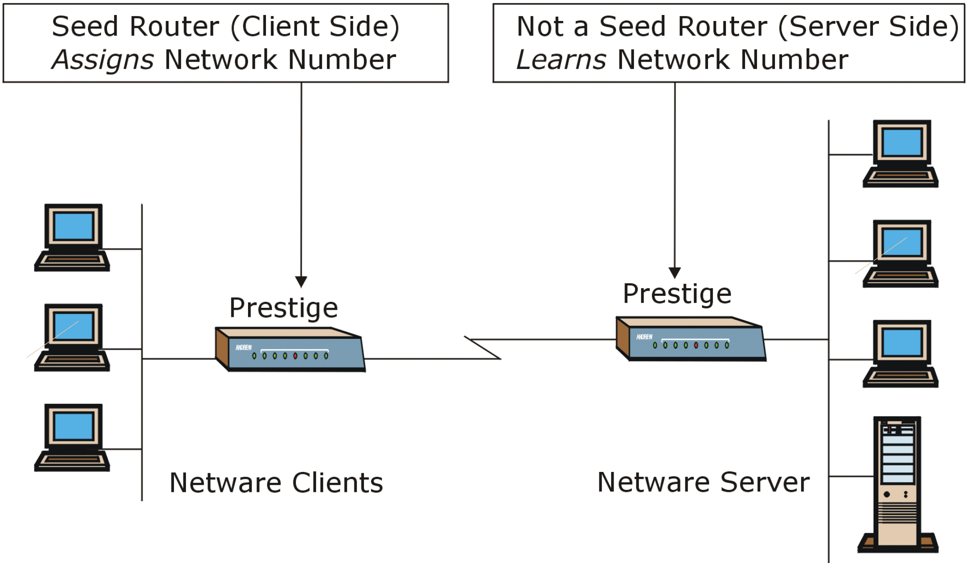


Figure 6-2 Prestige in an IPX Environment

6.2.1 Prestige 642R on LAN With Server

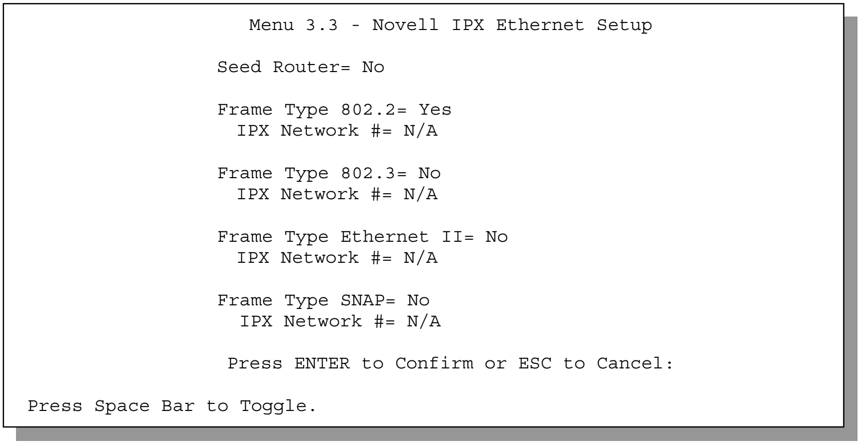
If your Prestige is on a LAN with a seed router, you do not need to configure the LAN network numbers. Your Prestige will learn the network number from the seed router and add the routes to its routing table.

6.2.2 Prestige 642R 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 **Ethernet Setup** menu.

6.3 IPX Ethernet Setup

From **Menu 3 – Ethernet Setup**, select option **3** to got to **Menu 3.3 - Novell IPX Ethernet Setup** as shown in Figure 6-3.



```
                    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

                  Press ENTER to Confirm or ESC to Cancel:

Press Space Bar to Toggle.
```

Figure 6-3 Menu 3.3 - Novell IPX Ethernet Setup

The following describes the Novell IPX Ethernet Setup menu.

Table 6-1 Novell IPX Ethernet Setup Fields

FIELD	DESCRIPTION	OPTIONS
Seed Router	Determines if your Prestige is to act as a seed router.	**Yes** or **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** **SNAP**
IPX Network #	If your Prestige is a seed router, enter a unique network number for each frame type enabled.	
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 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 next figure.

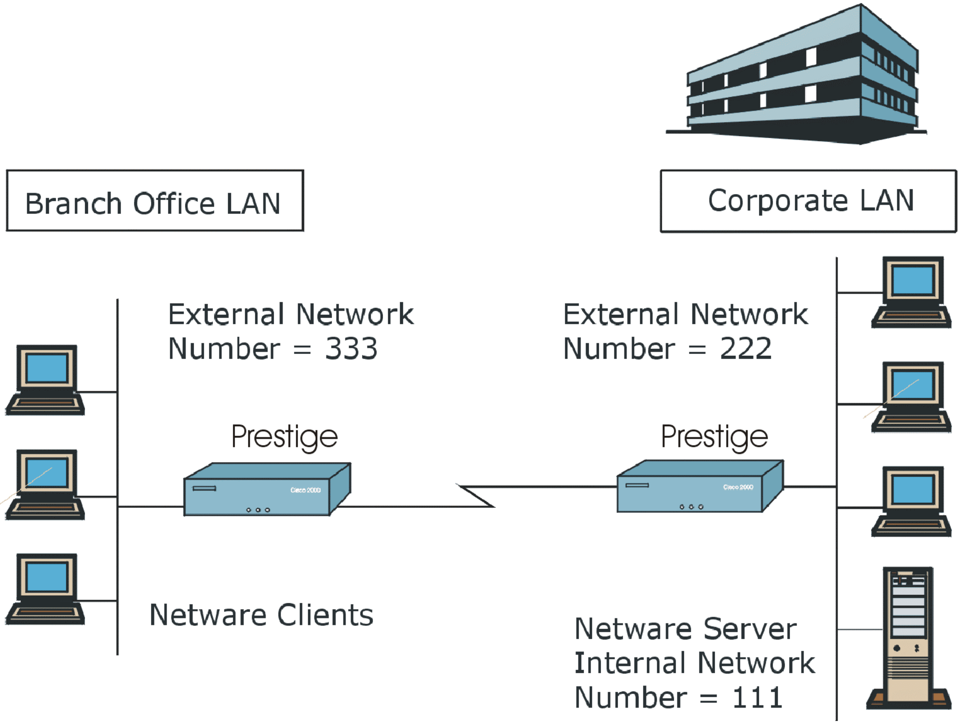

Branch Office LAN
Corporate LAN
External Network Number = 333
External Network Number = 222
Prestige
Prestige
Netware Clients
Netware Server Internal Network Number = 111

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

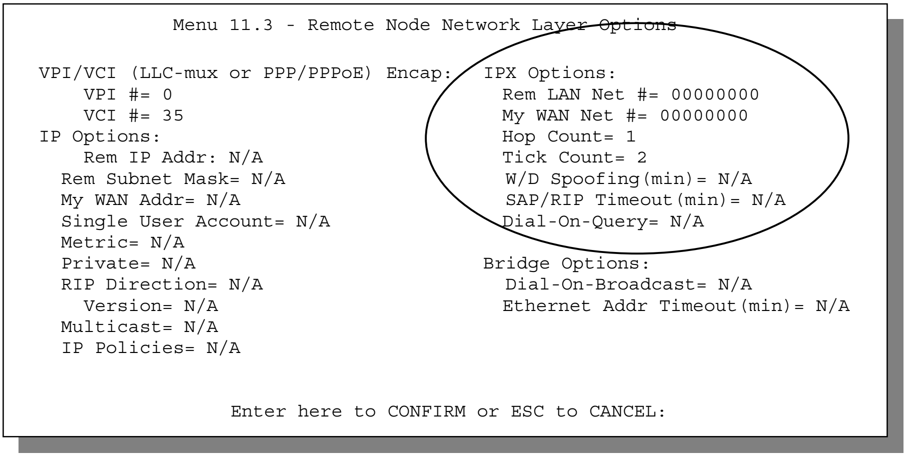
6.4.1 IPX Remote Node Setup

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

To edit **Menu 11.3 – Remote Node Network Layer Options** shown in Figure 6-5, follow these steps:

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 **IP + IPX**.)

Step 2. Move the cursor to the **Edit IP/IPX/Bridge** field, then press the [space bar] to set the value to **Yes**, and press [Enter] to open **Menu 11.3** – **Remote Node 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: N/A                     Tick Count= 2
     Rem Subnet Mask= N/A                   W/D Spoofing(min)= N/A
     My WAN Addr= N/A                       SAP/RIP Timeout(min)= N/A
     Single User Account= N/A               Dial-On-Query= N/A
     Metric= N/A
     Private= N/A                         Bridge Options:
     RIP Direction= N/A                     Dial-On-Broadcast= N/A
       Version= N/A                         Ethernet Addr Timeout(min)= N/A
     Multicast= N/A
     IP Policies= N/A


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

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

Table 6-2 describes the IPX protocol-dependent parameters of the Remote Node Setup.

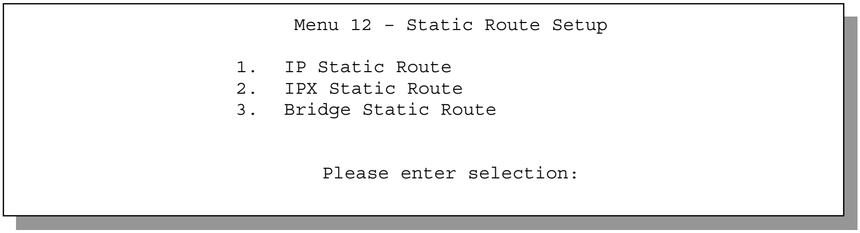
Table 6-2 Remote Node Novell IPX Options

FIELD	DESCRIPTION	OPTIONS
Rem LAN Net #	In this field, enter the internal network number of the NetWare server on the remote LAN.	
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)
Please note that the following 3 fields are only valid for PPPoE encapsulation.		
W/D Spoofing (min)	This field is for the Prestige on the server side. Your Prestige 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 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 the 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 node.	**Yes** or **No**
Once you have completed filling in the Remote Node 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 how to reach servers beyond a remote node before a connection to that remote node is established.

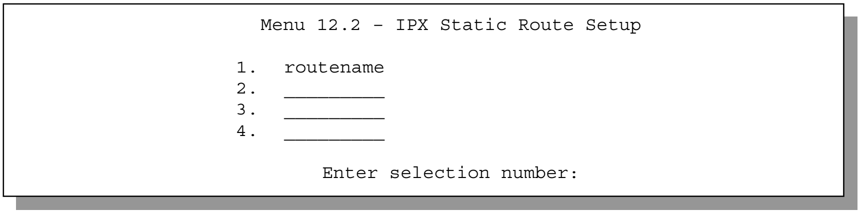
Step 1. Enter **12**, from the **Main Menu**, to bring up the following screen.



```
                  Menu 12 - Static Route Setup

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


                    Please enter selection:
```

Figure 6-6 Menu 12 - Static Route Setup

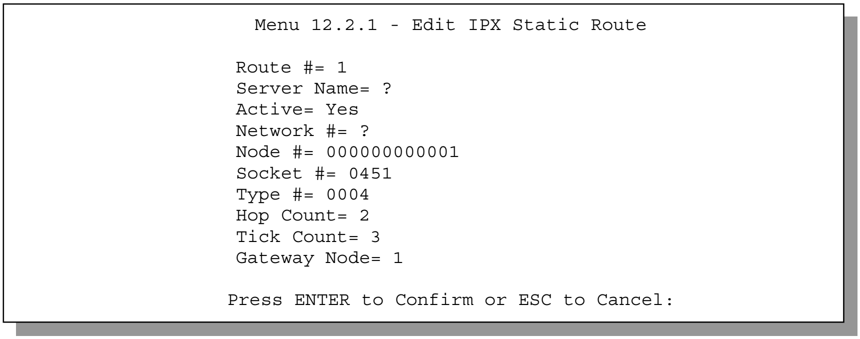
Step 2. Enter **2**, from **Menu 12**, to bring up the following screen.



```
               Menu 12.2 - IPX Static Route Setup

             1.   routename
             2.   _________
             3.   _________
             4.   _________

                    Enter selection number:
```

Figure 6-7 Menu12.2 - IPX Static Route Setup

Step 3. 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 #= 1
             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 6-8 Menu 12.2.1 - Edit IPX Static Route

The following table contains the instructions on how to configure the Edit IPX Static Route menu.

Table 6-3 Edit IPX Static Route Menu Fields

FIELD	DESCRIPTION
Route #	This is the index number of the route as listed in **Menu 12.2 – IPX Static Route Setup**.
Server Name	In this field, enter the name of the server. This must be the *exact* name configured in the NetWare server**.**
Active	This field allows you to activate/deactivate this static route.
Network #	This field contains the internal network number of the remote server that you wish to access. [00000000] and [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].
Hop Count	This field indicates the number of intermediate networks that must be passed through to reach the remote node.
Tick Count	This field indicates the time-ticks required to reach the remote node.
Gateway Node	In this field, enter the number of the remote node that is the gateway for this static route.
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

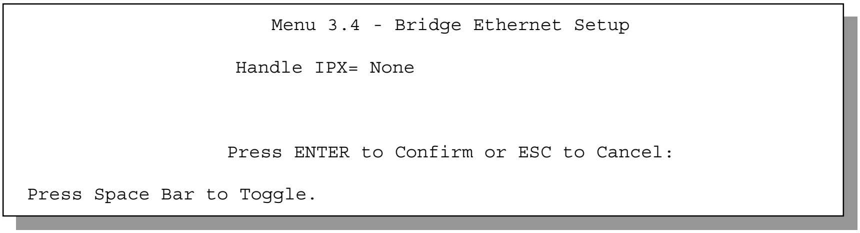
Bridging bases the forwarding decision on the MAC (Media Access Control), or hardware address, while routing does it on the network layer (IP or IPX) address. Bridging allows the Prestige to transport packets of network layer protocols that it does not route, e.g., SNA, from one network to another. The 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 can route.

7.2 Bridge Ethernet Setup

Basically, all non-local packets are bridged to the WAN, however, your Prestige 642 applies special handling for certain IPX packets to reduce the number of calls, depending on the setting of the *Handle IPX* field.

Enter **4**, from **Menu 3 – Ethernet Setup**, 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

FIELD	DESCRIPTION	OPTIONS
Handle IPX	Press the [space bar] to toggle between the options for this field.	
	When there is no IPX traffic on the LAN or when you do not want to apply any special handling for IPX.	**None**
	When there are only client workstations on the LAN. RIP and SAP (Service Advertising Protocol) response packets will not trigger calls.	**Client**
	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 will reply to WatchDog messages from the servers on behalf of remote clients. The period of time that your Prestige 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 timed out, there is no need to maintain its connection to the IPX server.	**Server**
	If there are both clients and servers on the LAN, and the local clients will access the remote servers, set this field to **Server** but turn on the **Dial-On-Broadcast** (if using PPPoE encapsulation) parameter in Menu 11.3 to allow the client queries to trigger calls.	

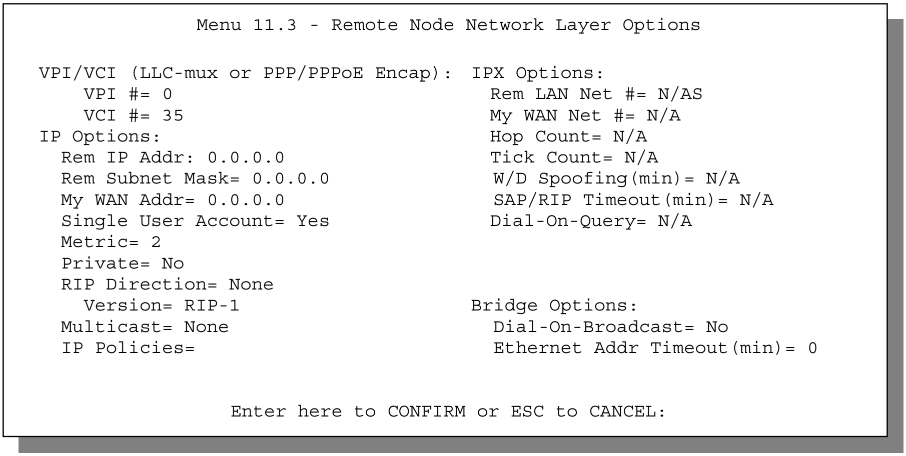
7.2.1 Remote Node Bridging Setup

Follow the procedure in **Chapter 5** to configure the protocol-independent parameters in **Menu 11.1 – Remote Node Profile**. For bridging-related 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, toggle the [space bar] to select **Yes** and then press [Enter] to open **Menu 11.3 – Remote Node 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 #= N/AS
      VCI #= 35                            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
    My WAN Addr= 0.0.0.0                    SAP/RIP Timeout(min)= N/A
    Single User Account= Yes               Dial-On-Query= N/A
    Metric= 2
    Private= No
    RIP Direction= None
      Version= RIP-1                     Bridge Options:
    Multicast= None                         Dial-On-Broadcast= No
    IP Policies=                            Ethernet Addr Timeout(min)= 0


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

Figure 7-2 Menu 11.3 - Remote Node Network Layer Options

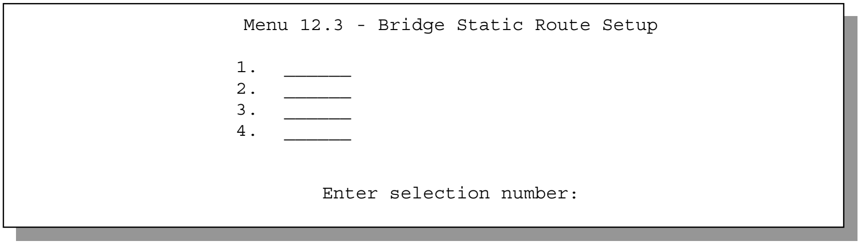
The following table describes the bridging-dependent parameters in the Remote Node Profile and Network Layers menus.

