Prestige 643

ADSL Router

User's Guide

Version 2.50

November 2002

ZyXEL

TOTAL INTERNET ACCESS SOLUTION

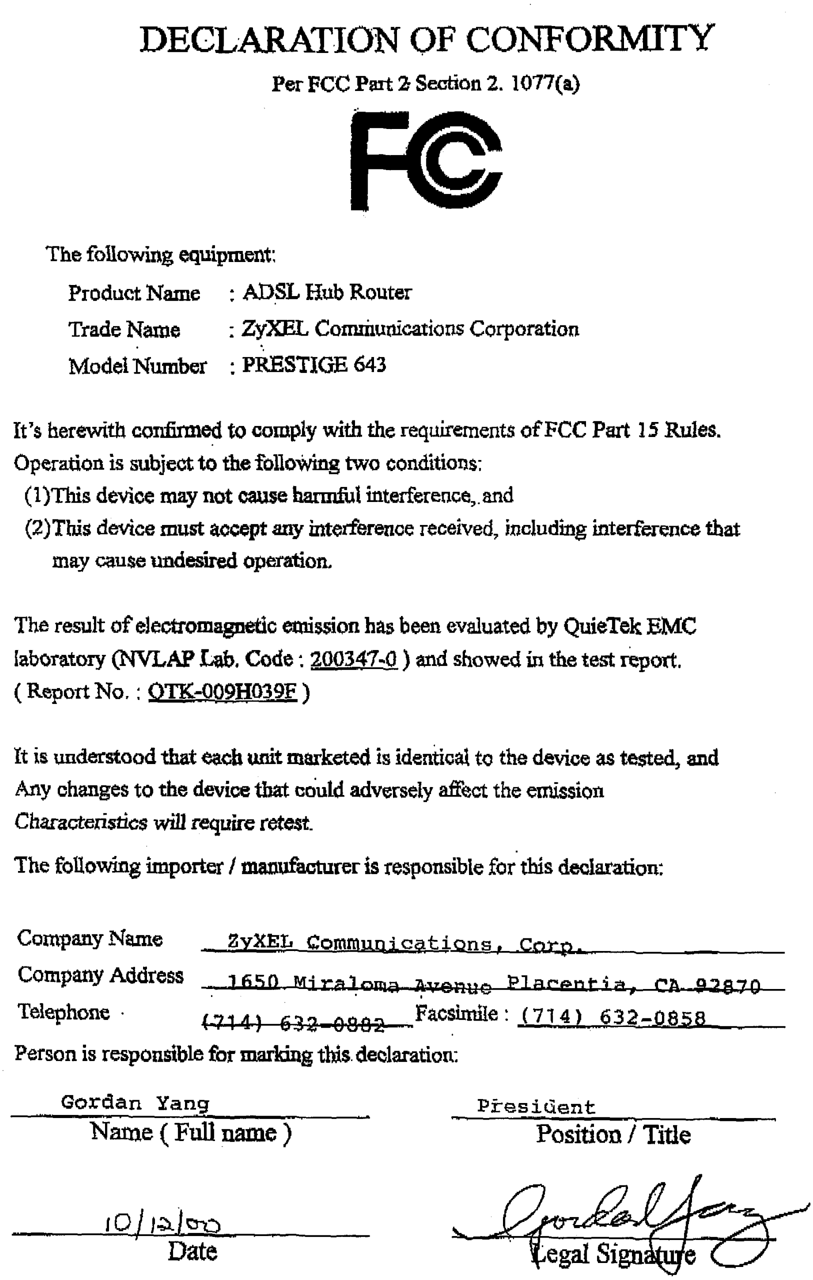
Copyright

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent’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.



DECLARATION OF CONFORMITY

Per FCC Part 2 Section 2. 1077(a)

The following equipment:

Product Name : ADSL Hub Router
Trade Name : ZyXEL Communications Corporation
Model Number : PRESTIGE 643

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-009H039F)

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:

Gordan Yang
Name (Full name)

President
Position / Title

10/12/00
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

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

Certifications

Refer to the product page at www.zyxel.com.

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.

Customer Support

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

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

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

Table of Contents

List of Figures

List of Tables

Preface

Congratulations on your purchase of the Prestige 643 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 643 is an ADSL router used for Internet/LAN access via an ADSL line.

The P643 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 P643'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).

About This User's Guide

This user's guide covers all aspects of the Prestige 643 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 643 for various applications.

Related Documentation

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.

- Supporting Disk

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

- Read Me First

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

- Packing List Card

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

- Glossary

Please refer to www.zyxel.com for an online glossary of networking terms.

- ZyXEL Web Site

The ZyXEL download library at www.zyxel.com contains additional support documentation.

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.
- We will refer to the Prestige 643 ADSL router as the Prestige 643, P643 or simply the Prestige from now on.

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

What is DSL?

DSL (Digital Subscriber Line) technology 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.

Part I:

GETTING STARTED

This part is 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 P643 ADSL Internet Access Router

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

1.1 Prestige 643 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 643

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

- **4-Port Switch**

A combination of switch and router makes your Prestige a cost-effective and viable network solution. A 4-port bandwidth-sensitive 10/100Mbps switch provides greater network efficiency than traditional hubs because the bandwidth is dedicated and not shared. An unlimited number of computers may be connected to your Prestige by adding other hubs - should your LAN consist of more than 4 computers.

- **High Speed Internet Access**

Your Prestige ADSL router can support downstream transmission rates of up to 8Mbps and upstream transmission rates of 1024 Kbps. Your Prestige 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 computers on the LAN, which see only Ethernet and are not aware of PPPoE thus saving you from having to manage PPPoE clients on individual computers.

- **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.

- **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.

[1] Depends on firmware release version.

- **10/100M Auto-negotiation Ethernet/Fast Ethernet Interface**

This auto-negotiation feature allows the Prestige to detect the speed of incoming transmissions and adjust appropriately without manual intervention. It allows data transfer of either 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode depending on your Ethernet network.

- **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.

- **Remote Management Control**

Remote management control allows you to manage Telnet, Web and FTP services. You can customize the service port, access interface, and the secured client IP address to enhance security and flexibility.

- **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 built-in DHCP server capability enabled by default. It can assign IP addresses, an IP default gateway and DNS servers to DHCP clients. The Prestige can now also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the 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 Series supports VC-based and LLC-based multiplexing.

- **Encapsulation**

The Prestige 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.

Network Management

- Menu driven SMT (System Management Terminal) management
- SNMP manageable
- Local SMT session via console port
- Remote SMT session via Telnet

- **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. The Prestige is easy to mount on your wall.

1.3 Applications for the Prestige 643

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.

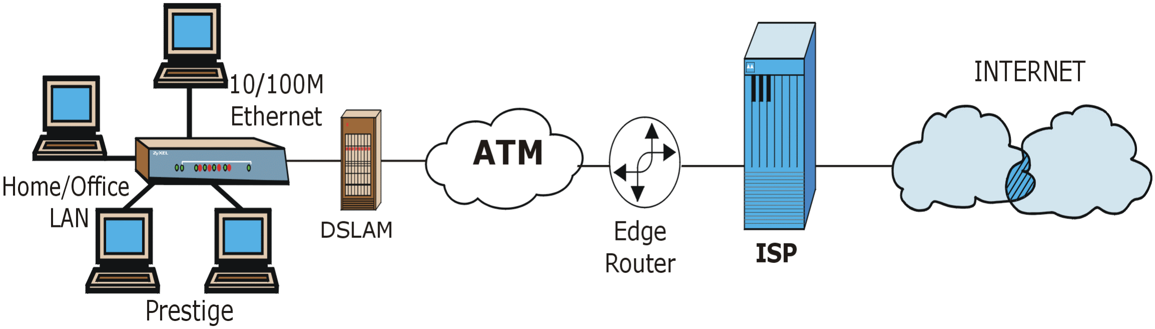


Figure 1-1 Internet Access Application

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 IP address.

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.

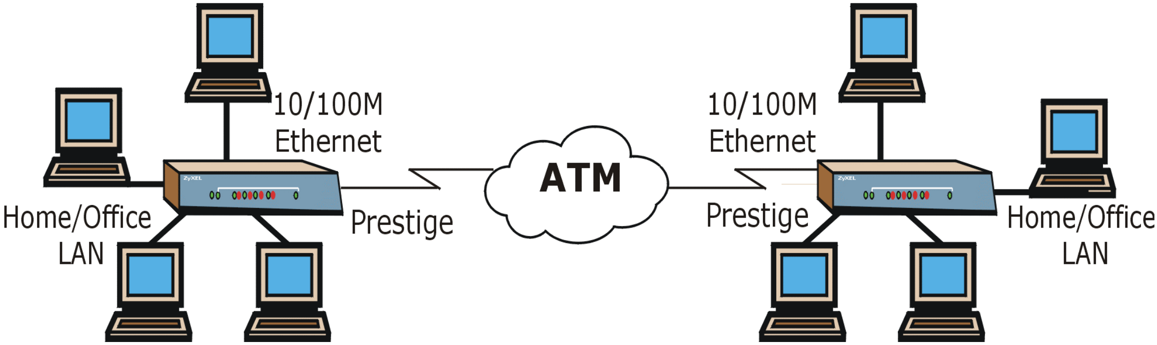


Figure 1-2 LAN-to-LAN Application

Chapter 2
Hardware Installation & Initial Setup

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

2.1 Front Panel LEDs of the P643

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

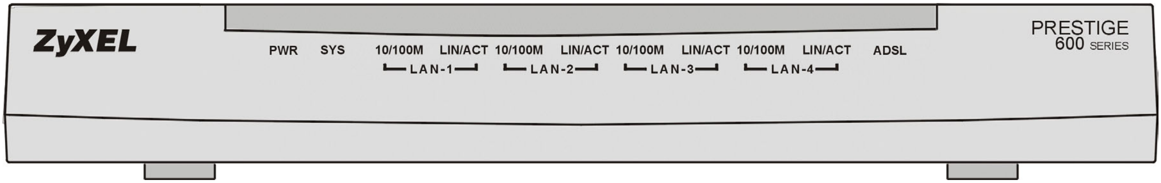


Figure 2-1 Prestige 643 Front Panel.

Table 2-1 Front Panel LED Description

LED NAME	DESCRIPTION
PWR	The PWR (Power) LED is on when power is applied to the Prestige.
SYS	The SYS (System) LED is on when the Prestige is functioning properly. The SYS LED blinks when the Prestige is rebooting. The SYS LED is off when the system is not ready or has malfunctioned.
LAN 10/100M	The LAN (Local Area Network) 10/100M LED is on when the Prestige has a successful 100Mb Ethernet connection. The LAN LED is off when the Prestige has a successful 10Mb Ethernet connection.
LIN/ACT	The LIN/ACT LED is on when the Prestige has a successful Ethernet connection. The LIN/ACT LED blinks when data is sent or received. The LIN/ACT LED is off when the system is not ready or has malfunctioned.
ADSL	The ADSL (Asynchronous Digital Subscriber Line) LED is on when the Prestige is linked successfully to a DSLAM. The ADSL LED blinks when initializing or when data is sent/received. The ADSL LED is off when the link is down.

2.2 Rear Panel and Connections of the Prestige 643

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

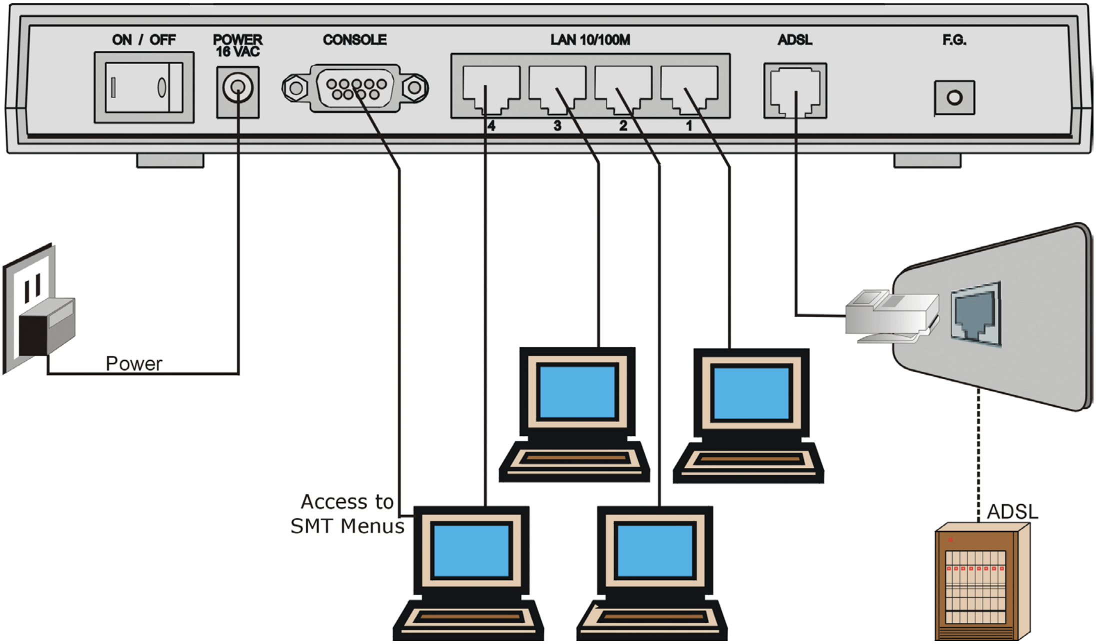


Figure 2-2 Prestige 643 Rear Panel

Step 1: Connecting the ADSL Line

Connect the Prestige directly to the wall jack using the included ADSL cable. Connect a microfilter(s) between the wall jack and your telephone(s). A microfilter acts as low-pass filter (voice transmission takes place in the 0 to 4KHz bandwidth) and is an optional purchase.

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 straight-through cable to connect your Prestige to a computer directly or use a crossover Ethernet cable to connect to an external hub, then connect one end of the straight-through cable 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 P643 models.

Step 4. Connecting the Console Port

For the initial configuration of your Prestige, use terminal emulator software on a computer for configuring your Prestige via 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 Prestige that follows the Full Rate (G.dmt) standard only. One major difference between ADSL and dial-up modems is the optional 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.

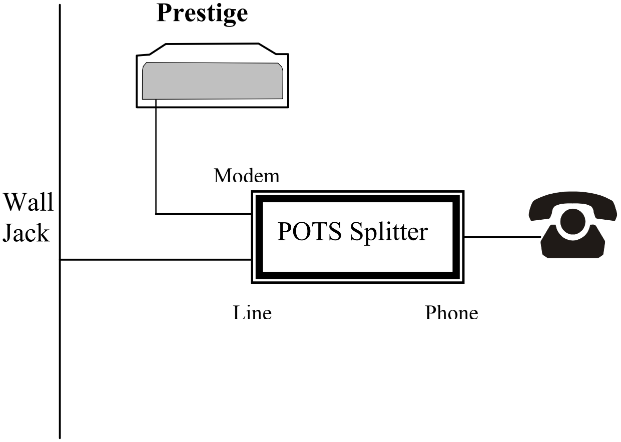


Figure 2-3 Connecting a POTS Splitter

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.

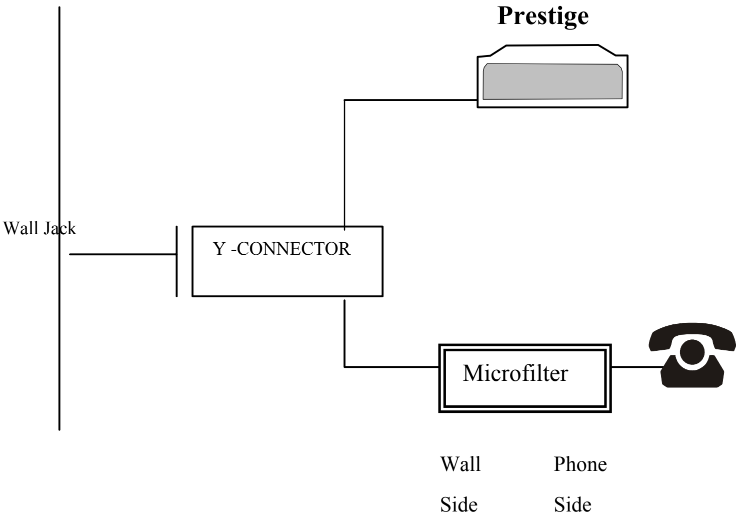


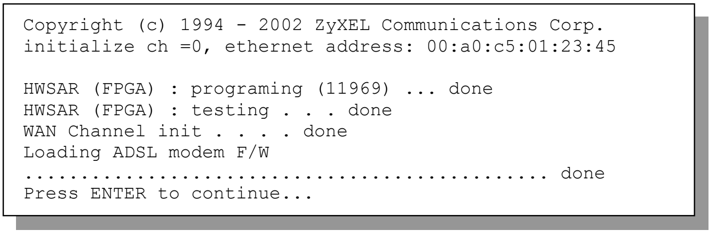
Figure 2-4 Connecting a Microfilter

2.6 Turning on 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 turn on 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 - 2002 ZyXEL Communications Corp.
initialize ch =0, ethernet address: 00:a0:c5:01:23:45

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

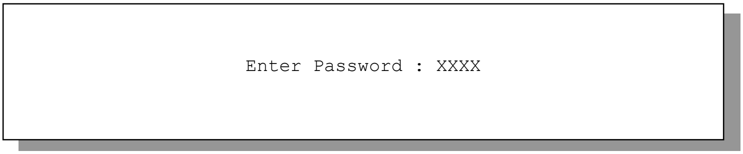
Figure 2-5 Power-On Display

Step 2. Entering Password

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

For your first login, enter the default password “1234”. As you type the password, the screen displays an ‘X’ for each character you type.

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



```
Enter Password : XXXX
```

Figure 2-6 Login Screen

2.6.1 Prestige 643 SMT Menu Overview

The following figure gives you an overview of the various SMT menu screens of your Prestige.

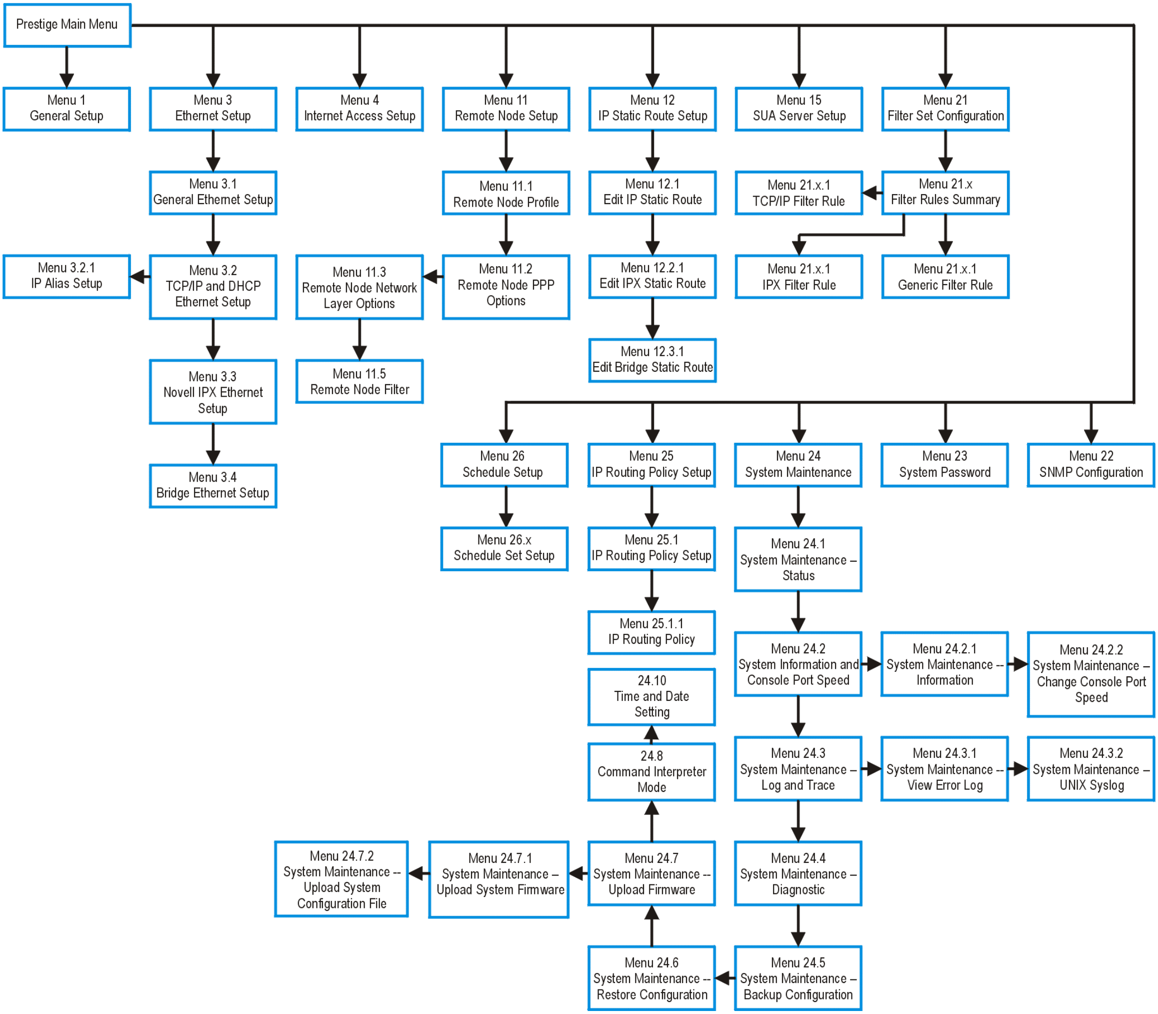

Prestige Main Menu
Menu 1 General Setup
Menu 3 Ethernet Setup
Menu 4 Internet Access Setup
Menu 11 Remote Node Setup
Menu 12 IP Static Route Setup
Menu 15 SUA Server Setup
Menu 21 Filter Set Configuration
Menu 3.1 General Ethernet Setup
Menu 11.1 Remote Node Profile
Menu 12.1 Edit IP Static Route
Menu 21.x.1 TCP/IP Filter Rule
Menu 21.x Filter Rules Summary
Menu 3.2.1 IP Alias Setup
Menu 3.2 TCP/IP and DHCP Ethernet Setup
Menu 11.3 Remote Node Network Layer Options
Menu 11.2 Remote Node PPP Options
Menu 12.2.1 Edit IPX Static Route
Menu 21.x.1 IPX Filter Rule
Menu 21.x.1 Generic Filter Rule
Menu 3.3 Novell IPX Ethernet Setup
Menu 11.5 Remote Node Filter
Menu 12.3.1 Edit Bridge Static Route
Menu 3.4 Bridge Ethernet Setup
Menu 26 Schedule Setup
Menu 25 IP Routing Policy Setup
Menu 24 System Maintenance
Menu 23 System Password
Menu 22 SNMP Configuration
Menu 26.x Schedule Set Setup
Menu 25.1 IP Routing Policy Setup
Menu 24.1 System Maintenance – Status
Menu 25.1.1 IP Routing Policy
24.10 Time and Date Setting
Menu 24.2 System Information and Console Port Speed
Menu 24.2.1 System Maintenance -- Information
Menu 24.2.2 System Maintenance – Change Console Port Speed
24.8 Command Interpreter Mode
Menu 24.3 System Maintenance – Log and Trace
Menu 24.3.1 System Maintenance -- View Error Log
Menu 24.3.2 System Maintenance – UNIX Syslog
Menu 24.7.2 System Maintenance -- Upload System Configuration File
Menu 24.7.1 System Maintenance – Upload System Firmware
Menu 24.7 System Maintenance -- Upload Firmware
Menu 24.4 System Maintenance – Diagnostic
Menu 24.6 System Maintenance -- Restore Configuration
Menu 24.5 System Maintenance – Backup Configuration

Figure 2-7 Prestige 643 SMT Menu Overview

2.7 Navigating the SMT Interface

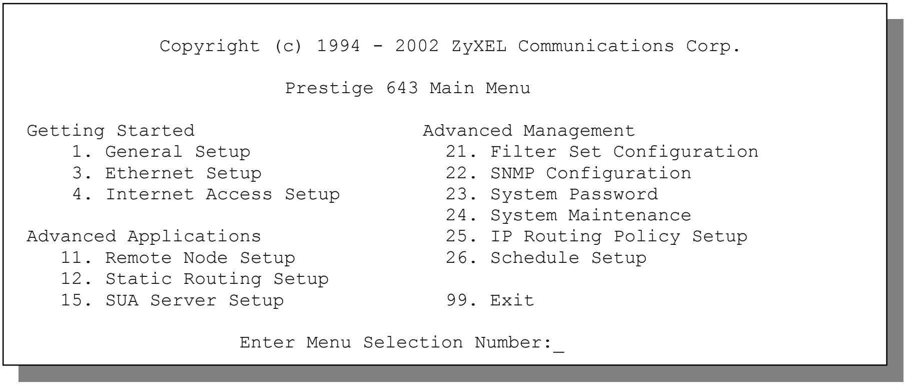
The SMT (System Management Terminal) is the interface that you use to configure your Prestige.