Table 7-2 Remote Node Network Layer Options

FIELD	DESCRIPTION
Bridge (Menu 11.1)	Make sure this field is set to **Yes**.
Edit IP/IPX/Bridge (Menu 11.1)	Press [space bar] to change it to **Yes** and press [Enter] to go to the Remote Node Network Layer Options menu.
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 Prestige 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 to retain the Ethernet Address information in its internal tables while the line is down. If this information is retained, your Prestige will not have to recompile the tables when the line is brought back up.
Once you have completed filling in the Remote Node 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.	

7.2.2 Bridge Static Route Setup

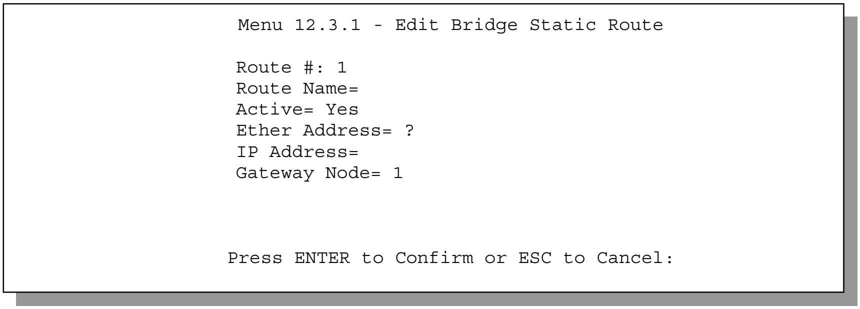
Similar to network layer static routes, a bridging static route tells the Prestige the route to a node before a connection is established. You configure bridge static routes in **Menu 12.3.1** by pressing **3** in Menu **12** as shown next.



```
              Menu 12.3 - Bridge Static Route Setup

             1.   ______
             2.   ______
             3.   ______
             4.   ______


                    Enter selection number:
```

Figure 7-3 Bridge Static Route Setup

Then select one of the bridge static routes.



```
             Menu 12.3.1 - Edit Bridge Static Route

             Route #: 1
             Route Name=
             Active= Yes
             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 **Edit Bridge Static Route Menu**.

Table 7-3 Edit Bridge Static Route Menu Fields

FIELD	DESCRIPTION
Route #	This is the index number of the route as listed in **Menu 12.3-Bridge Static Route Setup**.
Route Name	Enter a name for the bridge static route for identification purposes.
Active	Indicates whether the static route is active or not.
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 (Chapters 8-12) provides information on Filter Configuration, SNMP Configuration, System Maintenance, IP Policy Routing and Troubleshooting. Also included are some 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 to allow passage of a data packet and/or to make a call. There are two types of filter applications: data filtering and call filtering. Filters are subdivided into device and protocol filters, which are discussed later.

Data filtering screens the data to determine if the packet should be allowed to pass. Data filters are divided into incoming and outgoing filters, depending on the direction of the packet relative to a port. Data filtering can be applied on either the WAN side or the Ethernet side. Call filtering is used to determine if a packet should be allowed to trigger a call. Remote node call filtering is only applicable when using **PPPoE** encapsulation. Outgoing packets must undergo data filtering before they encounter call filtering as shown in the following figure.

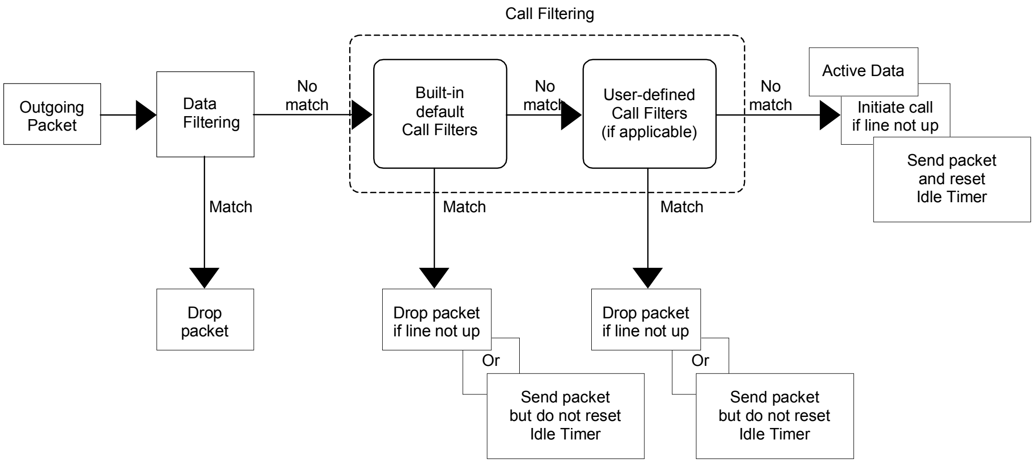

Call Filtering
Outgoing Packet
Data Filtering
No match
Built-in default Call Filters
No match
User-defined Call Filters (if applicable)
No match
Active Data
Initiate call if line not up
Send packet and reset Idle Timer
Match
Match
Match
Drop packet
Drop packet if line not up
Or
Send packet but do not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

Figure 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.

8.1.1 The Filter Structure of the Prestige

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

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

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

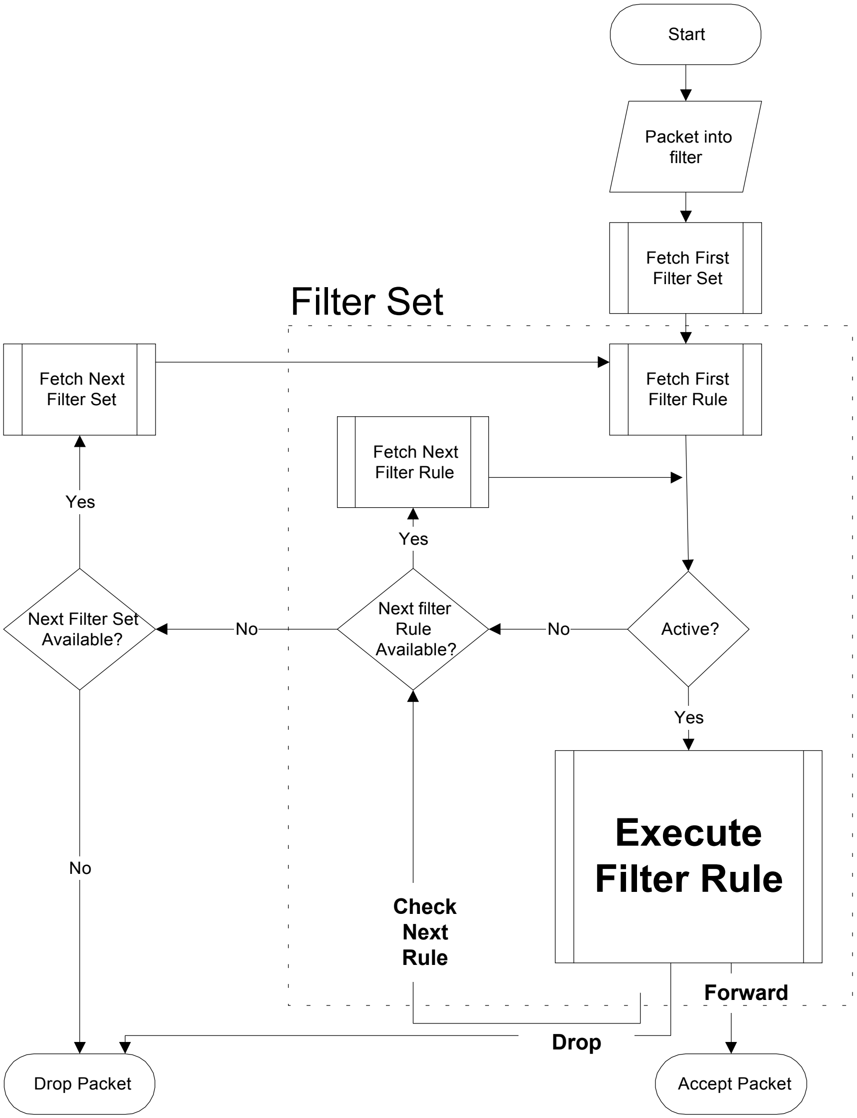


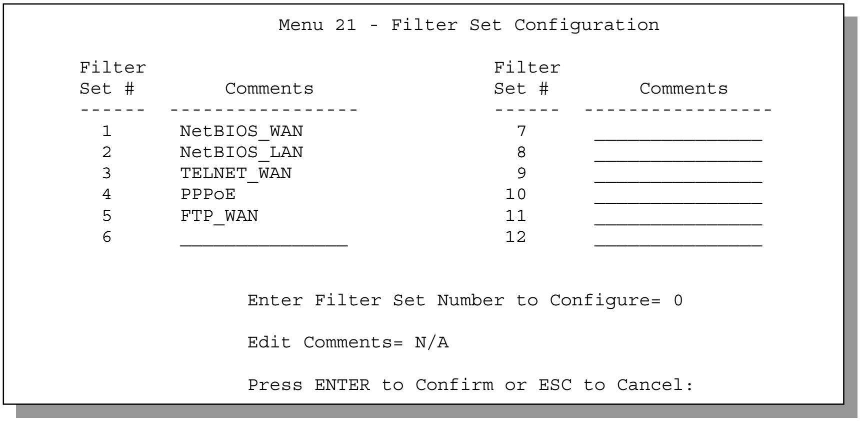
Figure 8-2 Filter Rule Process

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 the procedure below.

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



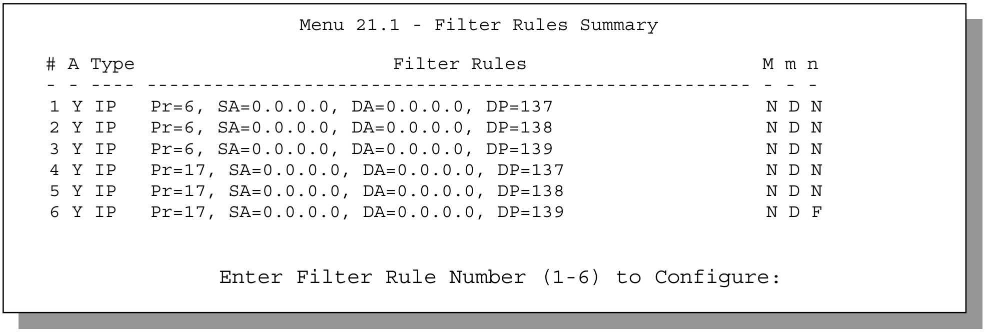
```
                      Menu 21 - Filter Set Configuration

    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      _______________                 12     _______________


                   Enter Filter Set Number to Configure= 0

                   Edit Comments= N/A

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

Figure 8-3 Menu 21 – Filter Setup

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

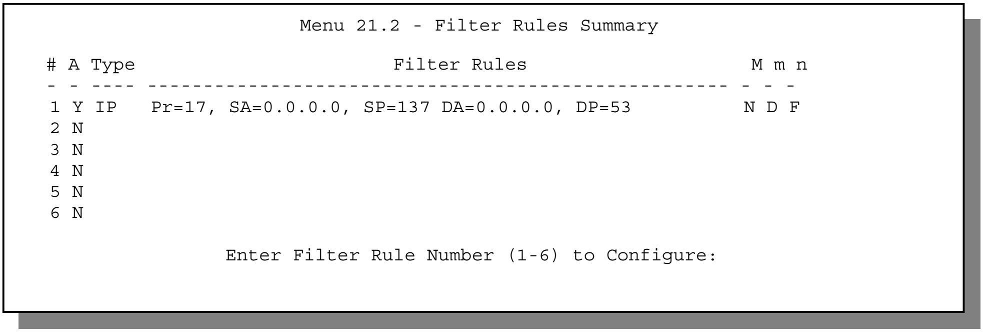
Step 3. Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].

Step 4. Press [ENTER] at the message: [Press ENTER to Confirm…] to open **Menu 21.1.1 - Filter Rules Summary**.



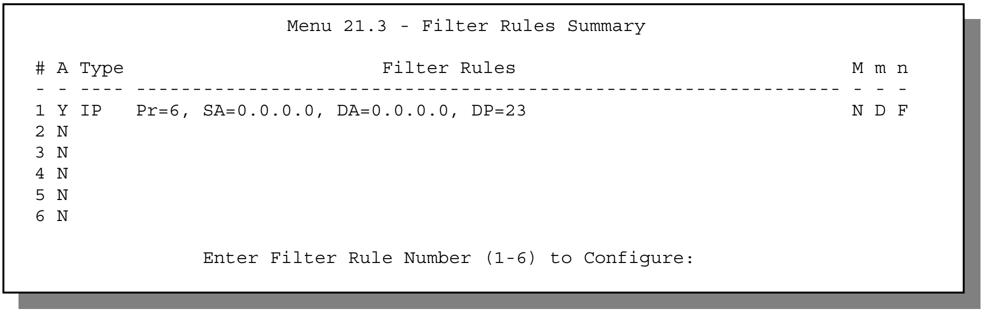
```
                          Menu 21.1 - Filter Rules Summary

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


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

Figure 8-4 NetBIOS_WAN Filter Rules Summary



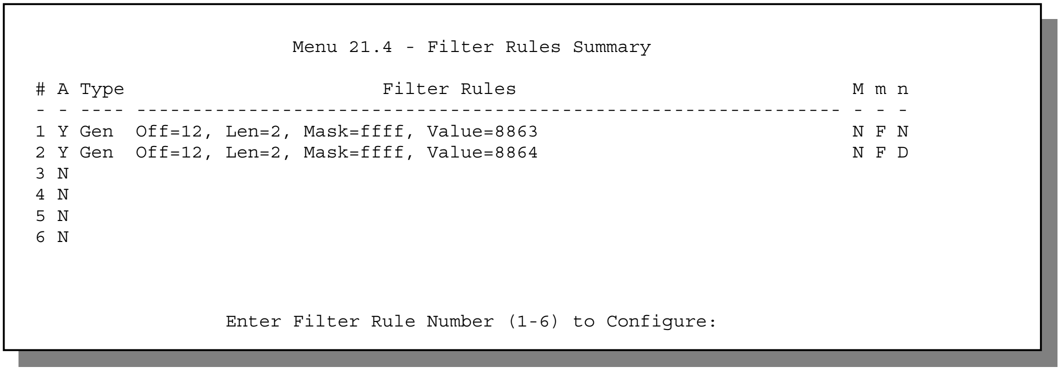
```
                          Menu 21.2 - Filter Rules Summary

 # 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 N
 3 N
 4 N
 5 N
 6 N

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

Figure 8-5 NetBIOS_LAN Filter Rules Summary



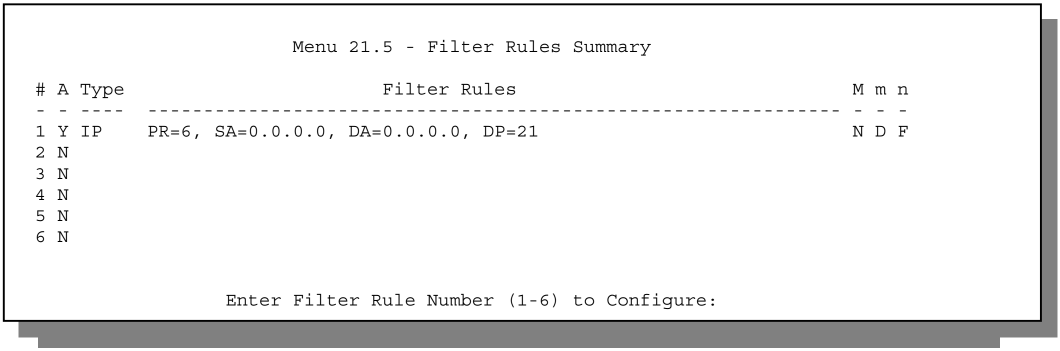
```
                         Menu 21.3 - Filter Rules Summary

 # 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:
```

Figure 8-6 Telnet_WAN 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

8.2.1 Filter Rules Summary Menu

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

Table 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. This shows GEN for generic, IP for	[GEN] for Generic [IP] for TCP/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 check, which are concatenated with the present rule to form a rule chain. When the rule chain is complete an action can be taken. [N] means you can now specify an action to be taken i.e., forward the packet, drop the packet or check the next rule. For the latter, the next rule is independent of the rule just checked. If More is **Yes**, then **Action Matched** and **Action Not Matched** will be **N/A**	[Y] means there are more rules to check. [N] means there are no more rules to check.
M	Refers to **Action Matched**. [F] means to forward the packet immediately and skip checking the remaining rules.	[F] means to forward the packet. [D] means to drop the packet. [N] means check the next rule.
N	Refers to **Action Not Matched.** [F] means to forward the packet immediately and skip checking the remaining rules.	[F] means to forward the packet. [D] means to drop the packet. [N] means check the next rule.

The protocol dependent filter rules abbreviation are listed as follows:

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

Table 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 following 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.

8.2.2 Configuring a Filter Rule

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

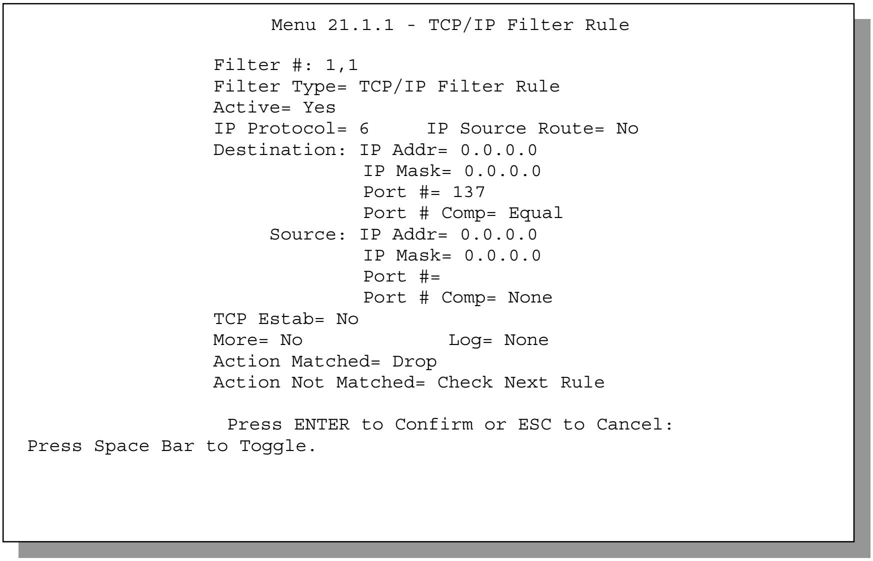
There are three types of filter rules: **TCP/IP**, **IPX** and **Generic**. Depending on the type of rule, the parameters below the type will be different. Use the space bar to select the type of rule that you wish to create in the **Filter Type** field and press [ENTER] to open the respective menu.

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.

8.2.3 TCP/IP Filter Rule

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

To configure a TCP/IP rules, select TCP/IP Filter Rule from the Filter Type field and press [ENTER] to open **Menu 21.1.1 - TCP/IP Filter Rule**, as shown below:



```
                       Menu 21.1.1 - TCP/IP Filter Rule

                  Filter #: 1,1
                  Filter Type= TCP/IP Filter Rule
                  Active= Yes
                  IP Protocol= 6     IP Source Route= No
                  Destination: IP Addr= 0.0.0.0
                               IP Mask= 0.0.0.0
                               Port #= 137
                               Port # Comp= Equal
                       Source: IP Addr= 0.0.0.0
                               IP Mask= 0.0.0.0
                               Port #=
                               Port # Comp= None
                  TCP Estab= No
                  More= No             Log= None
                  Action Matched= Drop
                  Action Not Matched= Check Next Rule

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

Figure 8-9 Menu 21.1.1.1 - 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	Option
Active	This field activates/deactivates the filter rule.	**Yes/No**
IP Protocol	Protocol refers to the upper layer protocol, e.g., TCP is 6, UDP is 17 and ICMP is 1. This value must be between 0 and 255	0-255
IP Source Route	If Yes, the rule applies to packet with IP source route option; else the packet must not have source route option. The majority of IP packets do not have source route.	**Yes/No**
Destination: IP Address	Enter the destination IP Address of the packet you wish to filter. This field is disregarded if it is 0.0.0.0.	IP address
Destination: IP Mask	Enter the IP mask to apply to the Destination: IP Addr.	IP mask
Destination: Port #	Enter the destination port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is disregarded if it is 0.	0-65535

Field	Description	Option
Destination: Port # Comp	Select the comparison to apply to the destination port in the packet against the value given in Destination: Port #.	**None/Less/Greater /Equal/Not Equal]**
Source: IP Address	Enter the source IP Address of the packet you wish to filter. This field is disregarded if it is 0.0.0.0.	IP Address
Source: IP Mask	Enter the IP mask to apply to the Source: IP Addr.	IP Mask
Source: Port #	Enter the source port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is disregarded if it is 0.	0-65535
Source: Port # Comp	Select the comparison to apply to the source port in the packet against the value given in Source: Port #.	**None/Less/Greater /Equal/Not Equal**
TCP Estab	This field is applicable only when IP Protocol field is 6, TCP. If yes, the rule matches only established TCP connections; else the rule matches all TCP packets.	**Yes/No**
More	If yes, a matching packet is passed to the next filter rule before an action is taken; else the packet is disposed of according to the action fields. If More is **Yes**, then Action Matched and Action Not Matched will be **N/A**.	**Yes / No**
Log	Select the logging option from the following: ● **None** – No packets will be logged. ● **Action Matched** – Only packets that match the rule parameters will be logged. ● **Action Not Matched** - Only packets that do not match the rule parameters will be logged. ● **Both** – All packets will be logged.	**None** **Action Matched** **Action Not Matched** **Both**
Action Matched	Select the action for a matching packet.	**Check Next Rule** **Forward** **Drop**
Action Not Matched	Select the action for a packet not matching the rule.	**Check Next Rule** **Forward** **Drop**

Field	Description	Option
Once you have completed filling in **Menu 21.1.1 - TCP/IP Filter Rule**, press [ENTER] at the message [Press ENTER to Confirm] to save your configuration, or press [ESC] to cancel. This data will now be displayed on **Menu 21.1 - Filter Rules Summary**.		

The following diagram illustrates the logic flow of an IP filter:

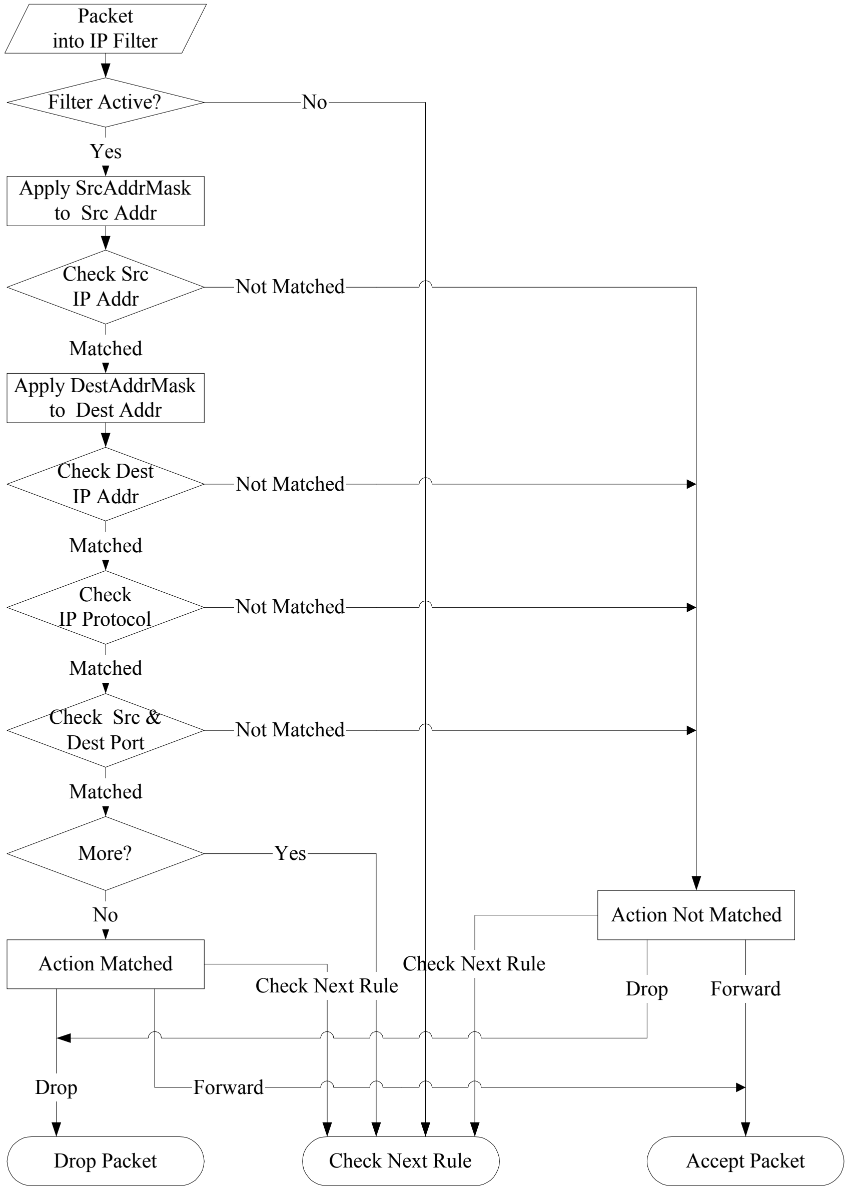


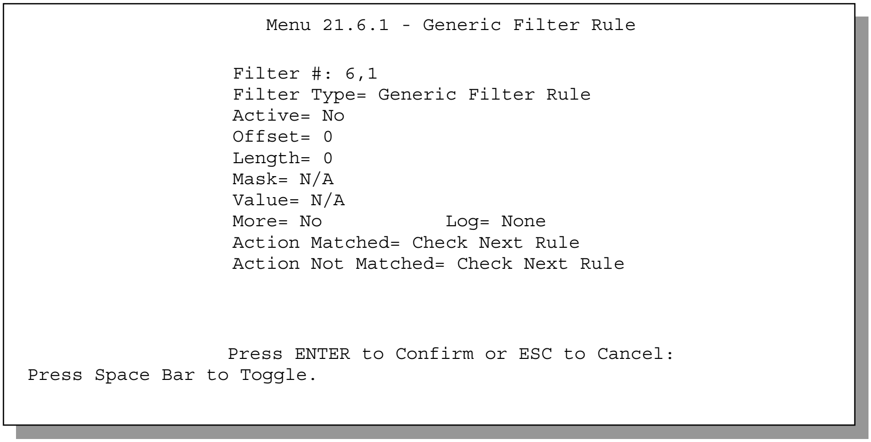
Figure 8-10 Executing an IP Filter

8.2.4 Generic Filter Rule

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

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

To configure a generic rule, select Generic Filter Rule in the Filter Type field in the **Menu 21.6.1** and press [ENTER] to open the Generic Filter Rule Menu, as shown below:



```
                       Menu 21.6.1 - Generic Filter Rule

                    Filter #: 6,1
                    Filter Type= Generic Filter Rule
                    Active= No
                    Offset= 0
                    Length= 0
                    Mask= N/A
                    Value= N/A
                    More= No           Log= None
                    Action Matched= Check Next Rule
                    Action Not Matched= Check Next Rule



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

Figure 8-11 Generic Filter Rule

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

Table 8-6 Generic Filter Rule Menu Fields

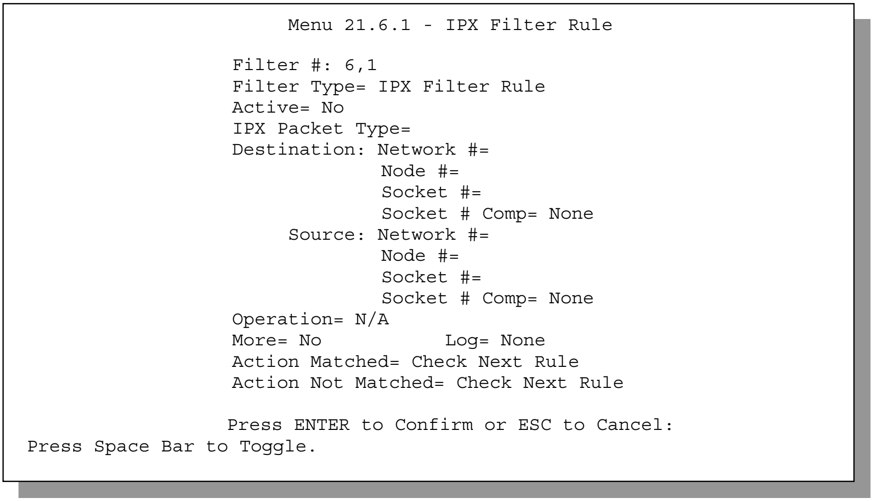
Field	Description	Option
Filter #	This is the filter set, filter rule co-ordinates, i.e., 2,3 refers to the second filter set and the third rule of that set.	
Filter Type	Use [SPACE BAR] to toggle between both types of rules. Parameters displayed below each type will be different.	**Generic Filter Rule/ TCP/IP Filter Rule**
Active	Select **Yes** to turn on the filter rule.	**Yes/No**

Field	Description	Option
Offset	Enter the starting byte of the data portion in the packet that you wish to compare. The range for this field is from 0 to 255.	Default = 0
Length	Enter the byte count of the data portion in the packet that you wish to compare. The range for this field is 0 to 8.	Default = 0
Mask	Enter the Mask (in Hexadecimal) to apply to the data portion before comparison.	
Value	Enter the Value (in Hexadecimal) to compare with the data portion.	
More	If yes, a matching packet is passed to the next filter rule before an action is taken; if no, the packet is disposed of according to the action fields. If More is **Yes**, then Action Matched and Action Not Matched will be **No**.	**Yes / No**
Log	Select the logging option from the following: ● **None** – No packets will be logged. ● **Action Matched** – Only packets that match the rule parameters will be logged. ● **Action Not Matched** - Only packets that do not match the rule parameters will be logged. ● **Both** – All packets will be logged.	**None** **Action Matched** **Action Not Matched** **Both**
Action Matched	Select the action for a matching packet.	**Check Next Rule** **Forward** **Drop**
Action Not Matched	Select the action for a packet not matching the rule.	**Check Next Rule** **Forward** **Drop**
Once you have completed filling in **Menu 21.4.1.1 - Generic Filter Rule**, press [ENTER] at the message [Press ENTER to Confirm] to save your configuration, or press [ESC] to cancel. This data will now be displayed on **Menu 21.1.1 - Filter Rules Summary**.		