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

Table 2-2 Main Menu Commands

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

After you enter the password, the SMT displays the main menu, as shown below.



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

                           Prestige 643 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                 26. Schedule 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.

2.7.1 System Management Terminal Interface Summary

Table 2-3 Main Menu Summary

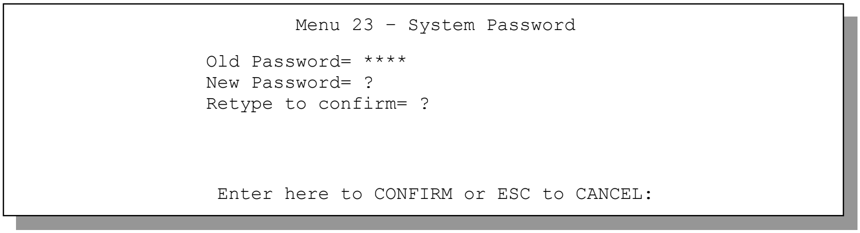
#	MENU TITLE	DESCRIPTION
1	General Setup	Use this menu to set up your general information.
3	Ethernet Setup	Use this menu to set up your LAN connection.
4	Internet Access Setup	A quick and easy way to set up an Internet connection.
11	Remote Node Setup	Use this menu to set up the Remote Node for LAN-to-LAN 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.
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.

2.8 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 display **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 - System Password

Step 2. Type in 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.

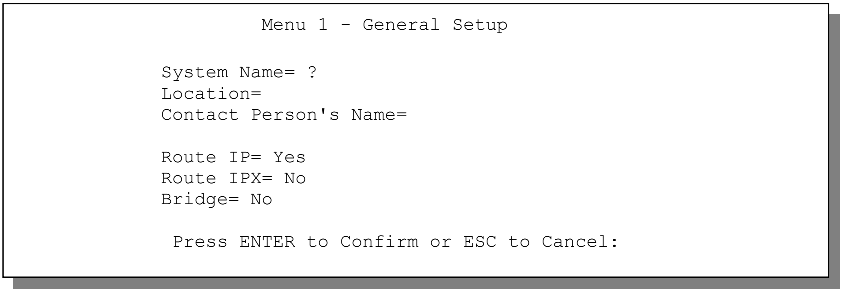
2.9 General Setup

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

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

Step 1. Enter **1** in Main Menu to display **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:
```

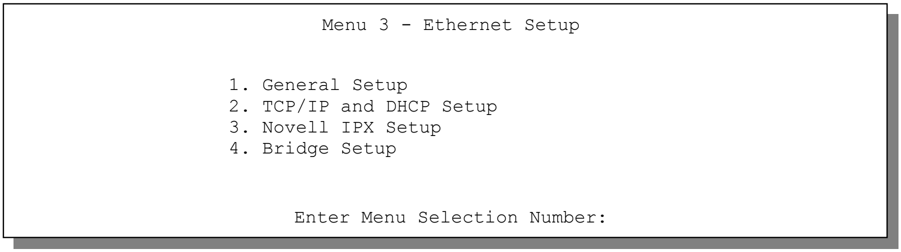
Figure 2-10 Menu 1 - General Setup

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.	P643
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
Route IP	Set this field to **Yes** to enable or **No** to disable IP routing. You must enable IP routing for Internet access.	**Yes**
Route IPX	Set this field **Yes** to enable or **No** to disable IPX routing.	**No**
Bridge	Turn on/off bridging for protocols not supported (e.g., SNA) or not turned on in the previous Route fields. Select **Yes** to turn bridging on; select **No** to turn bridging off.	**No**

2.10 Ethernet Setup

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

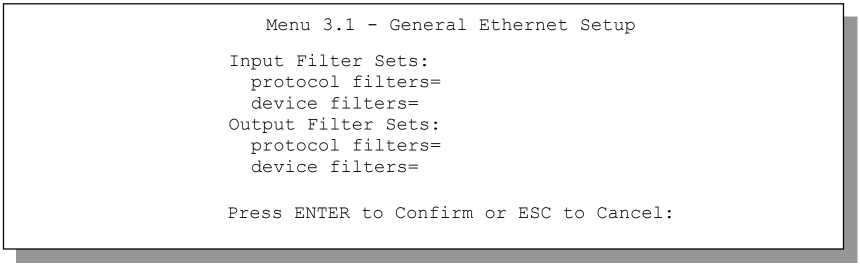


```
                    Menu 3 - Ethernet Setup


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



                  Enter Menu Selection Number:
```

Figure 2-11 Menu 3 - Ethernet Setup

2.10.1 General Ethernet Setup

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



```
                Menu 3.1 - General Ethernet Setup

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

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

Figure 2-12 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.

2.11 Protocol Dependent Ethernet Setup

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

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

Chapter 3
Internet Access

This chapter shows you how to configure the LAN and 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 *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 and 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:

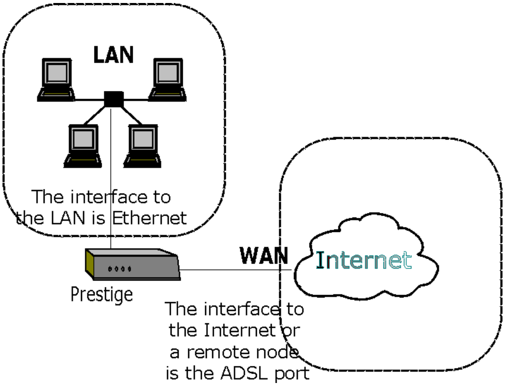

LAN
The interface to the LAN is Ethernet
WAN
Internet
Prestige
The interface to the Internet or a remote node is the ADSL port

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:

1. **Both -** the Prestige will broadcast its routing table periodically and incorporate the RIP information that it receives.
2. **In Only -** the Prestige will not send any RIP packets but will accept all RIP packets received.
3. **Out Only -** the Prestige will send out RIP packets but will not accept any RIP packets received.
4. **None -** the Prestige 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.

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.

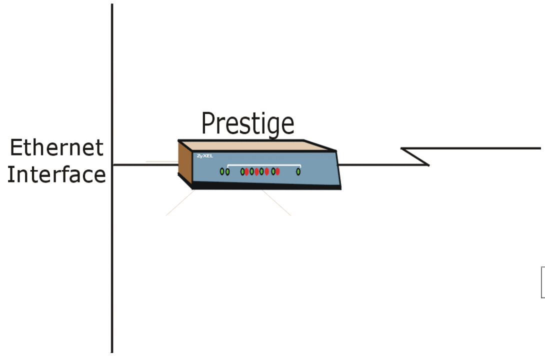
The Prestige supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). At start up, the Prestige queries all directly connected networks to gather group membership. After that, the Prestige periodically updates this information. IP Multicasting can be enabled/disabled on the Prestige LAN 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 *IP Policy Routing*) 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.



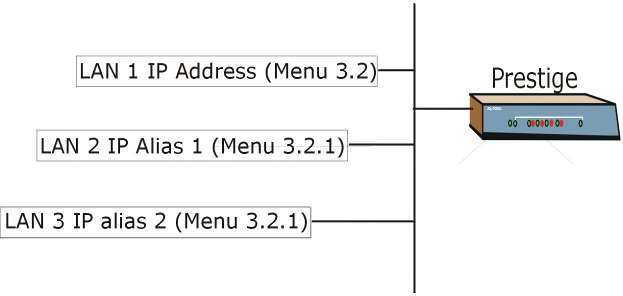

LAN 1 IP Address (Menu 3.2)
LAN 2 IP Alias 1 (Menu 3.2.1)
LAN 3 IP alias 2 (Menu 3.2.1)
Prestige

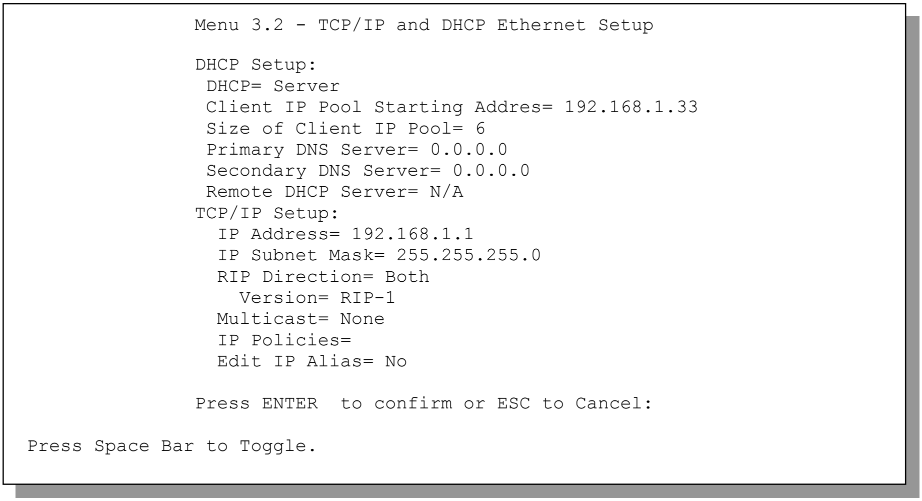
Figure 3-2 Physical Network

Figure 3-3 Partitioned Logical Networks

Use menu 3.2.1 to configure IP Alias on your Prestige.

3.6.1 IP Alias Setup

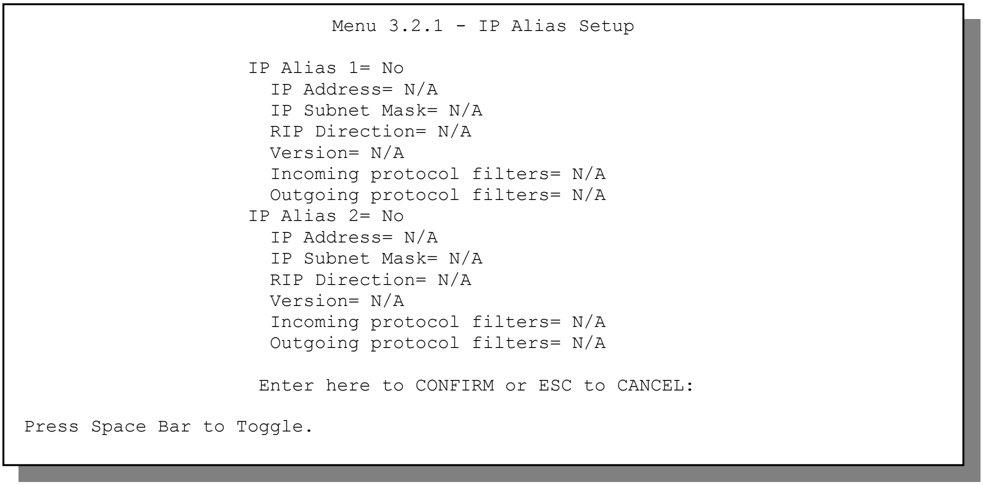
Use Menu 3.2 to configure the first network. Move the cursor to **Edit IP Alias** field and press [SPACEBAR] to choose **Yes** and press [ENTER] to configure the second and third network.



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

                 DHCP Setup:
                  DHCP= Server
                  Client IP Pool Starting Addres= 192.168.1.33
                  Size of Client IP Pool= 6
                  Primary DNS Server= 0.0.0.0
                  Secondary DNS Server= 0.0.0.0
                  Remote DHCP Server= N/A
                 TCP/IP Setup:
                   IP Address= 192.168.1.1
                   IP Subnet Mask= 255.255.255.0
                   RIP Direction= Both
                     Version= RIP-1
                   Multicast= None
                   IP Policies=
                   Edit IP Alias= No

                 Press ENTER  to confirm or ESC to Cancel:

  Press Space Bar to Toggle.
```

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

Pressing [ENTER] displays **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.

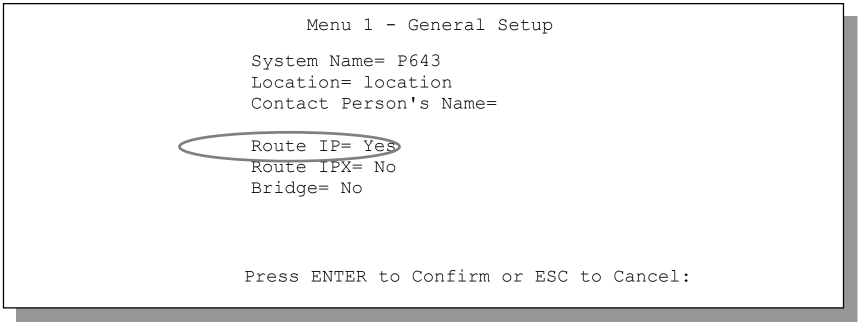
Table 3-1 IP Alias Setup Menu Fields

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

3.7 Route IP Setup

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

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



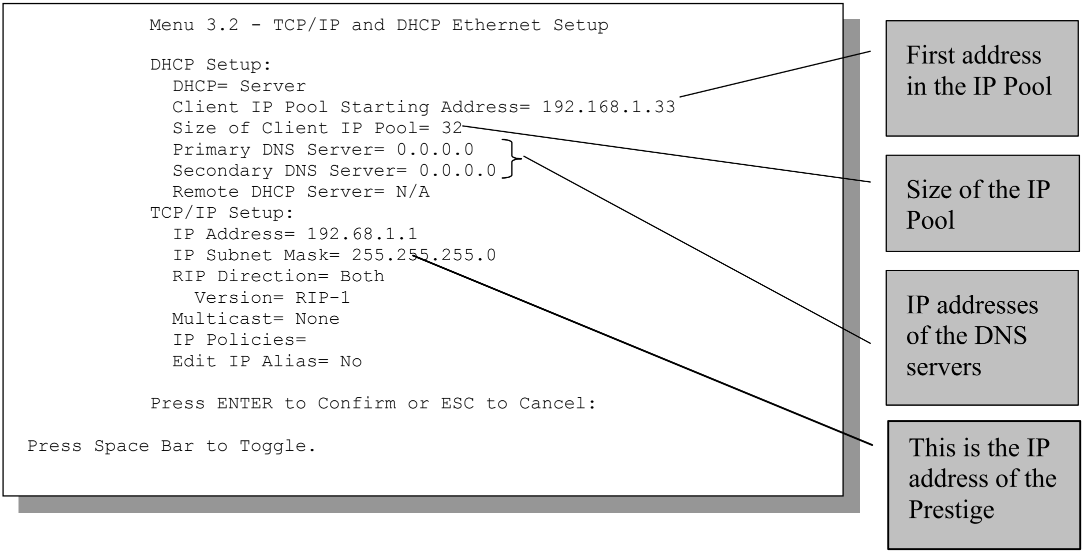
```
                    Menu 1 - General Setup

               System Name= P643
               Location= location
               Contact Person's 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

Use Menu 3.2 to configure your Prestige for TCP/IP.

To edit Menu 3.2, enter **3** from the main menu to display **Menu 3 - Ethernet Setup**. When Menu 3 appears, press **2** and press [ENTER] to display **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 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:	**Server** (default)
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.	192.168.1.33
Size of Client IP Pool	This field specifies the size or count of the IP address pool.	32
Primary DNS Server Secondary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.	

FIELD	DESCRIPTION	EXAMPLE
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
IP Subnet Mask	Your Prestige will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the Prestige.	255.255.255.0
RIP Direction	Press [SPACE BAR] to select the RIP direction. Choices are **Both**, **In Only**, **Out Only** or **None**.	**Both** (default)
Version	Press [SPACE BAR] to select the RIP version. Choices are **RIP-1**, **RIP-2B** or **RIP-2M**.	**RIP-1** (default)
Multicast	IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group. The Prestige supports both IGMP version 1 (**IGMP-v1**) and version 2 (**IGMP-v2**). Press the [SPACE BAR] to enable IP Multicasting or select **None** to disable it.	**None** (default)
IP Policies	Create policies using SMT Menu 25 (see the *IP Policy Routing chapter*) 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.	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 [SPACE BAR] to change **No** to **Yes** and press [ENTER] to for menu 3.2.1	**No** (default)
When you have completed this menu, press [ENTER] at the prompt “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.		

3.9 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 0 to 255 and for the VCI is 32 to 65535 (0 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 computer 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

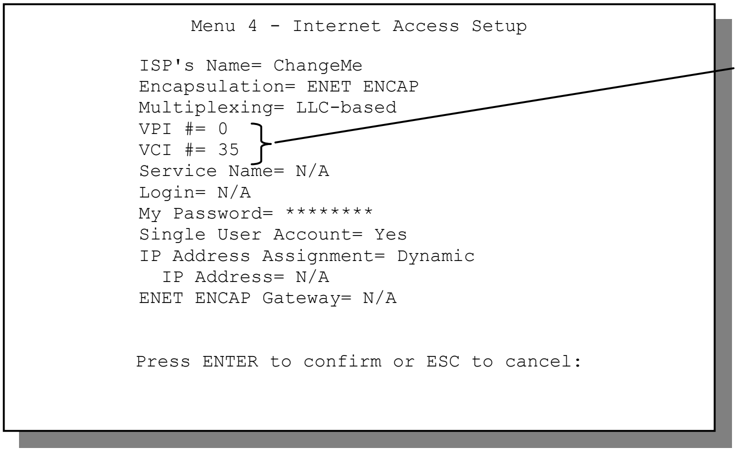
Menu 4 allows you to enter the Internet Access information in one screen. Menu 4 is actually a simplified setup for one of the remote nodes that you can access in Menu 11. Before you configure your Prestige for Internet access, you need to collect your Internet account information from your ISP and telephone 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 INFORMATION BELOW
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, type **4** to display **Menu 4 - Internet Access Setup**, as shown next.



```
                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= ********
          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

The following table contains instructions on how to configure your Prestige for Internet access.

Table 3-5 Internet Access Setup Menu Fields

F ELD	DESCRIPTION	XAMPLE
ISP's Name	Enter the name of your Internet Service Provider. This information is for identification purposes only.	MyISP
Encapsulation	Press [SPACE BAR] to select the method of encapsulation used by your ISP. Choices are **PPPoE**, **PPP**, **RFC 1483** or **ENET ENCAP**.	**ENET ENCAP**
Multiplexing	Press [SPACE BAR] to select the method of multiplexing used by your ISP. Choices are **VC-based** or **LLC-based**.	**VC-based**
VPI #	Enter the Virtual Path Identifier (VPI) that the telephone company gives you.	0
VCI #	Enter the Virtual Channel Identifier (VCI) that the telephone company gives you.	35
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.	
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.	Derek

F ELD	DESCRIPTION	XAMPLE
My Password	Enter the password associated with the login name above.	*******
Single User Account	Choose **Yes** to enable or **No** to disable SUA. Please see the following section for a more detailed discussion on the Single User Account feature.	**Yes**
IP Address Assignment	Press [SPACE BAR] to select **Static** or **Dynamic** address assignment.	**Dynamic**
IP Address	Enter the IP address supplied by your ISP if applicable.	192.168.1.1
ENET ENCAP Gateway	Enter the gateway IP address supplied by your ISP if applicable.	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.		

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 that want concurrent access to 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 a 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 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

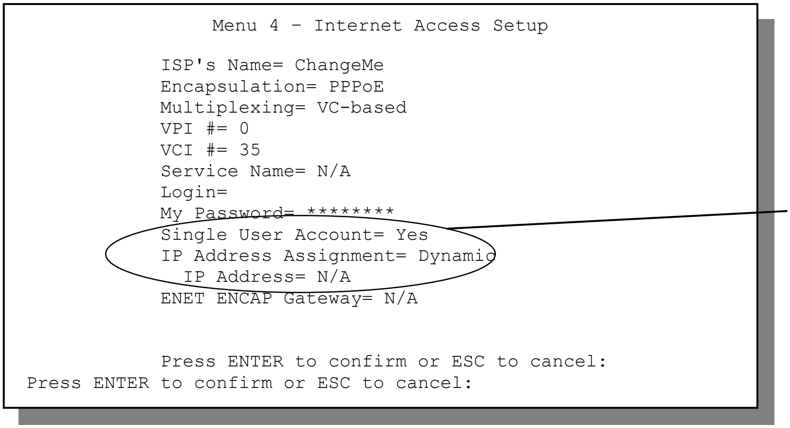
In summary:

- SUA is a cost-effective solution for small offices to access the Internet or other remote TCP/IP networks.
- SUA supports servers 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 next.



```
                  Menu 4 - Internet Access Setup

             ISP's Name= ChangeMe
             Encapsulation= PPPoE
             Multiplexing= VC-based
             VPI #= 0
             VCI #= 35
             Service Name= N/A
             Login=
             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:
 Press ENTER to confirm or ESC to cancel:
```

Configure SUA here.

.

Figure 3-9 Menu 4 - Internet Access Setup

To enable the SUA feature in Menu 4, move the cursor to the **Single User Account** field and select **Yes**. Then follow the instructions on how to configure the SUA fields.

Table 3-6 Single User Account Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Single User Account	Choose **Yes** to enable and **No** to disable SUA.	**Yes**
IP Address Assignment	Choose either **Dynamic** or **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**.	**Dynamic**
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**.	**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 a FTP server 192.168.1.3, then you need to specify port 80 (web) to the server at IP address 192.168.1.2 and port 21 (FTP) for the FTP server 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. Furthermore, 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.**

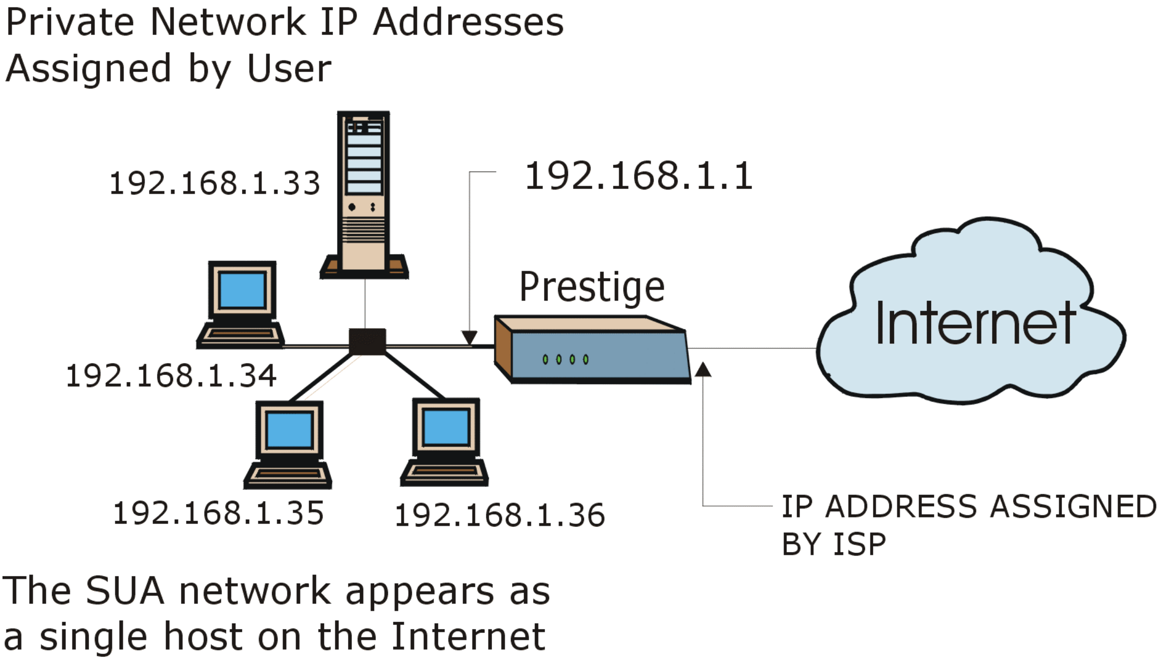


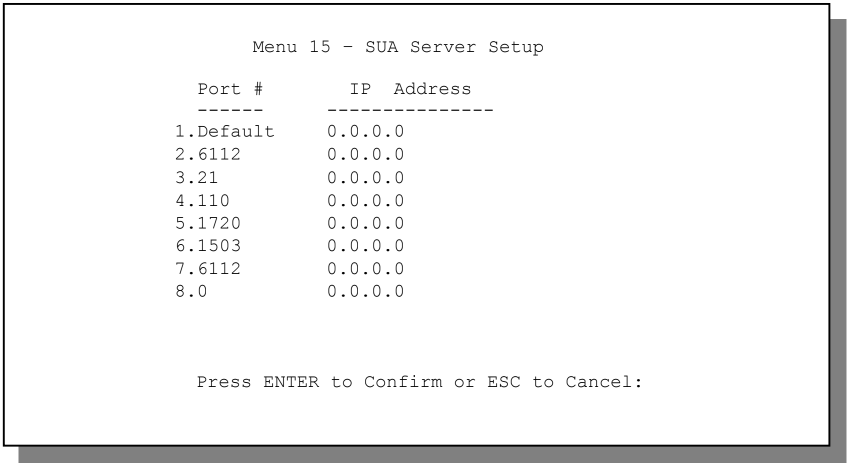
Figure 3-10 Single User Account Topology

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

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



```
                  Menu 15 - SUA Server Setup

             Port #        IP  Address
             ------      ---------------
           1.Default     0.0.0.0
           2.6112        0.0.0.0
           3.21          0.0.0.0
           4.110         0.0.0.0
           5.1720        0.0.0.0
           6.1503        0.0.0.0
           7.6112        0.0.0.0
           8.0           0.0.0.0



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

Figure 3-11 Menu 15 - SUA Server Setup: Multiple Server Configuration

The most often used port numbers are:

Table 3-7 Services vs. Port Number

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

Part II:

ADVANCED APPLICATIONS

This part describes 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

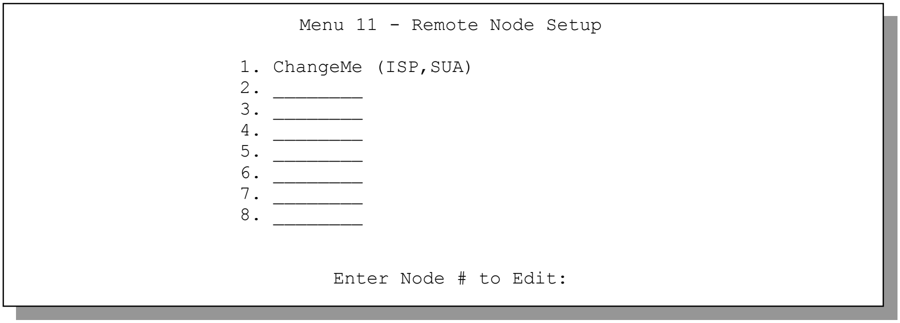
This section describes the protocol-independent parameters for a remote node.

4.1.1 Remote Node Profile

To configure a remote node, follow these steps:

Step 1. From the main menu, enter **11** to display Menu 11.

Step 2. When Menu 11 appears, as shown next, 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.

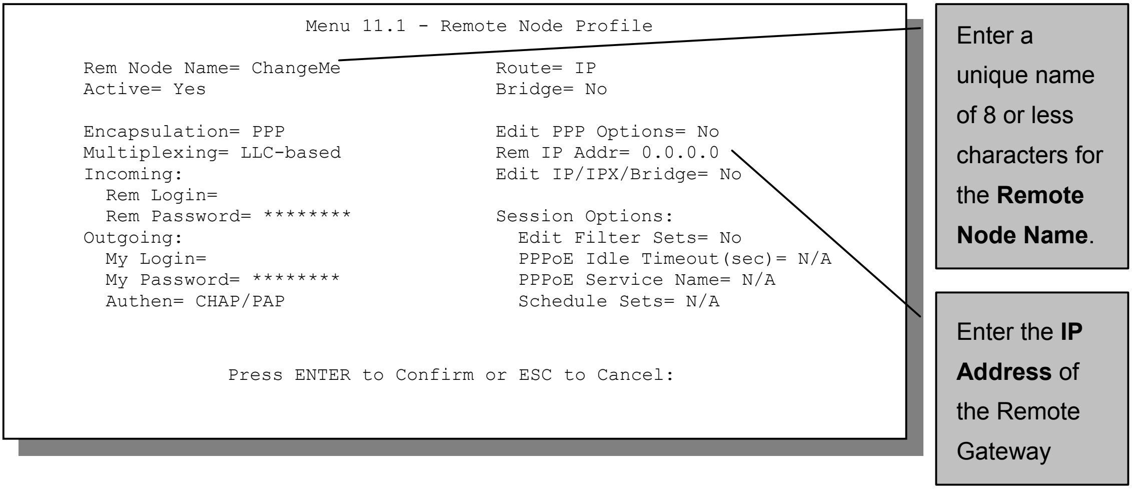
Scenario 2. One VC, One Protocol (IP)

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.



```
                          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= N/A
         Authen= CHAP/PAP                      Schedule Sets= N/A


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

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

Enter the **IP Address** of the Remote Gateway

Figure 4-2 Menu 11.1 - Remote Node Profile

The Remote Node Profile Menu Fields table, shown next, explains how to configure the Remote Node Menu.

Table 4-1 Remote Node Profile Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Rem Node Name	This is a required field. Enter a descriptive name for the remote node. 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.	Corp

FIELD	DESCRIPTION	EXAMPLE
Active	Choose **Yes** or **No**. Inactive nodes are displayed with a minus sign (–) at the beginning of the name in Menu 11.	**Yes**
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** is selected, then the **Rem Login**, **Rem Password**, **My Login**, **My Password**, **Edit PPP Options** and **Authen** fields are **N/A**. Moreover, **ENET ENCAP** encapsulaton does not apply for IPX routing. **PPPoE** (Point to Point Protocol over Ethernet) activates the fields shown in the above figure.	**ENET ENCAP**
Multiplexing	Choose the multiplexing method. Choices **are VC-base**d or **LLC-based**.	**LLC-based**
Incoming: Rem Login	Enter the login name that this remote node will use when it calls your Prestige. The login name combined with the Rem Password will 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 CHAP or PAP. **CHAP** – Your Prestige will accept CHAP (Challenge Handshake Authentication Protocol). **PAP** – Your Prestige will accept PAP (Password Authentication Protocol).	**CHAP**
Route	This field determines the protocol that your Prestige will route. Choices are **IP**, **IPX**, **IP+IPX** or **None**.	**IP**

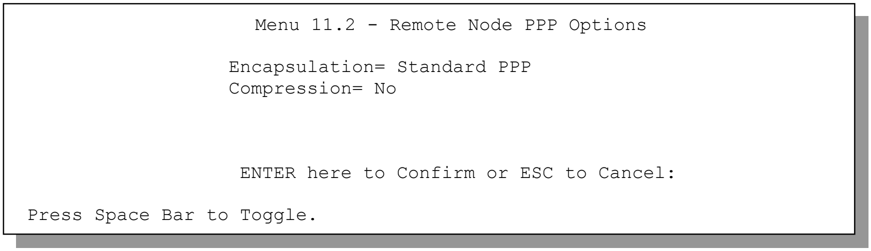
FIELD	DESCRIPTION	EXAMPLE
Bridge	Bridging is used for protocols that the Prestige does not route, e.g. SNA, or not turned on in the previous Route field. When bridging is enabled, your Prestige will forward any packet that it does not route to this remote node; otherwise, the packets are discarded. Choose **Yes** to enable or **No** to disable the Bridge field.	**No**
Edit PPP Options	Choose **Yes** and press [ENTER] to edit PPP options. This will display **Menu 11.2 – Remote Node PPP Options**. For more information on configuring PPP options, see the section titled Editing PPP Options.	**No**
Rem IP Addr	Enter the IP address of the remote gateway.	
Edit IP/IPX/Bridge	Choose **Yes** and press [ENTER] to display **Menu 11.3 – Remote Node Network Layer Options**.	**No**
Session Options: Edit Filter Sets	Choose **Yes** and press [ENTER] to open Menu 11.5 to edit the filter sets. See the Remote Node Filter section for more details.	**No**
PPPoE Idle Timeout (sec)	This value specifies the number of idle seconds that elapse before the Prestige automatically disconnects the PPPoE session.	0
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.	
Schedule Sets	Type in the schedule set number(s), separated by commas if more than 1 set, according to Menu 26 Schedule Setup. The maximum number of schedule sets is 4.	1,3,4,6
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 press [SPACE BAR] to select **Yes**. Press [ENTER] to display 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 how to configure the PPP options fields.

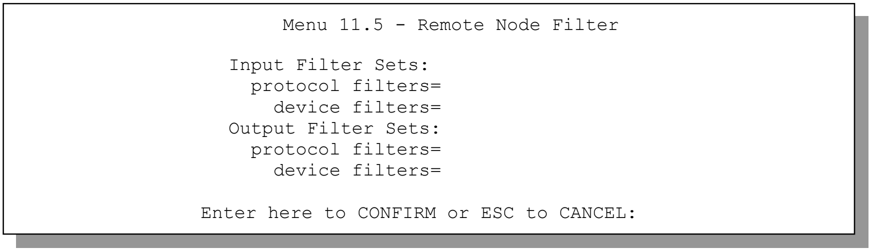
Table 4-2 Remote Node PPP Options Menu Fields

FIELD	DESCRIPTION	EXAMPLE
Encapsulation	Choose **CISCO PPP** only when this remote node is a Cisco machine; otherwise, select **Standard PPP**.	Standard PPP
Compression	Choose **Yes** to turn Stac Compression on or **No** to turn Stac Compression off.	No (default)
Once you have completed filling in **Menu 11.2 – Remote Node PPP Options**, press [ENTER] at the message “Press ENTER to Confirm…” to save your configuration, or press [ESC] at any time to cancel.		

4.1.5 Remote Node Filter

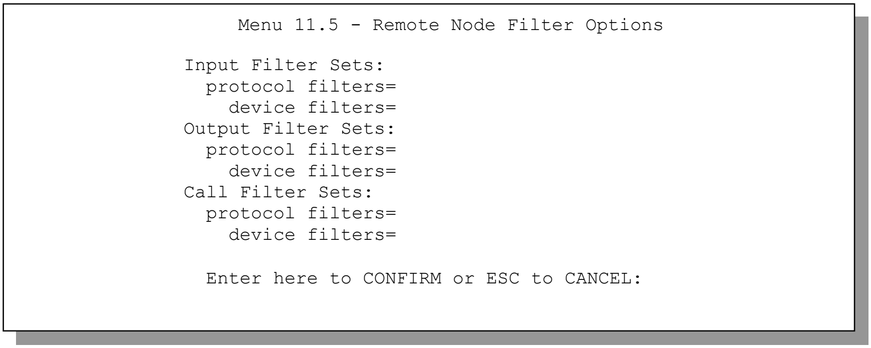
In **Menu 11.1 – Remote Node Profile** make sure the **Edit Filter Sets** field displays **Yes** by pressing the [SPACE BAR]. Press [ENTER] to access **Menu 11.5 – Remote Node Filter**.

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:
```

Figure 4-5 Menu 11.5 - 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 uses your Prestige to connect a branch office to the headquarters, as depicted in the following diagram.

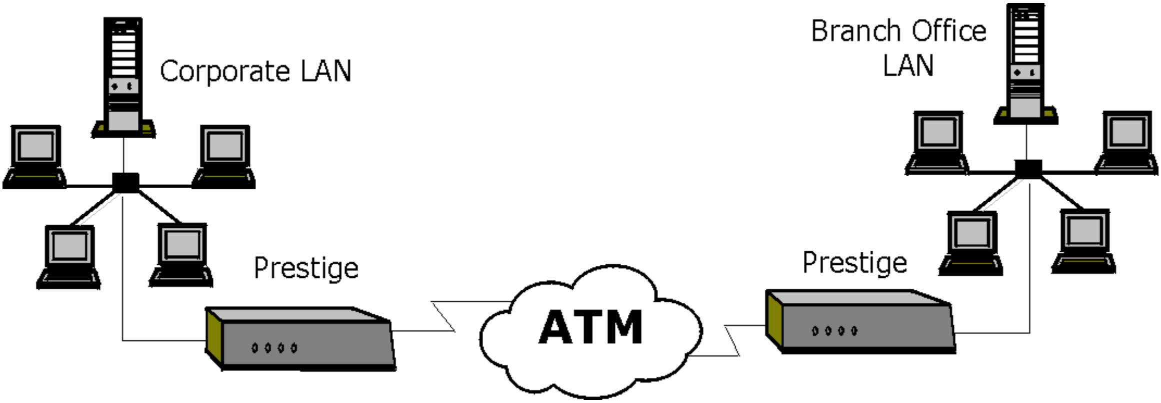


Figure 5-1 TCP/IP LAN-to-LAN Application

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

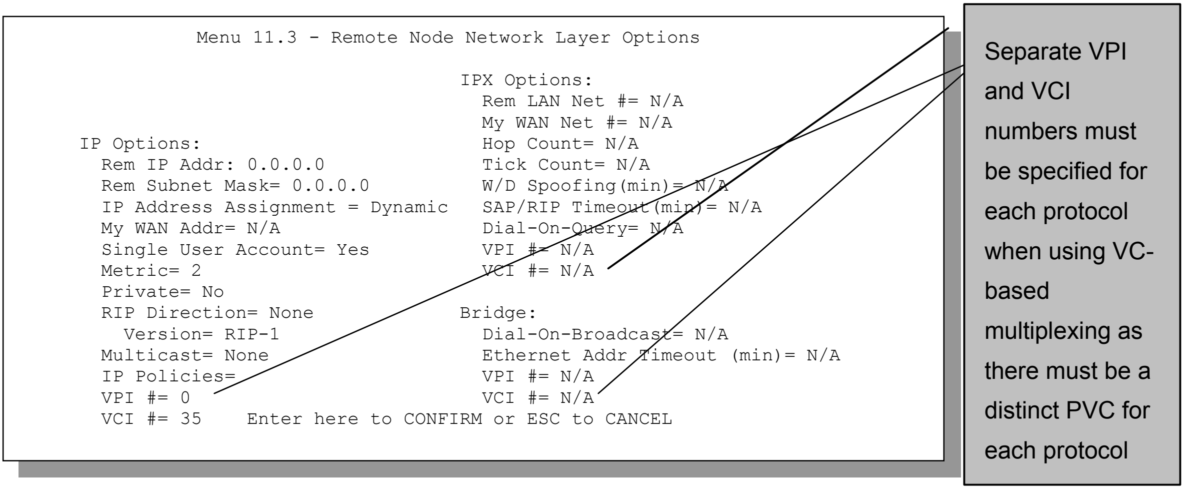
Follow the steps below to edit **Menu 11.3 – Remote Node Network Layer Options**.

In Menu 11.1, move the cursor to the **Edit IP/IPX/Bridge** field, then press [SPACE BAR] to set the value to **Yes**. Press [ENTER] to display **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
        IP Address Assignment = Dynamic SAP/RIP Timeout(min)= N/A
        My WAN Addr= N/A                Dial-On-Query= N/A
        Single User Account= Yes        VPI #= N/A
        Metric= 2                       VCI #= N/A
        Private= No
        RIP Direction= None           Bridge:
          Version= RIP-1                Dial-On-Broadcast= N/A
        Multicast= None                 Ethernet Addr Timeout (min)= N/A
        IP Policies=                    VPI #= N/A
        VPI #= 0                        VCI #= N/A
        VCI #= 35    Enter here to CONFIRM or ESC to CANCEL
```

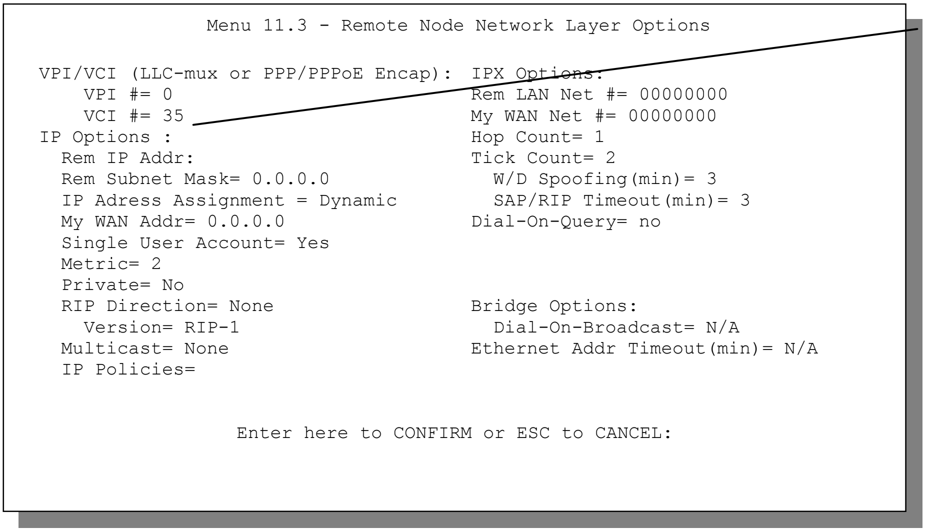
Separate VPI and VCI numbers must be specified for each protocol when using VC-based multiplexing as there must be a distinct PVC for each protocol

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 contained in each packet header.



```
                  Menu 11.3 - Remote Node Network Layer Options

   VPI/VCI (LLC-mux or PPP/PPPoE Encap):  IPX Options:
       VPI #= 0                           Rem LAN Net #= 00000000
       VCI #= 35                          My WAN Net #= 00000000
   IP Options :                           Hop Count= 1
     Rem IP Addr:                         Tick Count= 2
     Rem Subnet Mask= 0.0.0.0               W/D Spoofing(min)= 3
     IP Adress Assignment = Dynamic         SAP/RIP Timeout(min)= 3
     My WAN Addr= 0.0.0.0                 Dial-On-Query= no
     Single User Account= Yes
     Metric= 2
     Private= No
     RIP Direction= None                  Bridge Options:
       Version= RIP-1                       Dial-On-Broadcast= N/A
     Multicast= None                      Ethernet Addr Timeout(min)= N/A
     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** field indicates the local Prestige WAN IP while **Rem IP Addr** field indicates the peer WAN IP.

.

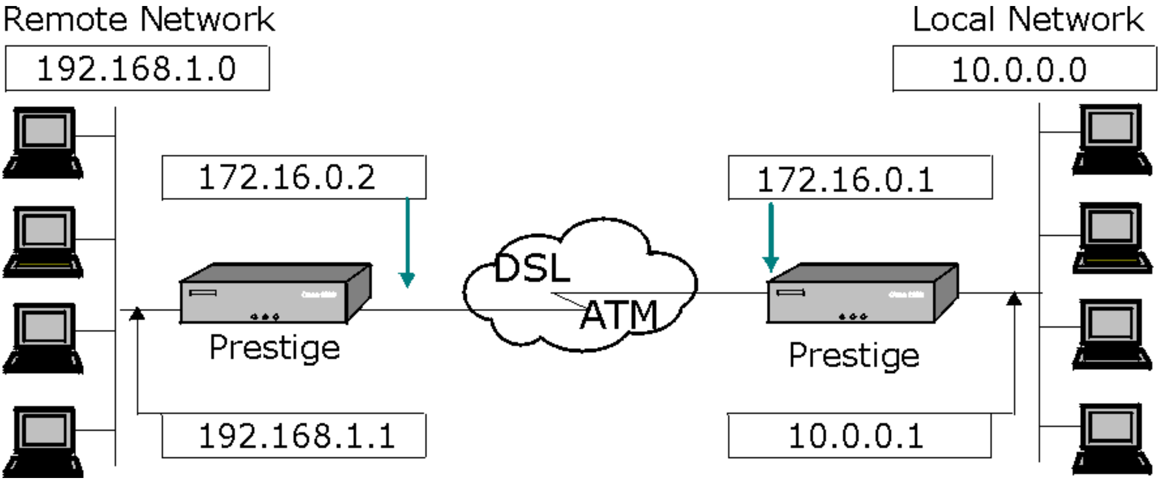


Figure 5-4 Sample IP Addresses for a TCPI/IP LAN-to-LAN Connection

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	EXAMPLE
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, eg. 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	Choose **Yes** and press [ENTER] to view **Menu 11.3 – Remote Node Network Layer Options**.	**No**

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

Table 5-2 TCP/IP Remote Node Configuration

FIELD	DESCRIPTION	EXAMPLE
VPI VCI	Enter the Virtual Path Identifier (VPI) supplied by your telephone company. Enter the Virtual Channel Identifier (VCI) supplied by your telephone company.	
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.	
IP Address Assignment	Choose **Dynamic** if you have a dynamically assigned IP address or **Static** if you have a static IP address.	**Dynamic**
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	Choose **Yes** to enable or **No** to disable the Single User Account feature. See the section on *Internet Access Applications* for more information on the Single User Account feature.	**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.	2

FIELD	DESCRIPTION	EXAMPLE
Private	This parameter determines if the Prestige will include the route to this remote node in its RIP broadcasts. Choose **Yes** to keep this route private and not include in RIP broadcast. Choose **No** to propagate this remote node to other hosts through RIP broadcasts.	**No**
RIP Direction	Press [SPACE BAR] to select the RIP Direction. Choices are **Both**, **In Only**, **Out Only** or **None**.	**None**
Version	Press [SPACE BAR] to select the RIP version. Choices are **RIP-1**, **RIP-2B** or **RIP-2M**.	**RIP-1**
Multicast	Choose **IGMP-v1** (IGMP version 1), **IGMP-v2** (IGMP version 2) or **None** (disable IGMP). IGMP (Internet Group Multicast Protocol) is a session-layer protocol used to establish membership in a Multicast group.	**None** (default)
IP Policies	Create policies using SMT Menu 25 (see *IP Routing Policy*) and apply them on the Prestige LAN interface here. You can apply up to four IP Policy sets (from 12) by entering their numbers separated by commas.	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.

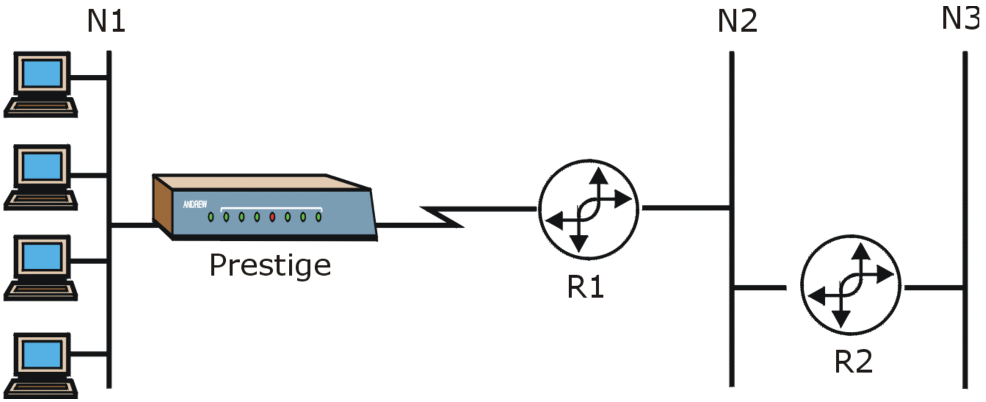
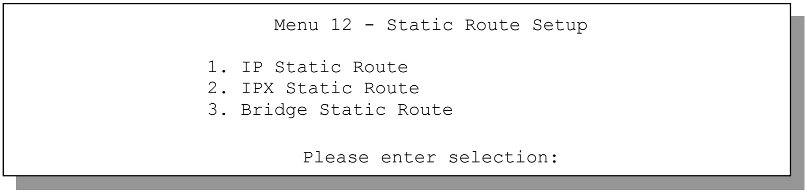


Figure 5-5 Sample Static Routing Topology

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

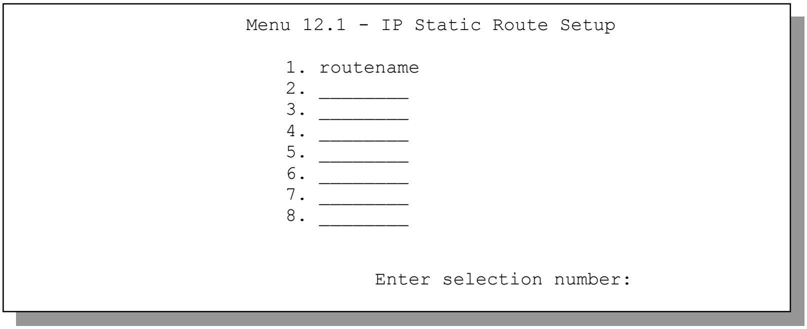
Step 1. Enter 12 from the Main Menu to bring up the following screen.



```
                         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

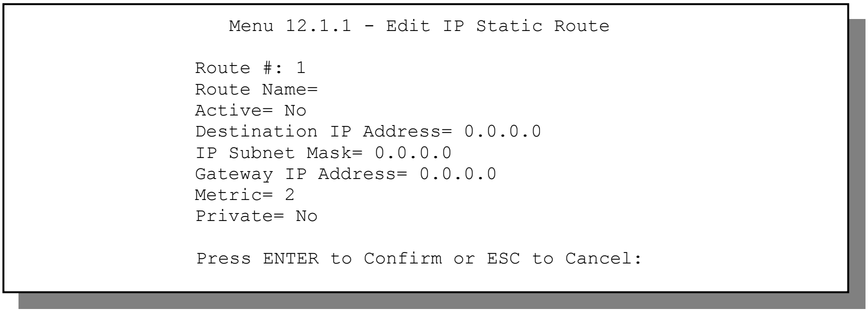
Step 2. Enter 1 From Menu 12 to bring up the next screen.