8.2.5 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 rules, select **IPX Filter Rule** from the **Filter Type** field and press [ENTER] to open **Menu 21.1.5 IPX Filter Rule**, as shown in the figure below.



```
                       Menu 21.6.1 - IPX Filter Rule

                  Filter #: 6,1
                  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 8-12 IPX Filter Rule

The table below 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
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 in 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.
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 21.6.3 - 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**.	

8.3 Example Filter

Let's look at the third default ZyXEL filter, TELNET_WAN (*see Figure* 8-6) as an example. Please see the PNC Disk for more example filters. This filter is designed to block outside users from telnetting into the Prestige.

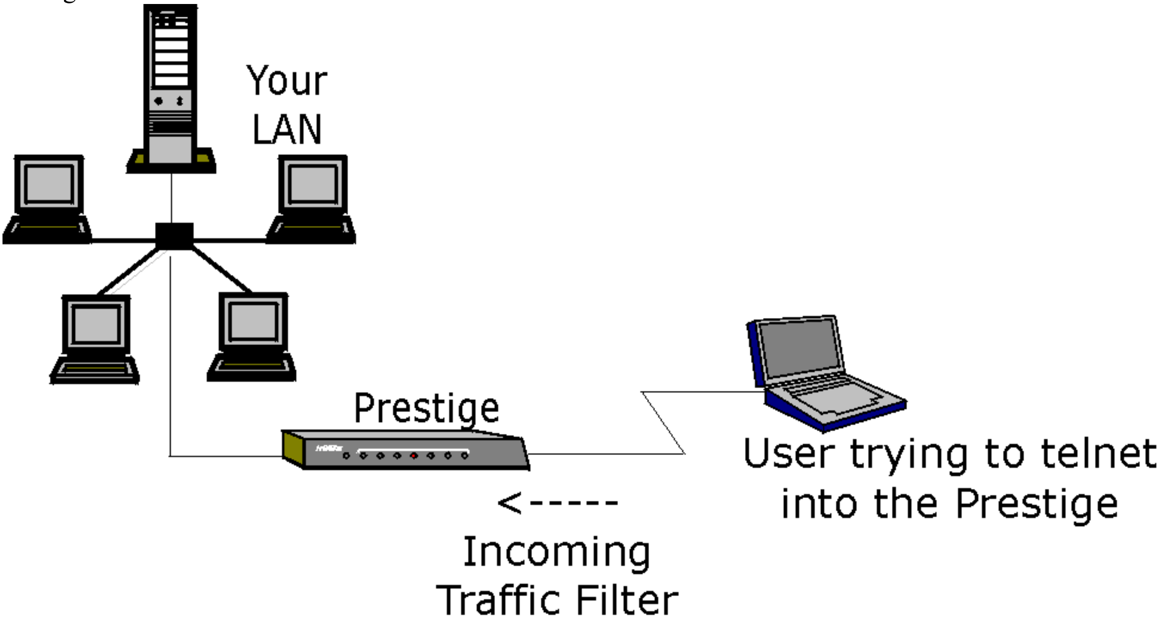


Figure 8-13 Telnet Filter Example

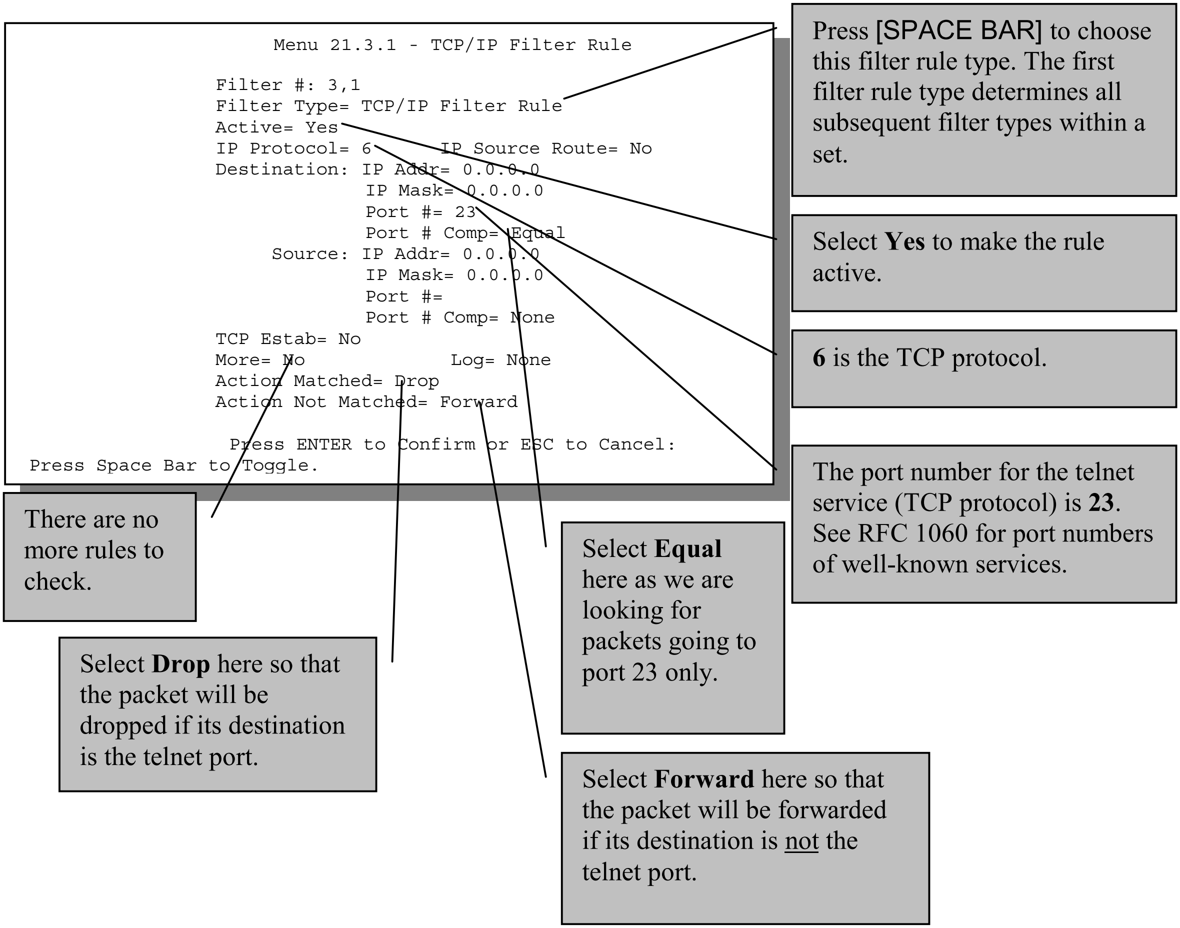
Step 1. Enter 21 from the Main Menu to open **Menu 21 - Filter Set Configuration**.

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

Step 3. Enter a descriptive name or comment in the **Edit Comments** field (in this case TELNET_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 #=
                              Port # Comp= None
                 TCP Estab= No
                 More= No              Log= None
                 Action Matched= Drop
                 Action Not Matched= Forward

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

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

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

6 is the TCP protocol.

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

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

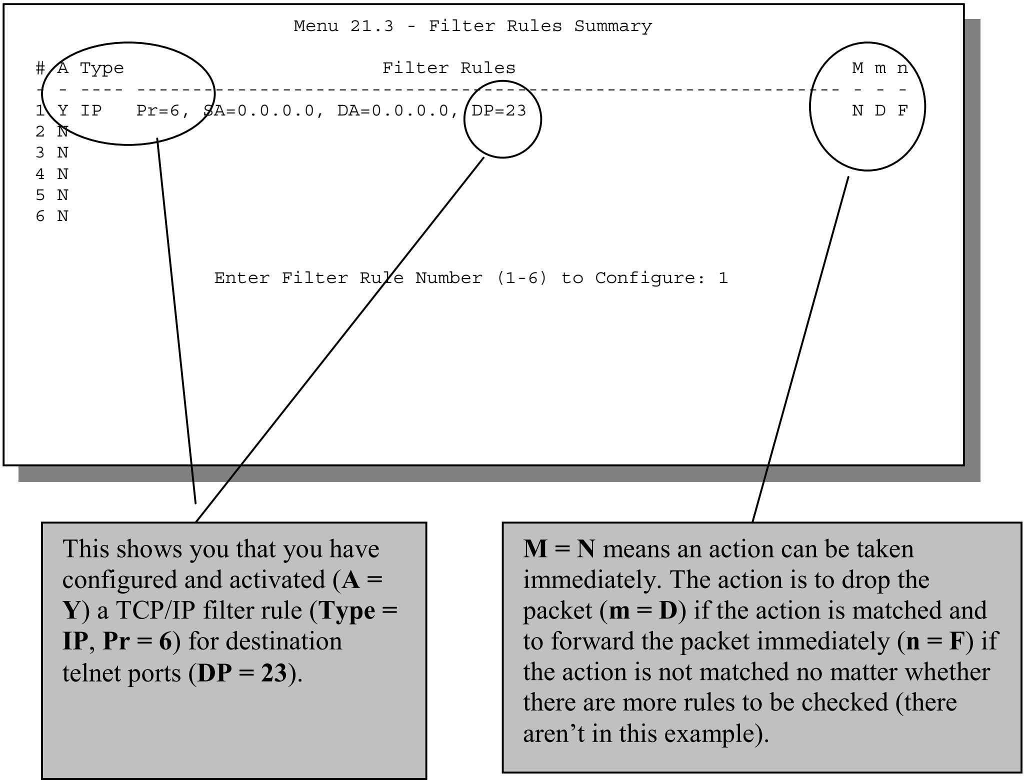
There are no more rules to check.

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

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

Figure 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


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

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

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

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

Step 3. This brings you to Menu 11.5. Apply the TELNET_WAN filter set (filter set 3) as shown in *Figure 8-18*.

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

8.4 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.

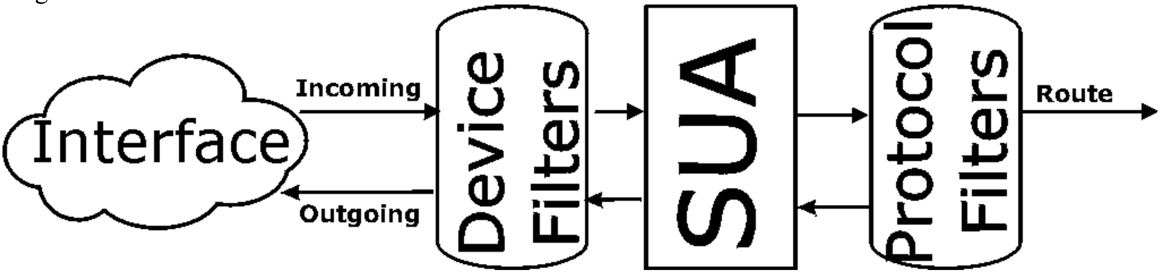


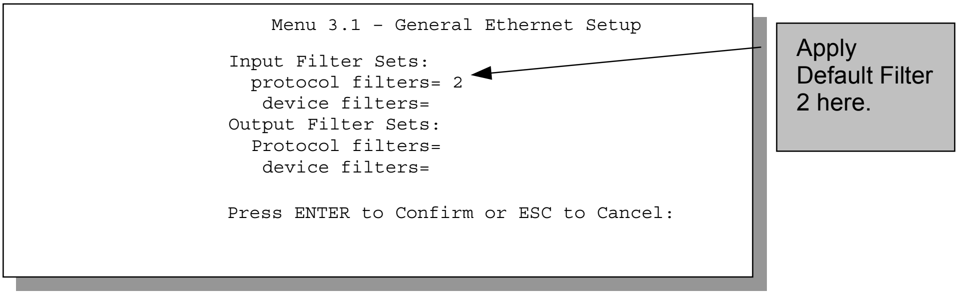
Figure 8-16 Protocol and Device Filter Sets

8.5 Applying a Filter and Factory Defaults

This section shows you where to apply the filter(s) after you design it (them). Sets of factory default filter rules have been configured in Menu 21 (but have not been applied) to prevent NetBIOS traffic from triggering calls, incoming telnet and sessions. The PPPoE filter filters out all packets *except* PPPoE packets going out from the Prestige to the ISP or remote node.

8.5.1 LAN traffic

LAN traffic filter sets may be useful to block certain packets, reduce traffic and prevent security breaches. Go to Menu 3.1 (shown next) and enter the number(s) of the filter set(s) that you want to apply as appropriate. You can choose up to four filter sets (from twelve) by entering their numbers separated by commas, e.g., 3, 4, 6, 11. Input filter sets filter incoming traffic to the Prestige and Output filter sets filter outgoing traffic from the Prestige. The factory default set, NetBIOS_LAN, can be inserted in the **protocol filters** field under **Input Filter Sets** in Menu 3.1 to block NetBIOS traffic to the Prestige from the LAN.



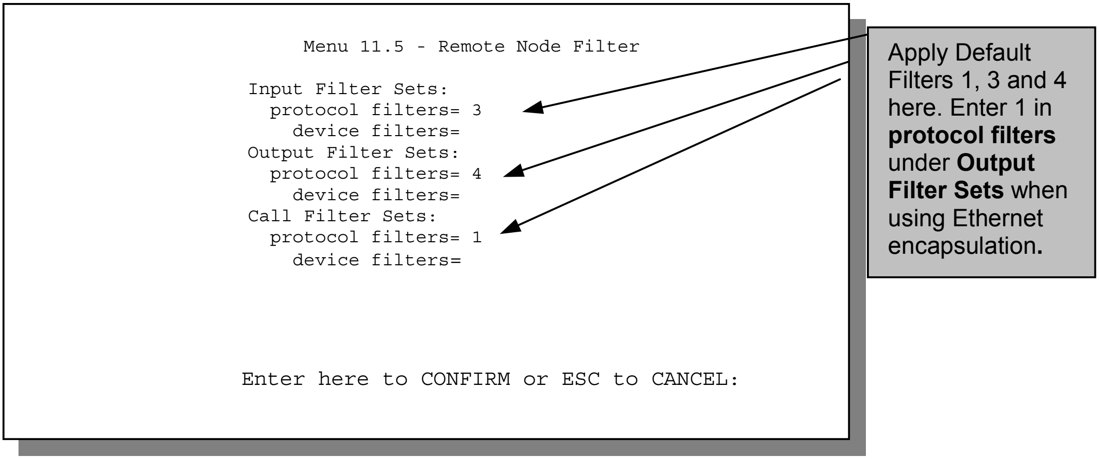
```
                    Menu 3.1 - General Ethernet Setup

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

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

Apply Default Filter 2 here.

Figure 8-17 Filtering LAN Traffic

8.5.2 Remote Node Filters

Go to Menu 11.5 (shown below – note that call filter sets are only present for PPPoE encapsulation) and enter the number(s) of the filter set(s) as appropriate. You can cascade up to four filter sets by entering their numbers separated by commas. The factory default filter set, NetBIOS_WAN, can be applied in Menu 11.5 to block local NetBIOS traffic from triggering calls to the ISP (when you are using **PPPoE** encapsulation only). Enter "1" in the **protocol filters** field under **Call Filter Sets** when using PPPoE encapsulation and in **protocol filters** under **Output Filter Sets – protocol filters** when using Ethernet encapsulation**.** Filter set "3", Telnet_WAN, blocks telnet connections from the WAN Port to help prevent security breaches. Filter set "4", 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= 3
                        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:
```

Apply Default Filters 1, 3 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

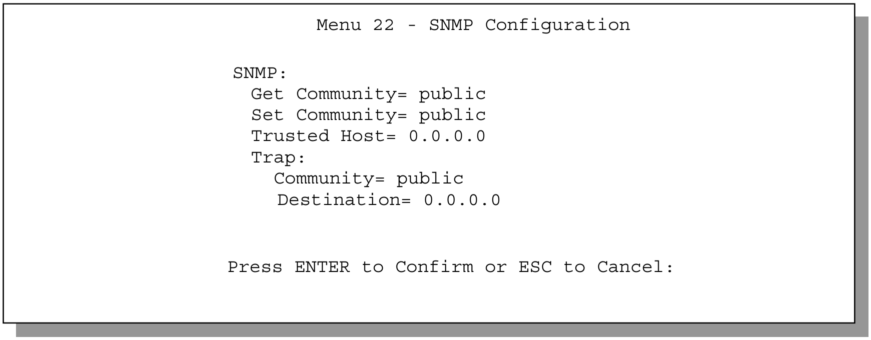
This chapter discusses SNMP (Simple Network Management Protocol) for network management and monitoring.

9.1 About SNMP

Your Prestige 642R supports SNMP agent functionality, which allows a manager station to manage and monitor the Prestige through the network. Keep in mind that SNMP is only available if TCP/IP is configured on your Prestige.

9.2 Configuring SNMP

To configure SNMP, 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 9-1 Menu 22 - SNMP Configuration

The following table describes the SNMP configuration parameters.

Table 9-1 SNMP Configuration Menu Fields

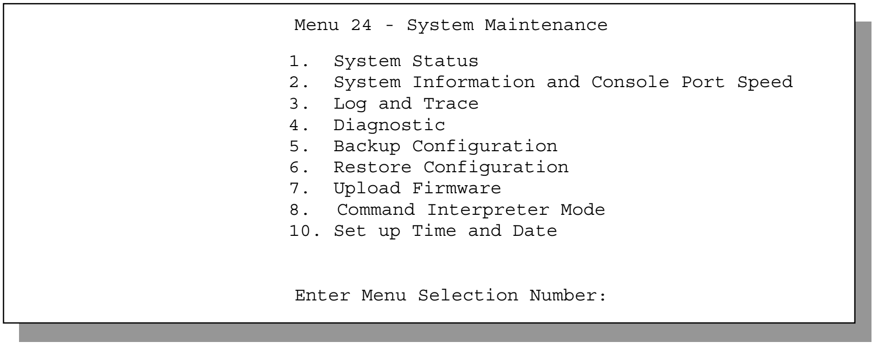
Field	Description	Default
SNMP:		
Get Community	Enter the get community, which is the password for the incoming Get- and GetNext- requests from the management station.	**public**
Set Community	Enter the set community, which is the password for incoming Set-requests from the management station.	**public**
Trusted Host	If you enter a trusted host, your Prestige will only respond to SNMP messages from this address. If you leave the field blank (default), your Prestige will respond to all SNMP messages it receives, regardless of source.	**blank**
Trap:		
Community	Enter the trap community, which is the password sent with each trap to the SNMP manager.	**public**
Destination	Enter the IP address of the station to send your SNMP traps to.	**blank**
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.		

Chapter 10
System Maintenance

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

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. Set up Time and Date


                           Enter Menu Selection Number:
```

Figure 10-1 Menu 24 - System Maintenance

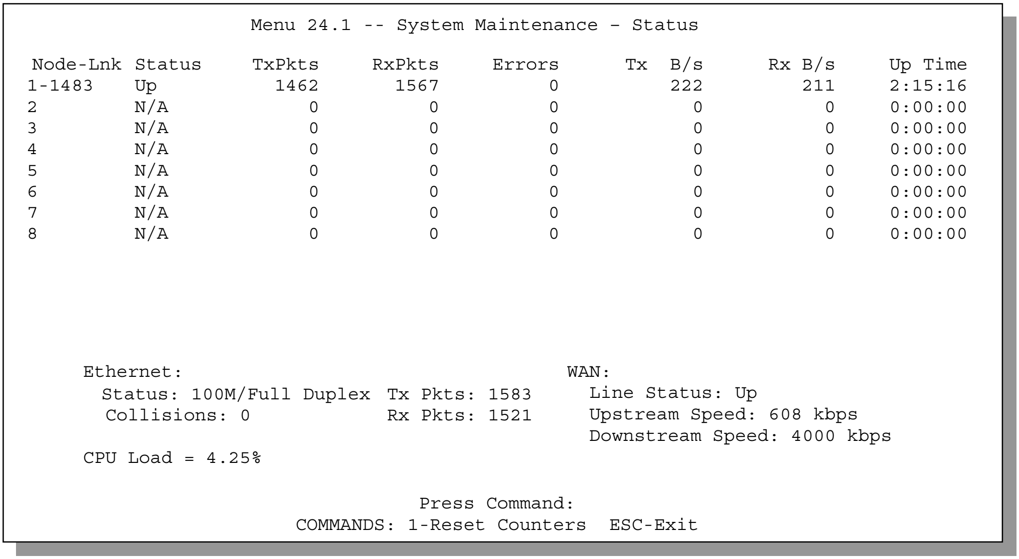
10.1 System Status

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 from the Main Menu 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.