```
                    Menu 12.1 - 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. In Menu 12.1, enter the index number of one of the static routes that you want to configure. Index number **1** was selected for the following figure.



```
                  Menu 12.1.1 - Edit IP Static Route

             Route #: 1
             Route Name=
             Active= No
             Destination IP Address= 0.0.0.0
             IP Subnet Mask= 0.0.0.0
             Gateway IP Address= 0.0.0.0
             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.

FIELD	DESCRIPTION
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. See *IP Subnet Mask*.
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.
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 needs to have the network numbers configured and all other stations (clients and servers) can obtain the network numbers from it. The server with configured network numbers is called a seed router.

If you have a NetWare server on the same LAN as the Prestige, 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.

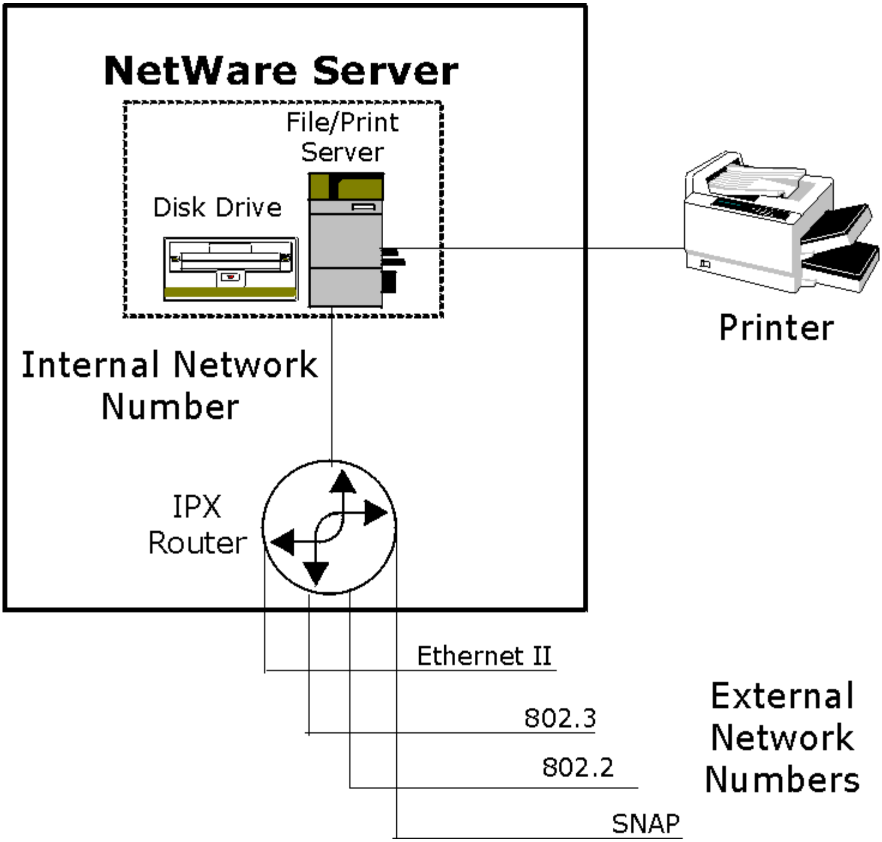


Figure 6-1 NetWare Network Numbers

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 643 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.

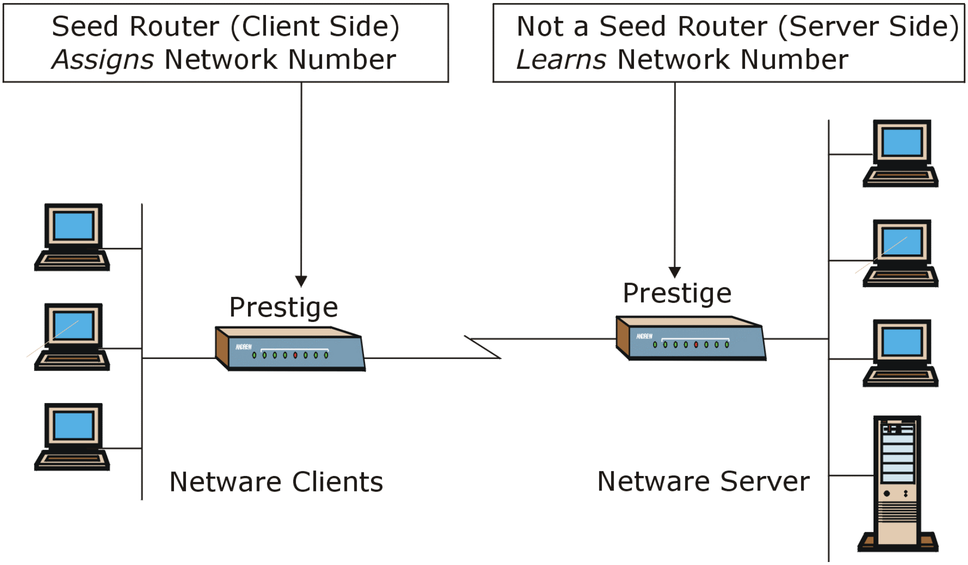


Figure 6-2 Prestige in an IPX Environment

6.2.1 Prestige 643 on LAN With Server

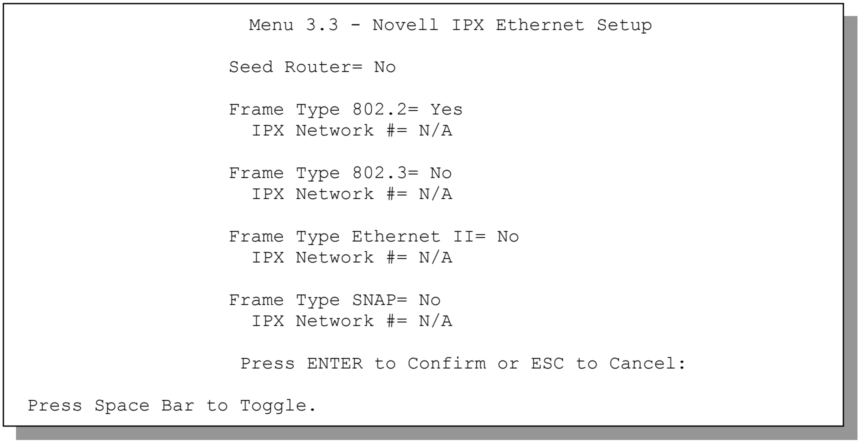
If your Prestige is on a LAN with a seed router, you do not need to configure the LAN network numbers. Your Prestige will learn the network number from the seed router and add the routes to its routing table.

6.2.2 Prestige 643 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

In **Menu 3 – Ethernet Setup**, press **3** to display **Menu 3.3 - Novell IPX Ethernet Setup** as shown next.



```
                    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	Choose **Yes** if your Prestige is to act as a seed router; otherwise, choose **No**.	**No** (default)
Frame Type	Choose Yes to enable or No to disable the individual frame type. Enable only the individual frame types that are actually used on your network. Frame types are **802.2**, **802.3**, **Ethernet II** and **SNAP**.	**No** (default)
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 uses your Prestige to call from a branch office to the corporate headquarters enabling the stations in the branch office to access the NetWare servers at the headquarters, as depicted in the next figure.

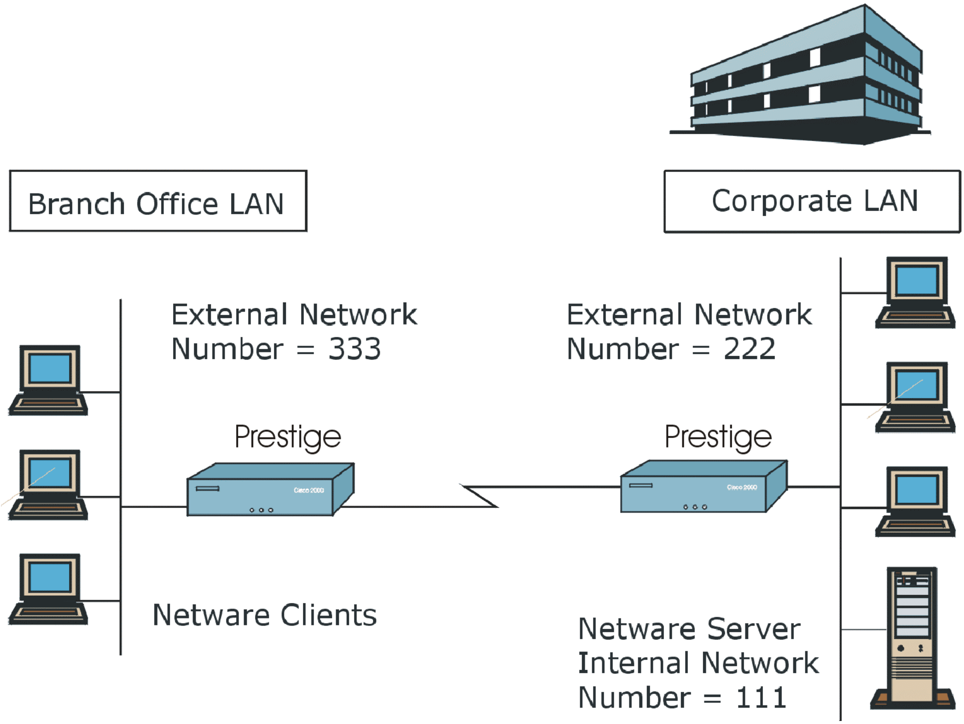

Branch Office LAN
Corporate LAN
External Network Number = 333
External Network Number = 222
Prestige
Prestige
Netware Clients
Netware Server Internal Network Number = 111

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

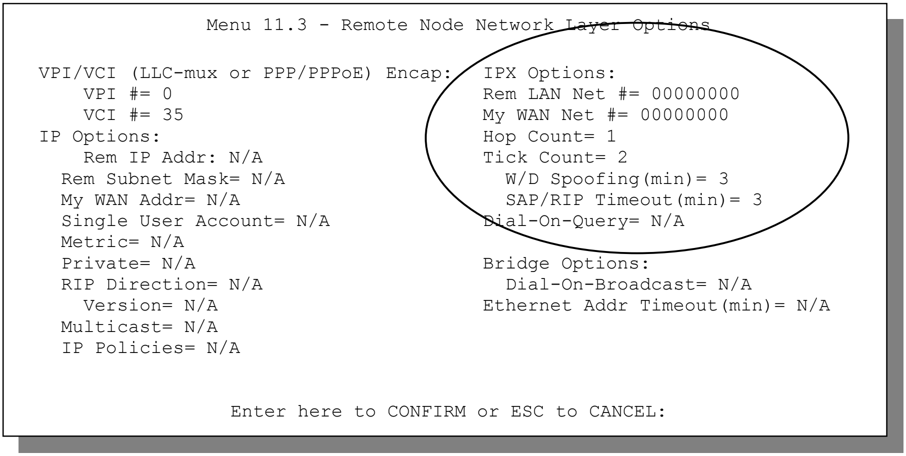
6.4.1 IPX Remote Node Setup

Follow the procedure in *Remote Node TCP/IP Configuration* 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 next, 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 display **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)= 3
     My WAN Addr= N/A                         SAP/RIP Timeout(min)= 3
     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

The table shown next describes the IPX protocol-dependent parameters of the Remote Node Setup.

Table 6-2 Remote Node Novell IPX Options

FIELD	DESCRIPTION	EXAMPLE
Rem LAN Net #	Enter the internal network number of the NetWare server on the remote LAN.	00000000 (default)
My WAN Net #	Enter the network number of the WAN link. If you leave this field as 00000000, your Prestige will automatically determine 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 three fields are only valid for PPPoE encapsulation.		

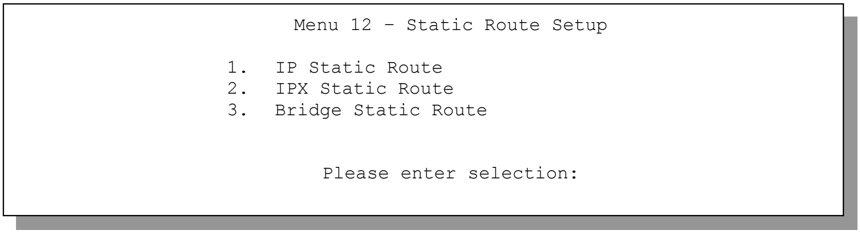
FIELD	DESCRIPTION	EXAMPLE
W/D Spoofing (min)	This field is for the Prestige on the server side. Your Prestige can spoof a response to a server's WatchDog request after the connection is dropped. In this field, type in the time (number of minutes) that you want your Prestige to spoof the WatchDog response.	3 (default)
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.	3 (default)
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.	**No** (default)

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.

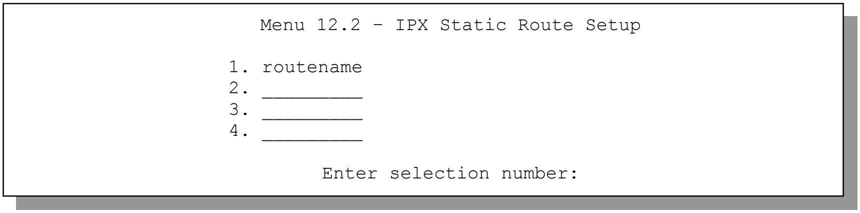
Step 1. Type in **12** from the main menu, to displaly the following screen.



```
                    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

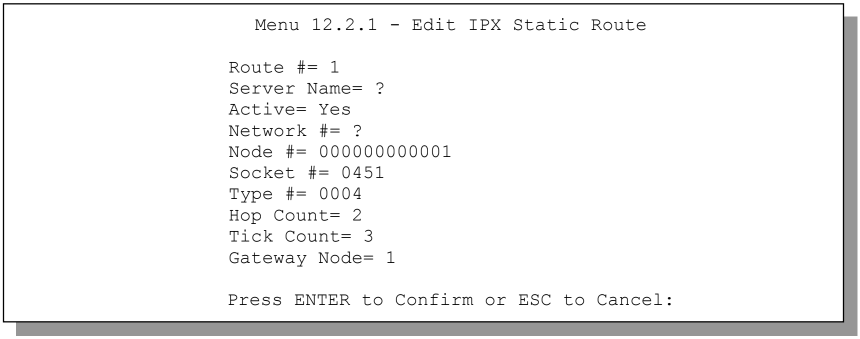
Step 2. Type in **2**, from Menu 12, to display the following screen.



```
                    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 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.

FIELD	DESCRIPTION
Active	Choose **Yes** to activate and **No** to 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

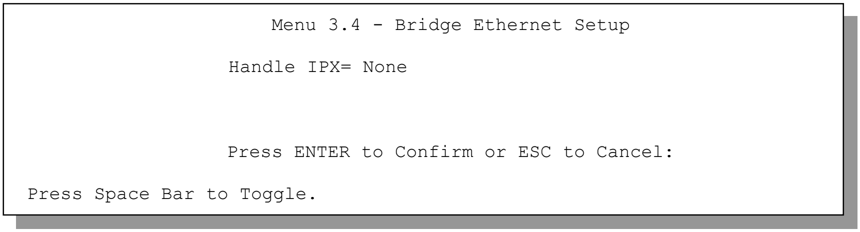
Bridging bases the forwarding decision on the MAC (Media Access Control), or hardware address, while routing does it on the network layer (IP or IPX) address. Bridging allows the Prestige to transport packets of network layer protocols that it does not route, e.g. SNA, from one network to another. The caveat is that, compared to routing, bridging generates more traffic for the same network layer protocol and 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 applies special handling for certain IPX packets to reduce the number of calls, depending on the setting of the **Handle IPX** field.

Type in **4**, from **Menu 3 – Ethernet Setup**, to display **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	EXAMPLE
Handle IPX	Press [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 choose **None**. When there are only client workstations on the LAN choose **Client**. RIP and SAP (Service Advertising Protocol) response packets will not trigger calls. When there are only IPX servers on the LAN choose **Server**. 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. 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, if there are both clients and servers on the LAN and local clients will access the remote servers.	**None** (default)

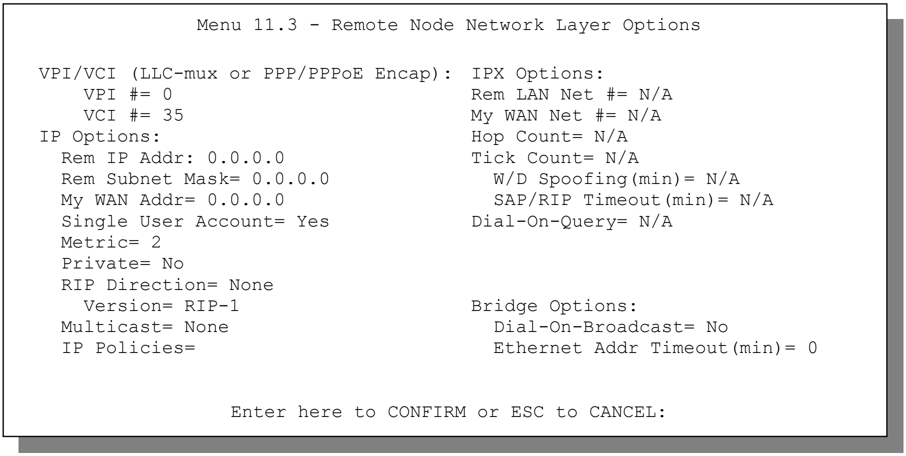
7.2.1 Remote Node Bridging Setup

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, set the **Bridge** field to **Yes**.

Step 2. Move the cursor to the **Edit IP/IPX/Bridge** field, press [SPACE BAR] to choose **Yes** and press [ENTER] to display **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/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
   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.

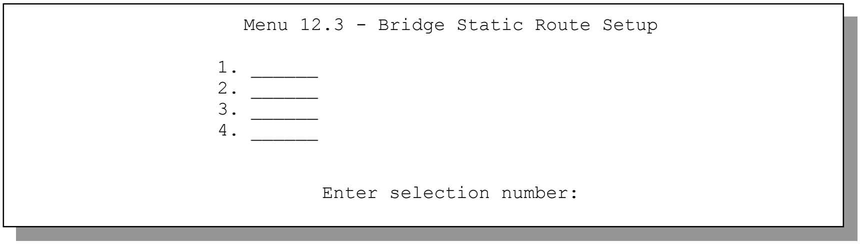
Table 7-2 Remote Node Network Layer Options

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.

FIELD	DESCRIPTION
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 filled 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

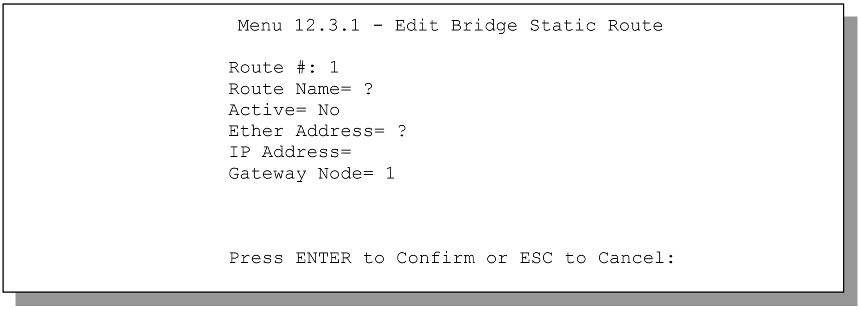
Similar to network layer static routes, a bridging static route tells the Prestige the route to a node before a connection is established. Configure bridge static routes in Menu 12.3.1. Display this menu by pressing **3** in Menu 12 as shown next.



```
                    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. Bridge Static Route number **1** is selected for the next figure.



```
                    Menu 12.3.1 - Edit Bridge Static Route

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



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

Figure 7-4 Menu 12.3.1 - Edit Bridge Static Route

The following table describes the 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

This part provides information on Filter Configuration, SNMP Configuration, System Maintenance, Remote Management, IP Policy Routing and Call Scheduling.

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.

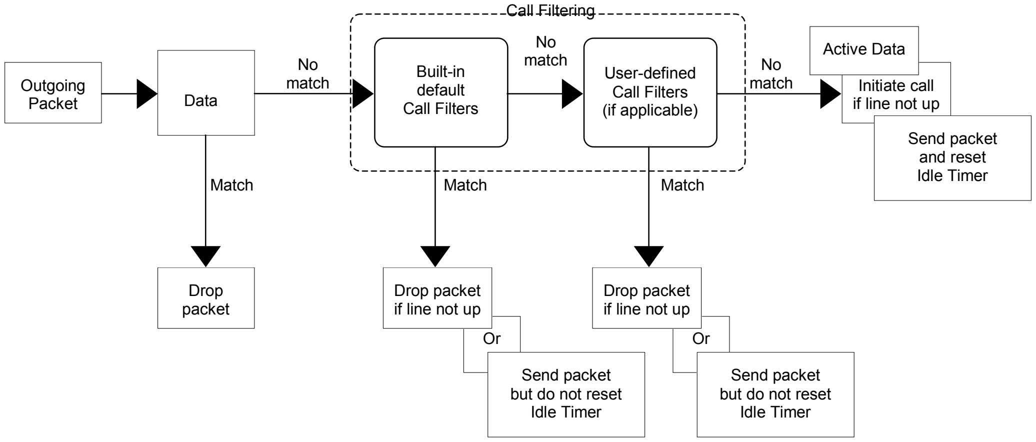

Call Filtering
Outgoing Packet
Data
No match
Built-in default Call Filters
No match
User-defined Call Filters (if applicable)
No match
Active Data
Initiate call if line not up
Send packet and reset Idle Timer
Match
Match
Match
Drop packet
Drop packet if line not up
Or
Send packet but do not reset Idle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

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:

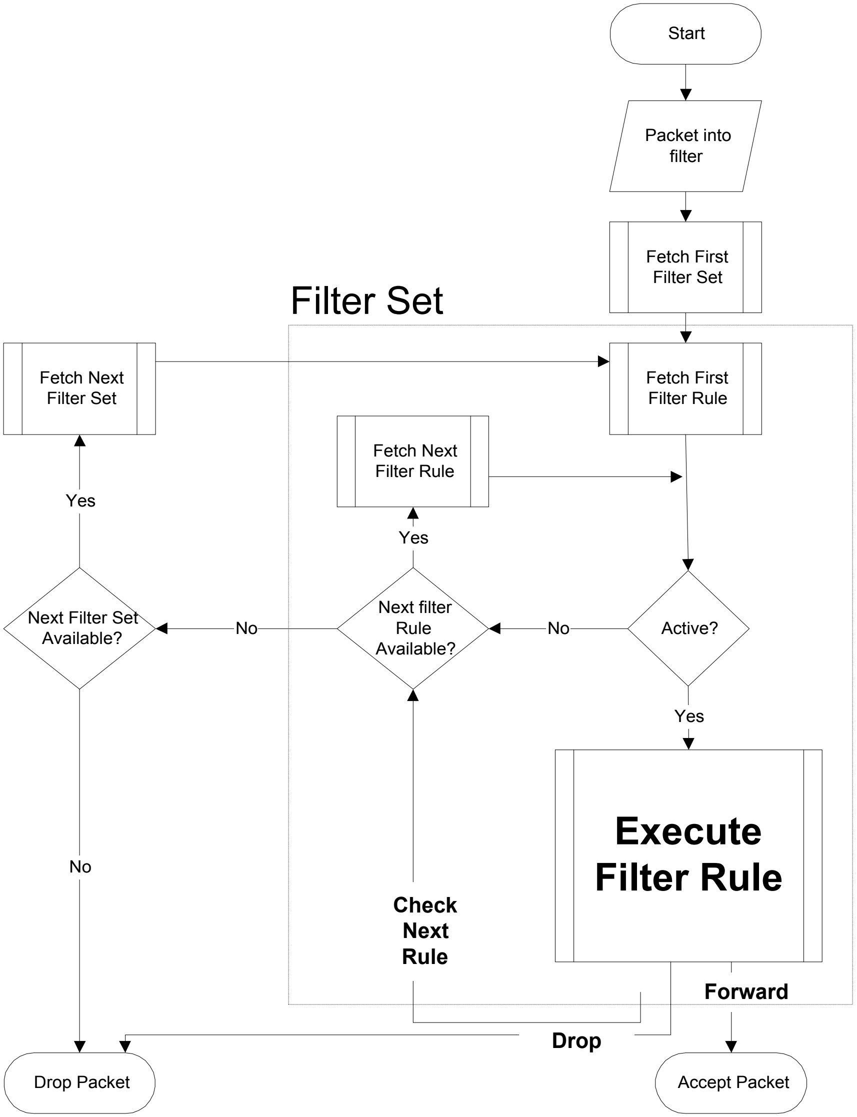


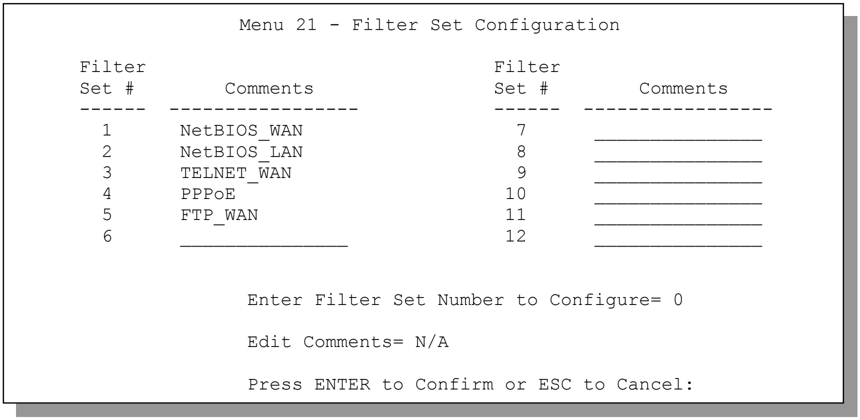
Figure 8-2 Filter Rule Process

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 display **Menu 21 – Filter Set Configuration**.



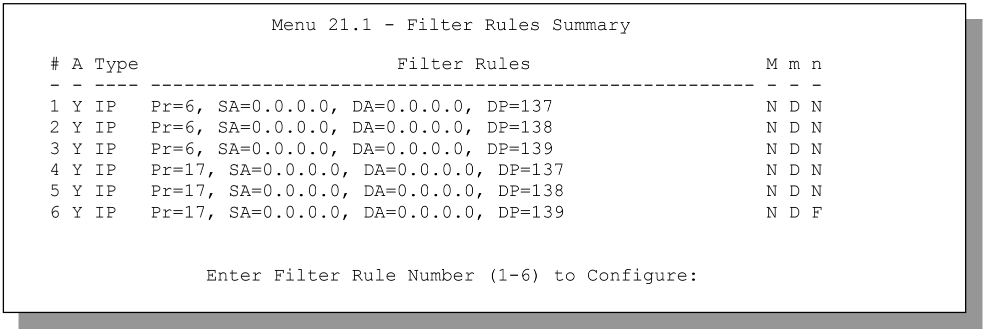
```
                     Menu 21 - Filter Set Configuration

       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 (1-12) you wish to configure and press [ENTER].

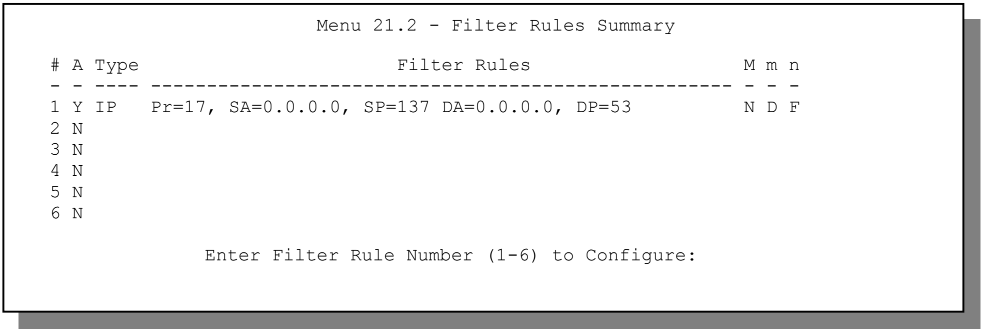
Step 3. Enter a descriptive name or comment in the **Edit Comments** field and press [ENTER].

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



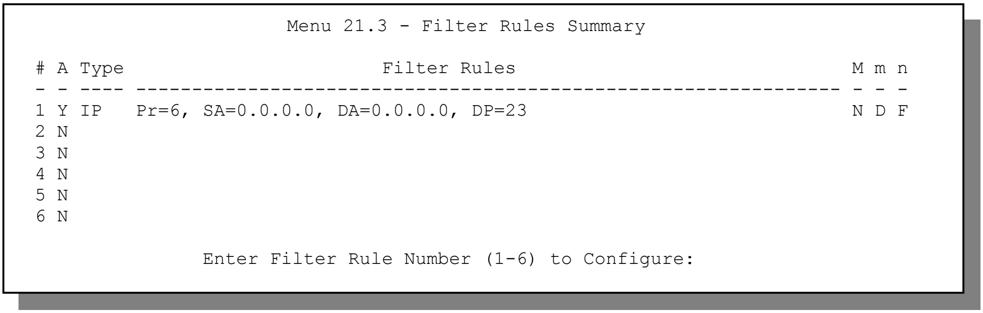
```
                    Menu 21.1 - Filter Rules Summary

  # 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



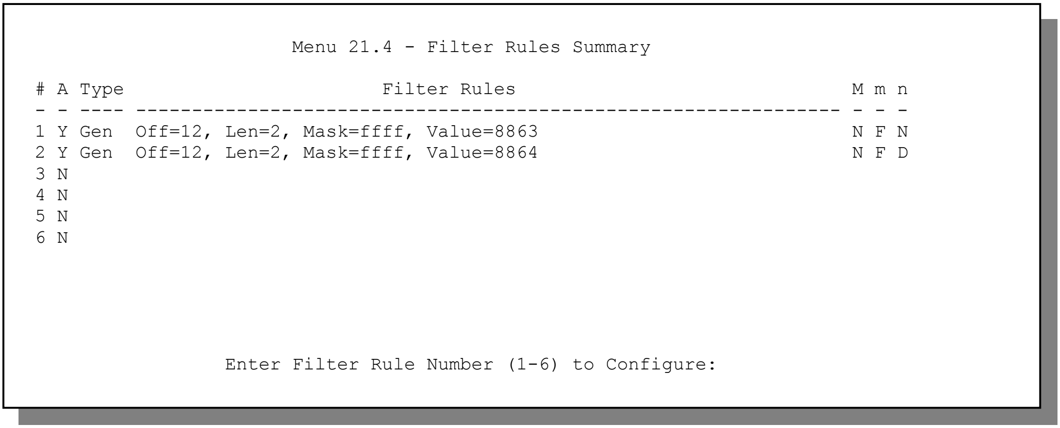
```
                        Menu 21.2 - Filter Rules Summary

  # 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



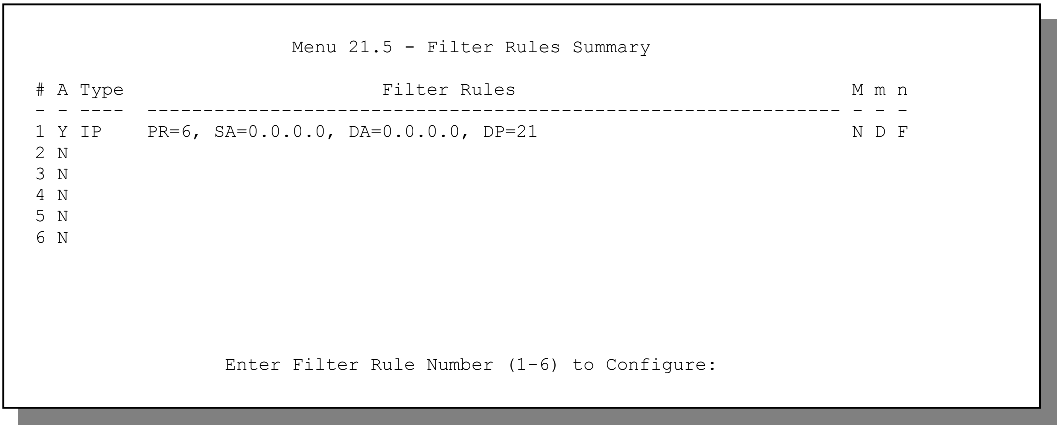
```
                      Menu 21.3 - Filter Rules Summary

  # 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

ABBI EVIATIONS	DESCRIPTIC N	DISPLAY
#	Refers to the filter rule number (1-6).	
A	Shows whether the rule is active or not.	[Y] means the filter rule is active. [N] means the filter rule is inactive.
Type	Refers to the type of filter rule.	[GEN] = Generic. [IP] = TCP/IP.
Filter Rules	The filter rule parameters will be displayed here (see below).	
M	Refers to **More**. **More** in a set behaves like a logical AND i.e., the set is only matched if ALL rules in it are matched. [Y] means an action can not yet be taken as there are more rules to 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:

- Abbreviations used if filter type is IP:

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

- Abbreviations used if filter type is GEN (generic):

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 display Menu 21.1.1 for the rule.

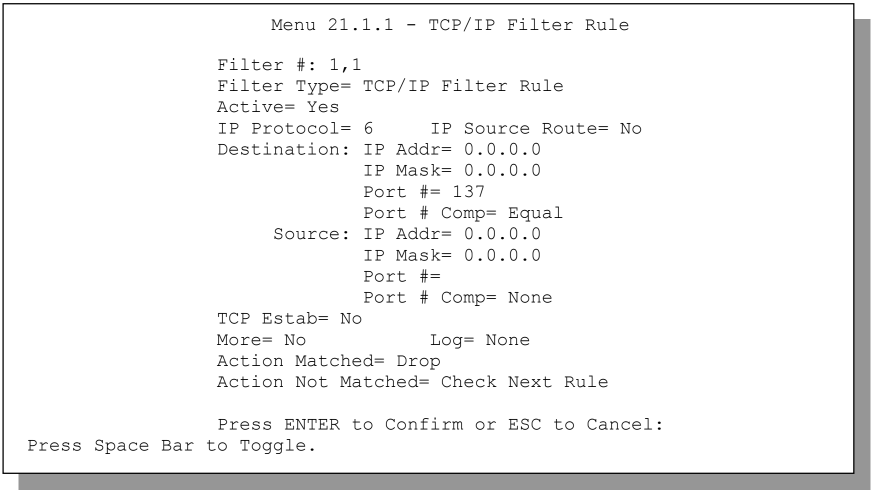
Factory default filter rules have been configured in Menu 21 to filter traffic. Depending on the type of rule, the parameters below the type will be different. Use the [SPACE BAR] to select the type of rule that you wish to create in the **Filter Type** field and press [ENTER] to open the respective 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 next:



```
                        Menu 21.1.1 - TCP/IP Filter Rule

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

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

Figure 8-9 Menu 21.1.1 - TCP/IP Filter Rule

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

Table 8-5 TCP/IP Filter Rule Menu Fields

'IELD	DESCRIPTION	EX \MPLE
Active	Choose **Yes** to activate and **No** to deactivate the filter rule.	**Yes** (default)
IP Protocol	Protocol refers to the upper layer protocol, e.g., TCP is 6, UDP is 17 and ICMP is 1. This value must be between 0 and 255	6
IP Source Route	Choose Yes if rule applyies to a packet with IP source route option. Choose No if the packet does not have source route option. The majority of IP packets do not have source route.	**No** (default)
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.	0.0.0.0
IP Mask	Enter the IP mask to apply to the Destination.	0.0.0.0
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.	137 (default)
Port # Comp	Select the comparison to apply to the destination port in the packet against the value given in the **Destination: Port #** field. Choices are **None**, **Less**, **Greater**, **Equal** or **Not Equal**.	**None**
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
IP Mask	Enter the IP mask to apply to the **Source: IP Addr** field.	IP Mask
Port #	Enter the source port of the packets that you wish to filter. The range of this field is 0 to 65535. This field is disregarded if it is 0.	0-65535
Port # Comp	Select the comparison to apply to the source port in the packet against the value given in **Source: Port #** field. Choices are **None**, **Less**, **Greater**, **Equal** or **Not Equal**	**Equal**
TCP Estab	This field is applicable only when the **IP Protocol** field is 6, TCP. If **Yes**, the rule matches packets that want to establish a TCP connection (SYN=1 and ACK=0); else it is ignored.	**No** (default)
More	If **Yes**, a matching packet is passed to the next filter rule before an action is taken; else the packet is disposed of	**No** (default)

FIELD	DESCRIPTION	EXAMPLE
	according to the action fields. If the **More** field is **Yes**, then the **Action Matched** field and **Action Not Matched** field will be **N/A**.	
Log	Choose one of 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** (default)
Action Matched	Select the action for a matching packet. Choices are **Check Next Rule**, **Forward** or **Drop**.	**Drop**
Action Not Matched	Select the action for a packet not matching the rule. Choices are **Check Next Rule**, **Forward** or **Drop.**	**Check Next Rule**
Once you have completed filling in **Menu 21.1.1 - TCP/IP Filter Rule**, press [ENTER] at the message “Press ENTER to Confirm” to save your configuration, or press [ESC] to cancel. This data will now be displayed on **Menu 21.1 - Filter Rules Summary**.		

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

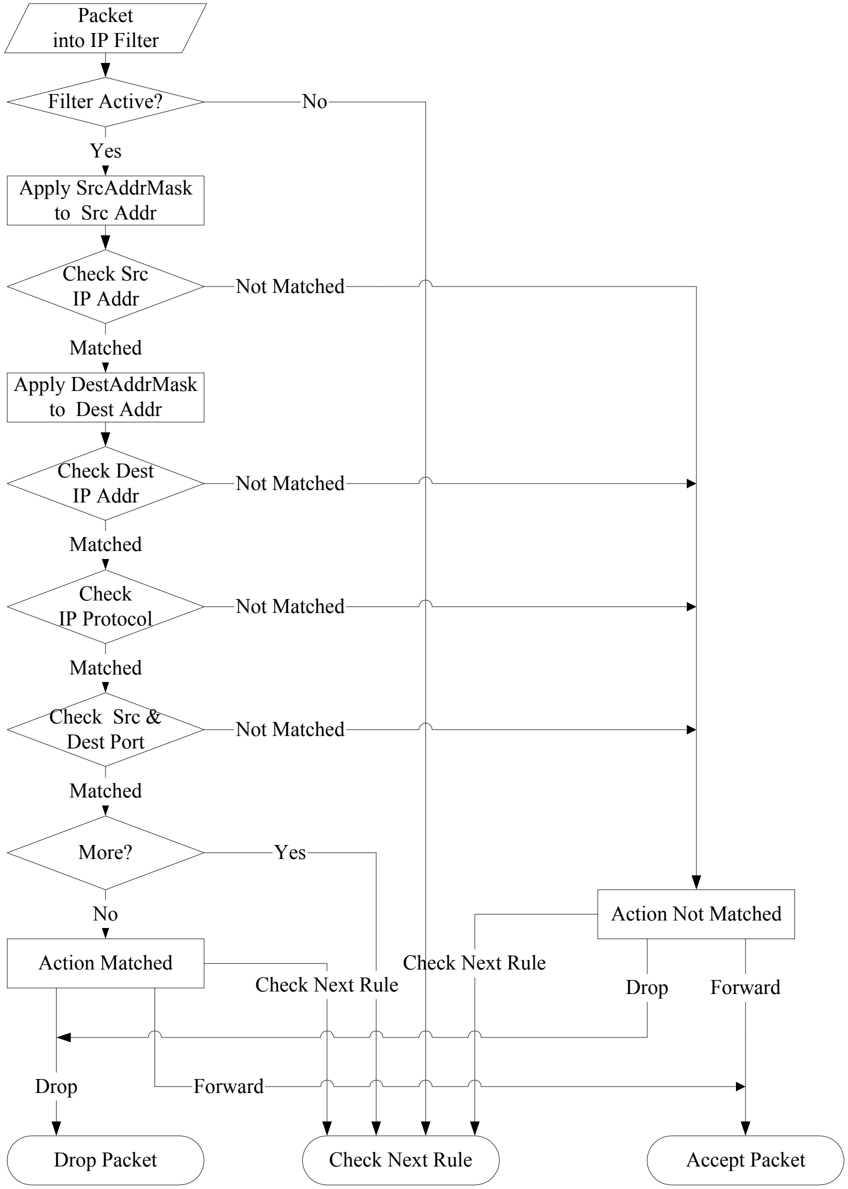


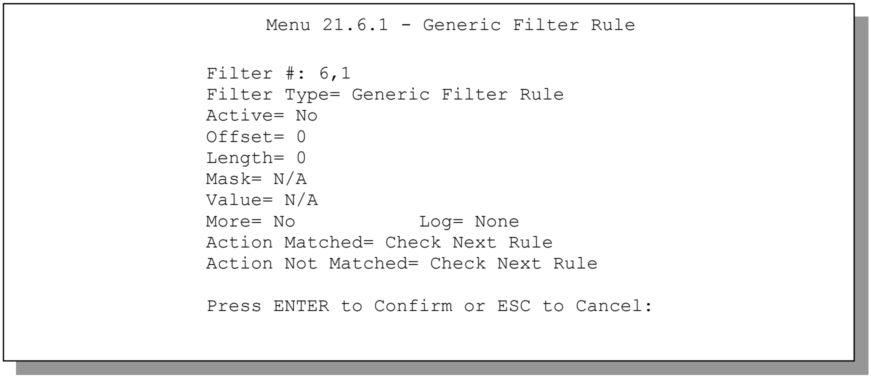
Figure 8-10 Executing an IP Filter

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, for example, `FFFFFFFF`.

To configure a generic rule, select **Generic Filter Rule** in the **Filter Type** field in menu 21.6 and press [ENTER] to open Generic Filter Rule, as shown next.



```
                     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:
```

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	EXAMPLE
Filter #	This is the filter set, filter rule co-ordinates, i.e., 6,1 refers to the sixth filter set and the first rule of that set.	6,1
Filter Type	Choose the rules you want to apply. Choices are Generic Filter Rule, TCP/IP or Filter Rule. Parameters for different rules will vary.	**Generic Filter Rule**
Active	Choose **Yes** to turn on and **No** to turn off a filter rule.	**No**
Offset	Enter the starting byte of the data portion in the packet that you wish to compare. The range for this field is from 0 to 255.	0 (Default)
Length	Enter the byte count of the data portion in the packet that you wish to compare. The range for this field is 0 to 8.	0 (Default)
Mask	Enter the Mask (in Hexadecimal) to apply to the data portion before comparison.	N/A
Value	Enter the Value (in Hexadecimal) to compare with the data portion.	N/A
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 the **Action Matched** field and the **Action Not Matched** field will be **No**.	**No**
Log	Select the logging option from the following: **None** – No packets will be logged. **Action Matched** – Only packets that match the rule parameters will be logged. **Action Not Matched** - Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.	**None** (default)
Action Matched	Select the action for a matching packet. Choices are **Check Next Rule, Forward** or **Drop.**	**Check Next Rule**
Action Not Matched	Select the action for a packet not matching the rule. Choices are **Check Next Rule**, **Forward** or **Drop**.	**Check Next Rule**
Once you have completed filling in **Menu 21.6.1 - 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 26.1 - 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, choose the **IPX Filter Rule** from the **Filter Type** field by pressing [SPACE BAR]. Press [ENTER] to open **Menu 21.6.1 - IPX Filter Rule**, as shown in next.

Figure 8-12 IPX Filter Rule

The table below describes the IPX Filter Rule:

Table 8-7 IPX Filter Rule Menu Fields

FIE D	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)

FIE D	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: Network #	Enter the destination/source network numbers (4-byte in hexadecimal) of the packet that you wish to filter.
Node #	Enter in the destination/source node number (6-byte in hexadecimal) of the packet you wish to filter.
Socket #	Enter the destination/source socket number (2-byte in hexadecimal) of the packets you wish to filter.
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. Choices are **None**, **RIP Request**, **RIP Response, SAP Request**, **SAP Response**, **SAP Get Nearest Server Request** or **SAP Get Nearest Server Response**.
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 the **Action Matched** and the **Action Not Matched** fields will be **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.

FIE D	DESCRIPTION
	Action Not Matched - Only packets that do not match the rule parameters will be logged. **Both** – All packets will be logged.
Action Matched	Select the action for a matching packet. Choices are **Check Next Rule**, **Forward** or **Drop.**
Action Not Matched	Select the action for a packet not matching the rule. Choices are **Check Next Rule**, **Forward** or **Drop.**
Once you have completed filling in **Menu 21.6.1 - IPX Filter Rule**, press [ENTER] at the message “Press Enter to Confirm…” to save your configuration, or press [ESC] to cancel. This data will now be displayed in **Menu 21.6 - Filter Rules Summary**.	

8.3 Example Filter

Let’s look at the third default ZyXEL filter, TELNET_WAN (see *Telnet_WAN Filter Rules Summary figure*) as an example. This filter is designed to block outside users from telnetting into the Prestige.

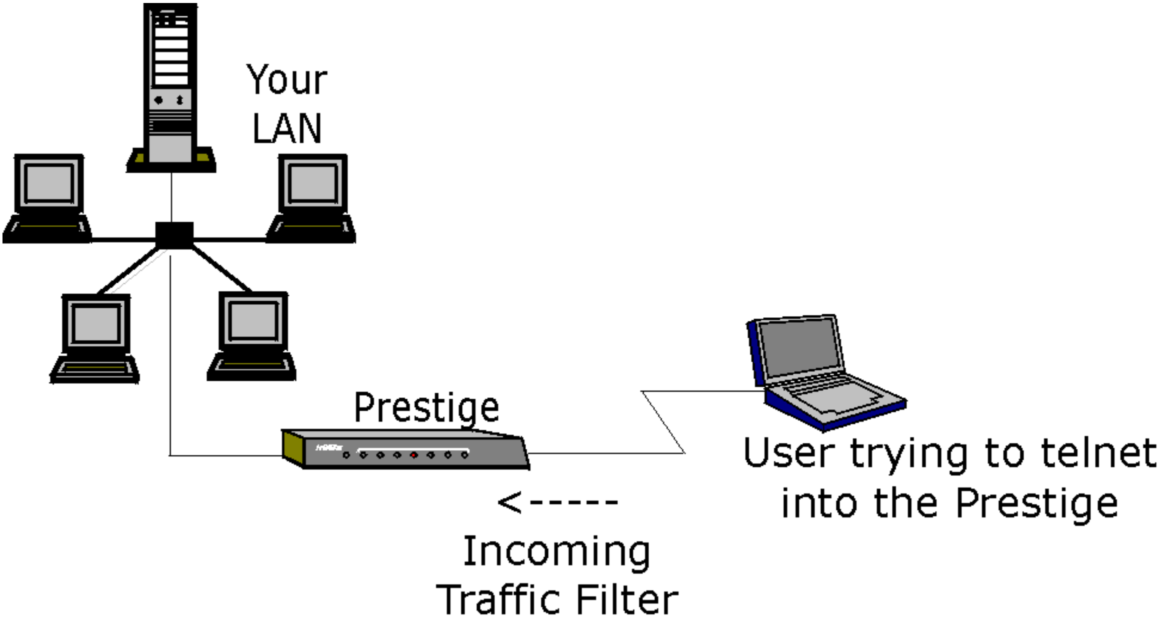


Figure 8-13 Telnet Filter Example

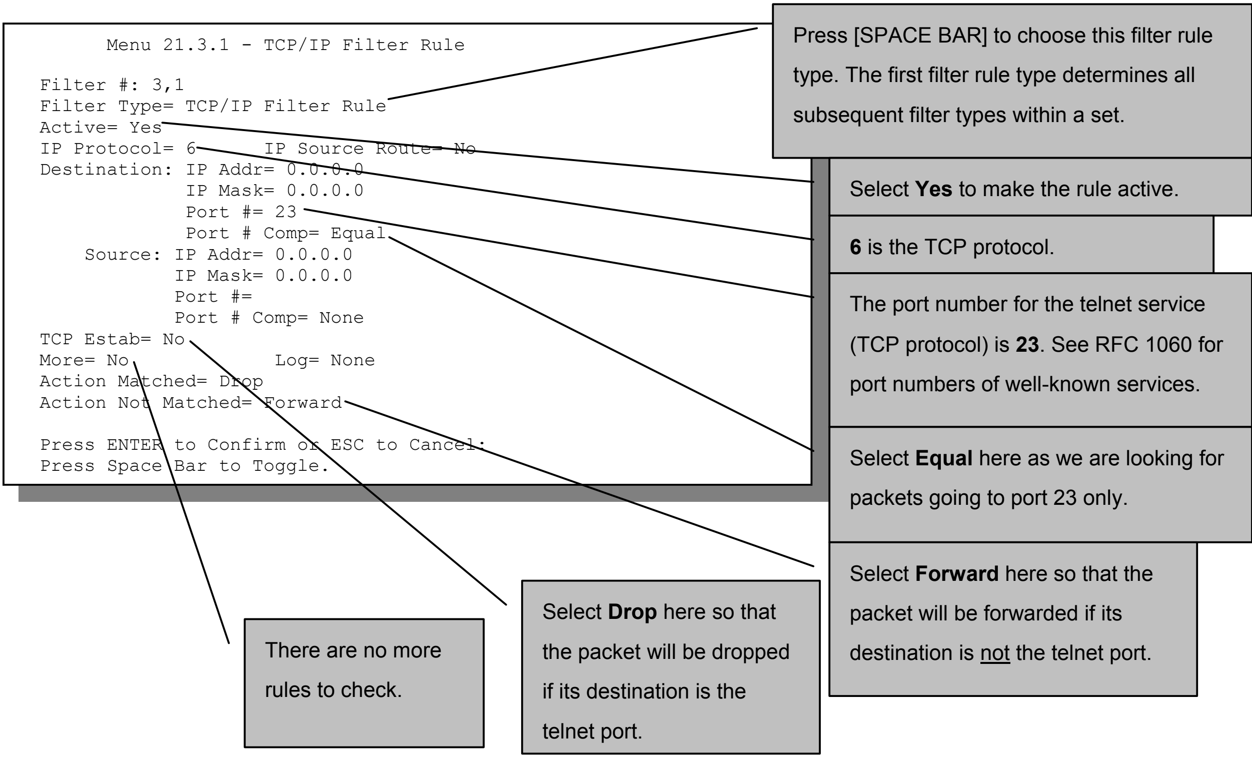
Step 1. Enter **21** from the main menu to open **Menu 21 - Filter Set Configuration**.

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 display **Menu 21.3 - Filter Rules Summary**.

Step 5. Enter **1** to configure the first filter rule. Make the entries in this menu as shown in next:



```
      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.