Note: 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: 100M/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
```

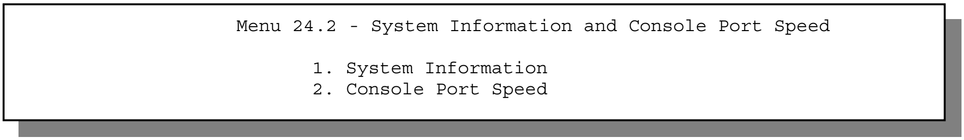
Figure 10-2 Menu 24.1 - System Maintenance - Status

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, 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.
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.

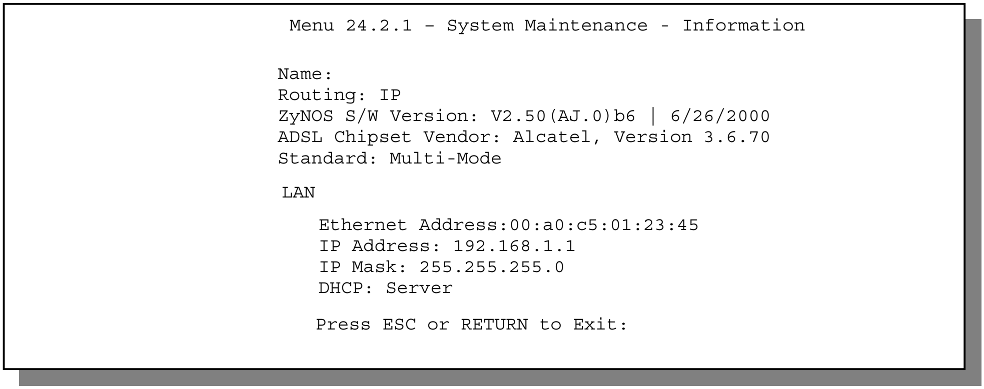
Menu 24.2 System Information and Console Port Speed is as follows:



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

                       1. System Information
                       2. 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 S/W Version: V2.50(AJ.0)b6 | 6/26/2000
                   ADSL Chipset Vendor: Alcatel, Version 3.6.70
                   Standard: Multi-Mode

                   LAN

                       Ethernet Address:00:a0:c5:01:23:45
                       IP Address: 192.168.1.1
                       IP Mask: 255.255.255.0
                       DHCP: Server

                       Press ESC or RETURN to Exit:
```

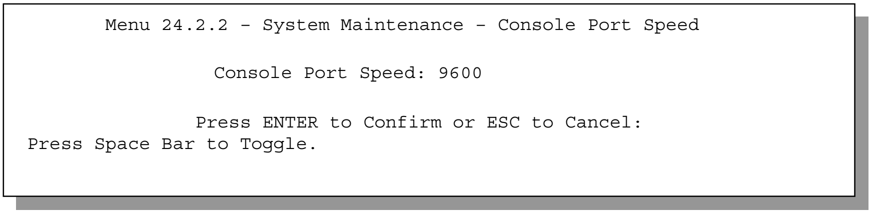
Figure 10-4 System Maintenance - Information

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 S/W Version	Refers to the ZyNOS (ZyXEL Network Operating System) software version. ZyNOS is a registered trademark of ZyXEL Communications Corporation.
ADSL Chipset Vendor	Displays the vendor of the ADSL chipset and ADSL modem software version.
Operational Command	This refers to the operational protocol the Prestige and the DSLAM (Digital Subscriber Line Access Multiplexer) are using.
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.

10.1.1 Console Port Speed

You can change the speed of the console port through **Menu 24.2.2 – Console Port Speed**. Your Prestige supports 9600 (default), 19200, 38400, 57600, and 115200 bps for the console port. Use the space bar to select the desired speed in Menu 24.2.2, as shown in the following figure.



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

                   Console Port Speed: 9600

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

Figure 10-5 Menu 24.2.2 - System Maintenance - Console Port Speed

10.2 Log and Trace

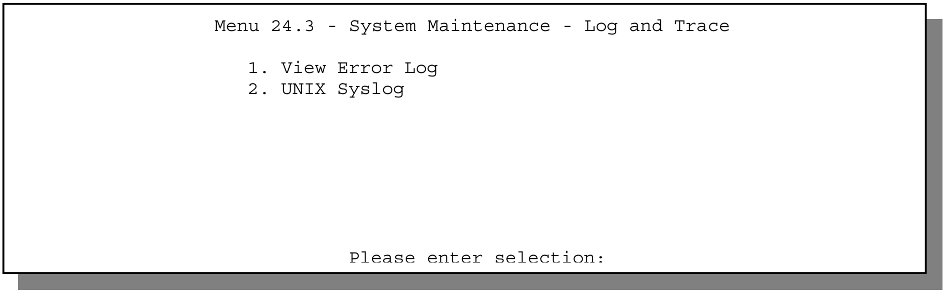
There are two logging facilities in the Prestige. The first is the error logs and trace records that are stored locally. The second is the UNIX syslog facility for message logging.

10.2.1 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**.



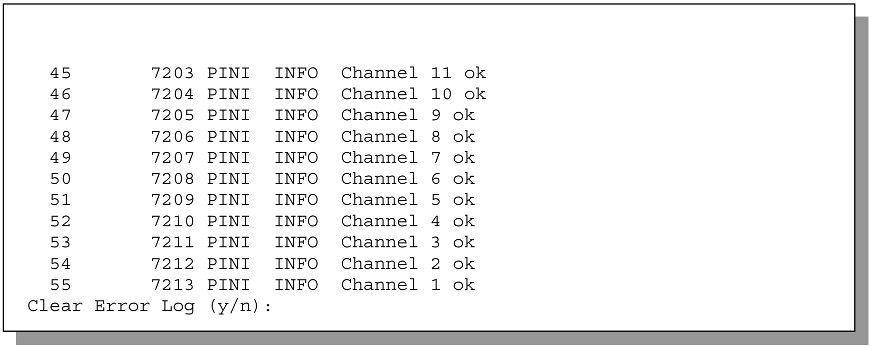
```
                    Menu 24.3 - System Maintenance - Log and Trace

                       1. View Error Log
                       2. UNIX Syslog










                             Please enter selection:
```

Figure 10-6 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.

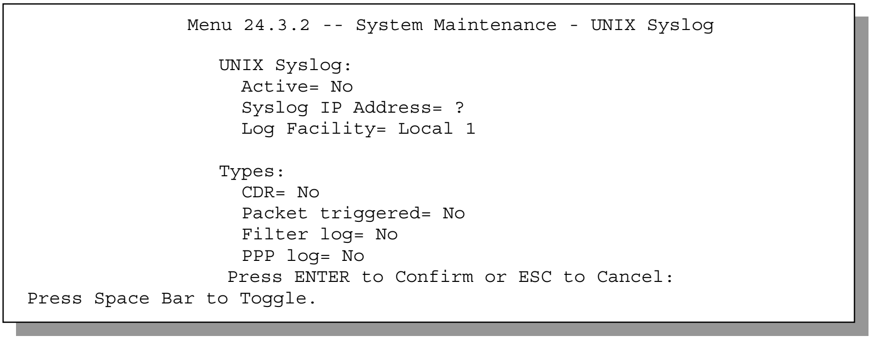


```
  45       7203 PINI  INFO  Channel 11 ok
  46       7204 PINI  INFO  Channel 10 ok
  47       7205 PINI  INFO  Channel 9 ok
  48       7206 PINI  INFO  Channel 8 ok
  49       7207 PINI  INFO  Channel 7 ok
  50       7208 PINI  INFO  Channel 6 ok
  51       7209 PINI  INFO  Channel 5 ok
  52       7210 PINI  INFO  Channel 4 ok
  53       7211 PINI  INFO  Channel 3 ok
  54       7212 PINI  INFO  Channel 2 ok
  55       7213 PINI  INFO  Channel 1 ok
Clear Error Log (y/n):
```

Figure 10-7 Examples of Error and Information Messages

10.2.2 Syslog And Accounting

The Prestige uses the UNIX syslog facility to log the CDR (Call Detail Record) and system messages to a syslog server. Syslog and accounting can be configured in **Menu 24.3.2 - System Maintenance - Syslog and Accounting**, 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 10-8 Menu 24.3.2 - System Maintenance - Syslog and Accounting

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

Table 10-3 System Maintenance Menu Syslog Parameters

Parameter	Description
UNIX Syslog:	
Active	Use the [SPACE BAR] to turn syslog **On** or **Off**.
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 toggle between 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 detail.
Types:	
CDR	Call Detail Record (CDR) logs all data phone line activity if set to **Yes.**
Packet triggered	The first 48 bytes or octets and protocol type of the triggering packet is sent to the UNIX syslog server when this field is set to **Yes.**
Filter log	No filters are logged when this field is set to **No.** Filters with the individual filter **Log Filter** field set to **Yes** 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=450000282400140001f06ac12c0a86614ca849a7b0427001700195b451d1430135004000077600000
```

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

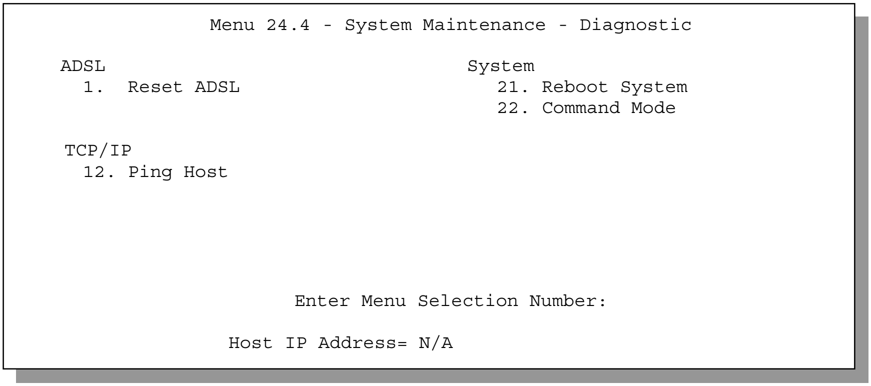
SdcmdSyslogSend(SYSLOG_PPPLOG, SYSLOG_NOTICE, String);
String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto Shutdown
Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP /
IPXCP

```
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

10.3 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 10-9 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.

10.4 Transferring Files - Filename conventions

The configuration file (often called the romfile or romfile-0) contains the factory default settings in the menus such as password, DHCP Setup, TCP/IP Setup etc. It arrives from ZyXEL with a name of

P642.ROM or something similar. Once you have customized the Prestige's setting, they can be saved back to your PC/workstation under a filename of your choosing. Choose something meaningful, e.g. "MyP642.cfg".

The ZyNOS firmware file (sometimes referred to as the ras file) is the file that contains the ZyXEL Network Operating System firmware and usually is the router model name with a *.bin extension, e.g., P642.bin.

With serial (Xmodem) transfer and many ftp and tftp clients (see next), the filenames on the PC are your choice.

```
ftp> put P642.bin ras
```

This is a sample ftp session showing the transfer of the PC file "P642.bin" to the Prestige.

```
ftp> get rom-0 MyP642.cfg
```

This is a sample ftp session saving the current configuration to the PC file MyP642.cfg.

If your [t]ftp client does not allow you to have a destination filename different from 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, i.e., on your workstation, local network or ftp site and so the name (but not the extension) will vary. The AT command is the command you enter after you press "Y" when prompted in the SMT menu to go into debug mode.

Table 10-5 Filename Conventions

File Type	Internal Name	External Name	Description	AT Command
Configuration File	Rom-0	*.rom	This is the router configuration filename on the Prestige. Uploading the rom-0 file replaces the entire ROM file system, including your Prestige configurations, system-related data (including the baud rate and default password), the error log and the trace log.	ATLC
Firmware	Ras	*.bin	This is the generic name for the ZyNOS firmware on the Prestige.	ATUR

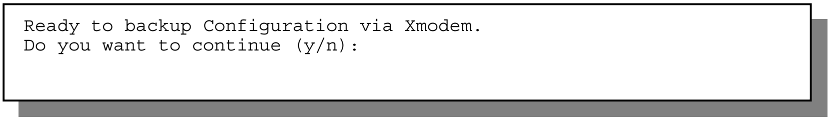
10.4.1 Firmware Development

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

10.5 Backup Configuration

Option 5 in **Menu 24 - System Maintenance** allows you to backup the current Prestige configuration to your workstation. Backup is highly recommended once your Prestige is functioning properly.
You must perform the backup and restore through the console port. Any serial communications program should work fine; however, you must use Xmodem protocol to perform the download/upload.

Step 1. Go to Menu 24.5 (shown next).

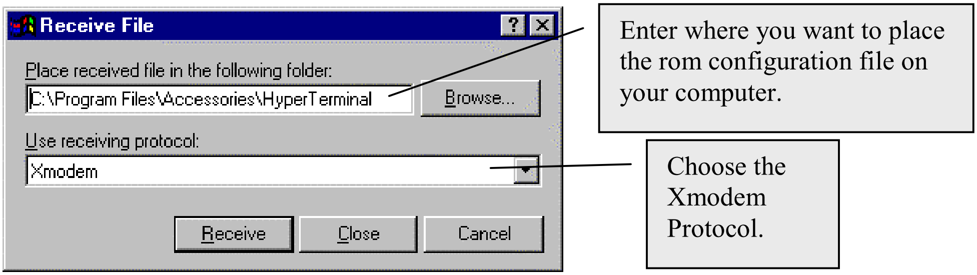


```
Ready to backup Configuration via Xmodem.
Do you want to continue (y/n):
```

Figure 10-10 Backup Configuration

Step 2. Press "Y" to indicate that you want to continue. The following procedure is for the HyperTerminal program. The procedure for other serial communications programs should be similar.

Step 3. Click "Transfer", then "Receive File" to display the following screen.



Receive File

Place received file in the following folder: C:\Program Files\Accessories\HyperTerminal

Use receiving protocol: Xmodem

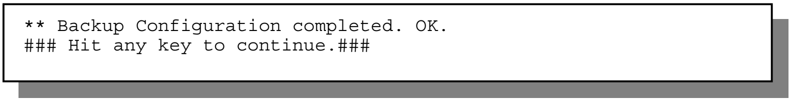
Enter where you want to place the rom configuration file on your computer.

Choose the Xmodem Protocol.

Figure 10-11 HyperTerminal Screen

Step 4. Enter where you want to place the rom configuration file on your computer, give it a suitable name, e.g., p642.rom and make sure you choose the Xmodem Protocol. Then click on "Receive".

Step 5. After a successful backup you will see the following screen. Press any key to return to the SMT menu.



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

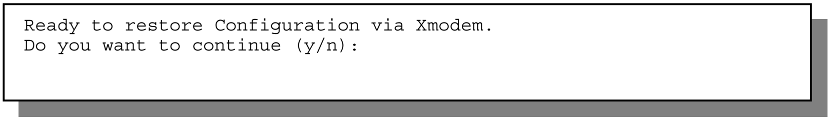
Figure 10-12 Successful Backup

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

10.6 Restore Configuration

Selecting option 6 from **Menu 24 - System Maintenance** to restore the configuration from your workstation to the Prestige. Again, you must use the console port and Xmodem protocol to restore the configuration.

Step 1. Go to Menu 24.6 (shown next).

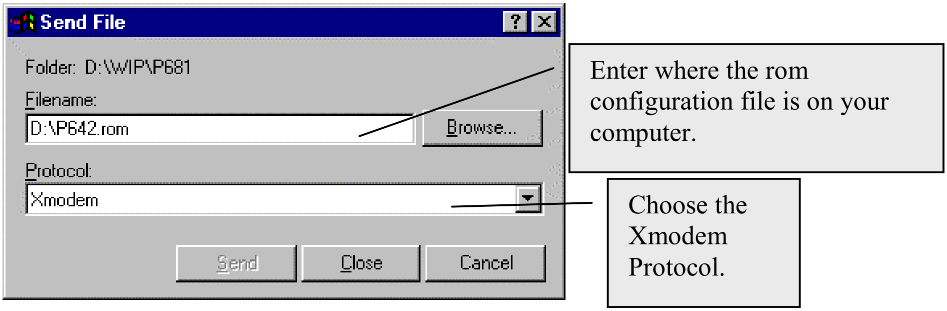


```
Ready to restore Configuration via Xmodem.
Do you want to continue (y/n):
```

Figure 10-13 Restore Configuration

Step 2. Press "Y" to indicate that you want to continue. The following procedure is for the HyperTerminal program. The procedure for other serial communications programs should be similar.

Step 3. Click "Transfer", then "Send File" to display the following screen.



Folder: D:\WIP\P681

Filename: D:\P642.rom

Protocol: Xmodem

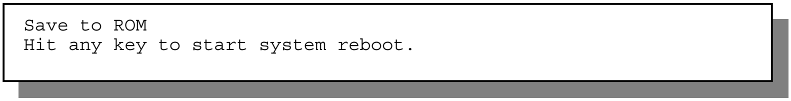
Enter where the rom configuration file is on your computer.

Choose the Xmodem Protocol.

Figure 10-14 HyperTerminal Screen

Step 4. Enter where the rom configuration file is on your computer, and make sure you choose the X-Modem Protocol. Then click on "Send".

Step 5. After a successful restoration you will see the following screen. Press any key to return to reboot the system.



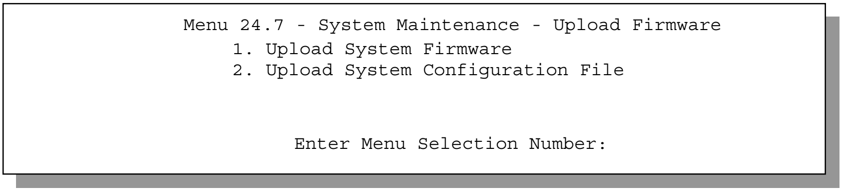
```
Save to ROM
Hit any key to start system reboot.
```

Figure 10-15 Successful Backup

Keep in mind that the configuration is stored in the flash ROM in the Prestige, so even if power failure should occur, your configuration is safe.