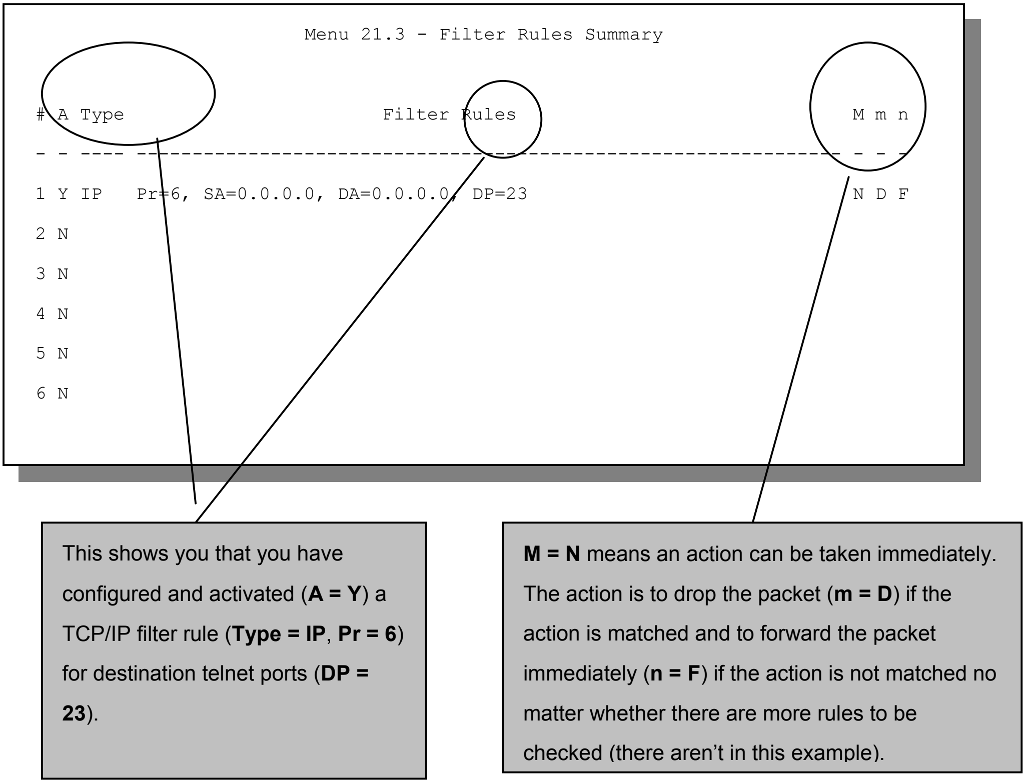
Select **Forward** here so that the packet will be forwarded if its destination is not the telnet port.

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

There are no more rules to check.

Figure 8-14 Example Filter – Menu 21.3.1

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



```
                    Menu 21.3 - Filter Rules Summary


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

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

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

Figure 8-15 Example Filter Rules Summary - Menu 21.3

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

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

Step 2. Go to the **Edit Filter Sets** field. Press [SPACE BAR] to change **No** to **Yes** and press [ENTER] to display Menu 11.5.

Step 3. Apply the TELNET_WAN filter set (filter set 3) as shown in the *Filtering Remote Node Traffic (PPPoE Encapsulation)* figure.

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.

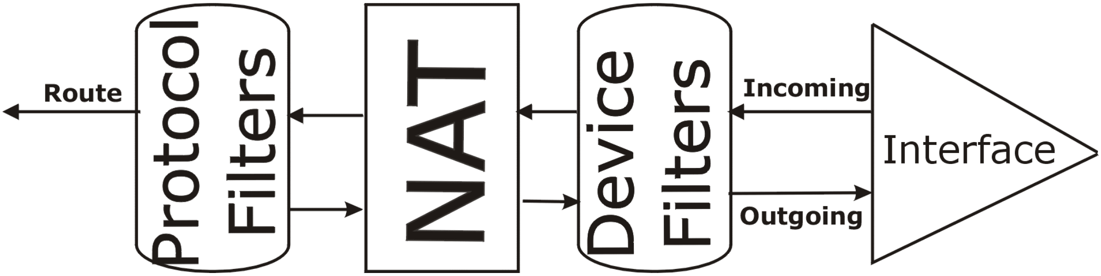


Figure 8-16 Protocol and Device Filter Sets

8.5 Applying a Filter and Factory Defaults

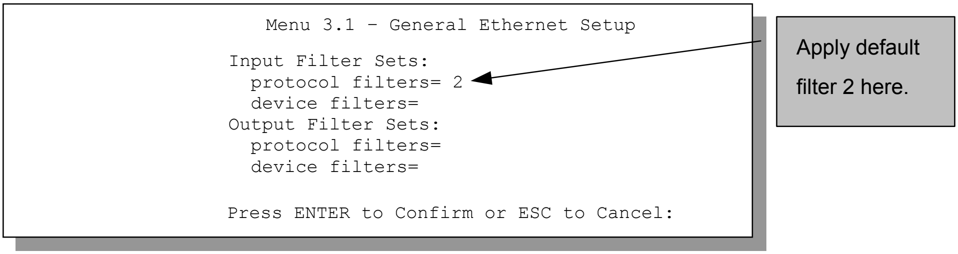
This section shows you where to apply the filter(s) after you design it (them). Sets of factory default filter rules have been configured in Menu 21 (but have not been applied) to filter telnet, FTP, NetBIOS and PPPoE traffic. The PPPoE filter filters out all packets *except* PPPoE packets going out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

Table 8-8 Input, Output and Call Filter Sets

FILTER SETS	DESCRIPTION
Input Filter Sets:	Apply filters for traffic coming into the Prestige. You may apply filter rules for protocol or device filters. See the next section for information on types of filters.
Output Filter Sets:	Apply filters for traffic going out of the Prestige. You may apply filter rules for protocol or device filters. See earlier in this section for information on types of filters.
Call Filter Sets:	Apply filters to determine if a packet should be allowed to trigger a call.

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:
```

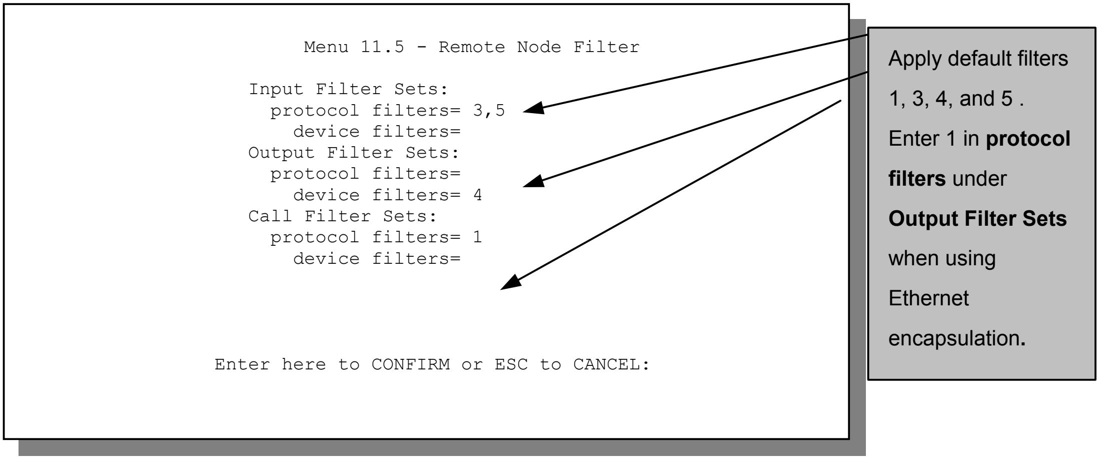
Apply default filter 2 here.

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 the **protocol filters** field under **Output Filter Sets** 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= 3,5
                   device filters=
               Output Filter Sets:
                 protocol filters=
                   device filters= 4
               Call Filter Sets:
                 protocol filters= 1
                   device filters=



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

Apply default filters 1, 3, 4, and 5 . 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

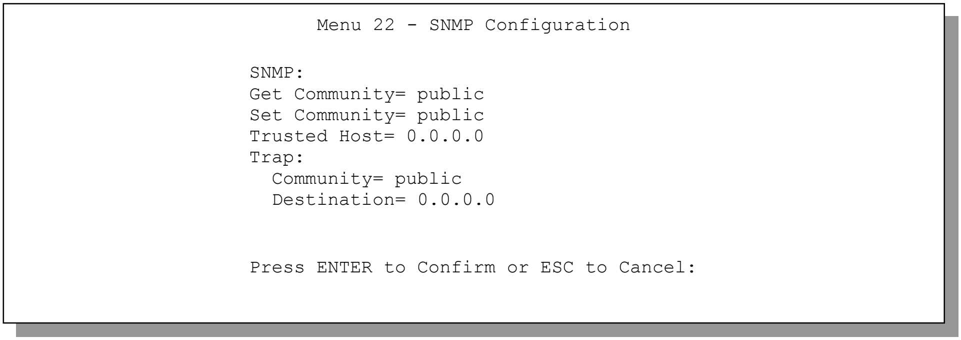
This chapter discusses SNMP (Simple Network Management Protocol) for network management and monitoring.

9.1 About SNMP

Your Prestige supports SNMP agent functionality. This functionality 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, select **22** from the main menu to display **Menu 22 - SNMP Configuration**, as shown next. 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

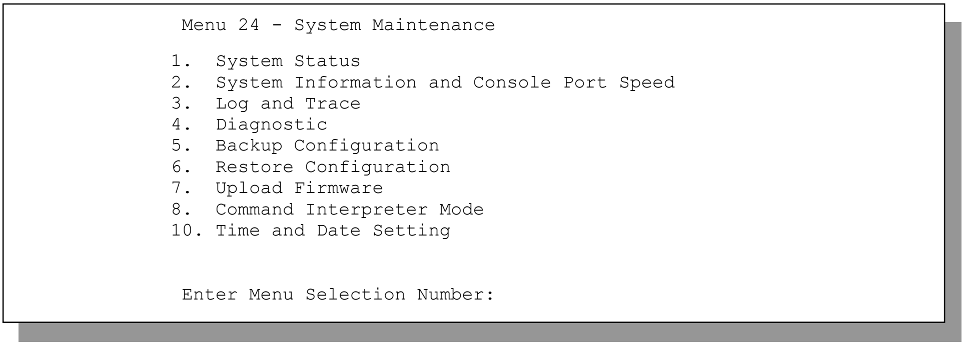
FIELD	DESCRIPTION	EXAMPLE
Get Community	Enter the get community, which is the password for the incoming Get- and GetNext- requests from the management station.	Public (default)
Set Community	Enter the set community, which is the password for incoming Set- requests from the management station.	Public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

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.

Type **24** in the main menu to display **Menu 24 - System Maintenance**, as shown below:



```
                Menu 24 - System Maintenance

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


                Enter Menu Selection Number:
```

Figure 10-1 Menu 24 - System Maintenance

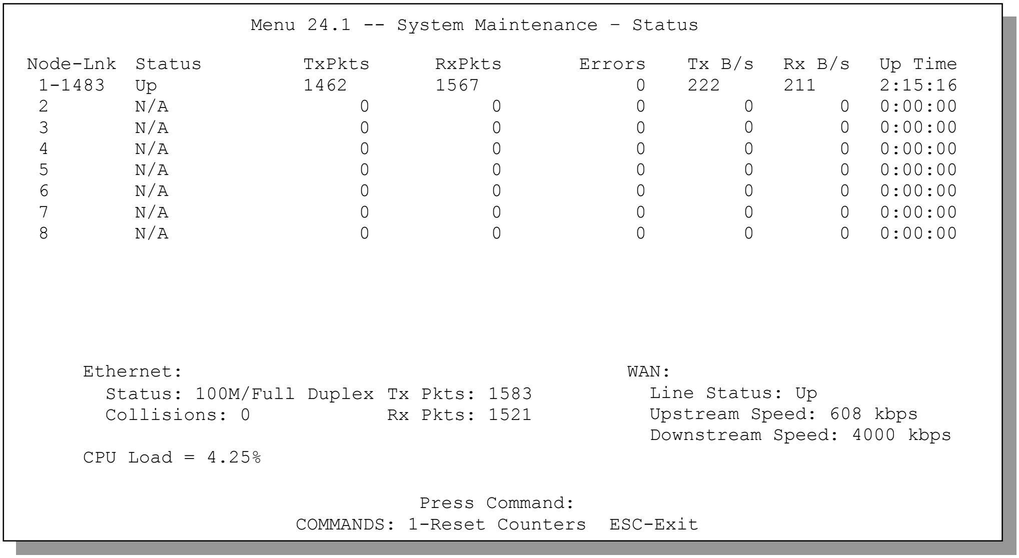
10.1 System Status

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

To get to the System Status, enter number **24** from the main menu to go to **Menu 24 - System Maintenance**. Type in **1** and press [ENTER] to display **Menu 24.1 - System Maintenance - Status** . Enter **1** to reset the counters and [ESC] to take you back to the previous screen.

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

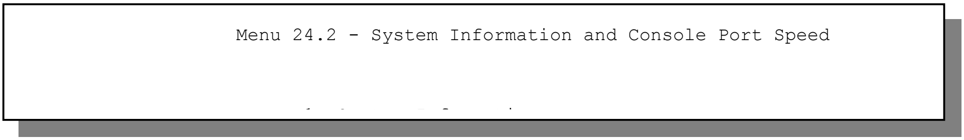
ǀ IELD	DESCRIPTION
Node-Lnk	This is the remote node index number and link type. Link types are PPP, ENET, 1483 or PPPoE
Status	Shows the status of the remote node.
TxPkts	The number of packets transmitted to this remote node.

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

10.2 System Information and Console Port Speed

System Information and Console Port Speed inform you about the various aspects of your Prestige.

Type **2**, in Menu 24, to display the screen shown next.

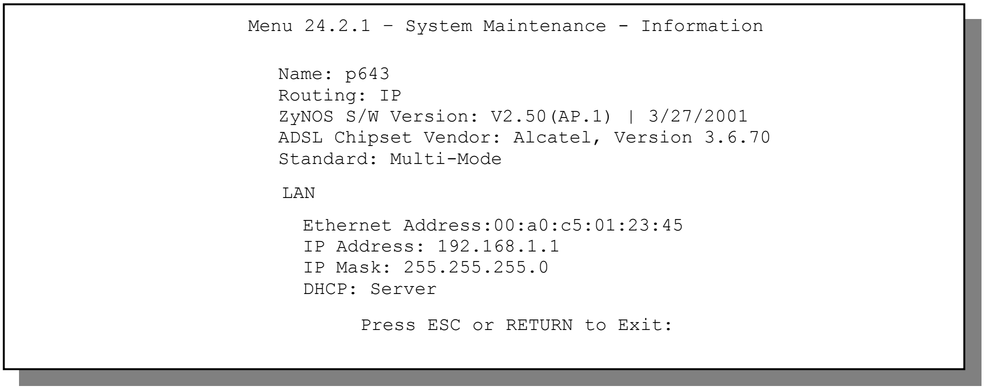


```
                    Menu 24.2 - System Information and Console Port Speed
```

Figure 10-3 Menu 24.2 - System Information and Console Port Speed

10.2.1 System Information

Type **1** in Menu 24.2 to display the screen shown next.



```
                    Menu 24.2.1 – System Maintenance - Information

                       Name: p643
                       Routing: IP
                       ZyNOS S/W Version: V2.50(AP.1) | 3/27/2001
                       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 Menu 24.2.1 - System Maintenance - Information

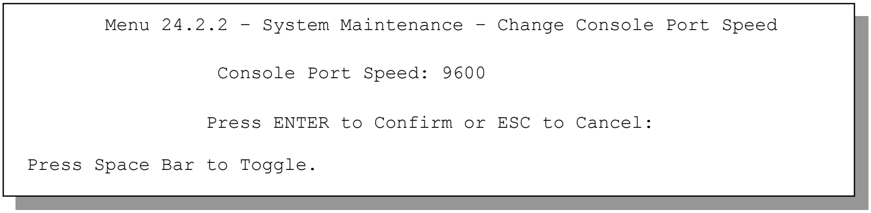
Table 10-2 Fields in System Maintenance - Information

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.
Standard	This refers to the operational protocol the Prestige and the DSLAM (Digital Subscriber Line Access Multiplexer) are using.

FIELD	DESCRIPTION
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.

10.2.2 Console Port Speed

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



```
        Menu 24.2.2 - System Maintenance - Change 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

10.3 Log and Trace

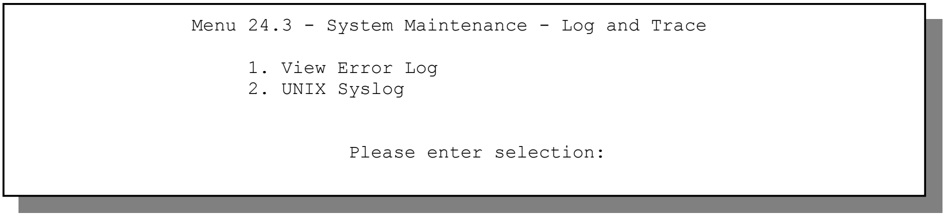
There are two logging facilities in the Prestige. The first is the error logs and trace records that are stored locally. The second is the UNIX syslog facility for message logging.

10.3.1 Viewing Error Log

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

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

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



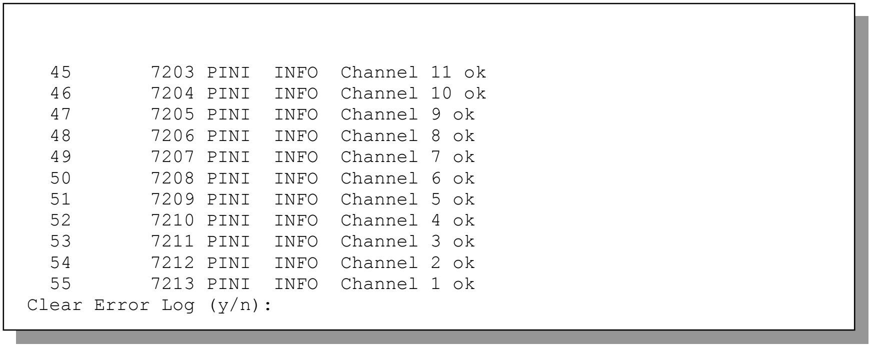
```
                Menu 24.3 - System Maintenance - Log and Trace

                     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.

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

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

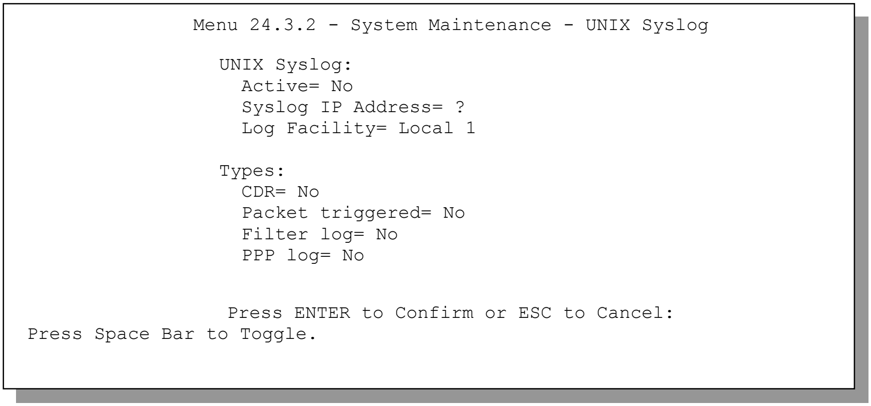


```
   45       7203 PINI  INFO  Channel 11 ok
   46       7204 PINI  INFO  Channel 10 ok
   47       7205 PINI  INFO  Channel 9 ok
   48       7206 PINI  INFO  Channel 8 ok
   49       7207 PINI  INFO  Channel 7 ok
   50       7208 PINI  INFO  Channel 6 ok
   51       7209 PINI  INFO  Channel 5 ok
   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

10.3.2 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

FIELD	DESCRIPTION
UNIX Syslog:	
Active	Choose **Yes** to turn on or **No** to turn off syslog.
Syslog IP Address	Enter the IP Address of the server that will log the CDR (Call Detail Record) and system messages i.e., the syslog server.
Log Facility	Choose **Local 1**, **Local 2**, **Local 3**, **Local 4**, **Local 4**, **Local 5**, **Local 6** or **Local 7**. 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	Choose **No** to log no filters; choose **Yes** to log filters.
PPP log	PPP events are logged when this field is set to **Yes**.

Your Prestige sends four types of syslog messages. Some examples of these syslog messages with their message formats are shown next:

1. CDR

CDR Message Format

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

```
Jul 19 11:19:27 192.168.102.2 ZyXEL Communications Corp.: board 0 line 0 channel 0, call 1, C01
Outgoing Call dev=2 ch=0 40002
```

```
Jul 19 11:19:32 192.168.102.2 ZyXEL Communications Corp.: board 0 line 0 channel 0, call
1, C02 OutCall Connected 64000 40002
```

```
Jul 19 11:20:06 192.168.102.2 ZyXEL Communications Corp.: board 0 line 0 channel 0, call
1, C02 Call Terminated
```

2. Packet triggered

Packet triggered Message Format

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

```
Jul 19 11:28:39 192.168.102.2 ZyXEL Communications Corp.: Packet Trigger: Protocol=1,
Data=4500003c100100001f010004c0a86614ca849a7b08004a5c020001006162636465666768696a6b6c6d6e6
f7071727374

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

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

3. Filter log

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

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

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

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

4. PPP log

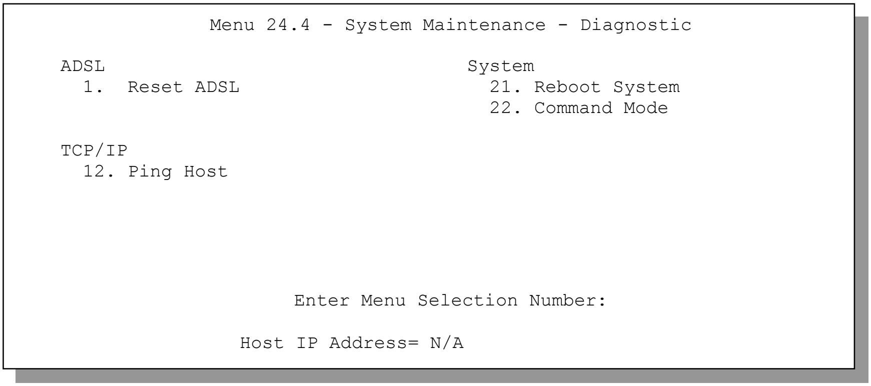
PPP Log Message Format
SdcmdSyslogSend(SYSLOG_PPPLOG, SYSLOG_NOTICE, String);
String = ppp:Proto Starting / ppp:Proto Opening / ppp:Proto Closing / ppp:Proto Shutdown
Proto = LCP / ATCP / BACP / BCP / CBCP / CCP / CHAP/ PAP / IPCP / IPXCP

```
Jul 19 11:42:44 192.168.102.2 ZyXEL Communications Corp.: ppp:LCP Closing

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

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

10.4 Diagnostic

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



```
                  Menu 24.4 - System Maintenance - Diagnostic

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


     TCP/IP
       12. Ping Host






                          Enter Menu Selection Number:

                     Host IP Address= N/A
```

Figure 10-9 Menu 24.4 - System Maintenance - Diagnostic

Follow the procedure below to get to Diagnostic:

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

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

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

Table 10-4 System Maintenance Menu Diagnostic

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

10.5 Filename Conventions

The configuration file (sometimes called the romfile or rom-0) contains the settings in the menus such as password, DHCP Setup defaults, TCP/IP Setup defaults, etc. The external (i.e., not on the Prestige) configuration filename is usually the router model name with a *.rom extension, e.g., P643.rom. The ZyNOS firmware file (sometimes referred to as the “ras” file) is the file that contains the ZyXEL Network Operating System firmware and the external firmware file is usually called the router model name with a *.bin extension, e.g., P643.bin. Rename the configuration filename to “rom-0” and the firmware filename to “ras” when transferring files to the Prestige (i.e., the internal filenames on the Prestige). Renaming the files is not necessary when you transfer files to the Prestige using the XMODEM protocol.

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. After uploading the new firmware see the **ZyNOS F/W Version** field in **Menu 24.2.1** to check if you have uploaded the correct firmware version.

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 speed 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

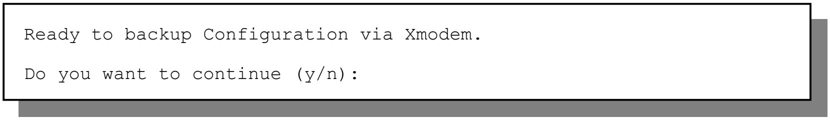
10.6 Backup Configuration

Entering 5 from **Menu 24** – **System Maintenance** allows you to backup the current Prestige configuration to your workstation. Backup is highly recommended once your Prestige is functioning properly.

You must perform 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.

Please note that the terms “download” and “upload” are relative to the workstation. Download means to transfer from another machine to the workstation; upload means from your workstation to another machine.

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



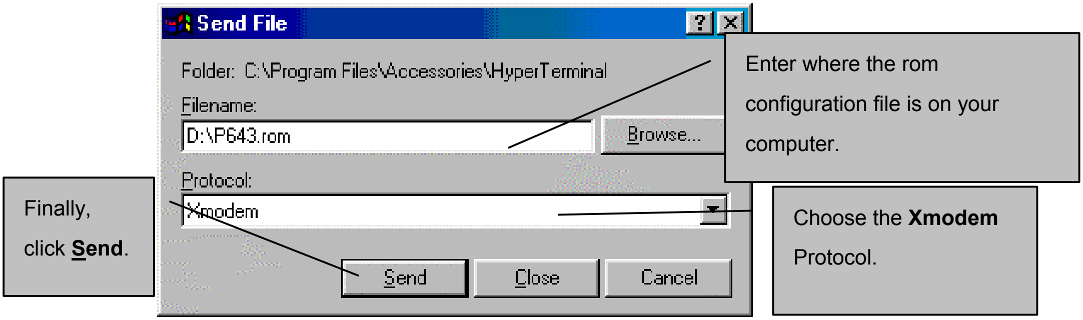
```
Ready to backup Configuration via Xmodem.

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. Run the HyperTerminal program.

Step 1. Click “Transfer”, then “Receive File” to display the following screen.



Send File

Folder: C:\Program Files\Accessories\HyperTerminal

Filename: D:\P643.rom

Protocol: Xmodem

Enter where the rom configuration file is on your computer.

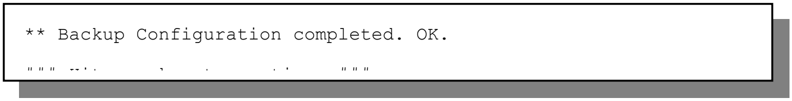
Choose the **Xmodem** Protocol.

Finally, click **Send**.

Figure 10-11 HyperTerminal Screen

Step 2. Enter a path and name for the rom configuration file on your computer and make sure you choose the XMODEM protocol. Then press “Receive”.

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



```
** Backup Configuration completed. OK.
```

Figure 10-12 Successful Backup

10.7 Restore Configuration

Enter 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.

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.

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

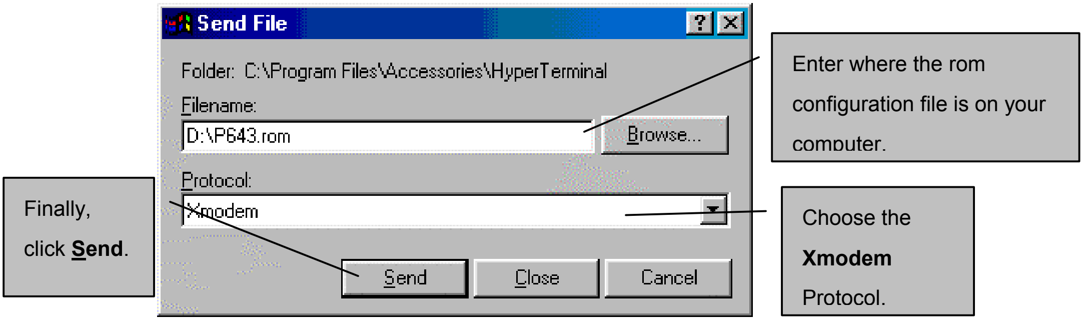
```
Ready to restore Configuration via Xmodem.

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. Run the HyperTerminal program.

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



Folder: C:\Program Files\Accessories\HyperTerminal

Filename: D:\P643.rom

Protocol: Xmodem

Enter where the rom configuration file is on your computer.

Choose the **Xmodem** Protocol.

Finally, click **Send**.

Figure 10-14 HyperTerminal Screen

Step 4. Enter where the rom configuration file is on your computer and make sure you choose the XMODEM protocol. Then press “Send”.

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

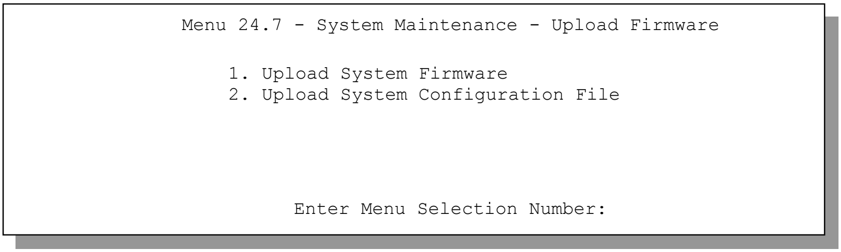
```
Save to ROM

Hit any key to start system reboot.
```

Figure 10-15 Successful Restoration

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.

10.8 Upload Firmware

Menu 24.7 – System Maintenance – Upload Firmware allows you to upgrade the firmware and the configuration file via the console port. The firmware and configuration file may also be uploaded via FTP. There are 2 components in the system: the router firmware and the configuration file, as shown in the next figure. Restoring the configuration as in Menu 24.6 copies your (customized) backup configuration from your computer to the Prestige. Note that you must be able to access the SMT to do this. Uploading the configuration file via Menu 24.7.2 on the other hand rewrites all configuration data, as well as system-related data, the error log and the trace log. If you forget your password for instance you will need to use Menu 24.7.2 as you can use this method in debug mode. However, your customized settings will be reset to the default values (including your password being reset to 1234, the Prestige default password).



```
                    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

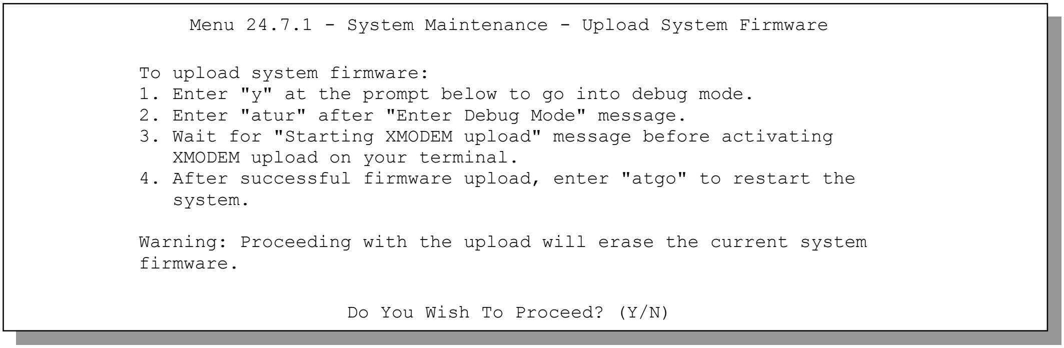
10.8.1 Upload Router Firmware

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` at the prompt, the Prestige will go into debug mode. Follow the procedure next 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 System Firmware

           To upload system 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
              system.

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

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

Figure 10-17 Menu 24.7.1 – Uploading Router Firmware

10.8.2 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.

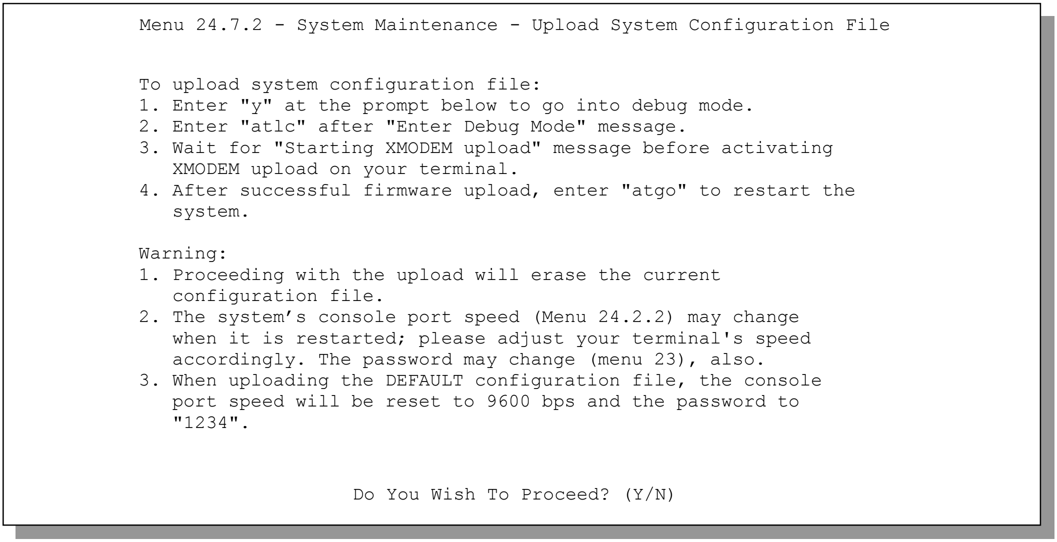
Menu 24.7.2 shows you the instructions for uploading the configuration file. If you answer `yes` to the prompt, the Prestige will go into debug mode. Follow the procedure next to upload the configuration file:

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

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

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

If you replace the current configuration file with the default configuration file, i.e., P643.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, 1 stop bit (8n1) and no Flow Control. You will need to change your serial communications software to the default before you can connect to the Prestige again. The password will be reset to the default of 1234, also.



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


            To upload system 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
               system.

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



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

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

10.8.3 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. Even though TFTP should work over WAN as well, it is not recommended.

To use TFTP, your workstation must have both telnet and TFTP clients. To transfer the firmware and the configuration file, follow the next procedures:

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

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

Step 3. Enter command "`sys stdio 0`" to disable SMT timeout, so the TFTP transfer will not be interrupted.

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

Step 5. Use the TFTP client to transfer files between the Prestige and the workstation. The file name for the firmware is "`ras`" and for the configuration file, "`rom-0`" (rom-zero, not capital o).

If you upload the firmware to the Prestige, it will reboot automatically when the file transfer is completed.

NOTE: Telnet connection must be active and the SMT in CI mode before and during the TFTP transfer.

For details on TFTP commands (see following example), please consult the documentation of your TFTP client program. For UNIX, use "`get`" to transfer from the Prestige to the workstation, "`put`" the other way around and "`binary`" to set binary transfer mode.

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

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

Using the FTP Command from the DOS Prompt

Step 1. Launch the FTP client on your workstation.

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

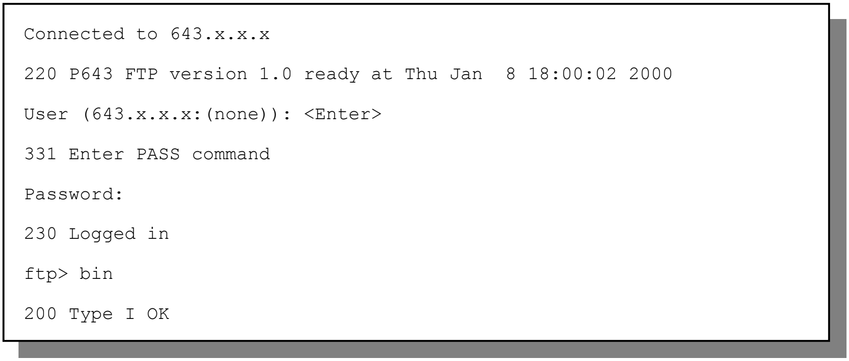
Step 3. You may press [ENTER] when prompted for a username.

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

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

Step 6. Use **`put`** to transfer files from the workstation to the Prestige, e.g., **`put P643.bin ras`** transfers the firmware on your computer (P643.bin) to the Prestige and renames it "ras". Similarly **`put P643.rom rom-0`** transfers the configuration file on your computer (P643.rom) to the Prestige and renames it "rom".

Step 7. Type **`quit`** to exit the ftp prompt.



```
Connected to 643.x.x.x

220 P643 FTP version 1.0 ready at Thu Jan  8 18:00:02 2000

User (643.x.x.x:(none)): <Enter>

331 Enter PASS command

Password:

230 Logged in

ftp> bin

200 Type I OK
```

Figure 10-19 Sample FTP Session

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

Table 10-6 Third Party FTP Clients – General Fields

FIELDS	DESCRIPTION	EXAMPLE
Host Address	Enter the address of the host server	
Login Type	♦ Anonymous A user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. ♦ Normal The server requires a unique User ID and Password to login.	Normal
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode.	Binary

FIELDS	DESCRIPTION	EXAMPLE
Initial Remote Directory	Specify the default remote directory (path).	
Initial Local Directory	Specify the default local directory (path).	

ftp> put P643.bin ras

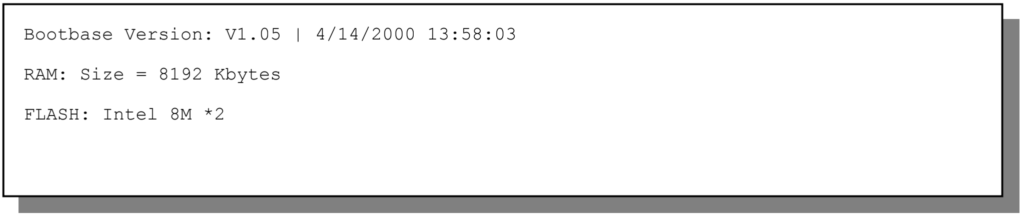
This is a sample ftp session showing the transfer of the PC file "P643.bin" to the Prestige.

ftp> get rom-0 MyP643.cfg

This is a sample ftp session saving the current configuration to the PC file MyP643.cfg.

10.8.4 Boot Module Commands

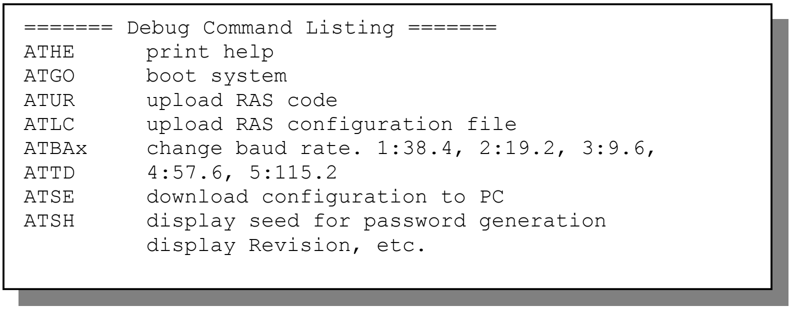
When you reboot your Prestige, you will be given a choice to go into debug mode by pressing a key at the prompt shown in the following screen. In debug mode you have access to a series of boot module commands, for example `ATUR` (for uploading firmware) and `ATLC` (for uploading the configuration file) already discussed in a previous section.



```
Bootbase Version: V1.05 | 4/14/2000 13:58:03

RAM: Size = 8192 Kbytes

FLASH: Intel 8M *2
```

Figure 10-20 Option to Enter Debug Mode

Enter ATHE to view all available Prestige boot module commands as shown in the next screen. ATBAx allows you to change the console port speed. The x denotes the number preceding the colon to give the console port speed following the colon in the list of numbers that follows; e.g., ATBA3 will give a console port speed of 9.6 Kbps. ATSE displays the seed that is used to generate a password to turn on the debug flag in the firmware. The ATSH command shows product-related information such as boot module version, vendor name, product model, RAS code revision, etc. ATGO allows you to continue booting the system. Most other commands aid in advanced troubleshooting and should only be used by qualified engineers.

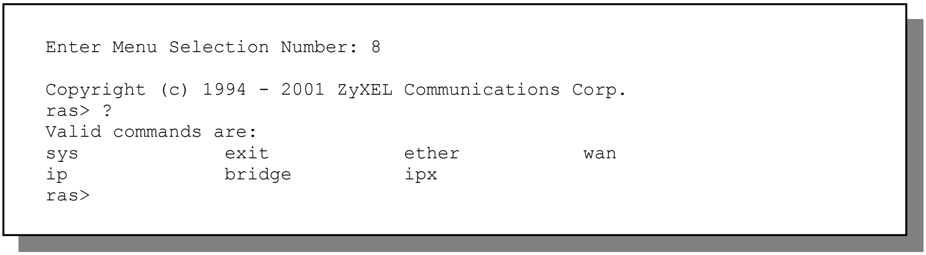


```
======= Debug Command Listing =======
ATHE      print help
ATGO      boot system
ATUR      upload RAS code
ATLC      upload RAS configuration file
ATBAx     change baud rate. 1:38.4, 2:19.2, 3:9.6,
ATTD      4:57.6, 5:115.2
ATSE      download configuration to PC
ATSH      display seed for password generation
          display Revision, etc.
```

Figure 10-21 Boot Module Commands

10.9 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.

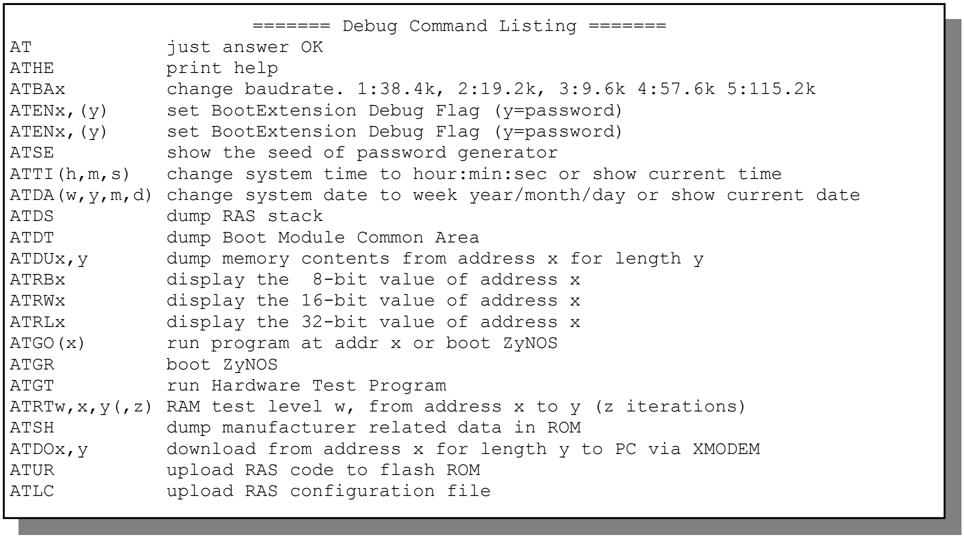


```
Enter Menu Selection Number: 8

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

Figure 10-22 Command Mode

10.10 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

10.11 Time and Date Setting

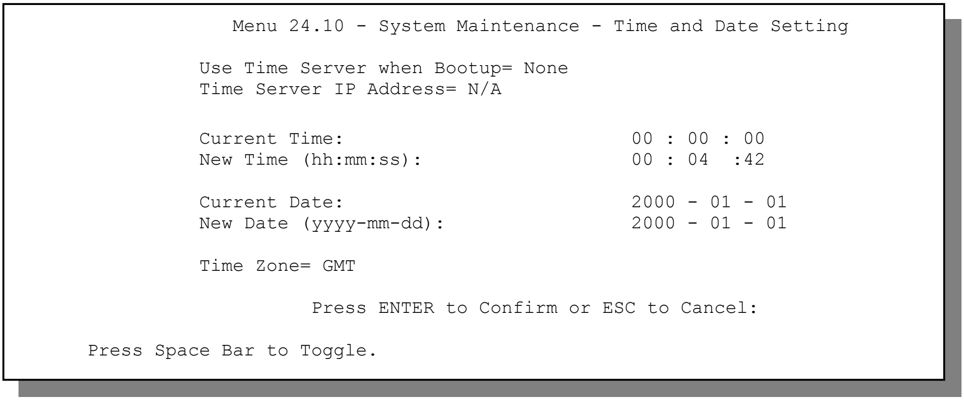
There is no Real Time Chip (RTC) chip in the Prestige, so we have a software mechanism to get the current time and date from an external server when you power up your Prestige. Menu 24.10 does just that – it allows you to update the time and date settings of your Prestige. The real time is then displayed 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**.

10.11.1 How often does the Prestige update the time?

The Prestige updates the time in three instances:

1. On leaving Menu 24.10 after making changes.
2. When the Prestige boots up and there is a time server configured in Menu 24.10.

3. 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 10-7 Time and Date Setting Fields

FI :LD	**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 **2000/1/1 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 year, month, day and format.

FIELD	DESCRIPTION
Time Zone = GMT	Press the [SPACE BAR] to set the time difference between your time zone and Greenwich Mean Time (GMT). Be aware when your time is altered by daylight savings.
Once you have filled in the new time and date, press [ENTER] to save the setting and press [ESC] to return to Menu 24.	

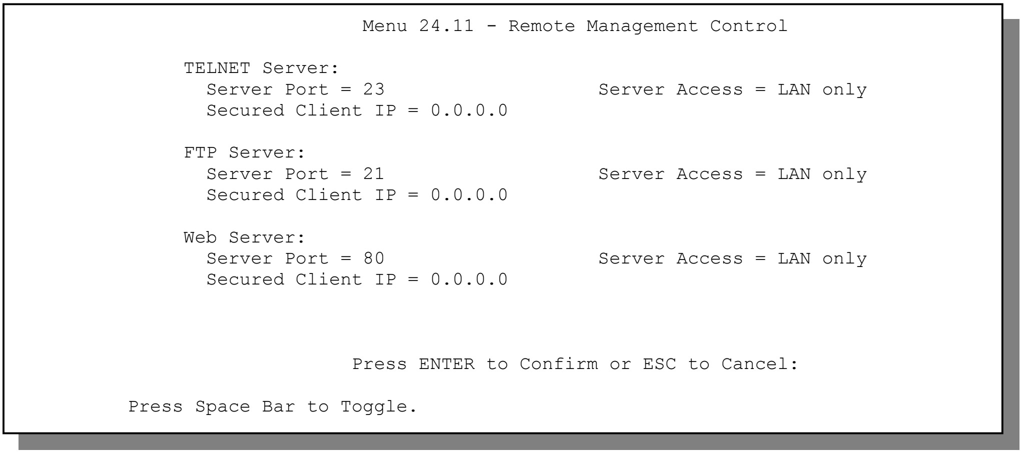
Chapter 11
Remote Management Control

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

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

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

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



```
                                Menu 24.11 - Remote Management Control

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

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

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



                               Press ENTER to Confirm or ESC to Cancel:

           Press Space Bar to Toggle.
```

Figure 11-1 Menu 24.11 – Remote Management Control

Table 11-1 Menu 24.11 – Remote Management Control

I IELD	DESCRIPTION	EXAMPLE
Servers	These read-only labels denote the kind of server (Telnet, FTP or Web) that you may remotely manage via LAN, WAN, both or neither.	

I IELD	DESCRIPTION	EXAMPLE
Server Port	This field shows the port number for the remote management service. You may change the port number for a service if needed, but you must use the same port number to use that service for remote management.	23
Server Access	Select the access interface (if any) by pressing the [SPACE BAR], then [ENTER] to choose from: **LAN only**, **WAN only**, **ALL** or **Disable**.	**LAN only**
Secured Client IP	The default value for **Secured Client IP** is 0.0.0.0, which means you don't care which host is trying to use a service (Telnet, FTP or Web). If you enter an IP address in this field, the Prestige will check if the client IP address matches the value here when a (Telnet, FTP or Web) session is up. If it does not match, the Prestige will disconnect the session immediately. If the **Server Access** field is set to **Disable**, then this field is **N/A**.	0.0.0.0
Once you have filled in this menu, press [ENTER] at the message "Press ENTER to Confirm or ESC to Cancel" to save your configuration, or press [ESC] to cancel.		

11.1.1 Remote Management Limitations

Remote management over LAN or WAN will not work when:

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

Chapter 12
IP Policy Routing

12.1 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.

12.1.1 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.