10.7 Upload Firmware

Menu 24.7 -- System Maintenance - Upload Firmware allows you to upgrade the firmware and the configuration file via the console port. Note that this function erases the old data before installing the new one; please do not attempt to update unless you have the new firmware at hand. There are 2 components in the system: the router firmware and the configuration file, as shown next.



```
                Menu 24.7 - System Maintenance - Upload Firmware
                     1. Upload System Firmware
                     2. Upload System Configuration File



                          Enter Menu Selection Number:
```

Figure 10-16 Menu 24.7 - System Maintenance - Upload Firmware

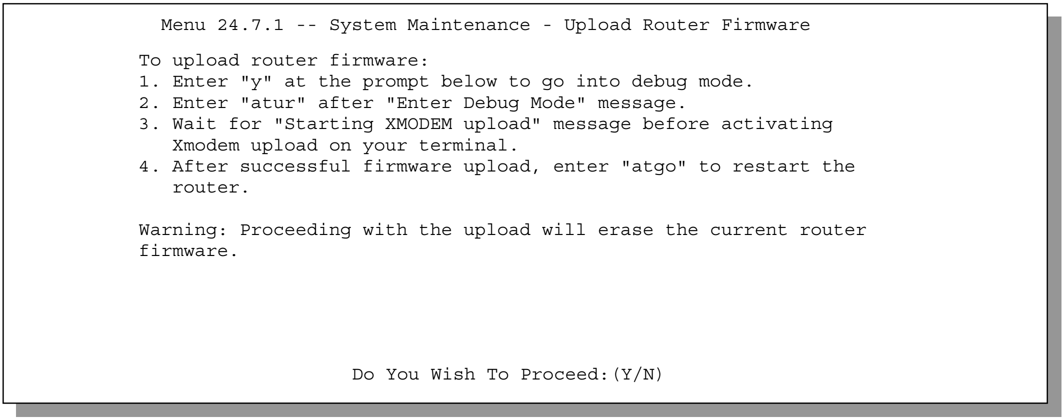
10.7.1 Upload Router Firmware

The firmware is the program that controls the functions of the Prestige. Menu 24.7.1 shows you the instructions for uploading the firmware. If you answer yes to the prompt, the Prestige will go into debug mode. Follow the procedure below to upload the firmware:

Step 1. Enter “`atur`” after the “`Enter Debug Mode`” message.

Step 2. Wait for the “`Starting XMODEM upload`” message before activating Xmodem upload on your terminal.

Step 3. After successful firmware upload, enter “`atgo`” to restart the Prestige.



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

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

            Warning: Proceeding with the upload will erase the current router
            firmware.





                                 Do You Wish To Proceed:(Y/N)
```

Figure 10-17 Menu 24.7.1 - Uploading Router Firmware

10.7.2 Uploading Router Configuration File

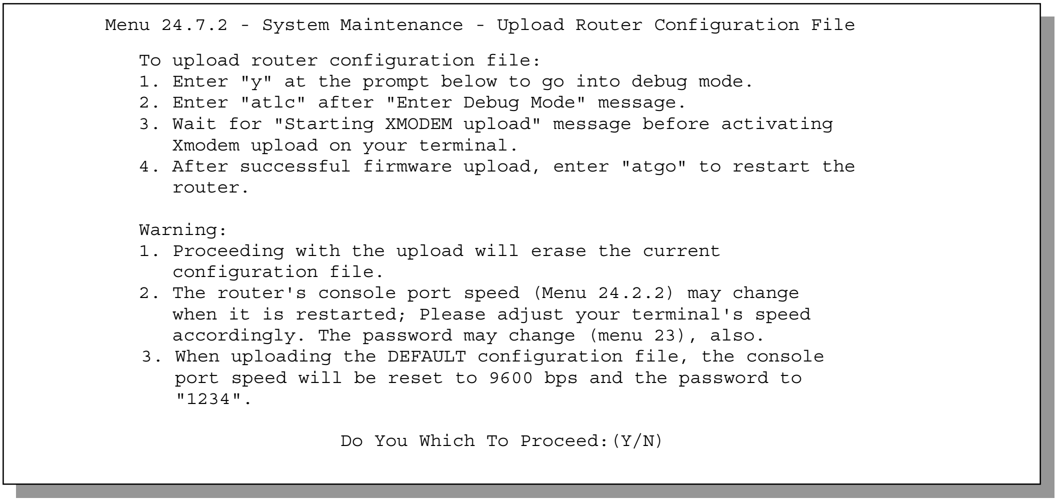
The configuration data, system-related data, the error log and the trace log are all stored in the configuration file. Please be aware that uploading the configuration file replaces everything contained within.
Menu 24.7.2 shows you the instructions for uploading the configuration file. If you answer yes to the prompt, the Prestige will go into debug mode. Follow the procedure below to upload the configuration file:

Note: Menu 24.6 **replaces the current configuration with your customized configuration you backed up previously.** Menu 24.7.2 **shows you the instructions for uploading the Router Configuration file that replaces the current configuration file with the default configuration file, i.e., P642.rom. You will lose all configurations that you had before and the speed of the console port will be reset to the default of 9600 bps with 8 data bit, no parity and 1 stop bit (8n1). You will need to change your serial communications software to the default before you can connect to the Prestige again. The password will be reset to the default of 1234 as well.**

Step 1. Enter "atlc" after the "Enter Debug Mode" message.

Step 2. Wait for the "Starting XMODEM upload" message before activating Xmodem upload on your terminal.

Step 3. After successful firmware upload, enter "atgo" to restart the Prestige.



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

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

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

                              Do You Which To Proceed:(Y/N)
```

Figure 10-18 Menu 24.7.2 - System Maintenance - Upload Router Configuration File

10.8 TFTP Transfer

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

To use TFTP, your workstation must have both Telnet and TFTP clients. To transfer the firmware and the configuration file, follow the procedure below:

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

Step 1. Put the SMT in command interpreter (CI) mode by entering 8 in **Menu 24 – System Maintenance**.

Step 2. Enter the command "sys stdio 0" (zero, not capital o) to disable the SMT timeout, so the TFTP transfer will not be interrupted. Enter the command "sys stdio 5" to restore the five-minute SMT timeout (default) when the file transfer is complete.

Step 3. Launch the TFTP client on your workstation and connect to the Prestige. Set the transfer mode to binary before starting data transfer.

Step 4. Use the TFTP client (see the example below) to transfer files between the Prestige and the workstation. The file name for the firmware is "`ras`" and for the configuration file, is "`rom-0`" (rom-zero, not capital o).

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

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

10.8.1 Example TFTP Command

The following is an example tftp command:

```
TFTP [-i] host put p312.bin ras
```

where "i" specifies binary image transfer mode (use this mode when transferring binary files), "host" is the Prestige IP address, "put" transfers the file source on the workstation (p312.bin – name of the firmware on the workstation) to the file destination on the remote host (ras - name of the firmware on the Prestige).

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

Table 10-6 Third Party TFTP Clients - General fields

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

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

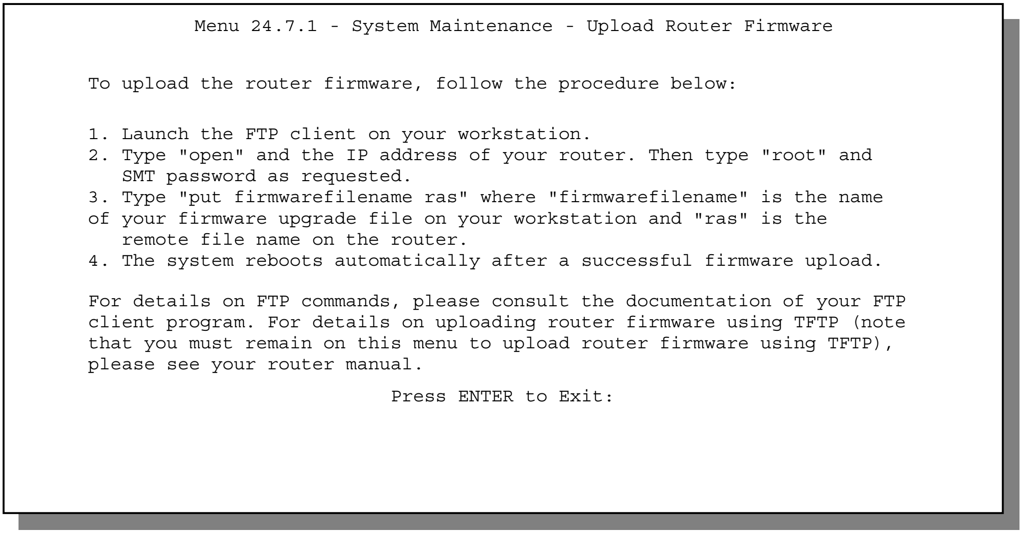
TFTP over WAN will not work if:

1. You have applied a filter in Menu 3.1 (LAN) or in Menu 11.5 (WAN) to block Telnet service.
2. You have an SMT console session running.

10.9 FTP File Transfer

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

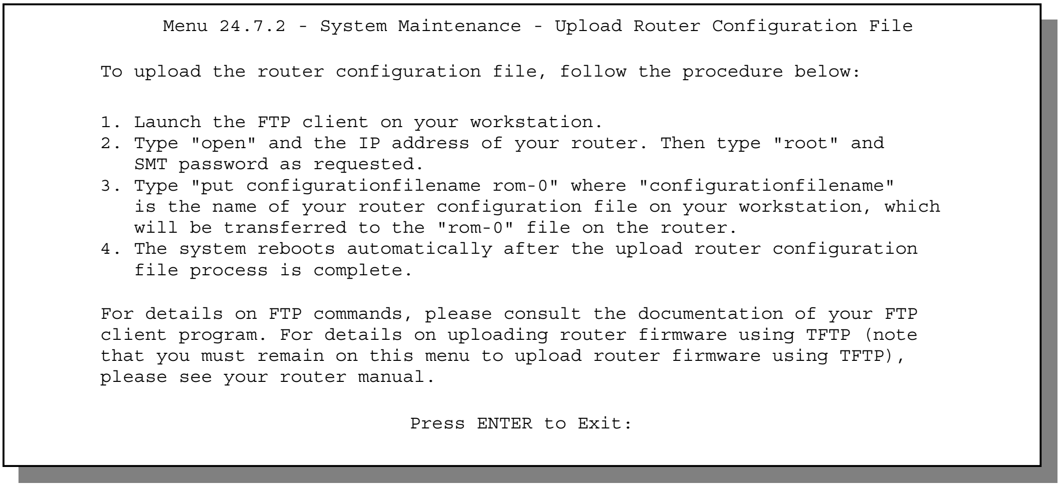
When you telnet into the Prestige, you will see the following screens for uploading firmware and the configuration file using FTP:



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


       To upload the router firmware, follow the procedure below:

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

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

Figure 10-19 Telnet into Menu 24.7.1

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



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

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

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

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

                              Press ENTER to Exit:
```

Figure 10-20 Telnet into Menu 24.7.2 - System Maintenance

:

10.9.1 Using the FTP command from the DOS Prompt

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

Step 1. Launch the FTP client on your workstation.

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

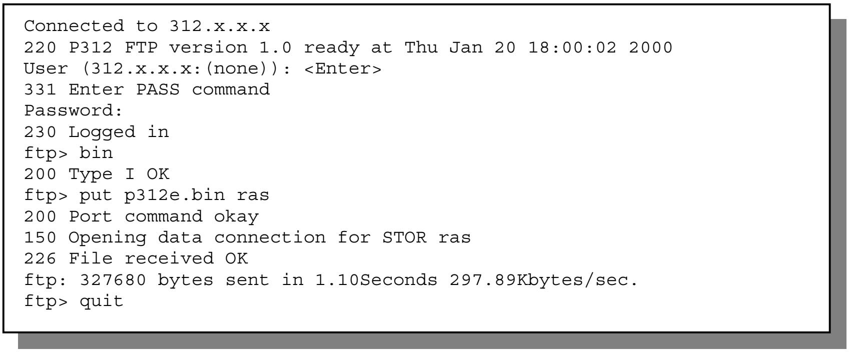
Step 3. You may press [ENTER] when prompted for a username.

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

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

Step 6. Use “put” to transfer files from the workstation to the Prestige, e.g., `put p642.bin ras` transfers the firmware on your computer (p642.bin) to the Prestige and renames it “ras”. Similarly `put p642.rom rom-0` transfers the configuration file on your computer (p642.rom) to the Prestige and renames it “rom-0”. See *Section 10.4* for more information on filename conventions.

Step 7. Type “quit” to exit the ftp prompt.



```
Connected to 312.x.x.x
220 P312 FTP version 1.0 ready at Thu Jan 20 18:00:02 2000
User (312.x.x.x:(none)): <Enter>
331 Enter PASS command
Password:
230 Logged in
ftp> bin
200 Type I OK
ftp> put p312e.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 10-21 FTP Session Example

Note: The system reboots after a successful upload.

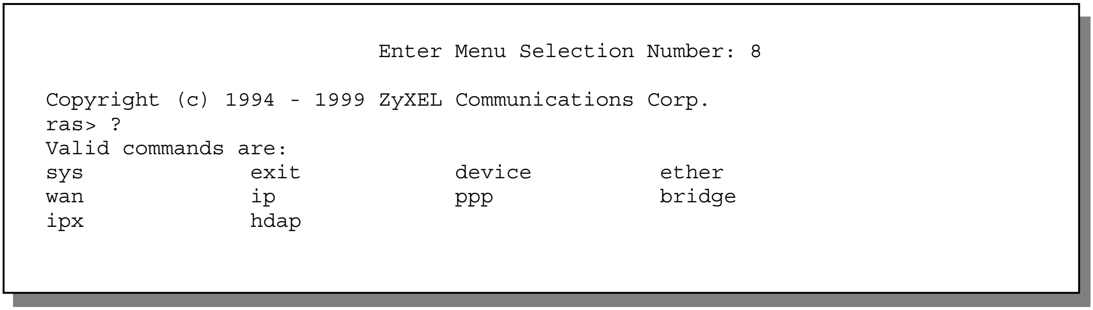
The following table describes some of the fields that you may see in third party FTP clients:

Table 10-7 Third Party FTP Clients - General fields

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).

10.10 Command Interpreter Mode

This option allows you to enter the command interpreter mode. A list of valid commands can be found by typing [help] at the command prompt. For more detailed information, check the ZyXEL Web site or send e-mail to the ZyXEL Support Group.

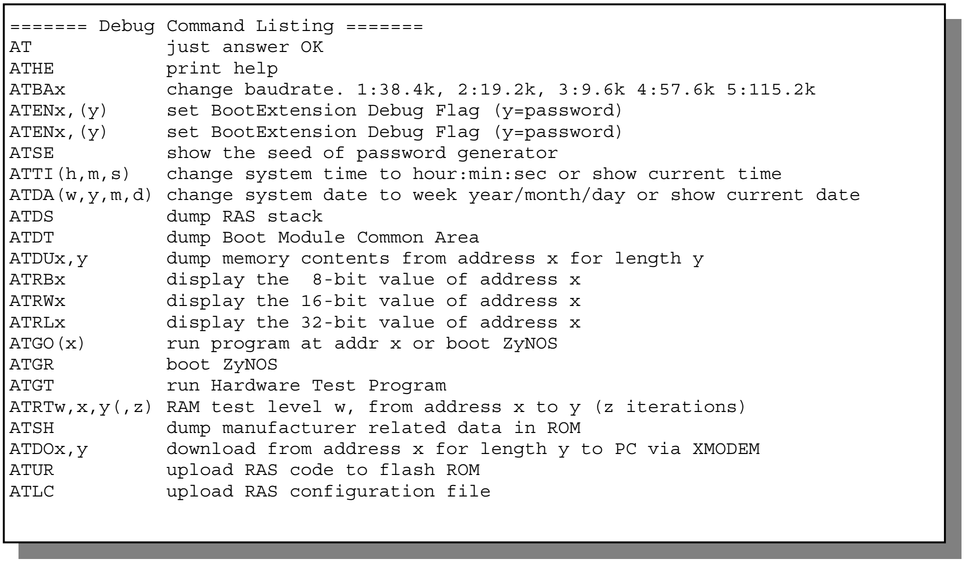


```
                          Enter Menu Selection Number: 8

Copyright (c) 1994 - 1999 ZyXEL Communications Corp.
ras> ?
Valid commands are:
sys             exit            device          ether
wan             ip              ppp             bridge
ipx             hdap
```

Figure 10-22 Command mode

10.11 Boot module commands

Prestige boot module commands with accompanying explanations are shown in the following table. For ATBAx, x denotes the number preceding the colon to give the console port speed following the colon in the list of numbers that follows; e.g. ATBA3 will give a console port speed of 9.6 Kbps. ATSE displays the seed that is used to generate a password to turn on the debug flag in the firmware. The ATSH command shows product-related information such as boot module version, vendor name, product model, RAS code revision, etc.