12.1.2 Routing Policy

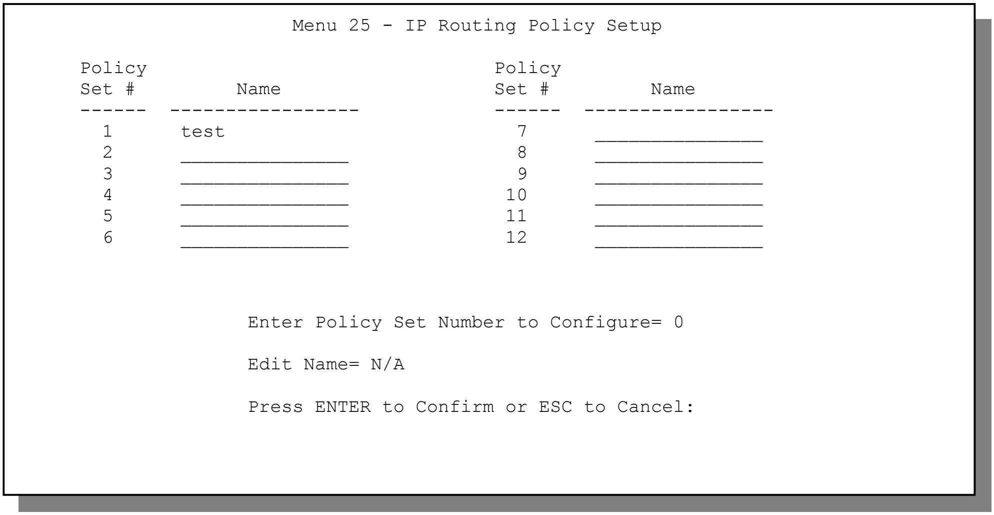
A policy defines the matching criteria and the action to take when a packet meets the criteria. The action is taken only when all the criteria are met. The criteria include the source address and port, IP protocol (ICMP, UDP, TCP, etc.), destination address and port, TOS and precedence (fields in the 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.

12.1.3 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:
```

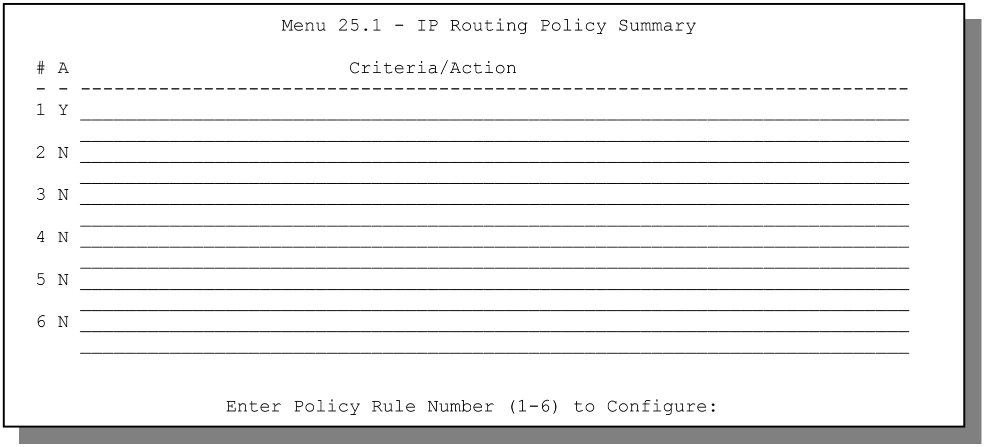
Figure 12-1 IP Routing Policy Setup

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 and a name that 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 ___________________________________________________________________________
      ___________________________________________________________________________
  2 N ___________________________________________________________________________
      ___________________________________________________________________________
  3 N ___________________________________________________________________________
      ___________________________________________________________________________
  4 N ___________________________________________________________________________
      ___________________________________________________________________________
  5 N ___________________________________________________________________________
      ___________________________________________________________________________
  6 N ___________________________________________________________________________
      ___________________________________________________________________________


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

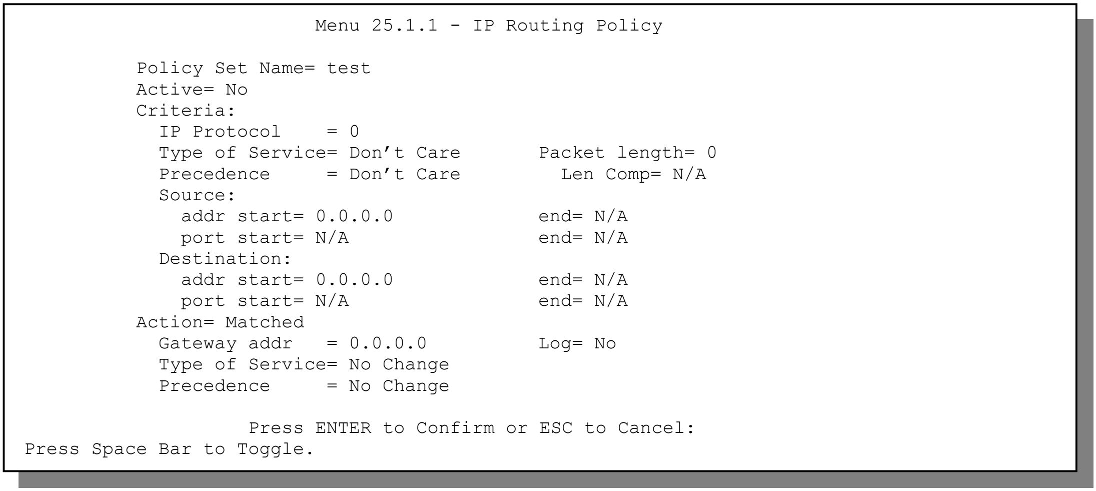
Figure 12-2 Menu 25 - IP Routing Policy Summary

Table 12-1 IP Routing Policy Summary

ABBRE 'IATION	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

ABBREVIATION	MEANING
Type Of Service	
NM	Normal
MD	Minimum Delay
MT	Maximum Throughput
MR	Maximum Reliable
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= No
           Criteria:
             IP Protocol    = 0
             Type of Service= Don't Care       Packet length= 0
             Precedence     = Don't Care         Len Comp= N/A
             Source:
               addr start= 0.0.0.0             end= N/A
               port start= N/A                 end= N/A
             Destination:
               addr start= 0.0.0.0             end= N/A
               port start= N/A                 end= N/A
           Action= Matched
             Gateway addr   = 0.0.0.0          Log= No
             Type of Service= No Change
             Precedence     = No Change

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

Figure 12-3 IP Routing Policy

Table 12-2 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	Choose **Yes** to activate and **No** to deactivate the policy.
Criteria	
IP Protocol	IP layer 4 protocol, e.g., UDP, TCP, ICMP, etc.

FIELD	DESCRIPTION
Type of Service	Prioritize incoming network traffic by choosing from **Don't Care**, **Normal**, **Min Delay**, **Max Thruput** or **Max Reliable**.
Packet Length	Enter the length of incoming packets (in bytes). The operators in the **Len Comp** field (next) apply to packets of this length.
Len Comp	Press [SPACE BAR] to choose from **Equal**, **Not Equal**, **Less**, **Greater**, **Less or Equal** or **Greater or Equal**.
Precedence	Precedence value of the incoming packet. Choices are **1**, **2**, **3**, **4**, **5**, **6**, **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=	Choose 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	Choose **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. Choices are **No Change**, **Normal**, **Min Delay**, **Max Thruput** or **Max Reliable**.
Precedence	Set the new precedence value of the outgoing packet. Choices are **1**, **2**, **3**, **4**, **5**, **6**, **7** or **Don't Care**.

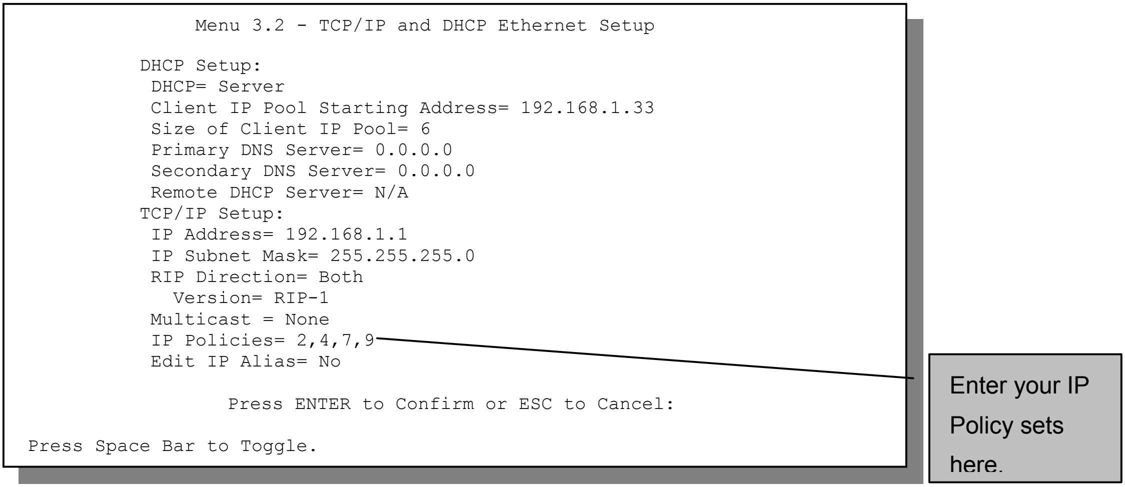
12.2 Applying an IP Policy

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

12.2.1 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.



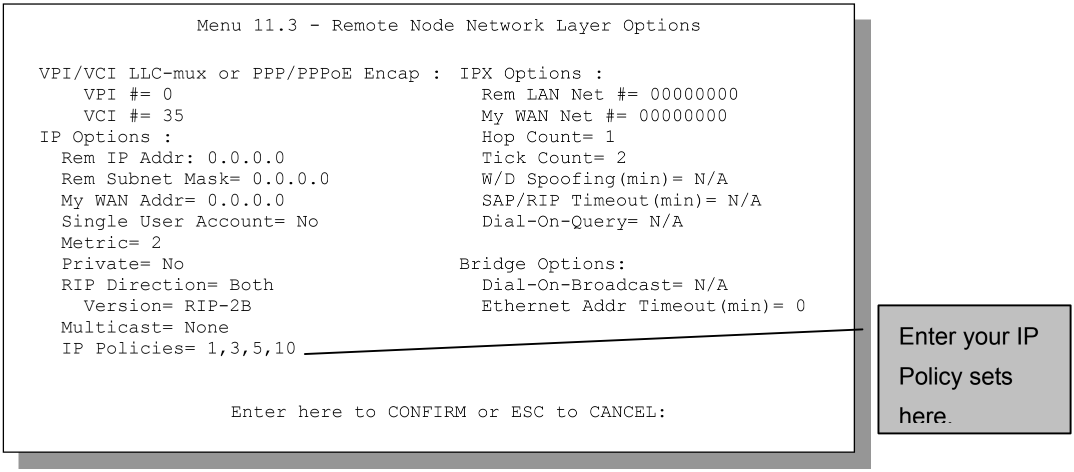
```
                 Menu 3.2 - TCP/IP and DHCP Ethernet Setup

            DHCP Setup:
             DHCP= Server
             Client IP Pool Starting Address= 192.168.1.33
             Size of Client IP Pool= 6
             Primary DNS Server= 0.0.0.0
             Secondary DNS Server= 0.0.0.0
             Remote DHCP Server= N/A
            TCP/IP Setup:
             IP Address= 192.168.1.1
             IP Subnet Mask= 255.255.255.0
             RIP Direction= Both
               Version= RIP-1
             Multicast = None
             IP Policies= 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 12-4 Menu 3.2 - General Ethernet Setup

12.2.2 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.



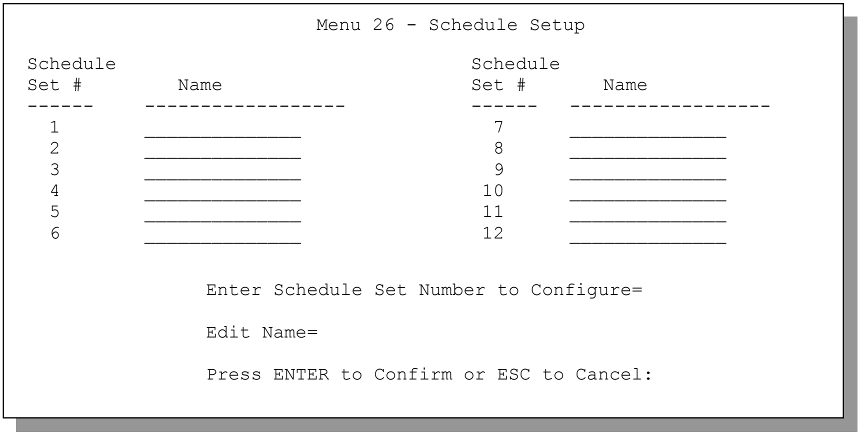
```
                 Menu 11.3 - Remote Node Network Layer Options

   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 12-5 Menu 11.3 - Remote Node Network Layer Options

Chapter 13
Call Scheduling

The call scheduling feature allows the Prestige to manage a remote node and dictate when a remote node should be called and for how long. This feature is to the scheduler in a video cassette recorder (you can record programs you want during a time that is specified by you). You can apply up to 4 schedule sets in **Menu 11.1 - Remote Node Profile**. From the main menu, enter **26** to access **Menu 26 - Schedule Setup** as shown next.



```
                         Menu 26 - Schedule Setup

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

                Enter Schedule Set Number to Configure=

                Edit Name=

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

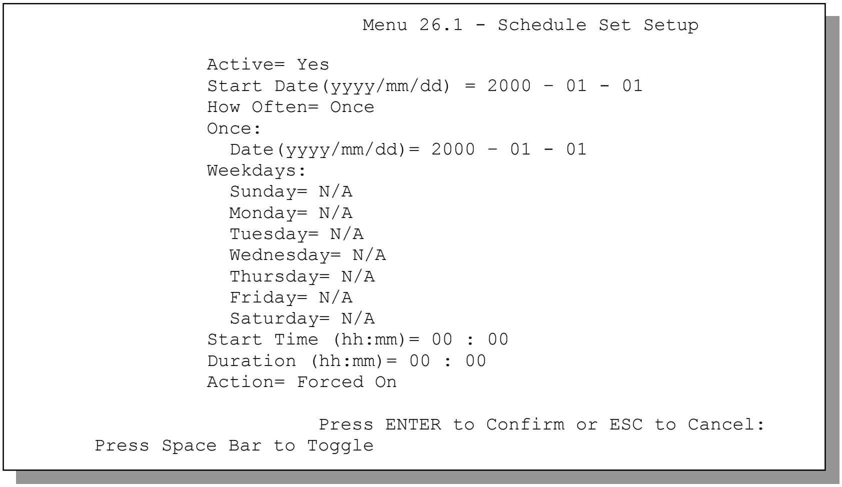
Figure 13-1 Schedule Setup

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

You can design up to 12 schedule sets but you can only apply up to 4 schedule sets for a remote node.

To delete a schedule set, enter the set number and press the [SPACE BAR] (or delete) in the Edit Name field.

To setup a schedule set select the schedule set you want to setup from **Menu 26** (1-12) and press [Enter] to see **Menu 26.1 - Schedule Set Setup** as shown next.



```
                              Menu 26.1 - Schedule Set Setup

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

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

Figure 13-2 Schedule Set Setup

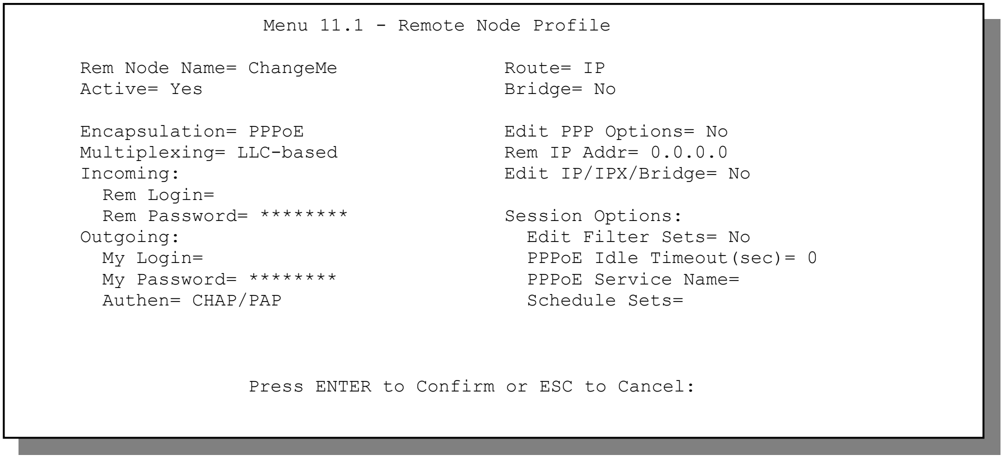
If a connection has been already established, your Prestige will not drop it. Once the connection is dropped manually or it times out, then that remote node can't be triggered up until the end of the **Duration**.

Table 13-1 Schedule Set Setup Fields

FIELD	DESCRIPTION	EXAMPLE
Active	Choose **Yes** to activate and **No** to deactivate the schedule set.	**Yes** (default)
Start Date	Enter the start date that you wish the set to take effect in year -month-day format. Valid dates are from the present to February 5, 2036.	
How Often	Should this schedule set recur weekly or be used just once only? Choose **Once** or **Weekly**. Both these options are mutually exclusive. If **Once** is selected, then all weekday settings are **N/A**. When **Once** is selected, the schedule rule deletes automatically after the scheduled time elapses.	**Once** (default)
Once: Date	If you selected **Once** in the **How Often** field above, then enter the date the set should activate in year-month-day format. If you did not select **Once** in the field above this field is **N/A**.	
Weekday: Day	If you selected **Weekly** in the **How Often** field above, then choose the day(s) the set should activate (and recur). Individual **Day** parameters are active when their fields read **Yes** and inactive when their fields read **No** or **N/A**.	**N/A** (default)

FIELD	DESCRIPTION	EXAMPLE
Start Time	Enter the start time that you wish the schedule set to take effect in hour : minute format.	
Duration	Enter the maximum duration allowed in hour : minute format for this scheduled connection.	
Action	Choose an action. Choices are: **Forced On** means that the connection is maintained whether or not there is a demand call on the line and will persist for the time period specified in the Duration field. **Forced Down** means that the connection is blocked whether or not there is a demand call on the line. **Enable Dial-On-Demand** means that this schedule permits a demand call on the line. **Disable Dial-On-Demand** means that this schedule prevents a demand call on the line.	**Forced On**

Once your schedule sets are configured, you must then apply them to the desired remote node(s). Enter **11** from the main menu and then enter the target remote node index. Using the [SPACE BAR], change the **Encapsulation** field to **PPPoE** to make the **Schedule Sets** field available as shown next.



```
                    Menu 11.1 - Remote Node Profile

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

    Encapsulation= PPPoE                    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)= 0
      My Password= ********                   PPPoE Service Name=
      Authen= CHAP/PAP                        Schedule Sets=



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

Figure 13-3 Applying Schedule Set(s) to A Remote Node

You can apply up to 4 schedule sets, separated by commas, for one remote node. Change the schedule set numbers to your preference(s).

Part IV:

TROUBLESHOOTING AND ADDITIONAL INFORMATION

This part provides information about solving common problems. Also included are Appendices and an Index.

Chapter 14
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.

14.1 Problems Starting Up the Prestige

Table 14-1 Troubleshooting the Start-Up of your Prestige

PROBLEM	CORRECTIVE ACTION	
None of the LEDs are on when you power on the Prestige	Check the connection between the AC adapter and the Prestige. 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, Flow Control set to None, 8 Data bits, 1 Stop bit.

14.2 Problems With the WAN Interface

Table 14-2 Troubleshooting the ADSL connection

PRC 3LEM	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.

14.3 Problems with the LAN Interface

Table 14-3 Troubleshooting the LAN Interface

PROBLEI	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.

14.4 Problems Connecting to a Remote Node or ISP

Table 14-4 Troubleshooting a Connection to a Remote Node or ISP

PROBLE 1	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 or ISP.

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.

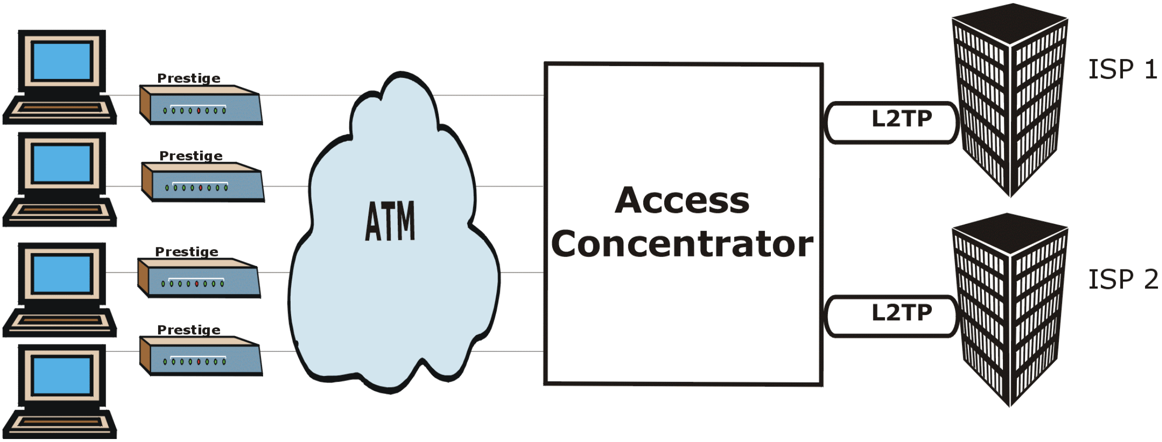


Diagram 1 Single-PC per Router Hardware Configuration

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.

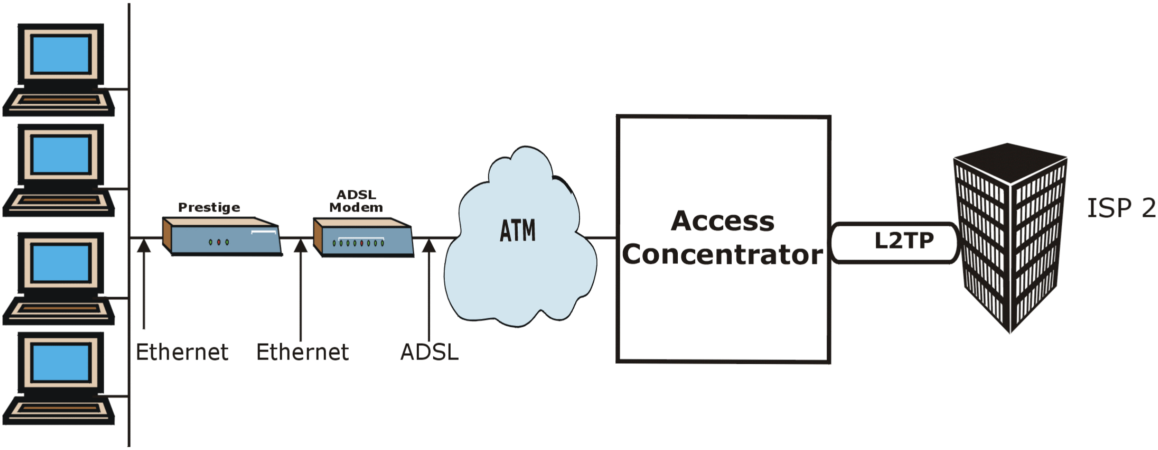


Diagram 2 Prestige as a PPPoE Client

Appendix B
Virtual Circuit Topology

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

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

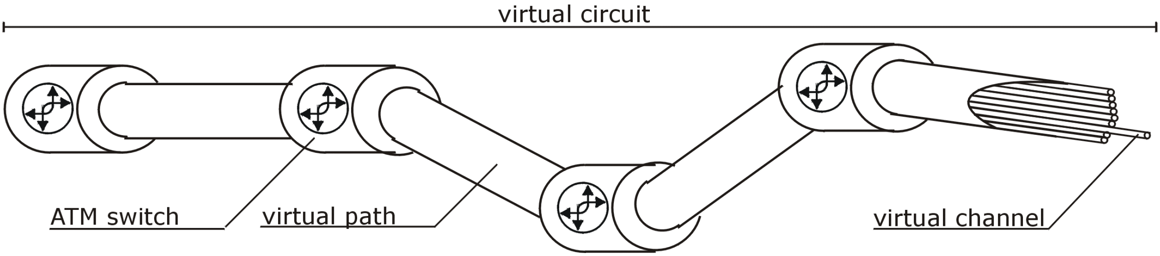


Diagram 3 Virtual Circuit Topology

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

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

Appendix C
AC Power Adapter Specifications

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