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

Figure 10-23 Boot module commands

10.12 Time and Date Setting

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

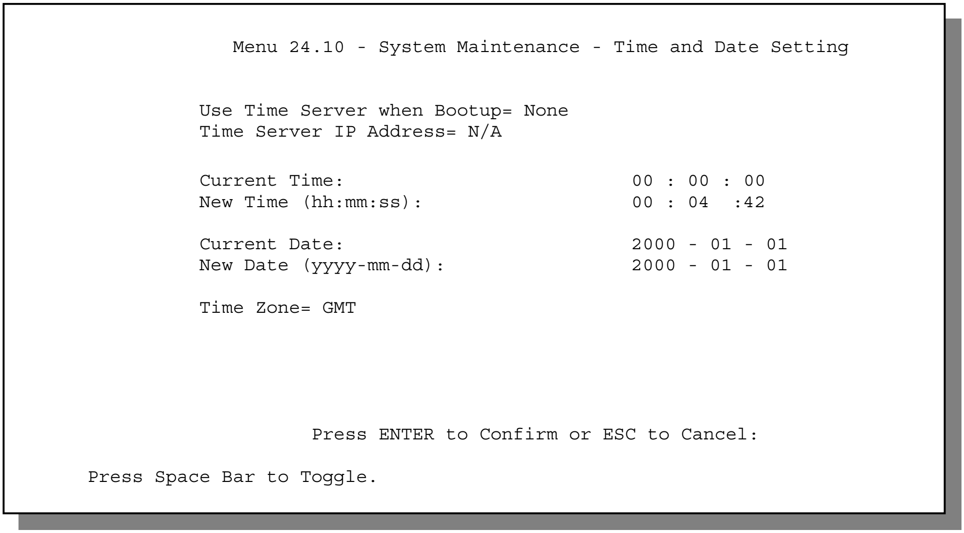
10.12.1 How often does the Prestige update the time?

The Prestige updates the time in three instances:

i. On leaving Menu 24.10 after making changes.

ii. When the Prestige boots up and there is a time server configured in Menu 24.9.

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



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


                 Use Time Server when Bootup= None
                 Time Server IP Address= N/A

                 Current Time:                         00 : 00 : 00
                 New Time (hh:mm:ss):                  00 : 04  :42

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

                 Time Zone= GMT





                           Press ENTER to Confirm or ESC to Cancel:

       Press Space Bar to Toggle.
```

Figure 10-24 System Maintenance - Time and Date Setting

Table 10-8 Time and Date Setting Fields

Field	Description
Use Time Server when Bootup	Enter the time service protocol that your timeserver will send when the Prestige powers up. Choices are **Daytime (RFC-867)**, **Time (RFC-868)**, **NTP (RFC-1305)** and **None**. The main differences between them are the format, e.g., the **Daytime (RFC 867)** format is day/month/date/year/time zone of the server while the **Time (RFC-868)** format gives a 4-byte integer giving the total number of seconds since **1970/1/1** at 0:0:0. The **NTP (RFC-1305)** format is similar. Not all timeservers support all protocols, so you may have to check with your ISP/network administrator or use trial and error to find a protocol that works. If you select **None** (this is the default value), you can enter the time manually but each time the system is booted, the time & date will be reset to **1970/1/1 0:0:0**.
Time Server IP Address	Enter the IP address of the your timeserver. Check with your ISP/network administrator if you are unsure of this information.
Current Time: New Time	 Enter the new time in hour, minute and second format.
Current Date:	

New Date	Enter the new date in month, date and year format.
Time Zone	Press the [SPACE BAR] to set the time difference between your time zone and Greenwich Mean Time (GMT). Be aware if/when daylight savings time alters this time difference for your time zone.
Once you have filled in the new time and date, press [ENTER] to save the setting and press [ESC] to return to Menu 24.	

Chapter 11
IP Policy Routing

11.1 Introduction

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

11.1.1 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.

11.1.2 Routing Policy

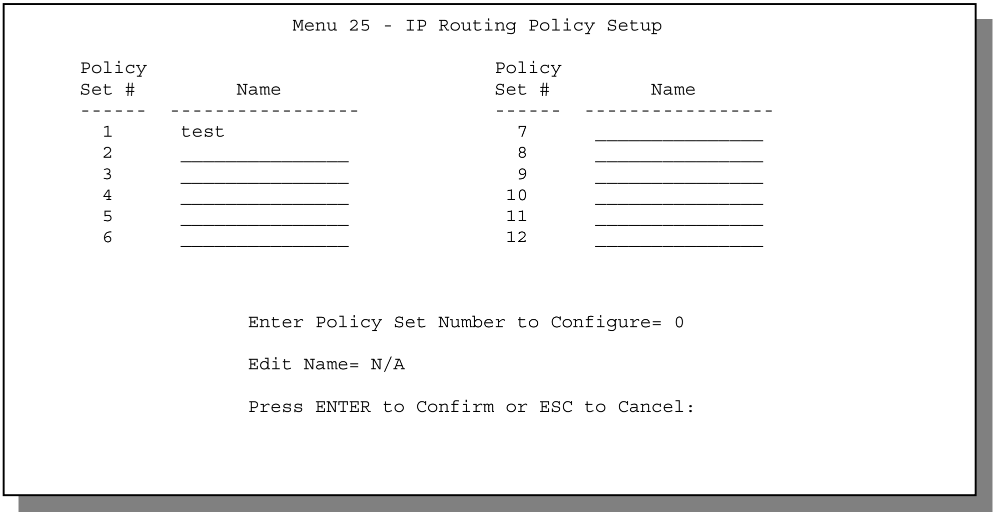
A policy defines the matching criteria and the action to take when a packet meets the criteria. The action is taken only when all the criteria are met. The criteria include the source address and port, IP protocol (ICMP, UDP, TCP, etc.), destination address and port, TOS and precedence (fields in the IP header) and length. The inclusion of length criterion is to differentiate between interactive and bulk traffic. Interactive applications, e.g., Telnet, tend to have short packets, while bulk traffic, e.g., file transfer, tends to have large packets.

The actions that can be taken include routing the packet to a different gateway (and hence the outgoing interface) and the TOS and precedence fields in the IP header.

IPPR follows the existing packet filtering facility of ZyNOS 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 6 policies in each set.

11.1.3 IP Policy Routing 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:
```

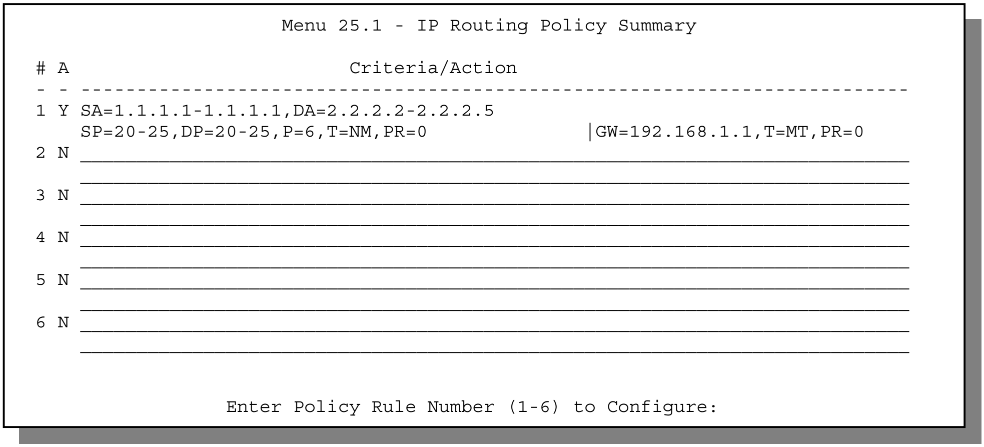
Figure 11-1 IP Routing Policy Setup

To setup a routing policy, follow the procedures below:

Step 1. Enter 25 in the Main Menu to open **Menu 25 – IP Policy Routing Setup.**

Step 2. Enter the index of the policy set you wish to configure to open **Menu 25.1 - IP Policy Routing Summary**.

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, the separator '|' means the action is taken on criteria matched and the separator '=' means the action is taken on criteria not matched.



```
                         Menu 25.1 - IP Routing Policy Summary

  # 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:
```

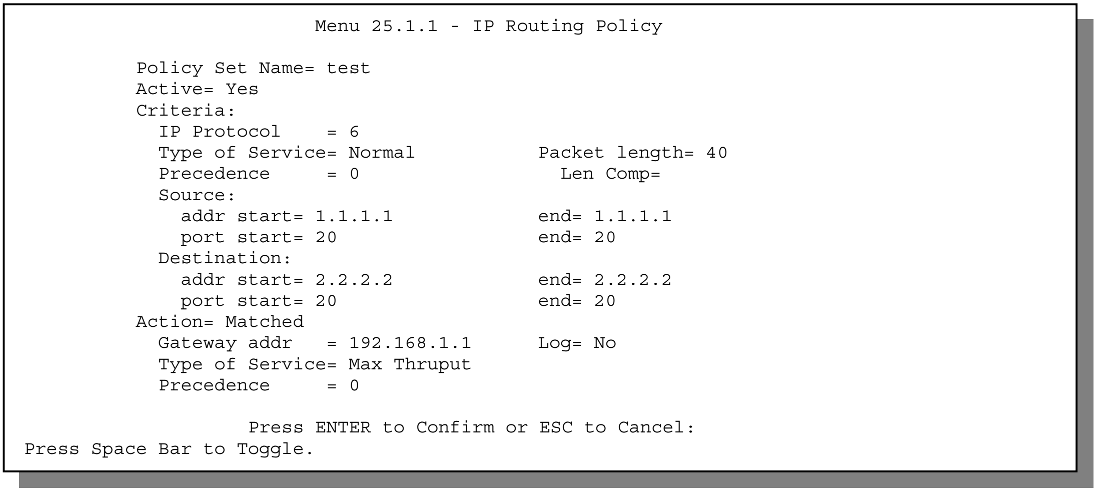
Figure 11-2 Menu 25 - IP Routing Policy Summary

Table 11-1 IP Routing Policy Summary

Abbreviation	Meaning
Criteria	
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
Type Of Service	
NM	Normal
mD	Minimum Delay

MT	Maximum Throughput
MR	Maximum Reliability
MC	Minimum Cost

Enter 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=
            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 11-3 IP Routing Policy

Table 11-2 IP Routing Policy

Field	Description
Policy Set Name	This is the name of the policy set 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] / [Max Reliability].
Packet Length	Enter the length of incoming packets (in bytes). The operators in the [Len Comp] (next) apply to packets of this length.
Len Comp	Press to choose from [Equal] / [Not Equal] / [Less] / [Greater] / [Less or Equal] / Greater or Equal].

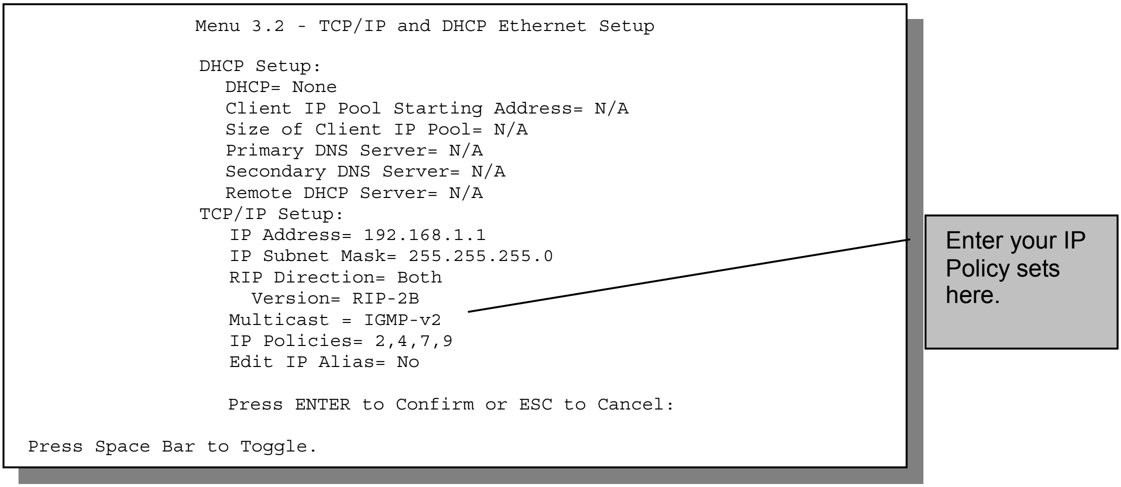
Precedence	Precedence value of the incoming packet. Values range from [0] to [7] or [Don't Care].
Source:	
addr start= / end=	Source IP address range from start to end.
port start= / end=	Source port number range from start to end; applicable only for TCP/UDP.
Destination:	
addr start= / end=	Destination IP address range from start to end.
port start= / end=	Destination port number range from start to end; applicable only for TCP/UDP.
Action=	Specifies whether action should be taken on criteria [Matched] or [Not Matched].
Gateway addr	Defines the outgoing gateway address. The gateway must be on the same subnet as the Prestige if it's 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.
Log	Press [SPACE BAR] to select **Yes** to make an entry in the system log when a policy is executed.
Type of Service	Set the new TOS value of the outgoing packet. Choose from Prioritize incoming network traffic by choosing from [No Change] / [Normal] / [Min Delay] / [Max Thruput] / [Max Reliability].
Precedence	Set the new precedence value of the outgoing packet. Values range from [0] to [7] or [No Change].

11.2 Applying an IP Policy

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

11.2.1 Ethernet IP Policies

From **Menu 3 - Ethernet Setup**, enter 2 to go to **Menu 3.2 -General Ethernet Setup**.
You can choose up to four IP Policy sets (from twelve) by entering their numbers separated by commas, e.g., 2, 4, 7, 9.



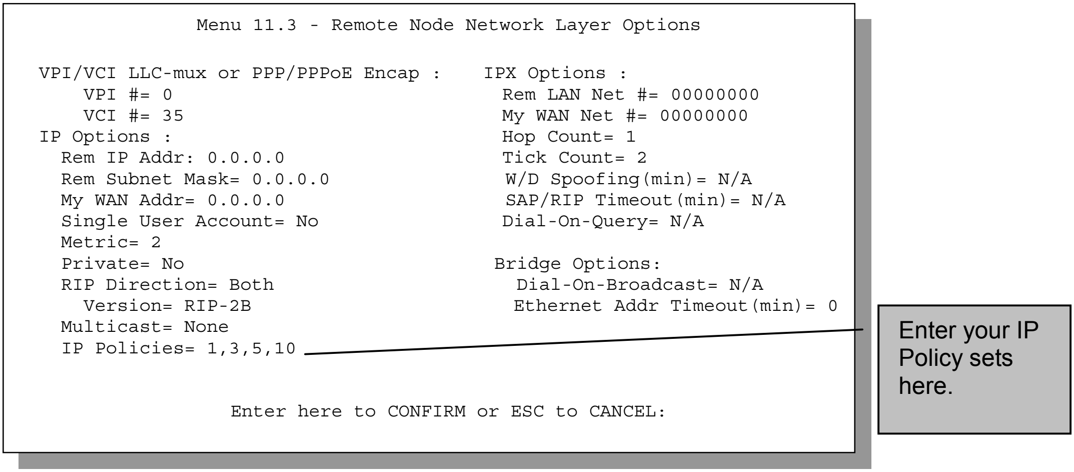
```
                Menu 3.2 - TCP/IP and DHCP Ethernet Setup

                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.
```

Enter your IP Policy sets here.

Figure 11-4 Menu 3.2 - General Ethernet Setup

11.2.2 Remote Node IP Routing Policies

Go to Menu 11.3 (shown next) and enter the number(s) of the IP Routing Policy set(s) as appropriate. You can cascade up to four policy sets by entering 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
    My WAN Addr= 0.0.0.0                    SAP/RIP Timeout(min)= N/A
    Single User Account= No                 Dial-On-Query= N/A
    Metric= 2
    Private= No                            Bridge Options:
    RIP Direction= Both                      Dial-On-Broadcast= N/A
      Version= RIP-2B                        Ethernet Addr Timeout(min)= 0
    Multicast= None
    IP Policies= 1,3,5,10


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

Enter your IP Policy sets here.

Figure 11-5 Menu 11.3 - Remote Node Network Layer Options

Chapter 12
Troubleshooting

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

12.1 Problems Starting Up the Prestige

Table 12-1 Troubleshooting the Start-Up of your Prestige

Problem	Corrective Action	
None of the LEDs are on when you turn on the Prestige.	Check the connection between the AC adapter and the Prestige. If the error persists, you may have a hardware problem. In this case you should contact technical support.	
Cannot access the Prestige via the console port.	1.Check to see if the Prestige is connected to your computer's serial port.	
	2. Check to see if the communications program is configured correctly. The communications software should be configured as follows:	VT100 terminal emulation
		9600 bps
		No parity, 8 Data bits, 1 Stop bit.

12.2 Problems With the WAN Interface

Table 12-2 Troubleshooting the ADSL connection

Problem	Corrective Action
Initialization of the PVC connection failed.	Ensure that the cable is connected properly from the ADSL port to the wall jack. The ADSL 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. Reboot the Prestige. If you still have problems, you may need to verify these variables with the telephone company and/or ISP.

12.3 Problems with the LAN Interface

Table 12-3 Troubleshooting the LAN Interface

Problem	Corrective Action
Can't ping any station on the LAN.	Check the Ethernet LEDs on the front panel. The LED should be on for a port that has a station connected. If it is off, check the cables between your Prestige and the station.
	Verify that the IP address and the subnet mask are consistent between the Prestige and the workstations.

12.4 Problems Connecting to a Remote Node or ISP

Table 12-4 Troubleshooting a Connection to a Remote Node or ISP

Problem	Corrective Action
Can't connect to a remote node or ISP.	Check Menu 24.1 to verify the line status. If it indicates [down], then refer to the section on the line problems.
	In Menu 11.1, verify your login name and password for the remote node.

Glossary

10BaseT The 10-Mbps baseband Ethernet specification that uses two pairs of twisted-pair cabling (Category 3 or 5): one pair for transmitting data and the other for receiving data.

ADSL Asymmetrical Digital Subscriber Line is an asymmetrical technology, meaning that the downstream data rate is much higher than the upstream data rate. ADSL operates in a frequency range that is above the frequency range of voice services, so the two systems can operate over the same cable.

ARP Address Resolution Protocol is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network.

Backbone A high-speed line or series of connections that forms a major pathway within a network.

Bandwidth This is the capacity on a link usually measured in bits-per-second (bps).

Bit (Binary Digit) -- A single digit number in base-2, in other words, either a 1 or a zero. The smallest unit of computerized data.

Byte A set of bits that represent a single character. There are 8 bits in a Byte.

CDR Call Detail Record. This is a name used by telephone companies for call related information.

CHAP Challenge Handshake Authentication Protocol is an alternative protocol that avoids sending passwords over the wire by using a challenge/response technique.

Client A software program that is used to contact and obtain data from a Server software program on another computer. Each Client program is designed to work with one or more specific kinds of Server programs, and each Server requires a specific kind of Client. A Web Browser is a specific kind of Client.

Crossover Ethernet Cable A cable that wires a pin to its opposite pin, for example, RX+ is wired to TX+. This cable connects two similar devices, for example, two data terminal equipment (DTE) or data communications equipment (DCE) devices.

CSU/DSU Channel Service Unit/Data Service Unit. CSUs (channel service units) and DSUs (data service units) are actually two separate devices, but they are used in conjunction and often combined into the same box. The devices are part of the hardware you need to connect computer equipment to digital transmission lines). The Channel Service Unit device connects with the digital communication line and provides a termination for the digital signal. The Data Service Unit device, sometimes called a digital service unit, is the hardware component you need to transmit digital data over the hardware channel. The device converts signals from bridges, routers, and multiplexors into the bipolar digital signals used by the digital lines. Multiplexors mix voice signals and data on the same line.

DCE Data Communications Equipment is typically a modem or other type of communication device. The DCE sits between the DTE (data terminal equipment) and a transmission circuit such as a phone line.

DHCP Dynamic Host Configuration Protocol automatically assigns IP addresses to clients when they log on. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses for a period of time which means that addresses are made available to assign to other systems.

DNS Domain Name System links names to IP addresses. When you access Web sites on the Internet, you can type the IP address of the site or the DNS name. When you type a domain name in a Web browser, a query is sent to the primary DNS server defined in your Web browser's configuration dialog box. The DNS server converts the name you specified to an IP address and returns this address to your system. From then on, the IP address is used in all subsequent communications.

Domain Name The unique name that identifies an Internet site. Domain Names always have 2 or more parts, separated by dots. The part on the left is the most specific, and the part on the right is the most general.

DRAM Dynamic RAM that stores information in capacitors that must be refreshed periodically.

DSL Digital Subscriber Line technologies enhances the data capacity of the existing twisted-pair wire that runs between the local telephone company switching offices and most homes and offices. There are actually seven types of DSL service, ranging in speeds from 16 Kbits/sec to 52 Mbits/sec. The services are either symmetrical (traffic flows at the same speed in both directions), or asymmetrical (the downstream capacity is higher than the upstream capacity). DSL connections are point-to-point dedicated circuits, meaning that they are always connected. There is no dial-up. There is also no switching, which means that the line is a direct connection into the carrier's frame relay, ATM (Asynchronous Transfer Mode), or Internet-connect system.

DSLAM A Digital Subscriber Line Access Multiplexer (DSLAM) is a network device, usually at a telephone company central office, that receives signals from multiple customer Digital Subscriber Line connections and puts the signals on a high-speed backbone line using multiplexing techniques. Depending on the product, DSLAM multiplexers connect DSL lines with some combination of asynchronous transfer mode ATM, frame relay, or IP networks.

DTE Originally, the DTE (Data Terminal Equipment) was a dumb terminal or printer, but today it is a computer, or a bridge or router that interconnects local area networks.

EMI ElectroMagnetic Interference. The interference by electromagnetic signals that can cause reduced data integrity and increased error rates on transmission channels.

Ethernet A very common method of networking computers in a LAN. There are a number of adaptations to the IEEE 802.3 Ethernet standard, including adaptations with data rates of 10 Mbits/sec and 100 Mbits/sec over coaxial cable, twisted-pair cable, and fiber-optic cable. The latest version of Ethernet, Gigabit Ethernet, has a data rate of 1 Gbit/sec.

FAQ (Frequently Asked Questions) -- FAQs are documents that list and answer the most common questions on a particular subject.

FCC The FCC (Federal Communications Commission) is in charge of allocating the electromagnetic spectrum and thus the bandwidth of various communication systems.

Flash Memory The nonvolatile storage that can be electrically erased and reprogrammed so that data can be stored, booted, and rewritten as necessary.

Gateway A gateway is a computer system or other device that acts as a translator between two systems that do not use the same communication protocols, data formatting structures, languages, and/or architecture.

Host Any computer on a network that is a repository for services available to other computers on the network. It is quite common to have one host machine provide several services, such as WWW and USENET.

IANA Internet Assigned Number Authority acts as the clearinghouse to assign and coordinate the use of numerous Internet protocol parameters such as Internet addresses, domain names, protocol numbers, and more. The IANA Web site is at http://www.isi.edu/iana.

ICMP Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and are not directly apparent to the application user.

Internet (Lower case i) Any time you connect 2 or more networks together, you have an internet.

Internet (Upper case I) The vast collection of inter-connected networks that all use the TCP/IP protocols and that evolved from the ARPANET of the late 60's and early 70's.

Intranet A private network inside a company or organization that uses the same kinds of software that you would find on the public Internet, but that is only for internal use.

IP Internet Protocol. The IP (currently IP version 4, or IPv4), is the underlying protocol for routing packets on the Internet and other TCP/IP-based networks.

IPCP (PPP) IP Control Protocol allows changes to IP parameters such as the IP address.

IPX Internetwork Packet eXchange The native NetWare internetworking protocol is IPX (Internetwork Packet Exchange). Like IP (Internet Protocol), IPX is an internetworking protocol that provides datagram services.

ISP Internet Service Providers provide connections into the Internet for home users and businesses. There are local, regional, national, and global ISPs. You can think of local ISPs as the gatekeepers into the Internet.

LAN Local Area Network is a shared communication system to which many computers are attached. A LAN, as its name implies, is limited to a local area. This has to do more with the electrical characteristics of the medium than the fact that many early LANs were designed for departments, although the latter accurately describes a LAN as well. LANs have different topologies, the most common being the linear bus and the star configuration.

MAC On a local area network (LAN) or other network, the MAC (Media Access Control) address is your computer's unique hardware number. (On an Ethernet LAN, it's the same as your Ethernet address.) The MAC layer frames data for transmission over the network, then passes the frame to the physical layer interface where it is transmitted as a stream of bits.

NAT Network Address Translation is the translation of an Internet Protocol address used within one network to a different IP address known within another network.

Network Any time you connect 2 or more computers together so that they can share resources, you have a computer network. Connect 2 or more networks together and you have an internet.

NIC Network Interface Card. A board that provides network communication capabilities to and from a computer system. Also called an adapter.

Node Any single computer connected to a network.

PAP Password Authentication Protocol. PAP is a security protocol that requires users to enter a password before accessing a secure system. The user's name and password are sent over the wire to a server, where they are compared with a database of user account names and passwords. This technique is vulnerable to wiretapping (eavesdropping) because the password can be captured and used by someone to log onto the system.

PNC Prestige Network Commander, a Windows-based setup wizard for Prestige routers (not all).

Port An Internet port refers to a number that is part of a URL, appearing after a colon (:) right after the domain name. Every service on an Internet server listens on a particular port number on that server. Most services have standard port numbers, e.g. Web servers normally listen on port 80.

POTS Plain Old Telephone Service is the analog telephone service that runs over copper twisted-pair wires and is based on the original Bell telephone system. Twisted-pair wires connect homes and businesses to a neighborhood central office. This is called the local loop. The central office is connected to other central offices and long-distance facilities.

PPP Point to Point Protocol. PPP encapsulates and transmits IP (Internet Protocol) datagrams over serial point-to-point links. PPP works with other protocols such as IPX (Internetwork Packet Exchange). The protocol is defined in IETF (Internet Engineering Task Force) RFC 1661 through 1663. PPP provides router-to-router, host-to-router, and host-to-host connections.

PSTN Public Switched Telephone Network was put into place many years ago as a voice telephone call-switching system. The system transmits voice calls as analog signals across copper twisted cables from homes and businesses to neighborhood COs (central offices); this is often called the local loop. The PSTN is a circuit-switched system, meaning that an end-to-end private circuit is established between caller and callee.

PVC Permanent Virtual Circuit. A PVC is a logical point-to-point circuit between customer sites. PVCs are low-delay circuits because routing decisions do not need to be made along the way. Permanent means that the circuit is preprogrammed by the carrier as a path through the network. It does not need to be set up or torn down for each session.

RFC An RFC (Request for Comments) is an Internet formal document or standard that is the result of committee drafting and subsequent review by interested parties. Some RFCs are informational in nature. Of those that are intended to become Internet standards, the final version of the RFC becomes the standard and no further comments or changes are permitted. Change can occur, however, through subsequent RFCs.

RIP Routing Information Protocol is an interior or intra-domain routing protocol that uses the distance-vector routing algorithms. RIP is used on the Internet and is common in the NetWare environment as a method for exchanging routing information between routers.

SAP In NetWare, the SAP (Service Advertising Protocol) broadcasts information about available services on the network that other network devices can listen to. A server sends out SAP messages every 60 seconds. A server also sends out SAP messages to inform other devices that it is closing down. Workstations use SAP to find services they need on the network.

Server A computer, or a software package, that provides a specific kind of service to client software running on other computers.

SNMP System Network Management Protocol is a popular management protocol defined by the Internet community for TCP/IP networks. It is a communication protocol for collecting information from devices on the network.

STP Twisted-pair cable consists of copper-core wires surrounded by an insulator. Two wires are twisted together to form a pair, and the pair form a balanced circuit. The twisting prevents interference problems. STP (shielded twisted-pair) provides protection against external crosstalk.

Straight Through Ethernet Cable A cable that wires a pin to its equivalent pin. This cable connects two dissimilar devices, for example, a data terminal equipment (DTE) and a data communications equipment (DCE) device. A straight through Ethernet cable is the most common cable used.

SUA Single User Account. The Prestige's SUA (Single User Account) feature allows multiple user Internet access for the cost of a single ISP account - see also NAT.

TCP Transmission Control Protocol handles flow control and packet recovery and IP providing basic addressing and packet-forwarding services.

Telnet Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.

Terminal A device that allows you to send commands to a computer somewhere else. At a minimum, this usually means a keyboard and a display screen and some simple circuitry.

Terminal Software Software that pretends to be (emulates) a physical terminal and allows you to type commands to a computer somewhere else.

TFTP Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP (File Transfer

Protocol), but it is scaled back in functionality so that it requires fewer resources to run. TFTP uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).

UDP User Datagram Protocol. UDP is a connectionless transport service that dispenses with the reliability services provided by TCP. UDP gives applications a direct interface with IP and the ability to address a particular application process running on a host via a port number without setting up a connection session.

URL Uniform Resource Locator. URL is an object on the Internet or an intranet that resides on a host system. Objects include directories and an assortment of file types, including text files, graphics, video, and audio. A URL is the address of an object that is normally typed in the Address field of a Web browser. The URL is basically a pointer to the location of an object.

VCI Virtual Channel Identifier. Identifies virtual channels between users or between users and networks.

VPI Virtual Path Identifier. Identifies virtual paths between users or between users and networks.

WAN Wide Area Networks link geographically dispersed offices in other cities or around the globe. Just about any long-distance communication medium can serve as a WAN link, including switched and permanent telephone circuits, terrestrial radio systems, and satellite systems.

WWW World Wide Web. Frequently used (incorrectly) when referring to "The Internet", WWW has two major meanings - First, loosely used: the whole constellation of resources that can be accessed using Gopher, FTP, HTTP, Telnet, USENET, WAIS and some other tools. Second: the universe of hypertext servers (HTTP servers).

Appendix A PPPoE

PPPoE in Action

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

Benefits of PPPoE

PPPoE offers the following benefits:

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

Traditional Dial-up Scenario

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

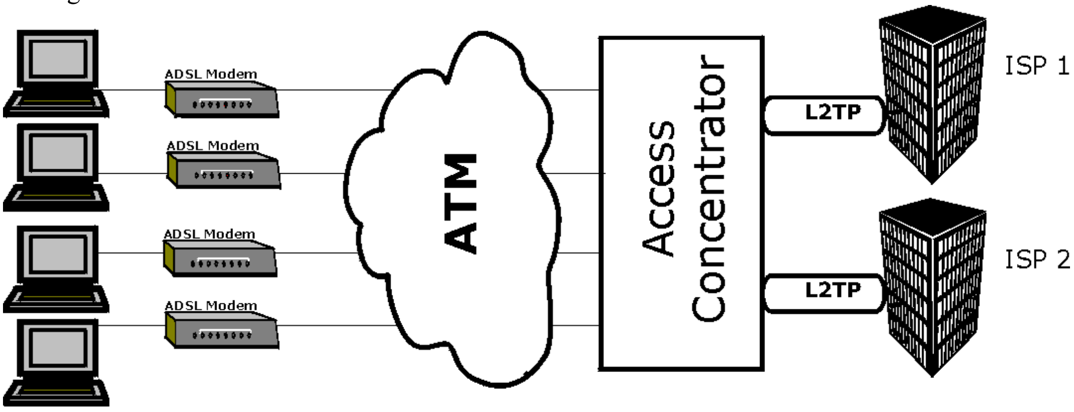


Diagram 1 Single-PC per Modem Hardware Configuration

How PPPoE Works

The PPPoE driver makes the Ethernet appear as a serial link to the PC and the PC runs PPP over it, while the modem bridges the Ethernet frames to the Access Concentrator (AC). Between the AC and an ISP, the

AC is acting as a L2TP (Layer 2 Tunneling Protocol) LAC (L2TP Access Concentrator) and tunnels the PPP frames to the ISP. The L2TP tunnel is capable of carrying multiple PPP sessions.

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

Prestige as a PPPoE Client

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

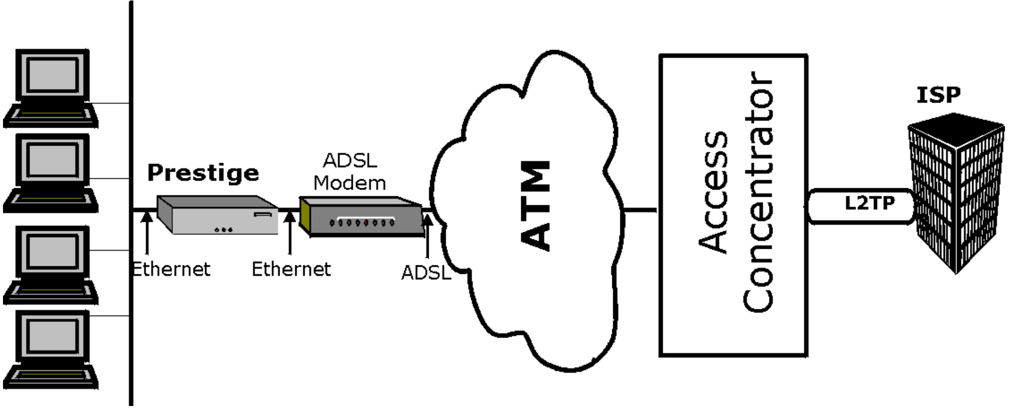


Diagram 2 Prestige as a PPPoE Client

Appendix B
Virtual Paths and Channels

VPI & VCI

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:

● **VC (virtual channel)**	Logical connections between end stations
● **VP (virtual path)**	A bundle of VCs

Think of a VP 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 and a **VCI** (Virtual Channel Identifier) identifies a channel within a virtual path. The **VPI** and **VCI** are identified and correspond to termination points at ATM switches as shown. Your telephone company should supply you with these numbers.

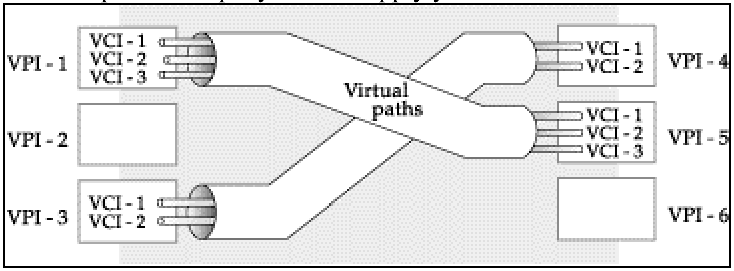


Diagram 3 VPI's & VCI's

Appendix C
Power Adapter Specs

AC Power Adapter Specifications
North America
AC Power Adapter model MW48-1601000A Input power: AC120Volts/60Hz/22W Output power: AC16Volts/1.0A Power consumption: 10 W Plug: North American standards Safety standards: UL, CUL (UL 1310, CSA C22.2 No.233-M91)
European Union
AC Power Adapter model SLA81610-3 Input power: AC230Volts/50Hz, Output power: AC16Volts/1.0A Power consumption: 10 W Plug: European Union standards Safety standards: TUV, CE (EN 60950)
UK
AC Power Adapter model JAA-161000F Input power: AC230Volts/50Hz, Output power: AC16Volts/1.0A Power consumption: 10 W Plug: United Kingdom standards Safety standards: TUV, CE (EN 60950, BS7002)

Index